DO NOT REPRINT
© FORTINET
Passedumps.com

FortiManager Study Guide

for FortiManager 7.2

FORTINET
Training Institute

Vouchers & Dumps are Available | WhatsApp +201 2435 0122

DO NOT REPRINT Brave-dumps.com
© FORTINET

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

1/10/2023

Vouchers & Dumps are Available | WhatsApp +201224560923

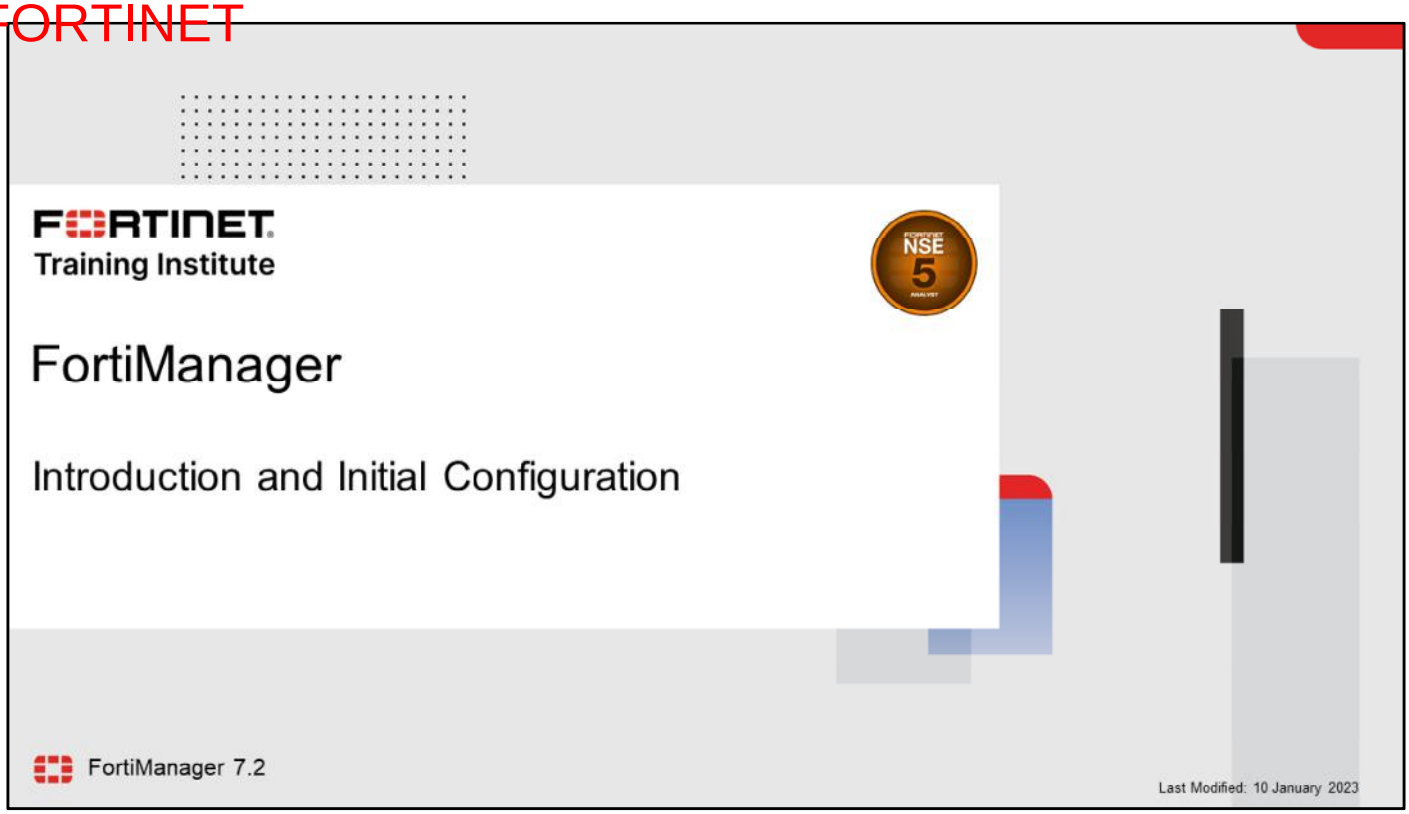
DO NOT REPRINT
© FORTINET
Brave-dumps.com

TABLE OF CONTENTS

01 Introduction and Initial Configuration 4
02 Administration and Management 46
03 Device Registration 103
04 Device-Level Configuration and Installation 149
05 Policy and Objects 200
06 Global ADOM and Central Management 251
07 Diagnostics and Troubleshooting 274
08 Additional Configuration 325

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn the basics of FortiManager. This includes how FortiManager fits into your existing network architecture.

FortiManager provides centralized policy provisioning, configuration, and update management for various Fortinet security devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Key Features
- Key Concepts
- Initial Configuration
- Use Cases

FORTINET Training Institute

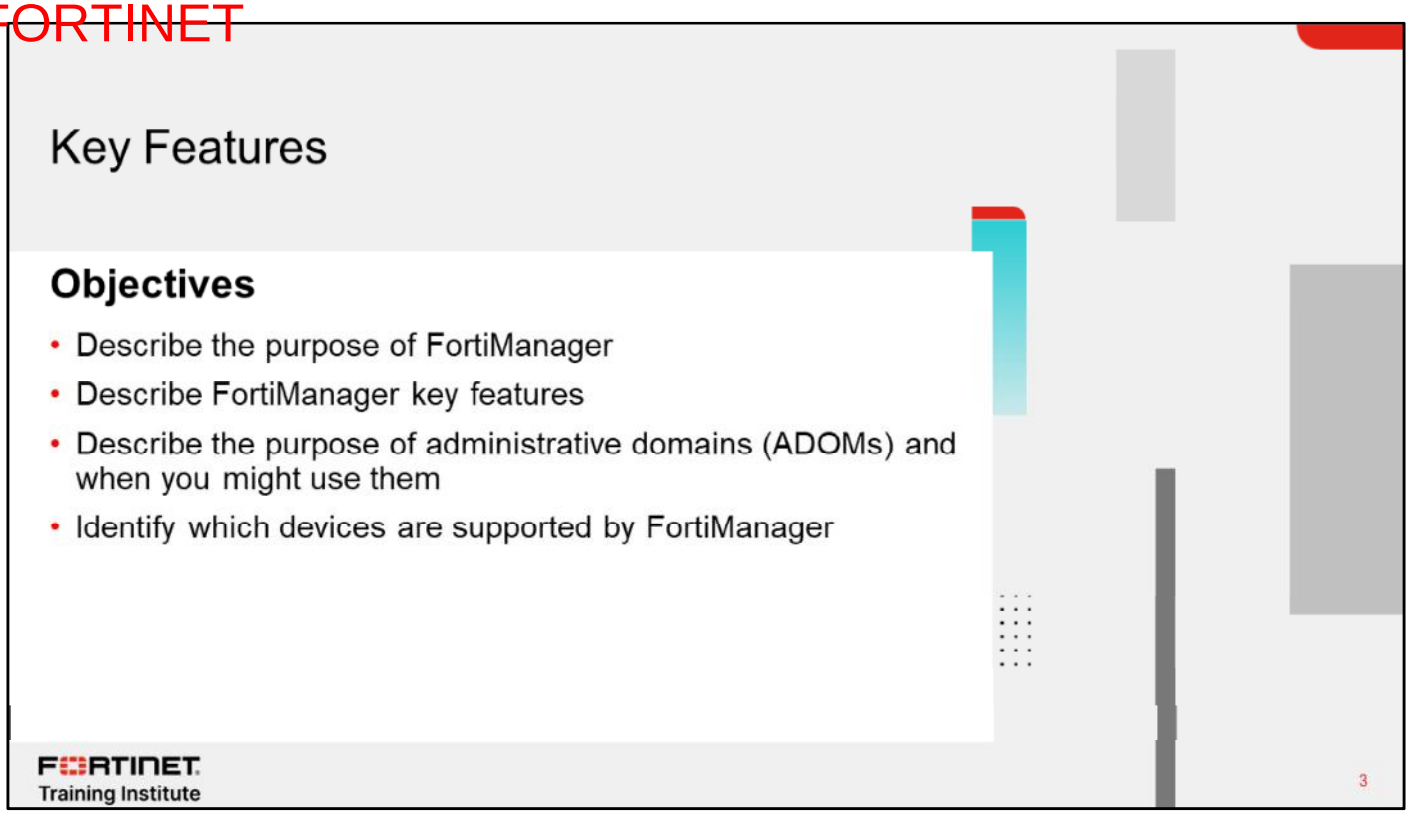
© Fortinet Inc. All Rights Reserved.

2

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 using FortiManager key features, you will be able to use the device effectively in your own network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

What Is FortiManager?

- Single pane of glass management
- Minimizes both initial costs and ongoing operating expenses for large deployments
- Helps maintain regulatory compliance
- Reduces WAN usage with local FortiGuard cache server
- Provides centralized device management for many Fortinet devices
- Automates mass device provisioning and maintains polices
  - Local distribution and control point for firmware and policy updates
  - Complex mesh and star IPsec VPN
- Provides logging and reporting

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

When should you use FortiManager in your network?

In large enterprises and managed security service providers (MSSPs), the size of the network introduces challenges that smaller networks don't have: mass provisioning; scheduling rollout of configuration changes; and maintaining, tracking, and auditing many changes.

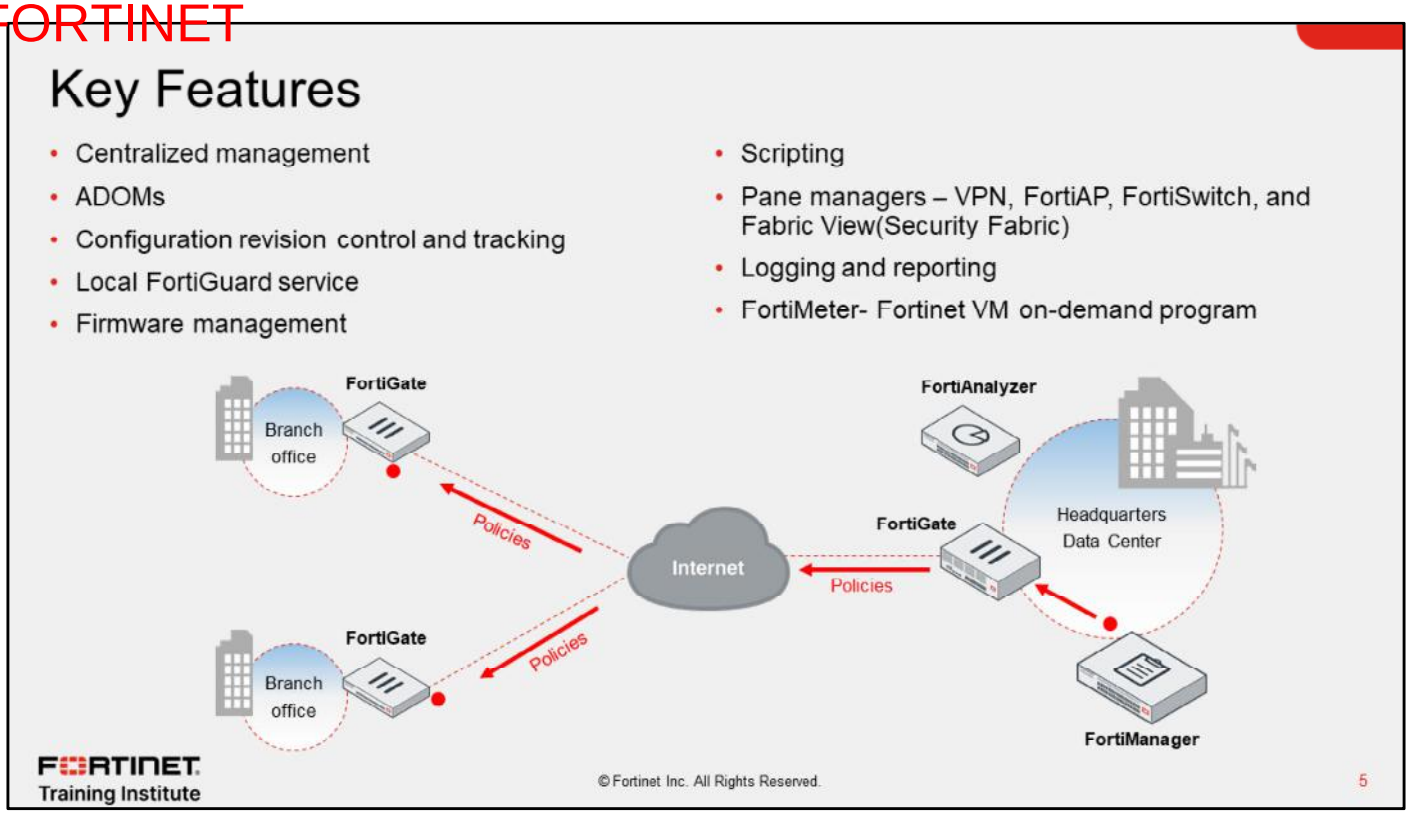
Centralized management through FortiManager can help you to more easily manage many deployment types with many devices, and to reduce cost of operation.

What can FortiManager do?

- Provision firewall policies across your network
- Act as a central repository for configuration revision control and security audits
- Deploy and manage complex mesh and star IPsec VPNs
- Act as a private FortiGuard Distribution Network (FDN) server for your managed devices
- Script and automate device provisioning, policy changes, and more with JSON APIs

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

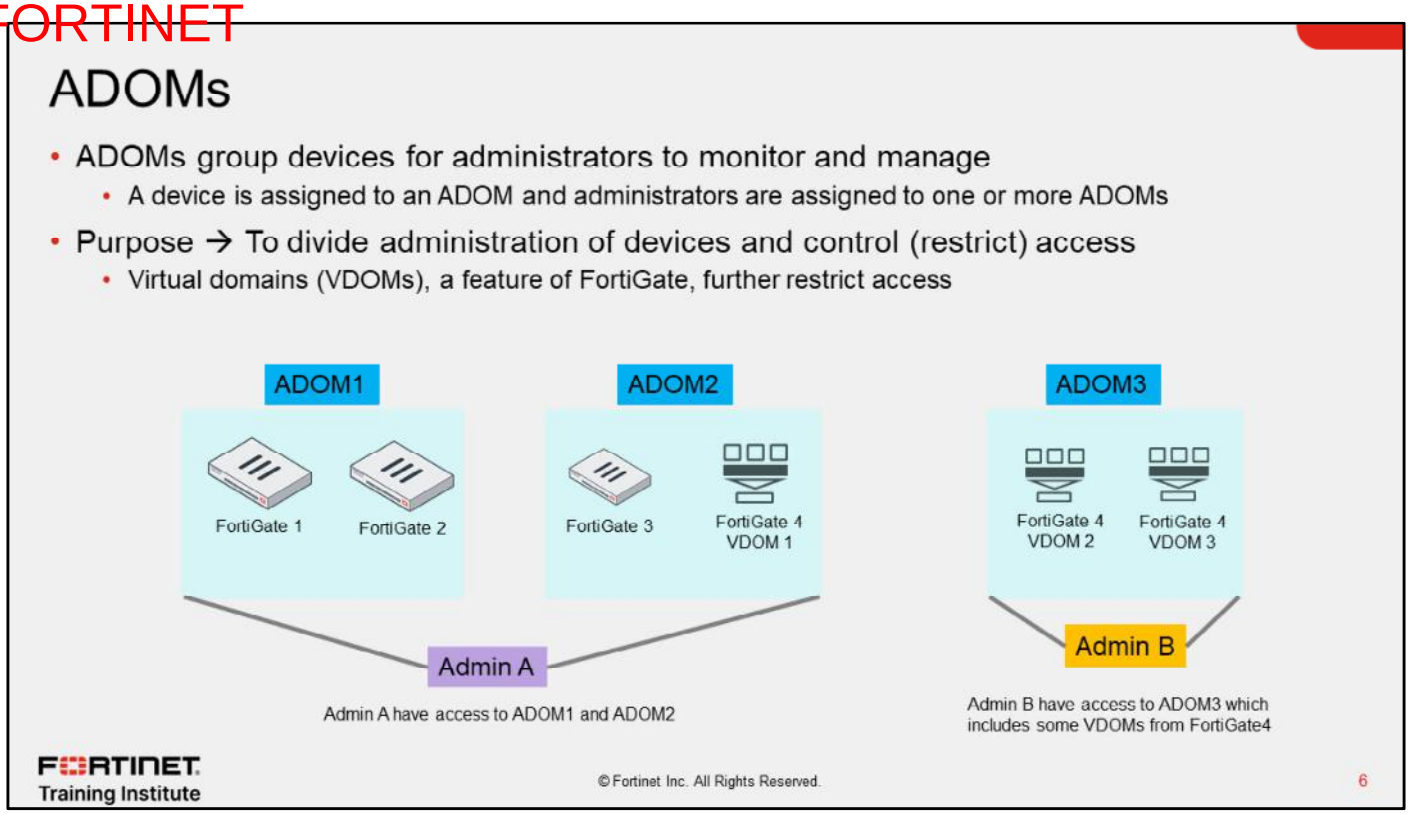


FortiManager can help you to better organize and manage your network. Key features of FortiManager include:

- Centralized management: Instead of logging in to hundreds of FortiGate devices individually, you can use FortiManager to manage them all from a single console.
- ADOMs: FortiManager can group devices into geographic or functional ADOMs, ideal if you have a large team of network security administrators.
- Configuration revision control: Your FortiManager keeps a history of all configuration changes. You can schedule FortiManager to deploy a new configuration or revert managed devices to a previous configuration.
- Local FortiGuard service provisioning: To reduce network delays and minimize internet bandwidth usage, your managed devices can use FortiManager as a private FDN server.
- Firmware management: FortiManager can schedule firmware upgrades for managed devices.
- Scripting: FortiManager supports CLI-based and TCL-based scripts for configuration deployments.
- Pane managers (VPN, FortiAP, FortiSwitch, Fabric View): FortiManager management panes simplify the deployment and administration of VPN, FortiAP, FortiSwitch, and Fabric View.
- Logging and reporting: Managed devices can store logs on FortiManager. From that log data, you can generate SQL-based reports, because FortiManager has many of the same logging and reporting features as FortiAnalyzer.
- FortiMeter: Provides large MSSPs with a cost-effective way of managing their client's security needs. The FortiManager metering module reports the traffic volume handled by the special FortiOS-VM to FortiGuard or FortiCare, which manages the point calculations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



ADOMs enable the *admin* administrator to create groupings of devices for administrators to monitor and manage. For example, administrators can manage devices specific to their geographic location or business division.

The purpose of ADOMs is to divide administration of devices by ADOM and to control (restrict) administrator access. If VDOMs are used, ADOMs can further restrict access to only data from a specific device VDOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the purpose of ADOMs on FortiManager?
   A. To enable FortiManager as a local FortiGuard distribution server
   ✓B. To divide administration of devices and restrict administrator access

2. What is the main benefit of using FortiManager as a local FDN?
   ✓A. The reduction of network delays and internet bandwidth use
   B. The maintenance of local active directory servers and users

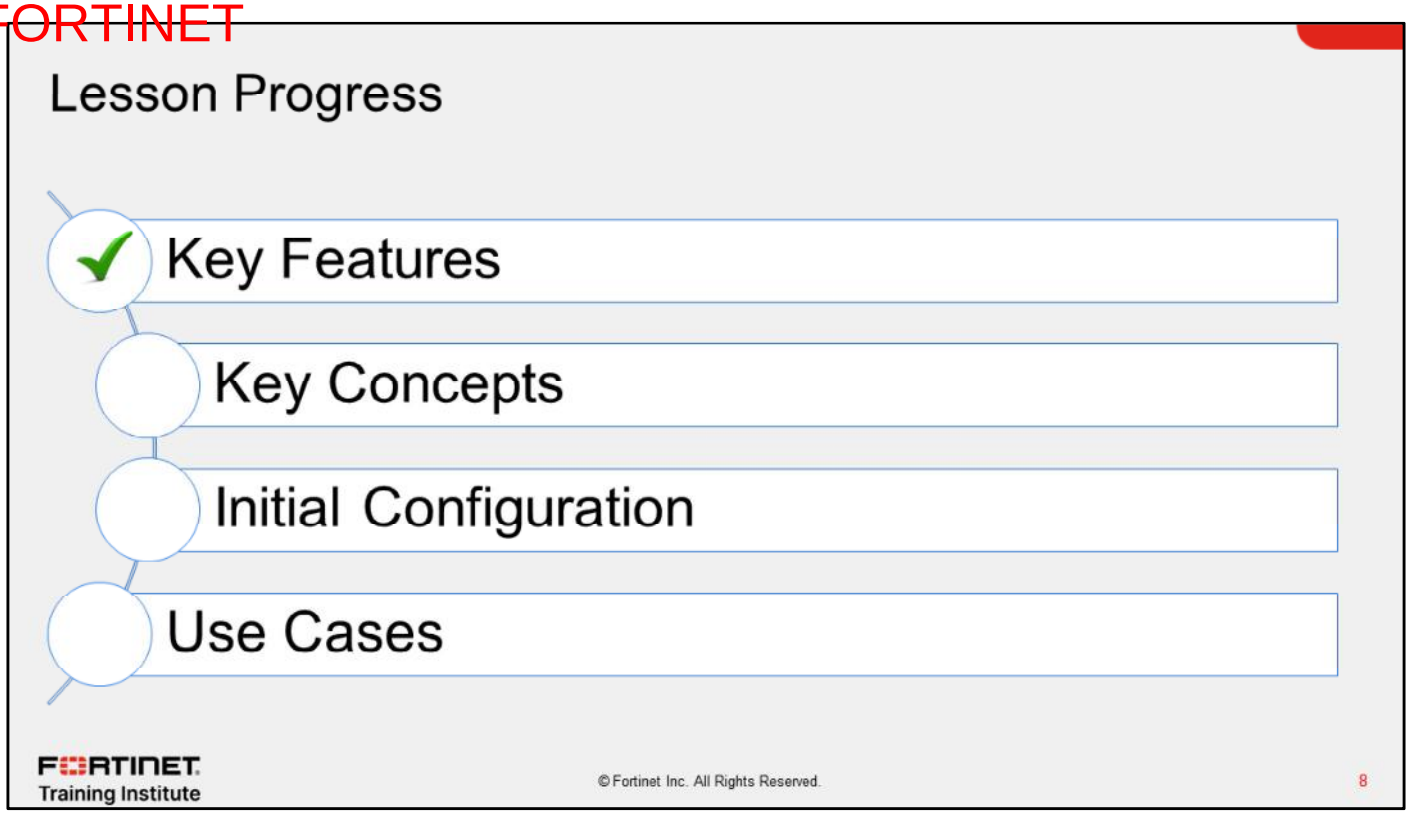
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

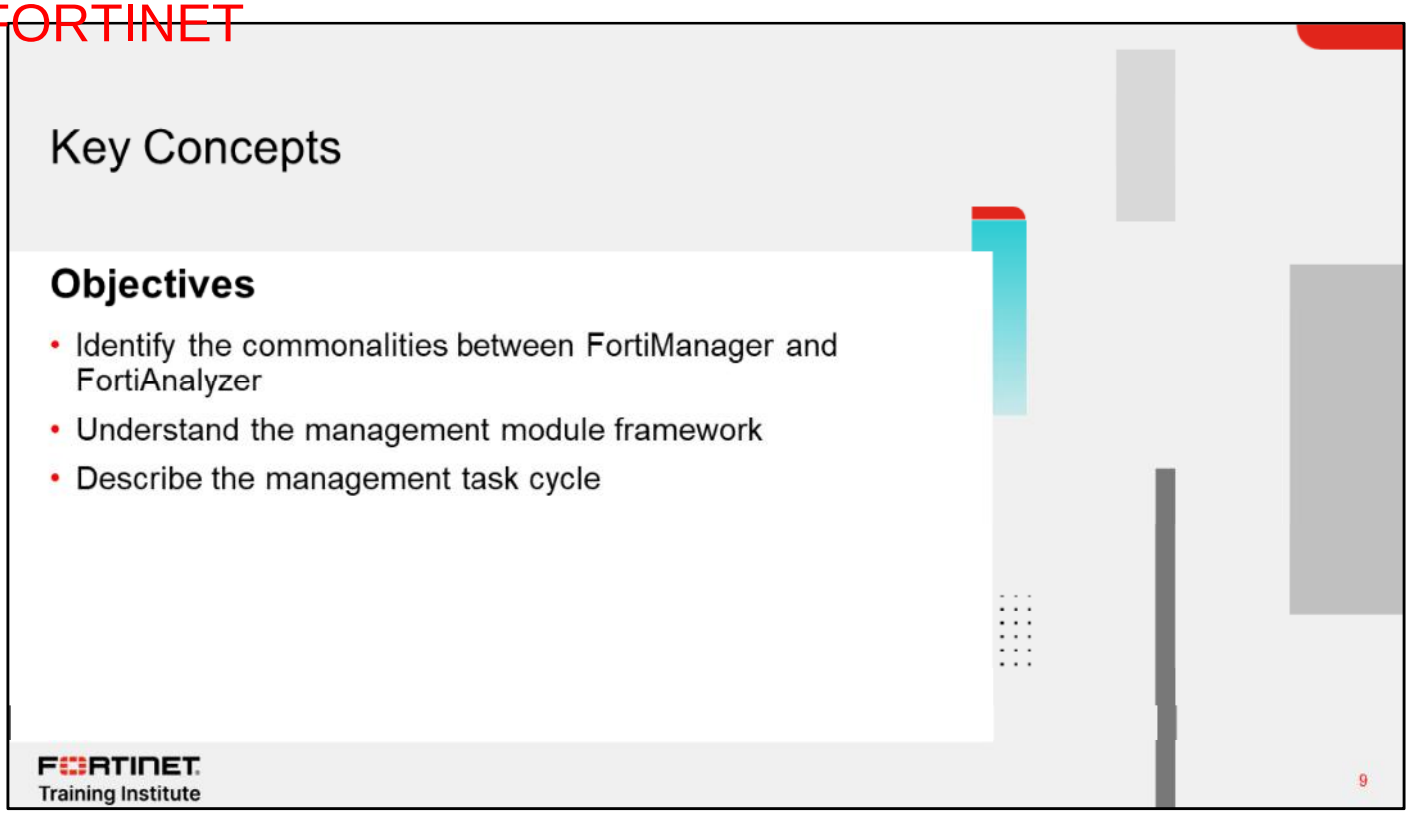


Good job! You now understand FortiManager key features.

Now, you will learn about FortiManager key concepts.

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.

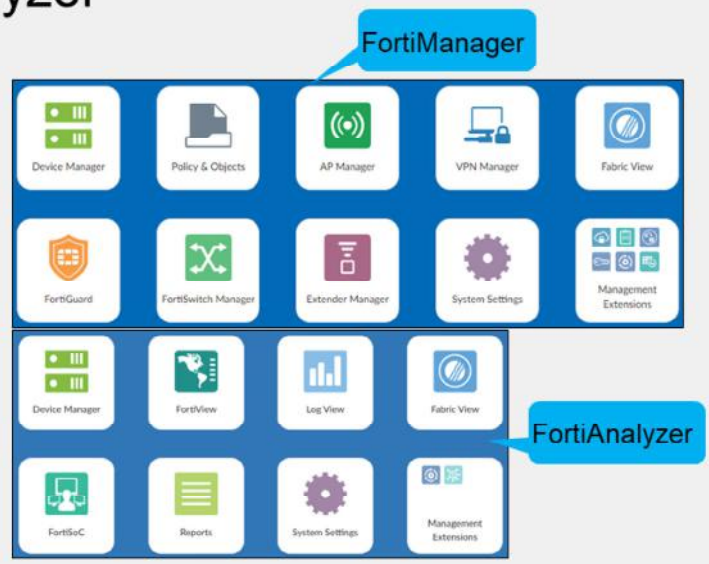
By demonstrating competence in understanding FortiManager key concepts, you will be able to more effectively use FortiManager in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager and FortiAnalyzer

- Common hardware and software platform
- Panes are used to organize central management and reporting functions on the GUI
- FortiManager includes all available panes
  - Log volumes are limited to a fixed amount each day
  - Resource intensive
- FortiAnalyzer includes logging and reporting panes including management extensions
  - Has much higher logging rate limits that FortiManager does



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

FortiManager and FortiAnalyzer run on the same hardware and software platform. Like FortiAnalyzer, FortiManager can also act as a logging and reporting device, but there are logging rate restrictions. Also, FortiManager requires additional resources (CPU, memory, disk) to process logs and reports.

FortiManager can be used as a fully functional logging and reporting device for *low* volumes of logs, but it needs to use some of its system resources for other features, such as configuration management.

If you have *high* log volumes, you should use a dedicated FortiAnalyzer.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiAnalyzer on FortiManager

- You can manage FortiAnalyzer from FortiManager
- Advantages are:
  - FortiManager visibility into the logs on the FortiAnalyzer, providing a single pane of glass on FortiManager
  - FortiManager can authorize and manage FortiAnalyzer ADOMs
  - Logs are stored on FortiAnalyzer, not FortiManager
  - Run reports from FortiManager

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

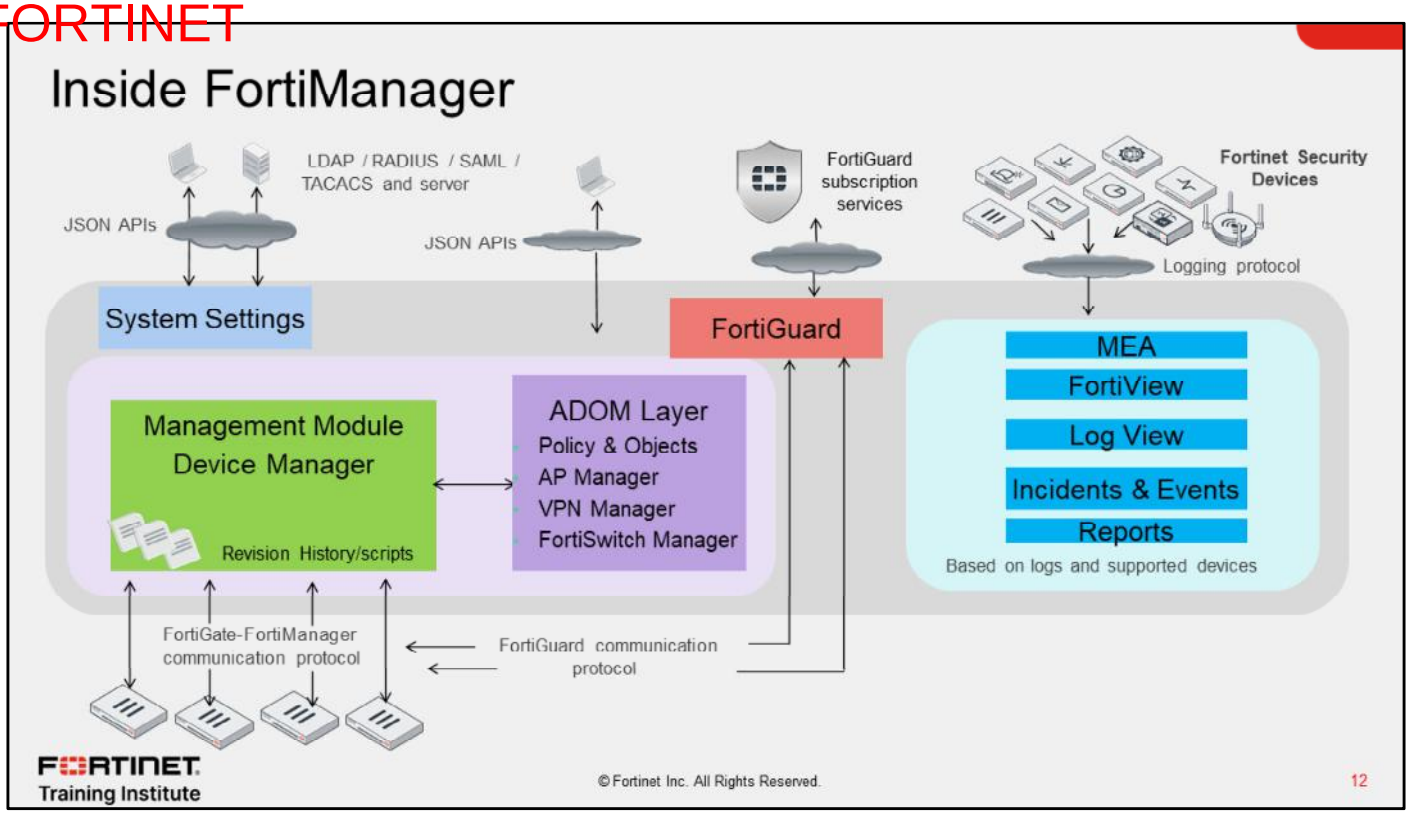
11

FortiManager gives visibility into the logs on FortiAnalyzer, providing a single pane of glass on FortiManager. When FortiManager manages a FortiAnalyzer device, all configuration and data is kept on FortiAnalyzer to support the following FortiAnalyzer features:

- FortiView
- Log View
- Incidents & Events
- Reports

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Inside FortiManager there are management layers that are represented as panes in the GUI. For example, the device management module is represented by the **Device Manager** pane, which you use to perform revision history and scripting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Management Layers

- Global ADOM layer
  - Global objects that can be shared across multiple ADOMs
  - All header and footer policies
- ADOM layer
  - Common object database, devices, device groups, policy packages
- Device manager layer
  - Name and type of managed devices, their IP addresses, revision history, and real-time status

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

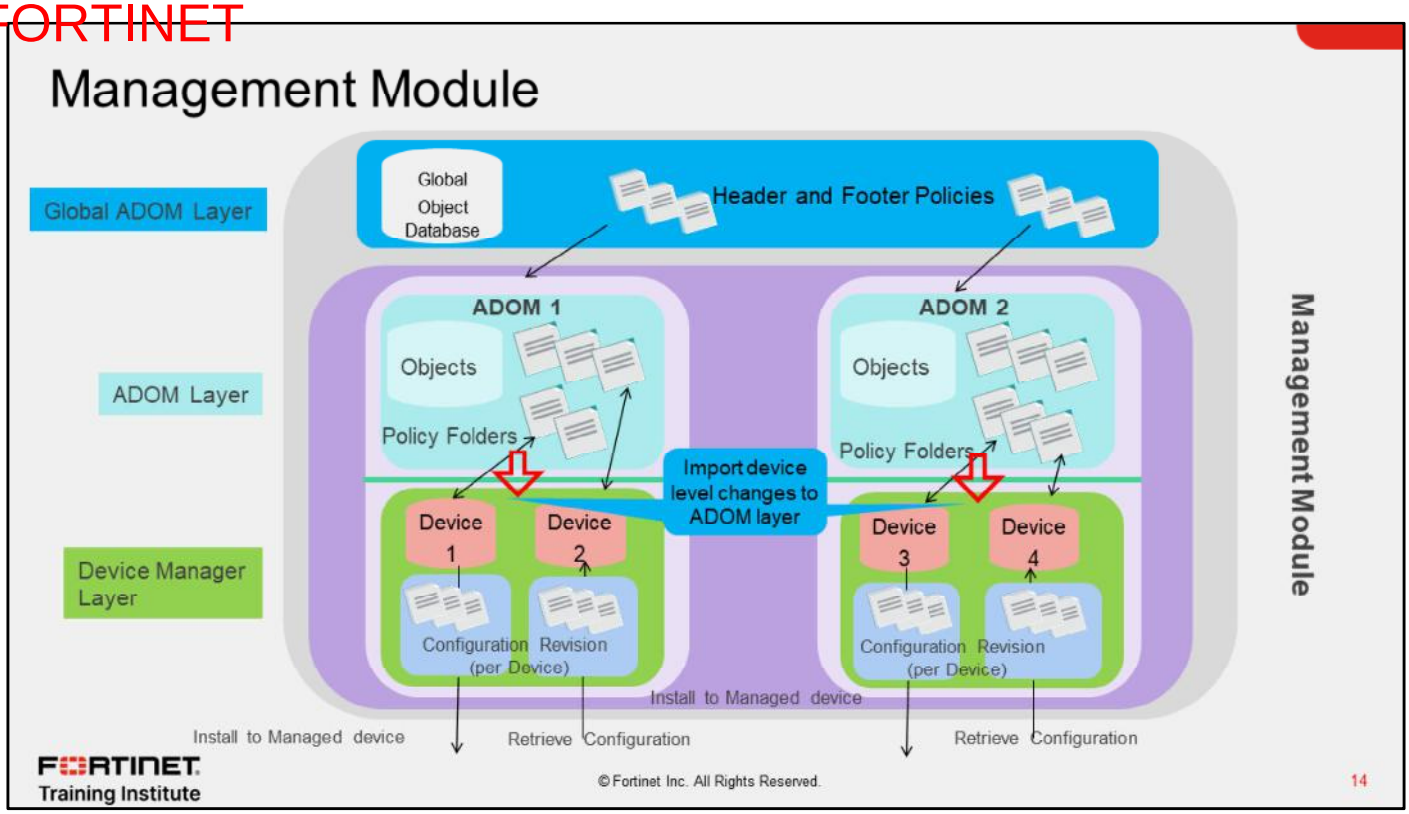
To organize and efficiently manage a large scale network, FortiManager has multiple layers:

- The global ADOM layer has two key pieces: the global object database, and all header and footer policy packages. Header and footer policy packages envelop each ADOM's policies. An example of where this would be used is in a carrier environment, where the carrier allows customer traffic to pass through their network, but would not allow the customer to have access to the carrier's network infrastructure.
- The ADOM layer is where policy packages are created, managed, and installed on managed devices or device groups. Multiple policy packages can be created here. The ADOM layer has one common object database for each ADOM. The databases contains information such as addresses, services, and security profiles.
- The device manager layer records information on devices that are centrally managed by the FortiManager device, such as the name and type of device, the model, IP address, current firmware installed, revision history, and real-time status.

Now take a look at how these layers are related.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Understanding the layers of the FortiManager device management model is important.

- In the global ADOM layer, you create header and footer policy rules. You can assign these policy rules to multiple ADOMs. If multiple ADOM policy packages require the same policies and objects, you can create them in this layer, so that you don't have to maintain copies in each ADOM.
- In the ADOM layer, objects and policy packages in each ADOM share a common object database. Policy packages , or you can import them from and install them on many managed devices at once.
- In the device manager layer, you can configure device settings and install them per device. If a configuration change is detected—whether the change is made locally or on the FortiManager—then, FortiManager compares the current configuration revision to the changed configuration, and creates a new configuration revision on FortiManager. Whether the configuration change is big or small, FortiManager records it and saves the new configuration. This can help administrators to audit configuration changes, and to revert to a previous revision, if required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about the global ADOM layer is true?
   - ✓A. The same policy can be assigned to multiple ADOMs.
   - B. Global ADOM rules are automatically installed on managed FortiGate devices.

2. Which information is recorded in the device manager layer for managed devices on FortiManager?
   - A. Common ADOM object database
   - ✓B. Real-time status of managed devices

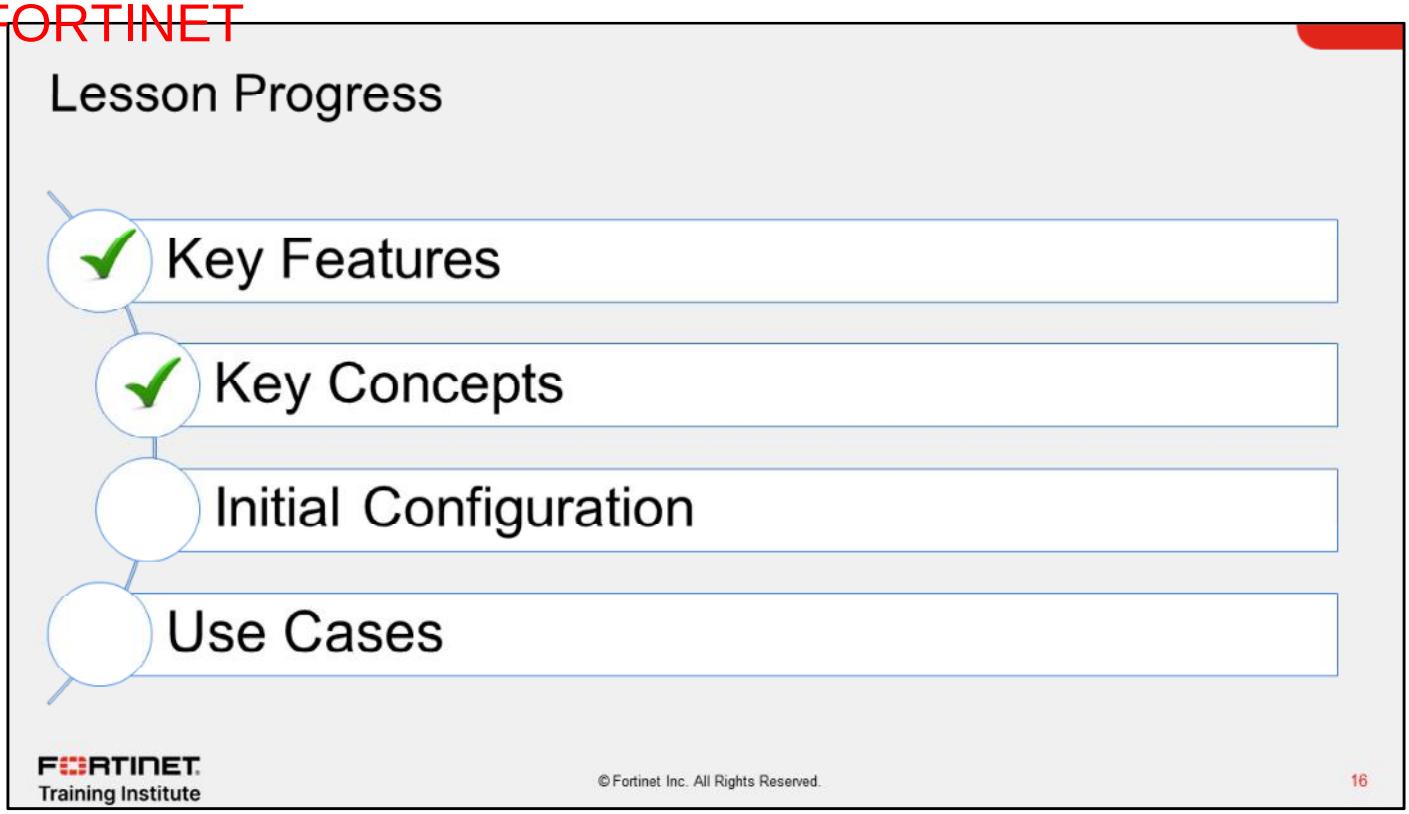
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

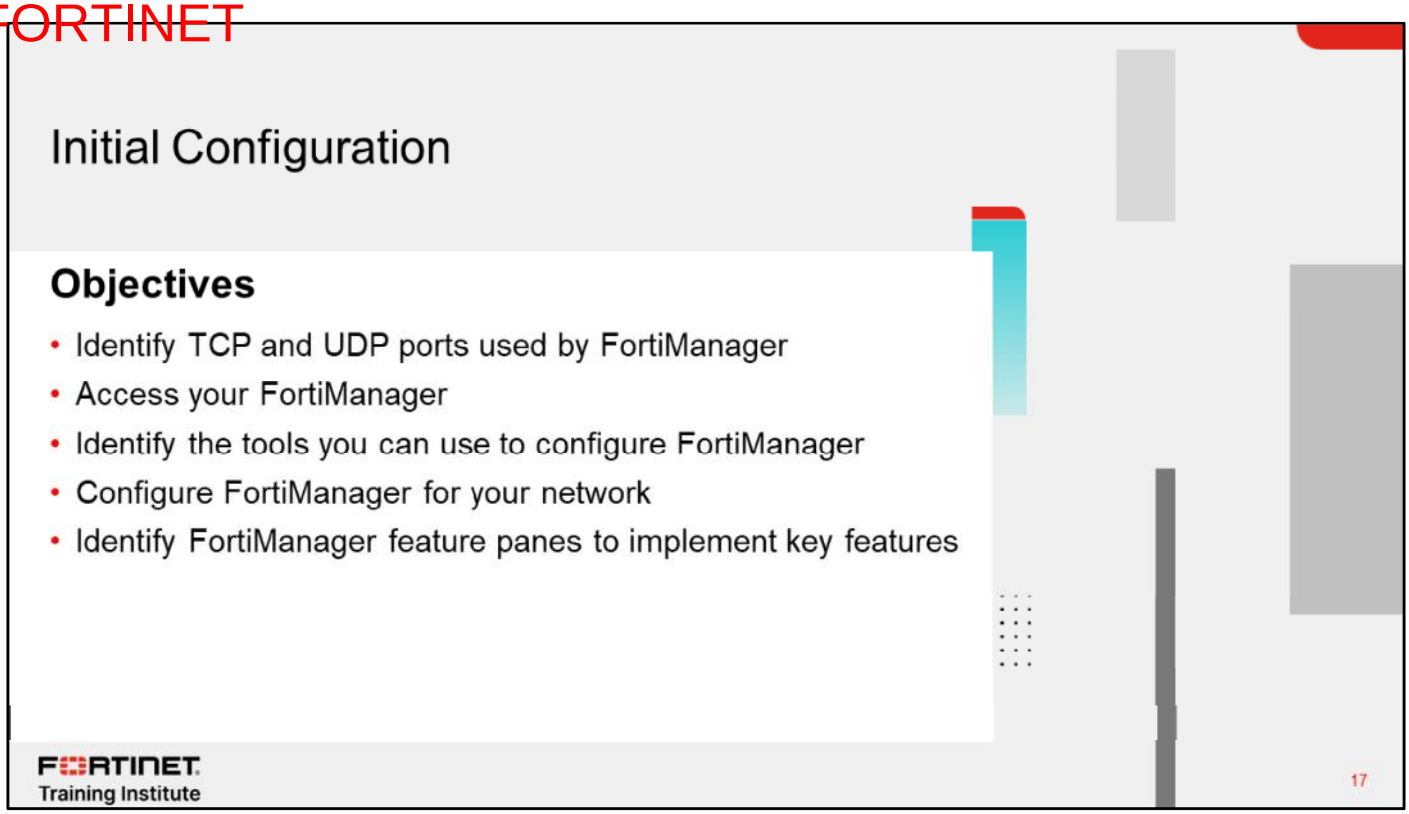


Good job! You now understand FortiManager key concepts.

Now, you will learn how to initially configure FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

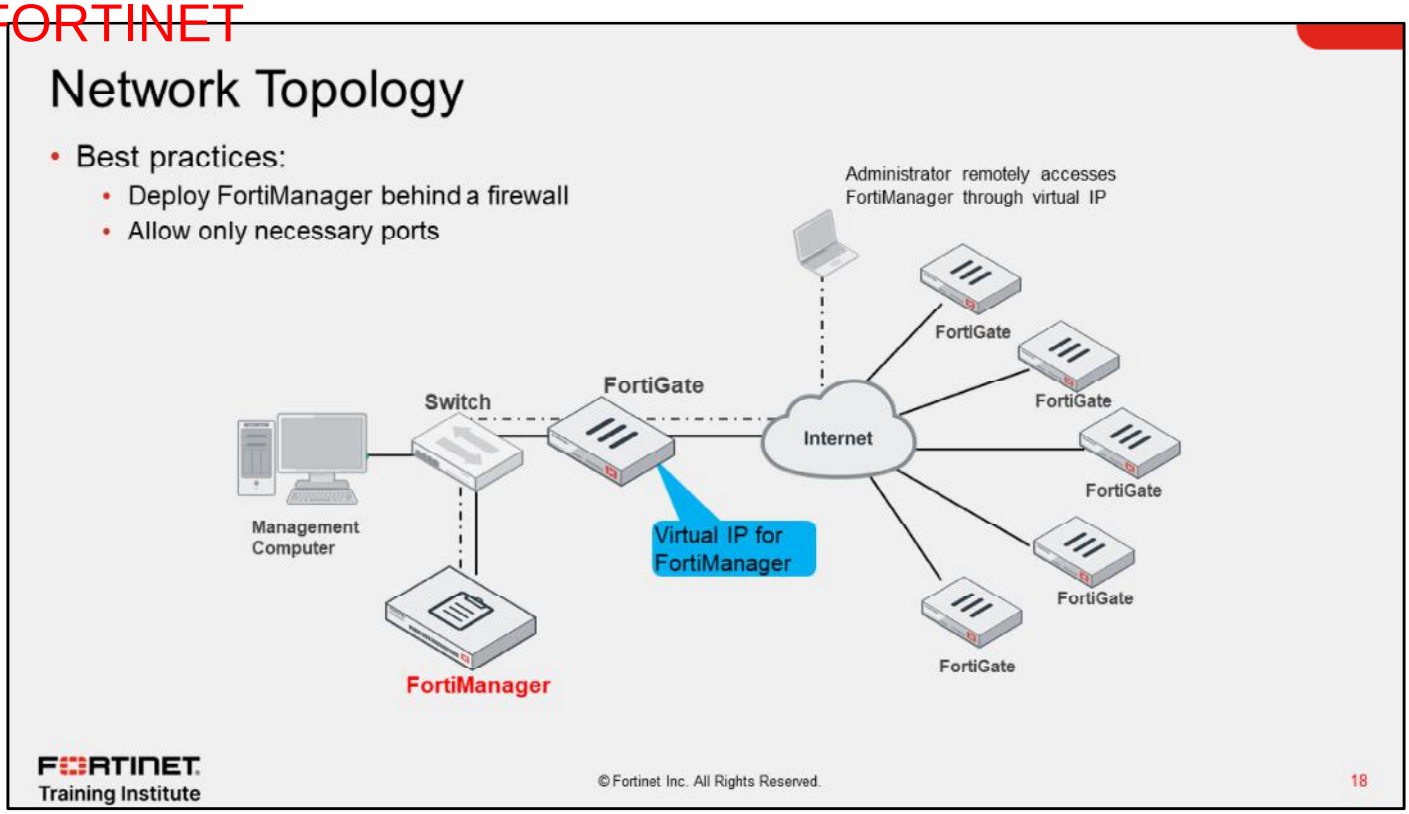


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the initial configuration of FortiManager, you will be able to add FortiManager to your network and perform basic administrative tasks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Often, your first consideration is where you should place FortiManager in your network.

Typically, you should deploy FortiManager behind a firewall, such as FortiGate. On the perimeter firewall, allow only relevant ports in the firewall policy for FortiManager, as a security consideration. If administrators or remote FortiGate devices will make inbound connections to FortiManager from outside your administrative subnet, such as from the internet, create a virtual IP.

To safeguard against losing access if your network is down, connect your management computer directly to FortiManager or through a switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager Ports

Functionality	Port(s)
Destination Ports	
Remote management of a FortiGate device	TCP 541 (IPv4), TCP 542 (IPv6)
Firmware image download	TCP 443
Antivirus, IPS, web filtering, antispam updates from FortiManager to FDN	TCP 443
DNS lookup	UDP 53
Syslog	UDP 514
Listening Ports	
FortiGuard antivirus and IPS update push	UDP 9443
FortiGuard antivirus or IPS update request from a FortiGate device	TCP 8890
FortiGuard antispam or web filtering rating lookup from a FortiClient or FortiGate	UDP 53 or 8888
Web Services (a.k.a XML API)	TCP 8080
Web GUI and JSON API	TCP 443
Antivirus and IPS updates for FortiClient	TCP 80
HA heartbeat or synchronization (FortiManager HA cluster)	TCP 5199
Two FortiManager devices configured in cascade mode	
FortiManager devices in cascade mode both listening and destination ports	TCP 8891, 8900 and 8901

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

FortiManager uses many TCP and UDP ports for its tasks. Only the most common default ports used by FortiManager are listed in this table. In addition, FortiManager uses standard management ports such as:

HTTP	Port 80 (TCP)
HTTPS	Port 443 (TCP)
SSH	Port 22 (TCP)

Especially if your FortiManager is deployed behind a firewall, it is always good to know what ports are being used. This can help you to analyze, diagnose, and resolve common network issues.

FortiManager cascade mode: optional upstream(cascade-mode) server for FortiGuard services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Security Recommendations

- Deploy FortiManager to a protected and trusted private network
- Use secure communication methods, even in a private network (HTTPS or SSH)
- Configure trusted hosts
  - If access from the outside is required, open only the ports necessary for proper communications
  - If access from the outside is required, set up special users and use only secure protocols (HTTPS/SSH)
- Secure passwords and password policy feature
- Check event logs, configure external syslog or mail server for quick notifications
- SAML SSO authentication
  - You must first register your FortiManager on FortiCloud

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

Before reviewing the configuration settings, it is necessary to discuss the importance of security. Your FortiManager manages all your Fortinet network security devices, so it is *vital* that data is properly protected.

Here are some security recommendations:

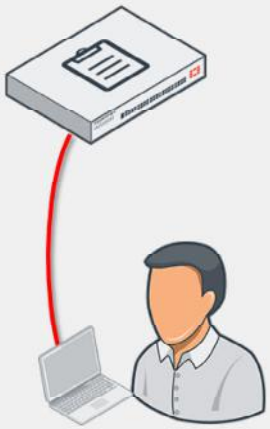
- Deploy your FortiManager in a protected and trusted private network. It should never be deployed directly on the internet.
- Always use secure connection methods to do administration: HTTPS for web-based management or SSH for the CLI. Insecure methods like HTTP are plain text, so an attacker can use packet sniffing tools to obtain information that can be used to breach your network.
- Use trusted hosts on your users and allow logins only from specific locations. If you do need to open outside access to the device so that remote devices can connect, open only the ports necessary for this. Additional open ports increases your security risk. If you need to open direct login access from the outside, be sure to set up special user accounts for this and open only protocols that are secure. Secure passwords should also be used and a password policy is highly recommended.
- Check event logs, configure external syslog or mail server for quick notifications.
- You can enable and configure following password policies:
  - **Minimum Length**: Specify the minimum number of characters that a password must be, from 8 to 32. The default is 8.
  - **Must Contain**: Specify the types of characters a password must contain: uppercase and lowercase letters, numbers, or special characters.
  - **Admin Password Expires after**: Specify the number of days a password is valid for. When the time expires, the administrator is prompted to enter a new password.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Factory Default Settings

- Use factory default settings to initially log in to your FortiManager and begin your own network configuration
  - Settings located in your FortiManager *QuickStart Guide* (docs.fortinet.com)
- Default settings:
  - Port 1 is default management port
    - Port1 interface IP: `192.168.1.99/24`
    - PING, HTTP, HTTPS, SSH protocols are enabled for management access
    - Username: `admin`
    - Password: (blank)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

It is important to know the factory default settings, such as the default user name and password, the port 1 IP address, netmask, and default supported management access protocols, so that you can initially connect to your management computer and configure FortiManager for your network.

You can find the default settings in your model-specific *Quick Start Guide.* Different FortiManager models have different numbers of ports, but port1 is the management port and will always have this default IP.

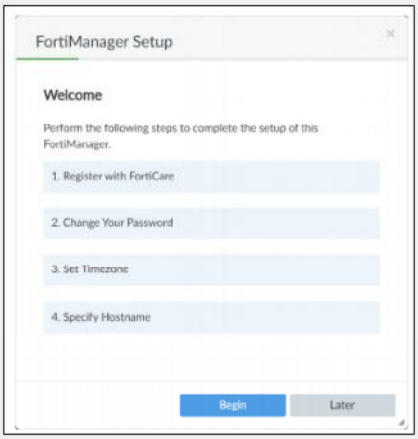
To log in to the FortiManager GUI for the first time, open a browser and enter the URL `https:// <the factory default IP address>`. After the login screen appears, use the factory default administrator credentials to log in. The default credentials are user name admin and a blank password.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager Setup Wizard

- When you first access FortiManager, The **FortiManager Setup** wizard displays
- The **FortiManager Setup** wizard lets you register with FortiCare and perform the following actions:
  - Registering with FortiCare
  - Changing your password
  - Setting the time zone
  - Specifying a hostname



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

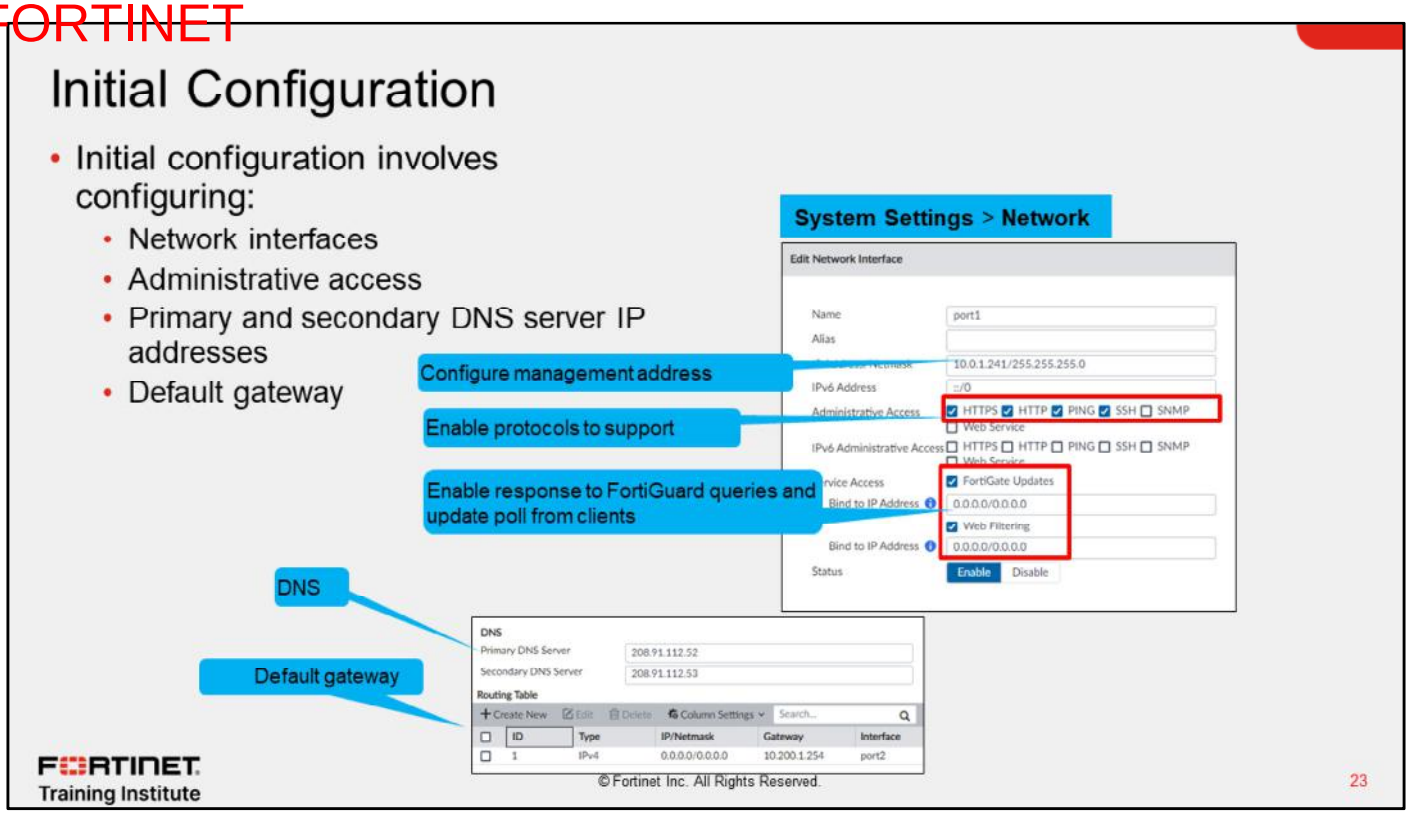
When you log in to FortiManager, the **FortiManager Setup** wizard displays to help you set up FortiManager by performing the following actions:

- Registering with FortiCare and enabling FortiCare single sign-on
- Changing your password
- Setting the time zone
- Specifying a hostname

You can choose whether to complete the wizard now or later. When you complete and action, a green check mark displays beside it in the wizard, and the wizard no longer displays after you log in to FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The initial configuration of FortiManager is very similar to FortiGate. In order to configure FortiManager for your network, you must set the IP address and netmask, select supported administrative access protocols, and specify a default gateway for routing packets. You can do all of this from the **Network** page.

Port1, the management interface, has a default IP address and netmask: `192.168.1.99/24`. If your management subnet uses a different subnet, or uses IPv6, change these settings . The IP address must be a unique static IP address. Relatedly, enter the IP address of the next hop router in **Gateway**, and specify your DNS servers. By default, FortiGuard DNS servers are configured in DNS server settings, to help guarantee connectivity for FortiGuard downloads and queries. But you can specify a local DNS server instead.

Service access allows you to enable the FortiManager response to the requests from managed devices for FortiGuard services on this interface. This includes FortiGate updates and web filtering. By default, all services to managed devices are enabled on port1 and disabled on other ports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Basic CLI Commands

- Use the following FortiManager CLI commands to examine or troubleshoot basic issues

Command	Information
# get system status	Displays the serial number, firmware version, ADOM status, HA status
# show system interface	Displays the network interface configuration, such as configured ports and associated IP addresses as well as enabled administrative access protocols
# show system dns	Displays DNS server addresses
# show system ntp	Displays automatic time setting using a network time protocol (NTP) server
# get system ntp	Displays how often FortiManager synchronizes its time with the NTP server
# show system route	Displays static routing table entries on your FortiManager device
# execute ping	Tests the network connection between FortiManager and another network device

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

Similar to FortiOS, you can use the CLI commands shown on this slide to examine or troubleshoot general issues on FortiManager. For example, you can view the general status, interface, and DNS settings of FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System Information

Use the `get system status` command to display FortiManager system information

```
FMG-VM64 # get system status
Platform Type                    : FMG-VM64-KVM
Platform Full Name               : FortiManager-VM64-KVM
Version                          : v7.2.0-build1215 220809 (GA)
Serial Number                    : FMG-VM0A16001583
BIOS version                     : 04000002
Hostname                         : FortiManager
Max Number of Admin Domains      : 10
Max Number of Device Groups      : 10
Admin Domain Configuration       : Enabled
FIPS Mode                        : Disabled
HA Mode                          : Stand Alone
Branch Point                     : 1124
Release Version Information      : GA
Current Time                     : Wed Aug 10 03:42:58 PDT 2022
Daylight Time Saving             : Yes
Time Zone                        : (GMT-8:00) Pacific Time (US & Canada)
x86-64 Applications              : Yes
Disk Usage                       : Free 25.87GB, Total 48.96GB
File System                      : Ext4
License Status                   : Valid
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

You can use this command to get basic FortiManager system information, which can be useful for troubleshooting. You can use the command to get information, such as:

- `Version`: Ensure the FortiManager firmware version is compatible with the device you are registering. (See the *FortiManager Release Notes* for supported firmware versions.)
- `Admin Domain Configuration`: Ensure ADOMs are enabled if attempting to register a non-FortiGate device. Also, it shows you how many ADOMs are supported on the FortiManager model.
- `Current Time`: Ensure your date and time is set according to your needs. For many features to work, including scheduling, FortiManager-FortiGate tunnel negotiations, and logging features, the FortiManager system time must be accurate. While you can manually set the date and time, you should synchronize with a Network Time Protocol (NTP) server.
- `License Status`: Ensure you have a valid licence.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about managed FortiAnalyzer on FortiManager is true?
   - ✓A. FortiManager supports FortiAnalyzer reports.
   - B. FortiManager has logging rate restrictions on managed FortiAnalyzer.

2. Which port is used between FortiManager and FortiGate for IPv4 remote configuration management of FortiGate devices?
   - ✓A. TCP 541
   - B. TCP 514

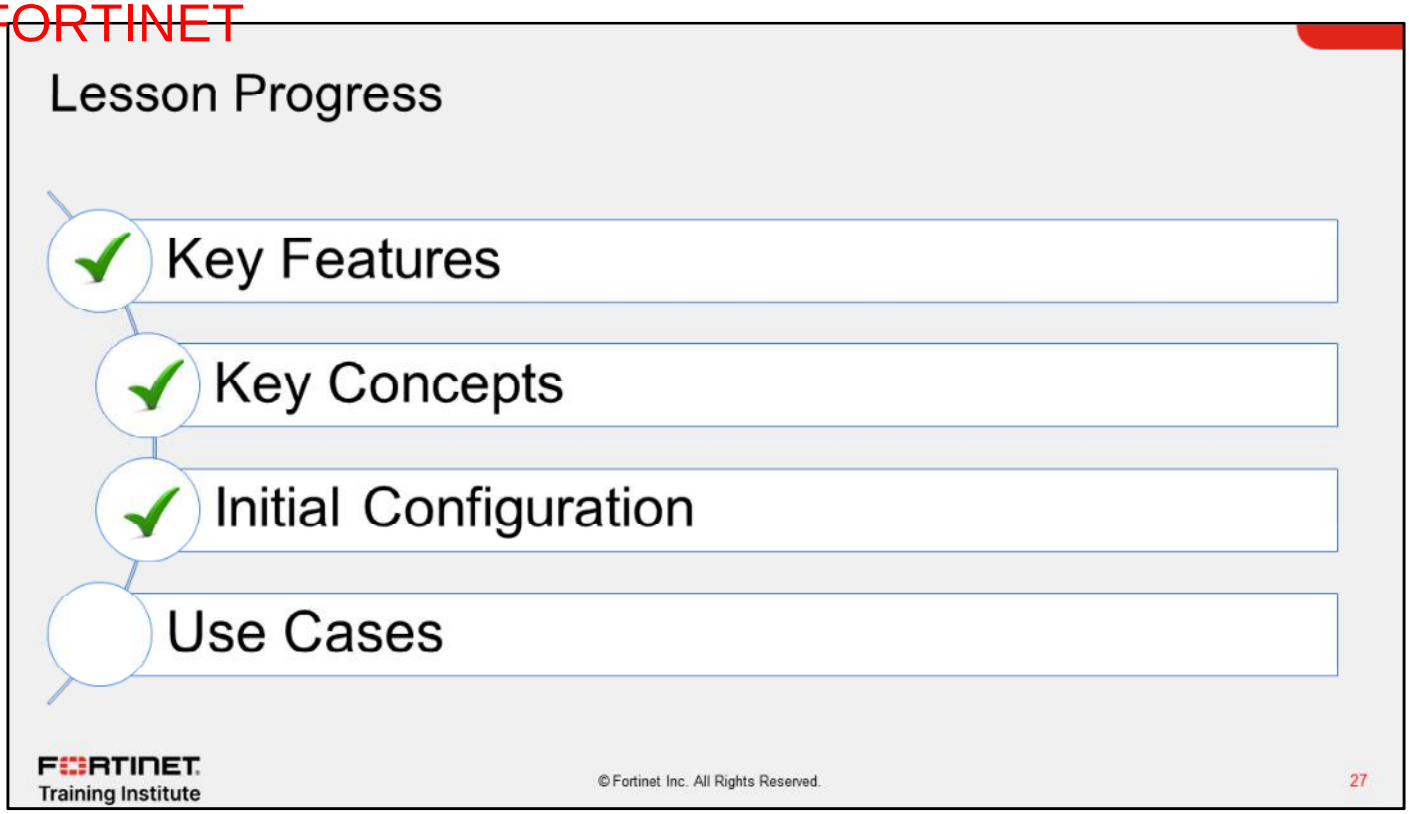
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

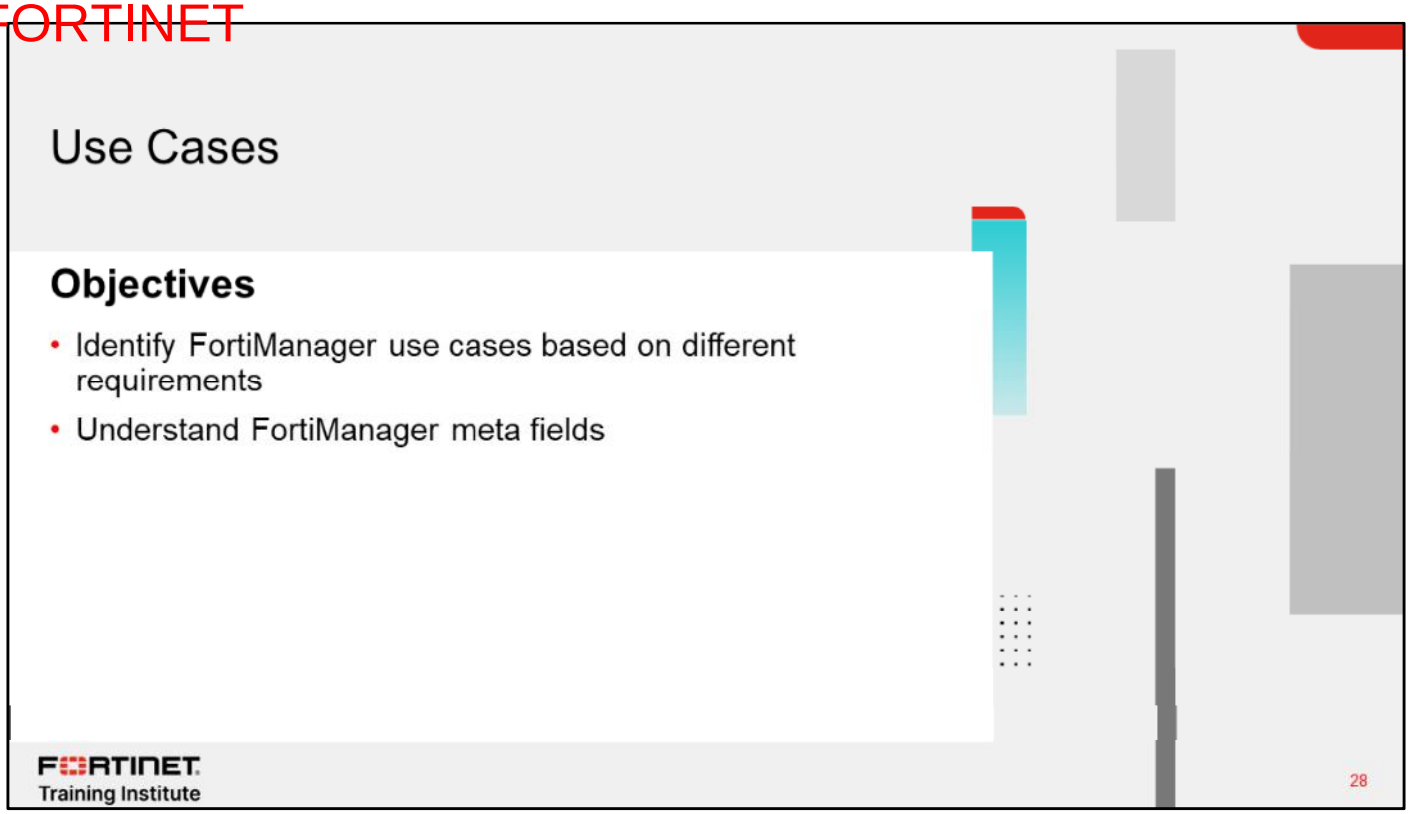


Good job! You now understand how to initially configure FortiManager.

Now, you will examine some of the use cases for FortiManager, based on different organizations.

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 FortiManager use cases, you will be able to see the different ways in which FortiManager is commonly used in other organizations and, if applicable, employ some of these strategies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Use Case—Retail

- Management of a large corporate network
  - Example: Retail or finance
- Characteristics:
  - Many remote sites (hundreds, maybe thousands) and several central hub sites and data centers
  - Operations team centrally provisioning and managing the firewall
  - Simple initial deployment – *phone home* configuration
  - Shared firewall objects across many firewalls: addresses and services
  - Firewall policies common to many sites

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

One common FortiManager use case involves large retail customers or distributed enterprises, because they tend to have many smaller customer premises equipment (CPE) devices in their branches, plus remote sites, and several main sites. These customers benefit from centralized firewall provisioning and monitoring.

In large scale enterprise deployments, administrators usually prefer a basic initial configuration that the installation technician loads through a USB, or copies and pastes into the console. This basic configuration allows FortiGate to contact FortiManager, where the administrator can add it to the appropriate device group or ADOM, then send the full configuration to that FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Use Case—Managed Security Service Provider (MSSP)

- Management of customer devices
- Characteristics:
  - Many smaller CPE devices or customer virtual domains (VDOMs) on a large firewall platform in the data center
  - Customers typically have read-only access to their firewalls/VDOMs in order to monitor their infrastructure and open change requests
  - Few shared objects between customers
  - No direct customer interaction with the managed firewall
  - Service provider may want to automate some of their provisioning
  - *Pay-as-you-go* business models pass cost savings to end-user customers

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

Another common use case involves MSSP.

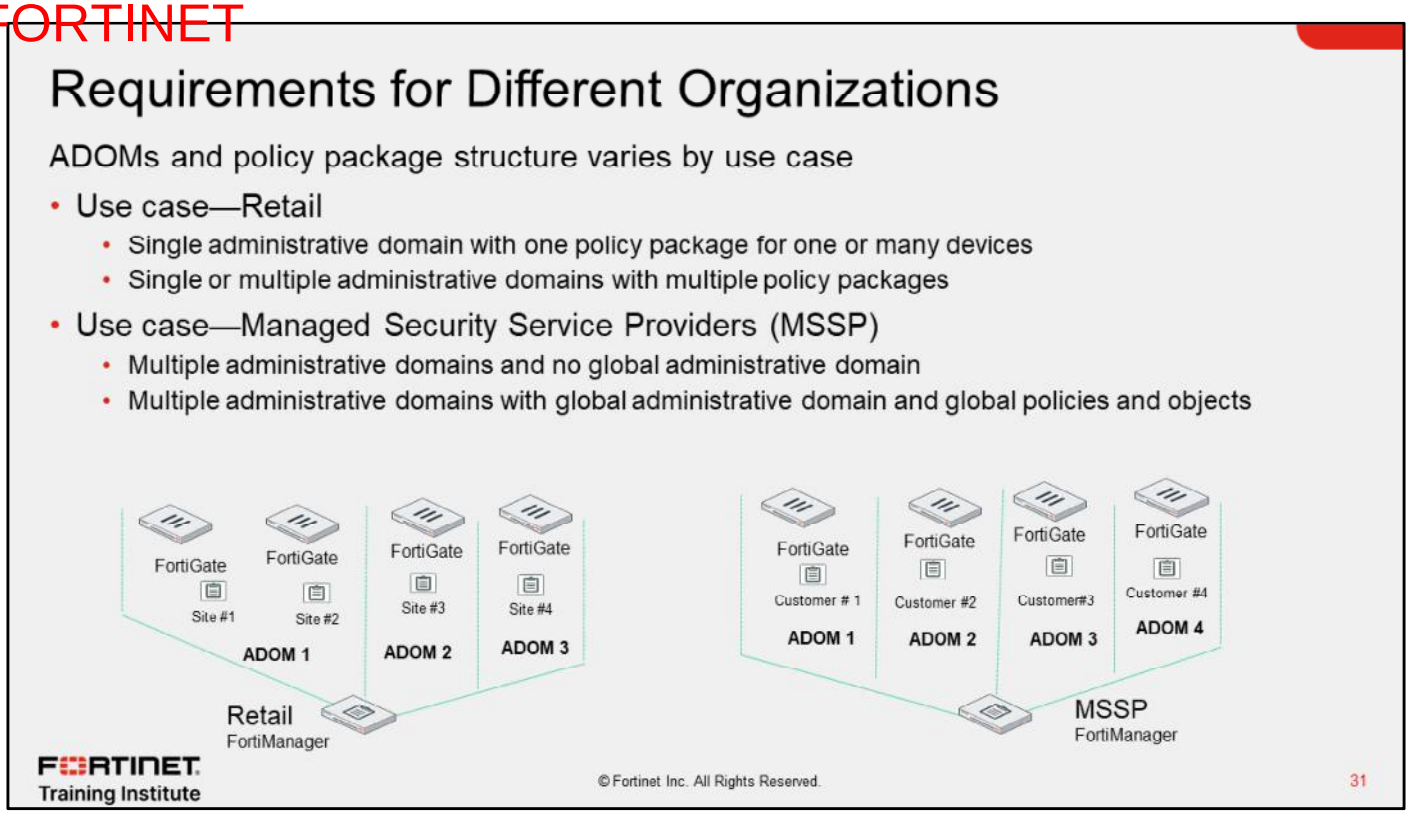
Carriers often may have many powerful firewalls and require strict configuration control, which is achievable by restricting configuration from the FortiManager. MSSPs may subdivide their firewalls into virtual firewalls that they provide to customers, or they may manage devices on customer premises. In both cases, they need to maintain configuration revisions for the customer and, optionally, provide a portal where customers can view or edit some of their settings.

Another important use case for MSSPs is being able to determine (or report) which firewall or configuration objects are in use or not in use. Firewall policies change over time and associated objects are substituted for other new objects. However, administrators often want to keep the old objects temporarily, in case they need to revert changes. Eventually, unused objects clutter the FortiGate configuration, making it harder to understand and troubleshoot. So, performing periodic clean-ups of these orphan configuration objects is useful.

Now able to meet the demand for pay-as-you-go service models, FortiManager allows MSSPs to avoid the overhead of perpetual licenses through the use of the Fortinet VM On-Demand Program.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



As you can see, different organizations may use FortiManager ADOMs and policy packages differently. In a retail organization, you may have a single ADOM with many FortiGate devices, or multiple ADOMs with one FortiGate. In MSSPs, each customer's FortiGate devices are placed in their ADOM.

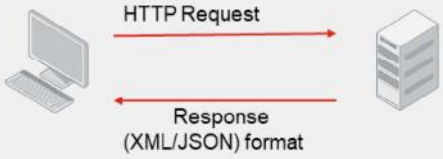
We will cover these topics in detail so you can have the practical skills necessary to manage devices for diverse organizations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager—Application Program Interface

- Application program interface (API) is a set of rules that allow programs to talk to each other
- FortiManager API is based on the JSON RPC standard
- Allow MSSP and large enterprise to create FortiManager self-service web portals
  - Using FortiPortal or any other third-party applications
- A RESTful API uses standard HTTP methods (GET, POST, DELETE) to provide interactions between a client and a server
- The following operations are supported by a RESTful API:
  - Fetch data by sending a GET request
  - Add data by sending a POST request
  - Update data by sending a POST request
  - Delete data by sending a DELETE request
- More details: FNDN and Fortinet document library



JSON Example

```
{"employees":[
  { "firstName":"John", "lastName":"Doe" },
  { "firstName":"Anna", "lastName":"Smith" },
  { "firstName":"Peter", "lastName":"Jones" }
]}
```

XML Example

```
<employees>
  <employee>
    <firstName>John</firstName> <lastName>Doe</lastName>
  </employee>
  <employee>
    <firstName>Anna</firstName> <lastName>Smith</lastName>
  </employee>
  <employee>
    <firstName>Peter</firstName> <lastName>Jones</lastName>
  </employee>
</employees>
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

32

The FortiManager JSON API allows you to perform configuration and monitoring operations on a FortiManager appliance or VM. The JSON API is based on JSON-RPC, a remote procedure call protocol encoded in JSON. The API allows you to do many of the same tasks as the FortiManager GUI using FortiPortal or other third-party applications. It allows MSSP and large enterprises to create customized, branded web portals for FortiManager administration, without directly logging in to FortiManager. This method is very useful in an MSSP environment, where many MSSP customers need their own portal to access FortiManager.

FortiPortal uses the REST API to communicate with FortiManager and gather device details. A RESTful API uses standard HTTP methods (GET, POST, DELETE) for client-server interactions. When FortiPortal (client) makes an HTTP request, FortiManager or FortiAnalyzer (server) responds by returning the requested data in XML or JSON format. This process is similar to what happens when a web browser requests a web page from a server, and then the server responds with the web page in HTML format. When REST API is being used, the application (FortiPortal) cannot parse the data in HTML format. The application works only with the XML or JSON formats.

The FNDN provides access tools, sample code, documentation, and access the Fortinet developer community when you subscribe. You can also get more details from the Fortinet document library.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

API HTTP Response Codes

- The API returns an HTTP status code to indicate the status of the request

Code	Message	Details
200	Status ok	Request successful
400	Bad request	Bad request
403	Forbidden	Request is missing the CSRF token or administrator is missing access profile permissions
404	Not Found	Unable to find the specified resource
405	Method Not Allowed	Specified HTTP method is not allowed for this resource
413	Request Entity Too Large	
424	Failed Dependency	
500	Internal Server Error	

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

33

As shown on this table, the API returns an HTTP status code to indicate the status of the request.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

API—Example

- Adding customer site

Request

```
POST https://<ip address>:<port>/fpc/api/customers/1/sites
```

Headers

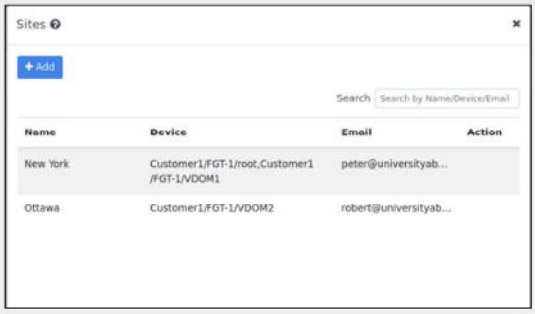
```
Content-type: application/json
fpc-sid: $FPCSID
Cookie: JSESSIONID=$FPCSID
```

Payload

```
{
"networkName" : "New York",
"contactName" : "Peter",
"contactEmail" : peter@universityabc.com,
"fpcDeviceModels": [ {"deviceId" : 3}]
}
```

Response

```
Status : 200 OK
{
"networked" : 5
}
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

34

The API example on this slide shows how to create a new site for the customer with an ID.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

API—Example (Contd)

- To change policy tab permissions

Request

```
GET http://localhost:8080/fpc/api/customers/1/policytabs
```

Headers

```
accept: application/json
content-type: application/json
fpc-sid: $FPCSID
Cookie: JSESSIONID=$FPCSID
```

Response

```
{
"centralNat": false,
"interfacePolicy6": false,
"dosPolicy6": false,
"policy64": false,
"interfacePolicy": false,
"policy6": false,
"dosPolicy": false,
"policy46": false,
"id": 1,
"customerId": 1
}
```

Policy Tab Permissions

- [ ] All
- [ ] Central NAT
- [ ] IPv6 Interface Policy
- [ ] IPv6 DoS Policy
- [ ] NAT64 Policy
- [ ] Interface Policy
- [ ] IPv6 Policy
- [ ] DoS Policy
- [ ] NAT46 Policy

Request

```
POST http://localhost:8080/fpc/api/customers/1/policytabs
```

Headers

```
accept: application/json
content-type: application/json
fpc-sid: $FPCSID
Cookie: JSESSIONID=$FPCSID
```

Payload

```
{
"centralNat": true,
"interfacePolicy6": false,
"dosPolicy6": false,
"policy64": false,
"interfacePolicy": true,
"policy6": false,
"dosPolicy": false,
"policy46": false,
"id": 1,
"customerId": 1
}
```

Response

```
Status 200 OK
```

Policy Tab Permissions

- [ ] All
- [x] Central NAT
- [ ] IPv6 Interface Policy
- [ ] IPv6 DoS Policy
- [ ] NAT64 Policy
- [x] Interface Policy
- [ ] IPv6 Policy
- [ ] DoS Policy
- [ ] NAT46 Policy

FORTINET Training Institute

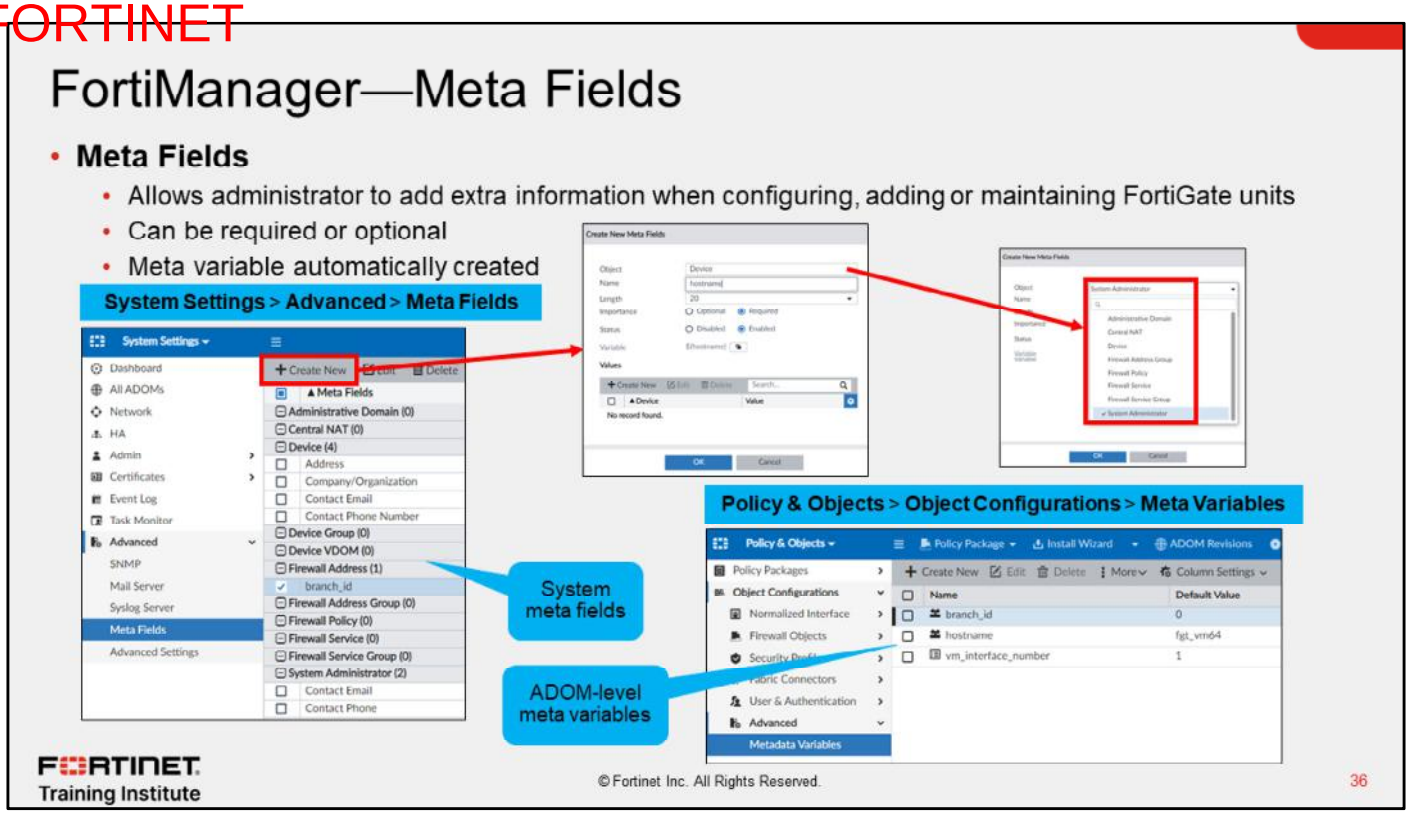
© Fortinet Inc. All Rights Reserved.

35

The API example on this slide shows how to change customer policy tab permissions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Meta Fields allow administrators to add extra information when configuring, adding, or maintaining FortiGate devices or adding new administrators. You can make meta fields required or optional. When meta fields are required, administrators must supply additional information when they create an associated object. For example, if you create a required meta field for a device object, administrators must define a value for the meta field for all devices.

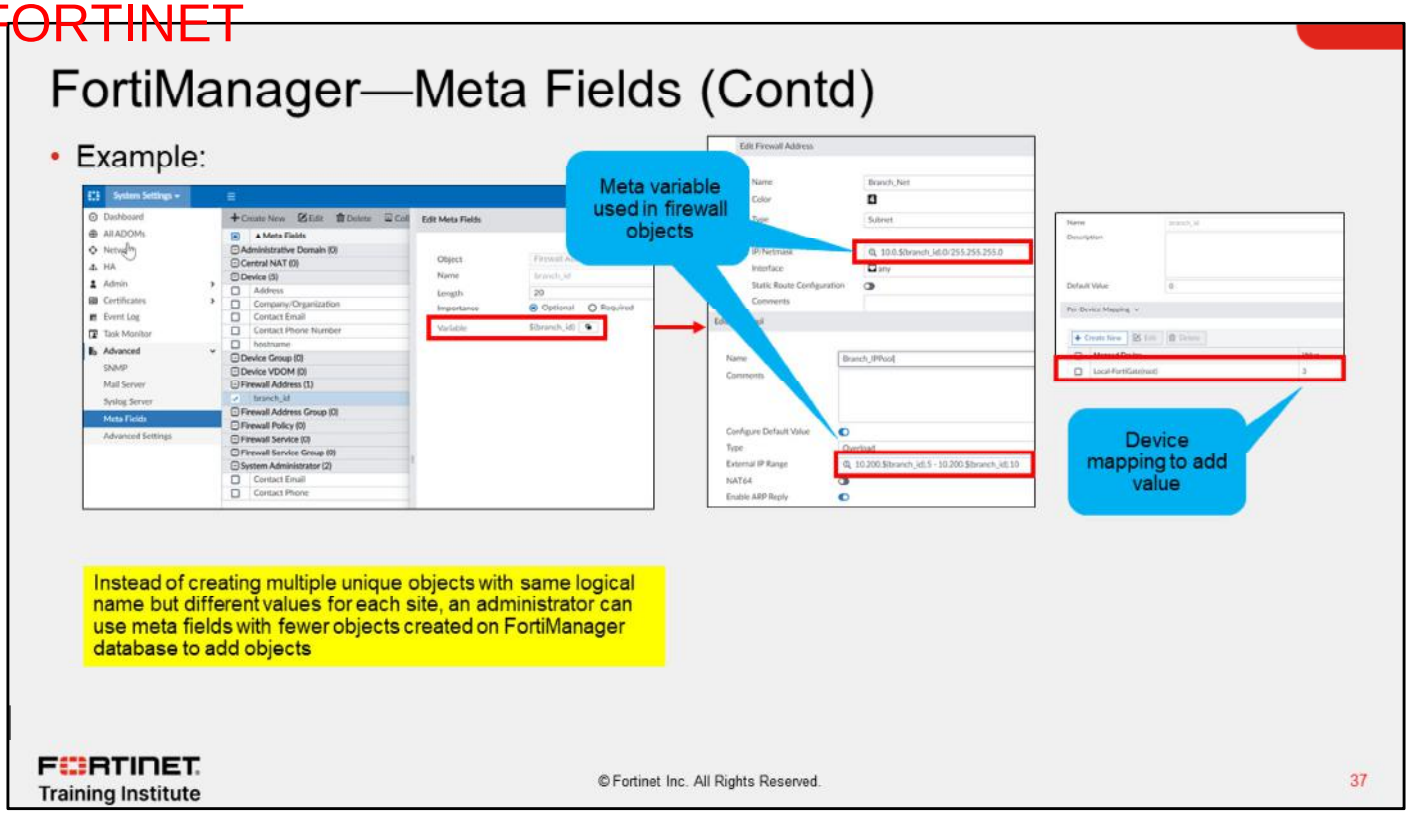
When you create a meta field, a variable for the meta field is automatically created:

Object: allows you to select the object type, such as administrative domain, firewall address group, firewall policy, central NAT, administrator, and so on. This determines where the meta field is used in the configuration.
Importance: allows you to make the meta field setting compulsory on the object that has the meta field option available. For example, to create a new administrator, if the **Contact Email** meta field is set to **Required**, the FortiManager administrator must provide this information to create a new administrator, otherwise select **Optional**.
Status: determines the availability of meta fields to select in the objects. If **Disabled**, you cannot see or select the meta field. This option is available only for non-firewall objects.

In FortiManager, ADOM-level meta variables are also available for general use in scripts, templates, and model devices. This slide shows both system and ADOM-level meta variables. In system meta fields, you must also select the object type such as **Device**, **System Administrator**, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Meta fields are useful when an enterprise has global offices or branches and the FortiManager administrator needs to create multiple objects with the same logical name but different values. Instead of creating hundreds of separate address objects or IPPools in the FortiManager ADOM database, an administrator can create a few logical objects and then map each object to create specific address objects for each FortiGate.

In the example shown on this slide, the meta variable **branch_id** is used in the firewall address object and IPPool. A **branch_id** value is unique for each branch FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager—Meta Fields (Contd)

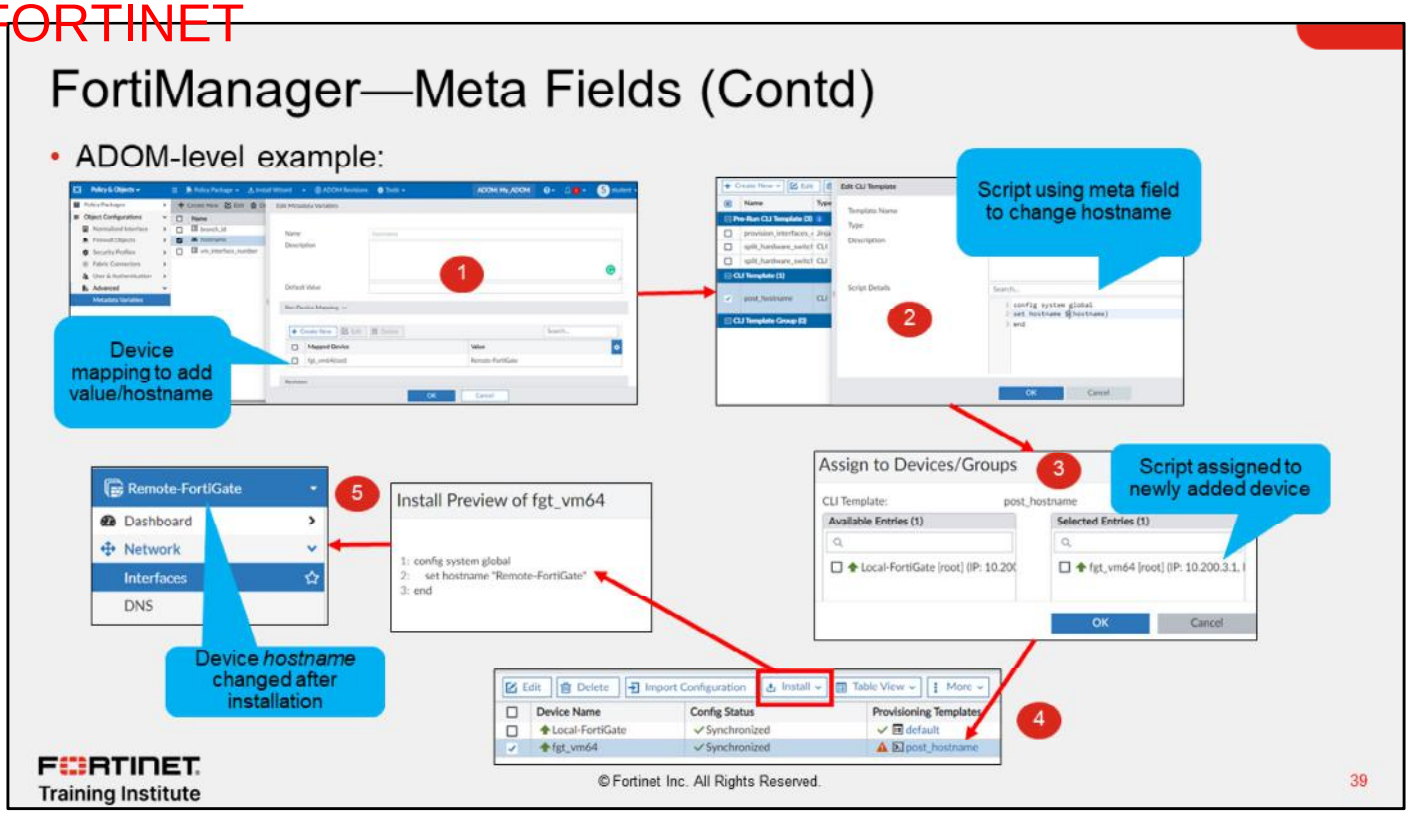
- Example:

© Fortinet Inc. All Rights Reserved.

After firewall objects are assigned and the policy package is installed, the **Firewall Policy** on FortiGate shows that the variable **(branch_id)** has been substituted as per its **per-device** value **3**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this example, the CLI template is assigned to and installed on FortiGate **fgt_vm64**. When an installation is performed, the install preview shows that the variable (hostname) has been substituted as per its per-device value **Remote-FortiGate**.

1. Create or edit the meta variable to map the device and type value. Here you use `Remote-FortiGate` as the value.
2. Use the meta variable in the script.
3. Assign the script to the targeted FortiGate.
4. Install to apply the device-level configuration.
5. The device hostname changes to the defined meta variable value.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about a large MSSP using FortiManager is true?
   A. Each customer must have a dedicated FortiManager device.
   ✓B. ADOMs can be used to separate customers.

2. Which API is available on FortiManager?
   ✓A. JSON API
   B. UML API

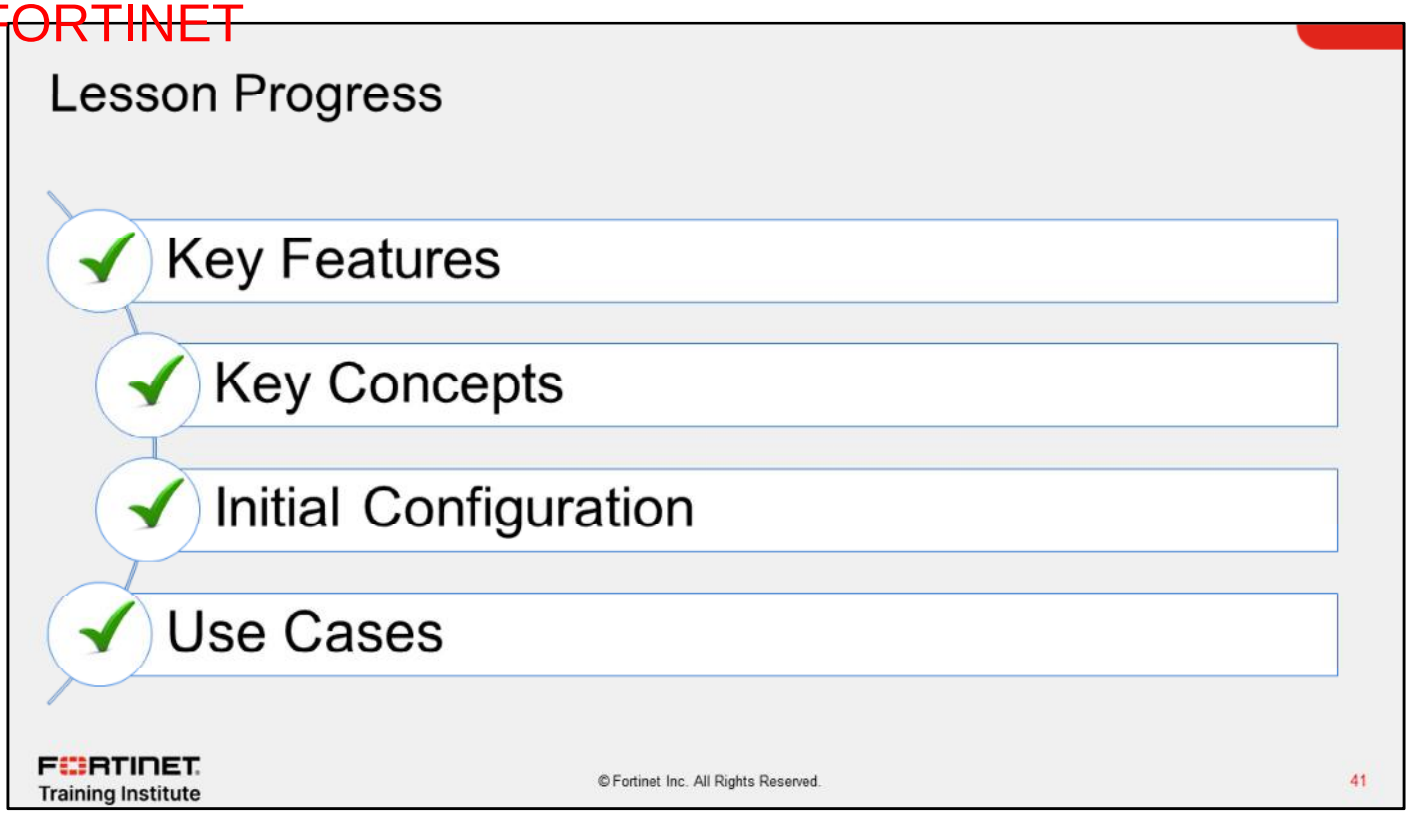
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

40

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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 Brave-dumps.com
© FORTINET

Review

- ✓ Identify key features of FortiManager
- ✓ Describe the purpose of ADOMs
- ✓ Identify devices are supported by FortiManager
- ✓ Identify commonalities between FortiManager and FortiAnalyzer
- ✓ Describe the management module framework
- ✓ Access your FortiManager for the first time
- ✓ Identify the tools you can use to configure FortiManager
- ✓ Add FortiManager to your network
- ✓ Manage FortiAnalyzer features
- ✓ Identify FortiManager use cases
- ✓ Identify the APIs supported by FortiManager
- ✓ Understand the meta fields available on FortiManager

FORTINET Training Institute

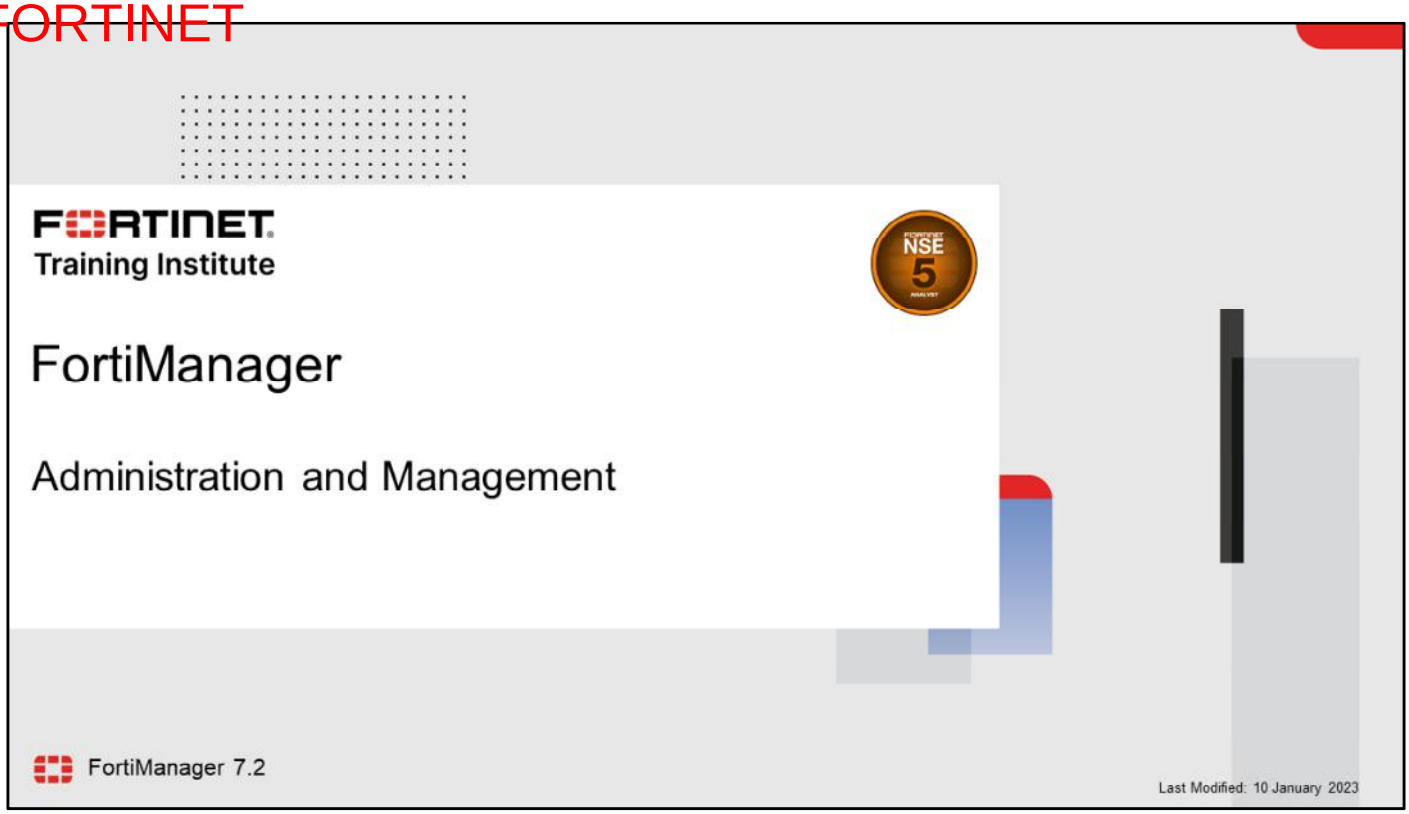
© Fortinet Inc. All Rights Reserved.

42

This slide shows the objectives covered in this lesson. By mastering the objectives covered in this lesson, you learned the basics of FortiManager and how to use it in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn how to set up and administer FortiManager. You will also learn how to use features that are critical to day-to-day use, such as ADOMs, event monitoring, backup, and restore.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Overview

- ADOMs
- Administrator Accounts
- Concurrent Administrators
- ADOM Best Practices and Troubleshooting
- Back up and Restore
- Monitoring Events

FORTINET Training Institute

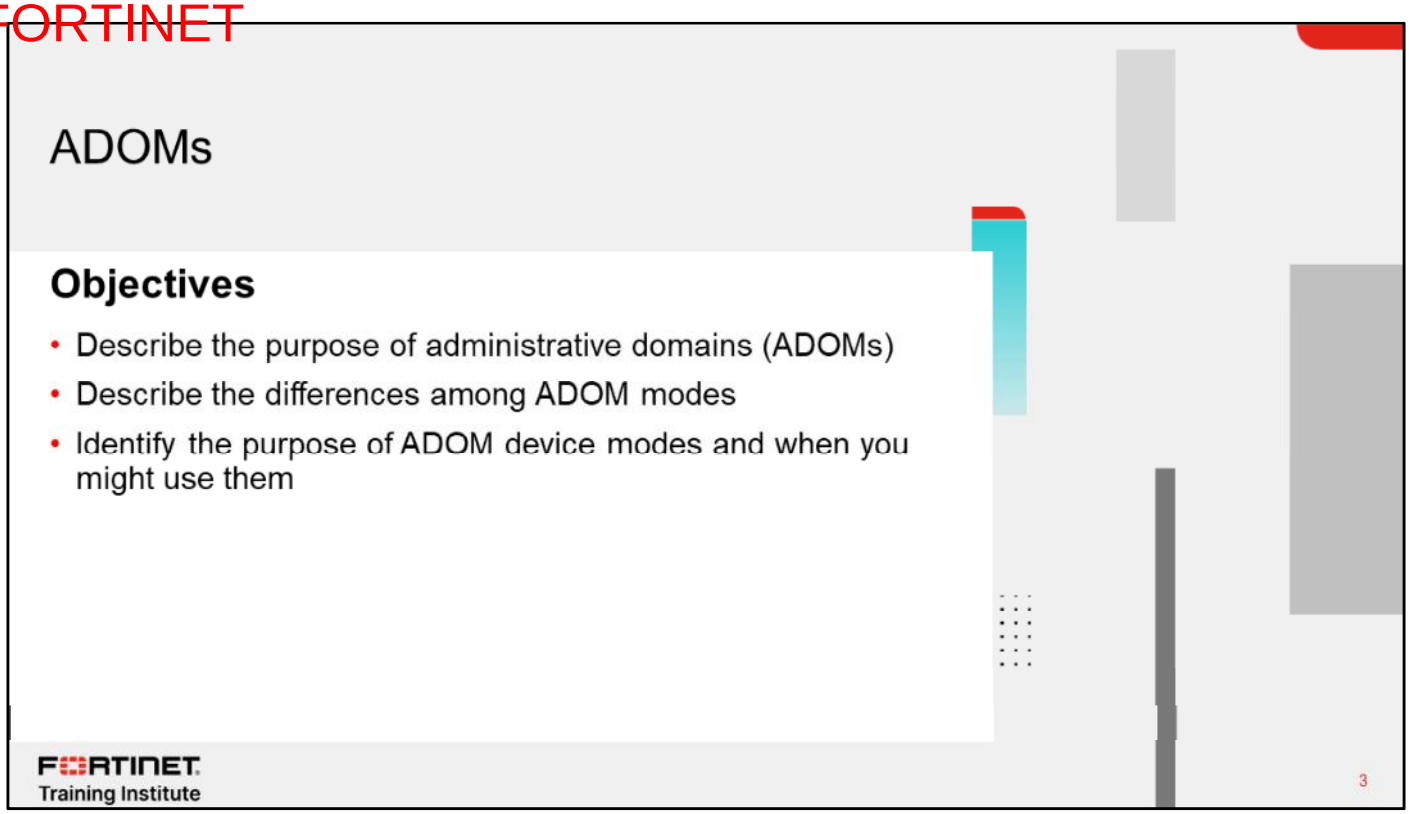
© Fortinet Inc. All Rights Reserved.

2

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

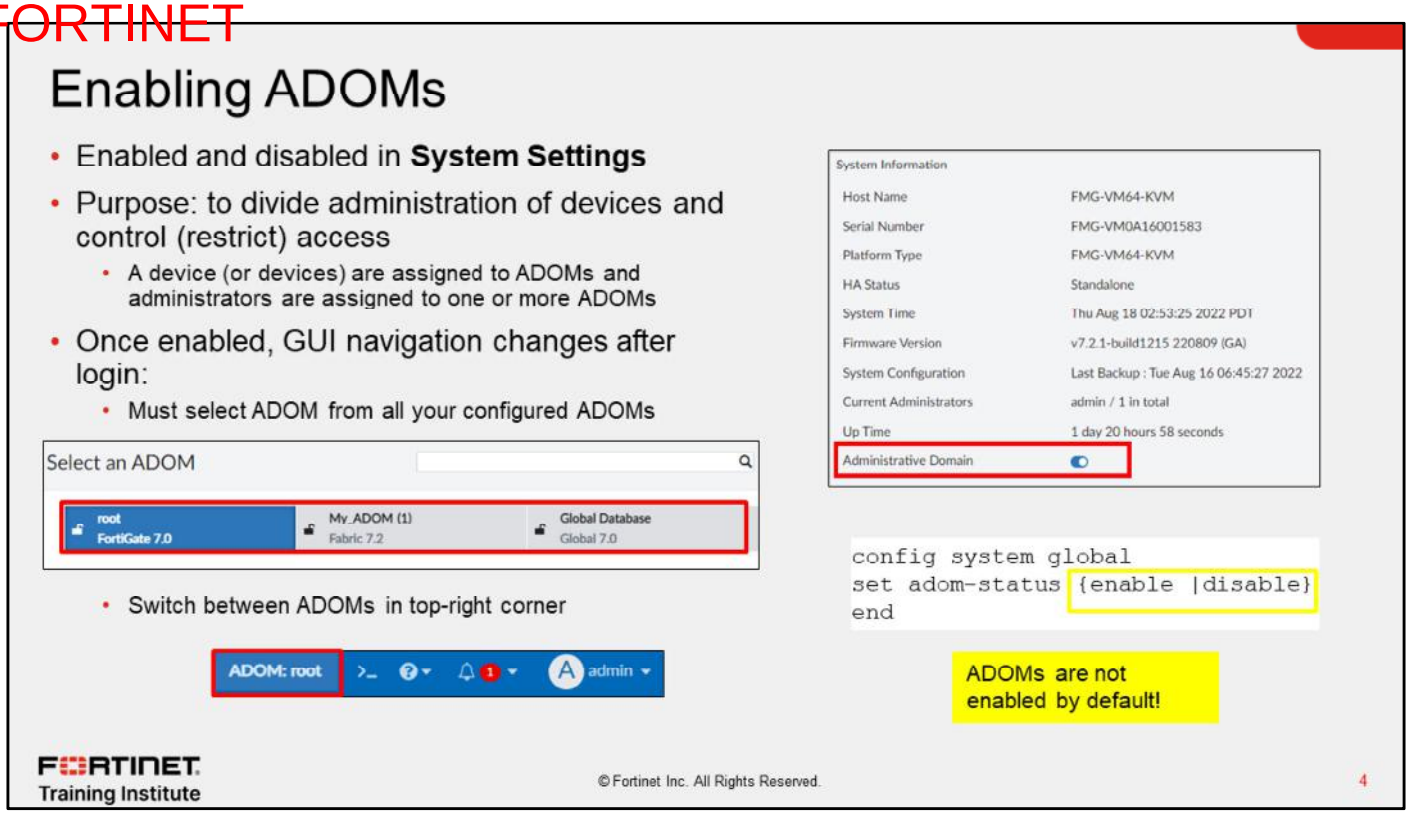


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in ADOMs, you will be able to organize FortiGate devices effectively within FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



ADOMs enable the admin administrator to create groupings of devices for administrators to monitor and manage. For example, administrators can manage devices specific to their geographic location or business division. The purpose of ADOMs is to divide the administration of devices by ADOM, and to control (restrict) administrator access.

ADOMs are not enabled by default and can be enabled (or disabled) only by the admin administrator or an administrator that has the Super_User profile. After you change the ADOM mode, you are logged out so the system can reinitialize with the new settings. When you log in with ADOMs enabled, you must select the ADOM you want to view from your list of configured ADOMs. You can easily switch between ADOMs by clicking the ADOM list in the upper-right corner of the GUI.

Remember, the maximum number of ADOMs varies by FortiManager physical model or VM license.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

ADOM Modes

- Two modes when creating an ADOM: **Normal** and **Backup**
  - **System Settings** > **All ADOMs**

- **Normal** mode:
  - Provides full access to make configuration changes from FortiManager to ADOM and managed devices
- **Backup** mode:
  - Back up configuration changes made directly on managed device

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

5

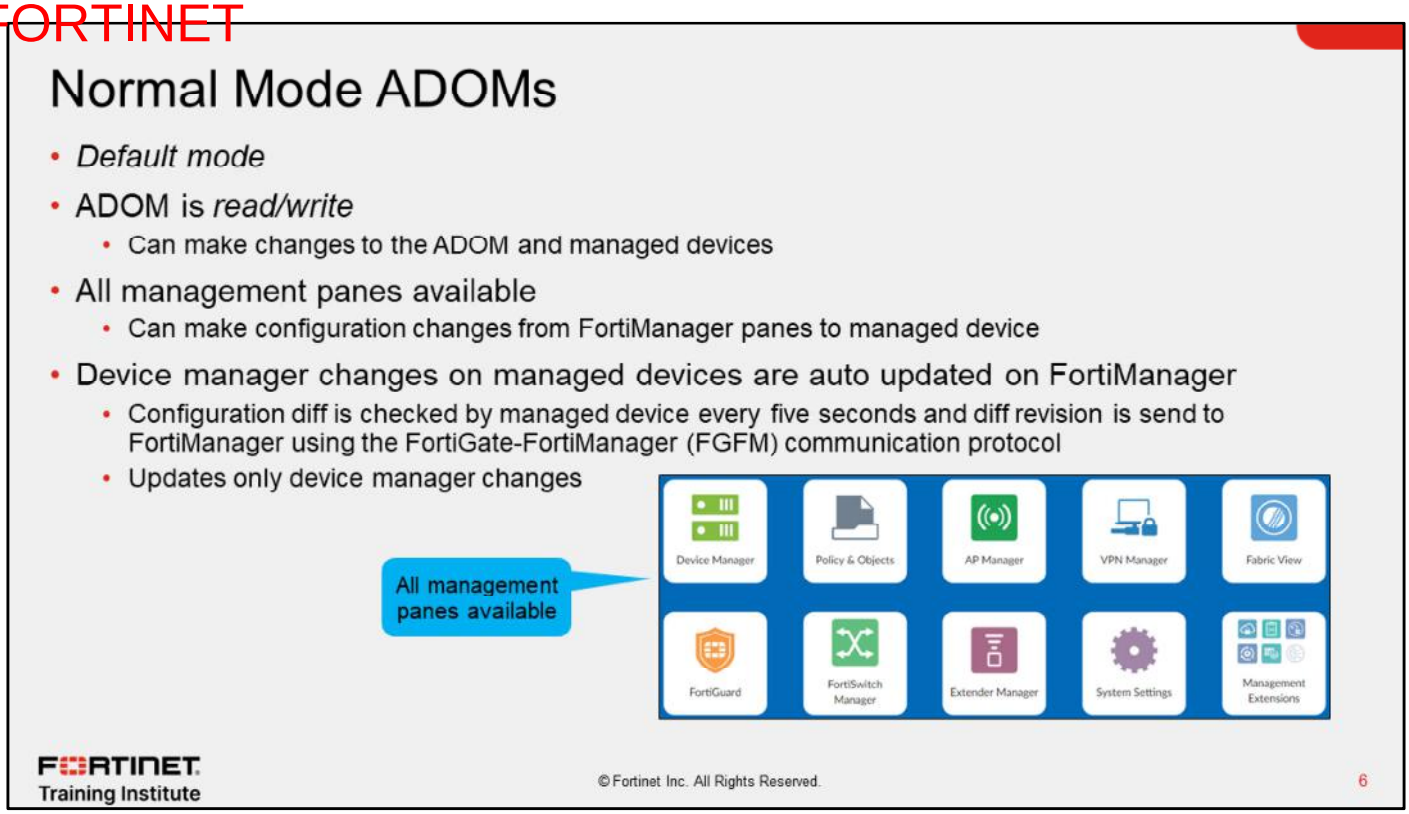
When you configure ADOMs, you can choose between two modes: **Normal** or **Backup**.

In **Normal** mode, you can make configuration changes to an ADOM and the managed devices.

The main purpose of **Backup** mode is to back up the configuration changes made directly on the managed device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

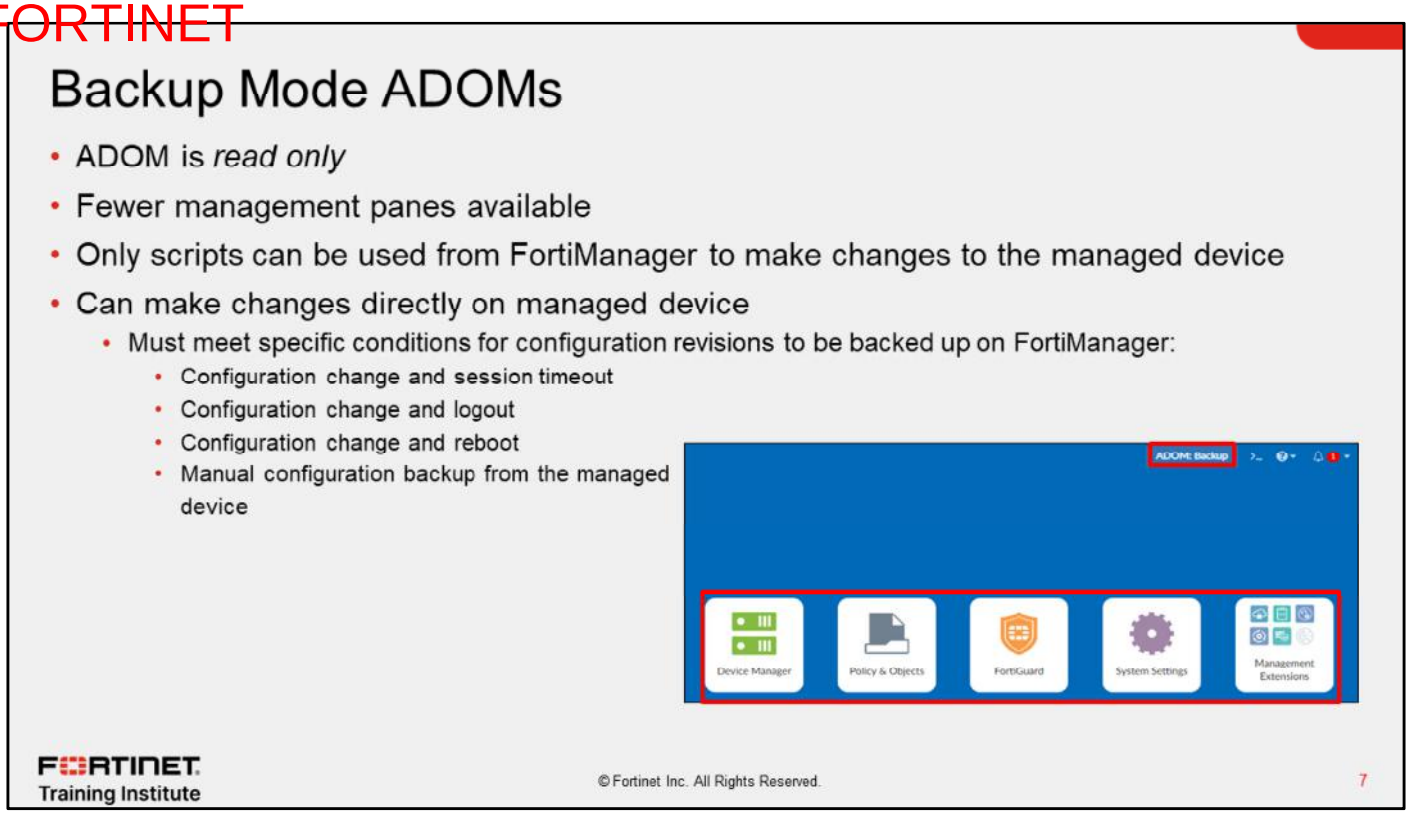


By default, ADOMs run in **Normal** mode and all panes are available. The ADOM is read-write, which allows you to make configuration changes to managed devices stored in the ADOM database and then install those changes on managed devices.

You can also make configuration changes directly to each managed device through the FortiGate CLI or GUI. This will trigger the managed device to automatically update the FortiGate revision history on FortiManager. However, auto-update has a limitation in that it updates *only* device manager changes and not policy and object changes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



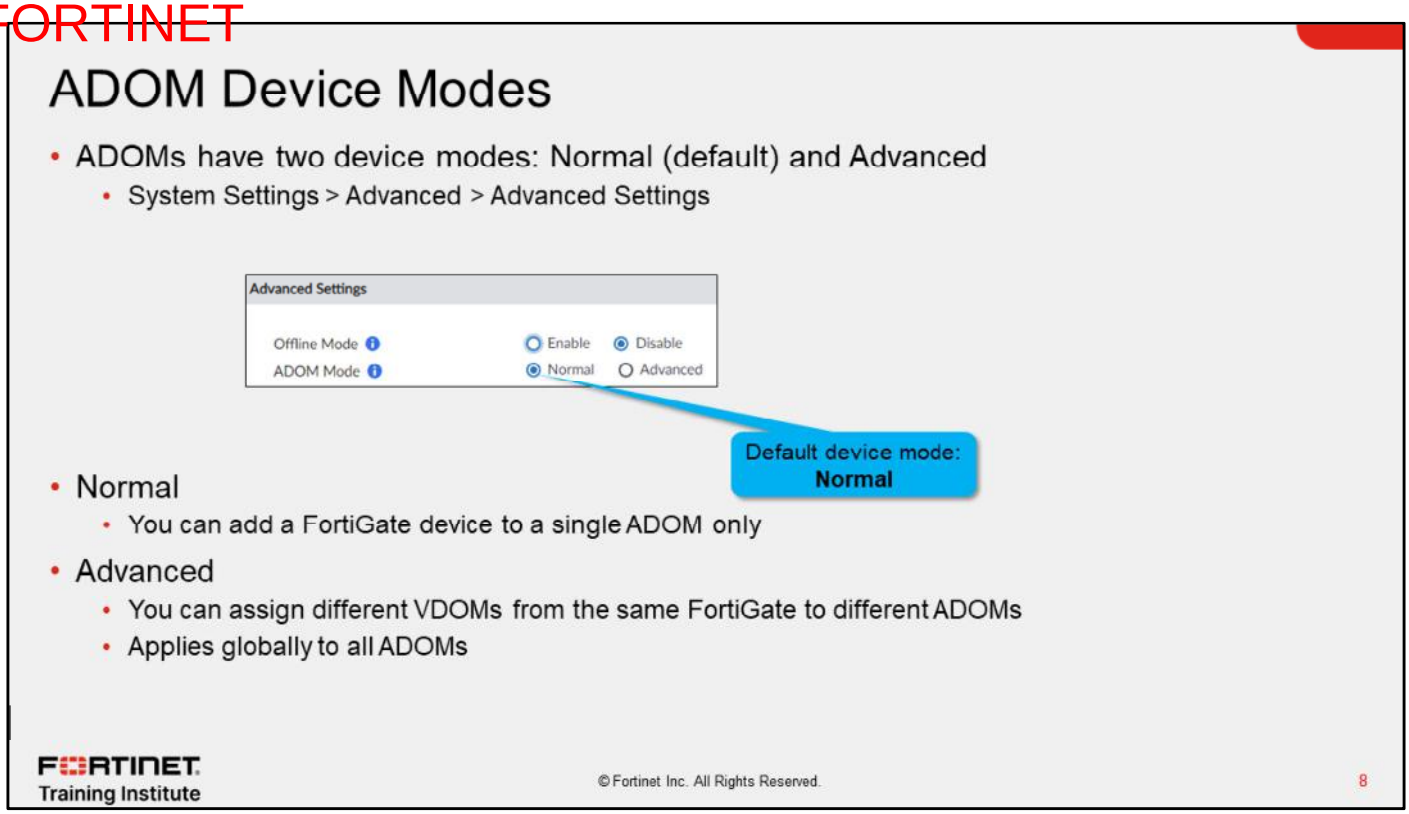
What if managed device configuration changes always need to be made directly on the device and you want to use FortiManager only for revision control and tracking purposes? In this case, you can configure the ADOM in **Backup** mode.

When in **Backup** mode, the ADOM is *read-only*, so the **Device Manager** pane is restricted. You can add and delete devices, but the device-level settings are not available for configuration and installation. For the same reason, other panes such as **AP Manager**, **VPN Manager**, **FortiSwitch Manager** are not available. In **Backup** mode, you can import firewall address and service objects into FortiManager, and FortiManager stores the objects in the **Device Manager** database. You can view the objects on the **Policy & Objects** pane. Although you can view the objects on the **Policy & Objects** pane, the objects are not stored in the central database. This lets you maintain a repository of objects used by all devices in the backup ADOM that is separate from the central database.

You can use the script feature on FortiManager to make configuration changes to managed devices. If you make changes directly on the managed device, those changes need to meet specific conditions in order to trigger the device to back up its configuration to FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



An ADOM has two device modes: **Normal**, which is the default mode, and **Advanced**. In **Normal** mode, you cannot assign different FortiGate virtual domains (VDOMs) to different FortiManager ADOMs.

What if you are a managed security service provider (MSSP), have FortiGate VDOMs for different customers, and want to separate those VDOMs in different ADOMs?

In **Advanced** mode, you can assign different VDOMs from the same FortiGate device to different ADOMs. The system applies this setting globally to *all* ADOMs. This results in more *complicated* management scenarios. It is *recommended for advanced users only.*

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Organizing Devices by ADOM

Can organize managed devices by:

- Device type
  - FortiGate, FortiMail, FortiWeb
- Firmware version
  - FortiOS 6.4, 7.0, and 7.2 valid CLI syntax varies. Separate by version.
- Assigned administrator
- Geographic region
  - East Coast, Australia, Europe, North Africa, remote offices, and so on
- Customer (MSSP scenario)
- Organizational aspect
  - Production networks or staging networks, and so on

Maximum number of ADOMs varies by model

Always group based on device type, then FortiOS firmware version. For example, create two ADOMs if there are devices running version 6.4 and 7.0 in the same geographic region. However, a best practice is to use the FortiManager ADOM upgrade feature instead of maintaining two different ADOMs.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

Which devices should be in each ADOM?

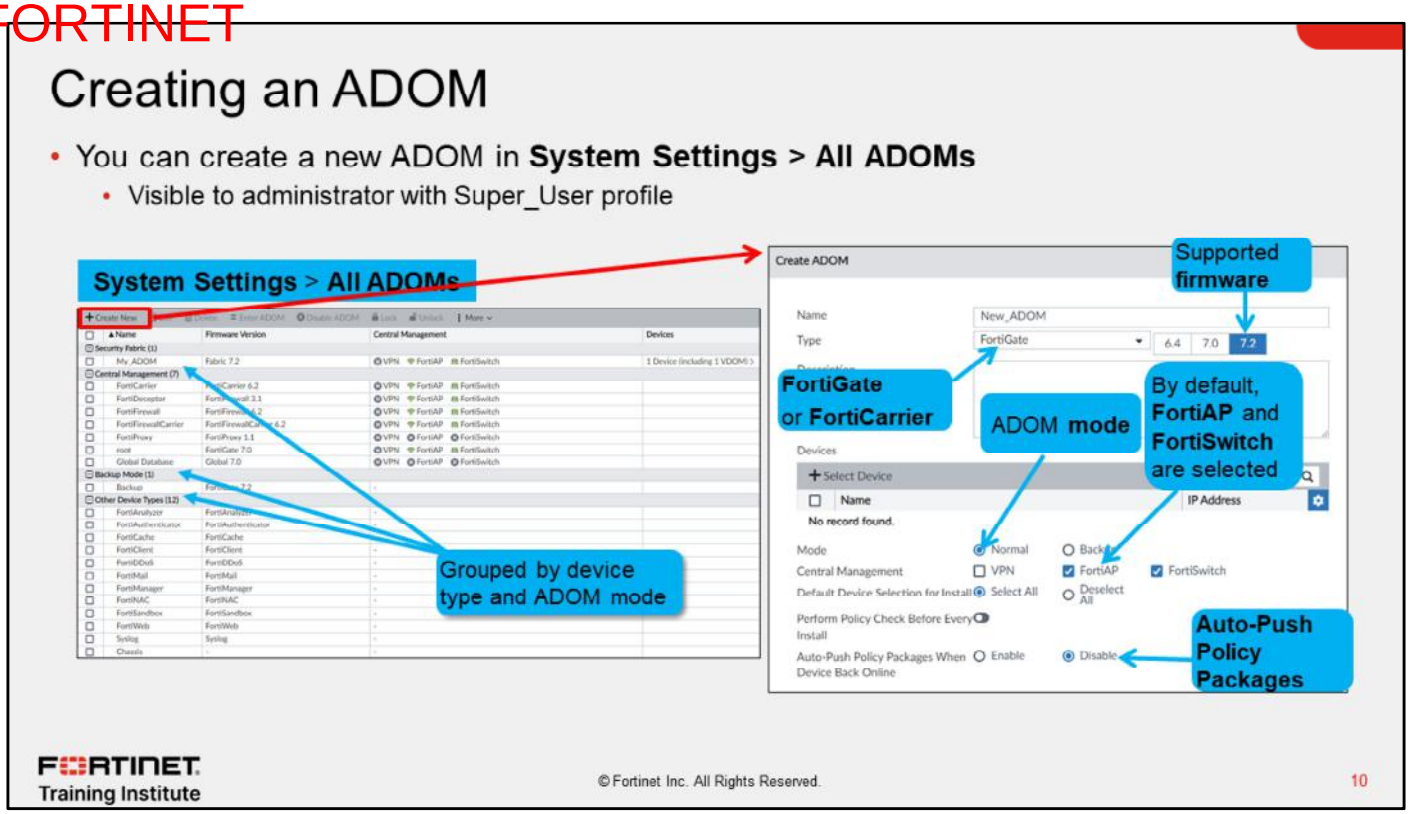
Use a scheme that simplifies management. For example, you could organize your devices by:

- Firmware version: You can group all devices with the same firmware version in the same ADOM. For example, if FortiGate devices are running firmware version 7.0, you can group these devices in a version 7.0 ADOM.
- Geographic regions: You can group all devices for a specific geographic region into an ADOM, and devices for a different region into another ADOM.
- Assigned administrators: You can group devices into separate ADOMs and assign them to specific administrators.
- Customers: You can group all devices for one customer into an ADOM, and devices for another customer into another ADOM.
- Device type: You can create a separate ADOM for each device type. Non-FortiGate devices are automatically located in specific ADOMs for their device type. They cannot be moved to other ADOMs.
- Organizational needs: You can separate production and test network FortiGate devices into separate ADOMs.

When organizing managed FortiGate devices, always group them based on the device type first, then the FortiOS firmware version. Valid command syntax varies by firmware version, which affects script compatibility and other features. For example, if you are grouping based on geographic region and have FortiGate devices running FortiOS 7.0 and 7.2 firmware in the same region, you should create two ADOMs based on the firmware version, for that geographic region. Then, you would assign both ADOMs to the administrator for that region. However, a best practice is to use the FortiManager ADOM upgrade feature and upgrade all the devices to the same firmware version.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



With ADOMs enabled, administrators with the Super_User profile have access to the **All ADOMs** page, where all default ADOMs and custom ADOMs created by the administrator appear. You can restrict the access of other administrators to one or more specific ADOMs.

FortiGate ADOMs are grouped together. If the default ADOMs do not fit your requirements, you can create your own. While you can edit these default ADOMs, you cannot edit the device type or firmware version of the device. This is because, internally, the database structure depends on what types of data that FortiManager needs to store for that device type or firmware.

The ADOM type you create *must match* the device type you are adding. For example, if you want to create an ADOM for FortiGate, you must select FortiGate as the ADOM type. With FortiGate ADOMs specifically, you must also select the firmware version of the FortiGate device.

Different firmware versions have different features, and therefore different CLI syntaxes. Your ADOM setting *must* match the device's firmware.

The default ADOM mode is **Normal**. In the **Central Management** field, you can select **VPN** to centrally manage IPsec VPNs for all managed devices in that ADOM. By default, **FortiAP** and **FortiSwitch** central management are selected.

Auto-Push-Policy: If auto-push is enabled, policy packages and device settings will be installed to offline devices when they come back online.

The maximum number of ADOMs you can create varies by FortiManager model.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the main purpose of backup ADOM mode?
   - ✓A. To maintain the backup configuration of managed devices
   - B. To install policy package changes offline

2. Which action can you perform in advanced ADOM mode?
   - ✓A. You can assign different VDOMs from FortiGate to different ADOMs
   - B. You can assign the same VDOM from FortiGate to different ADOMs

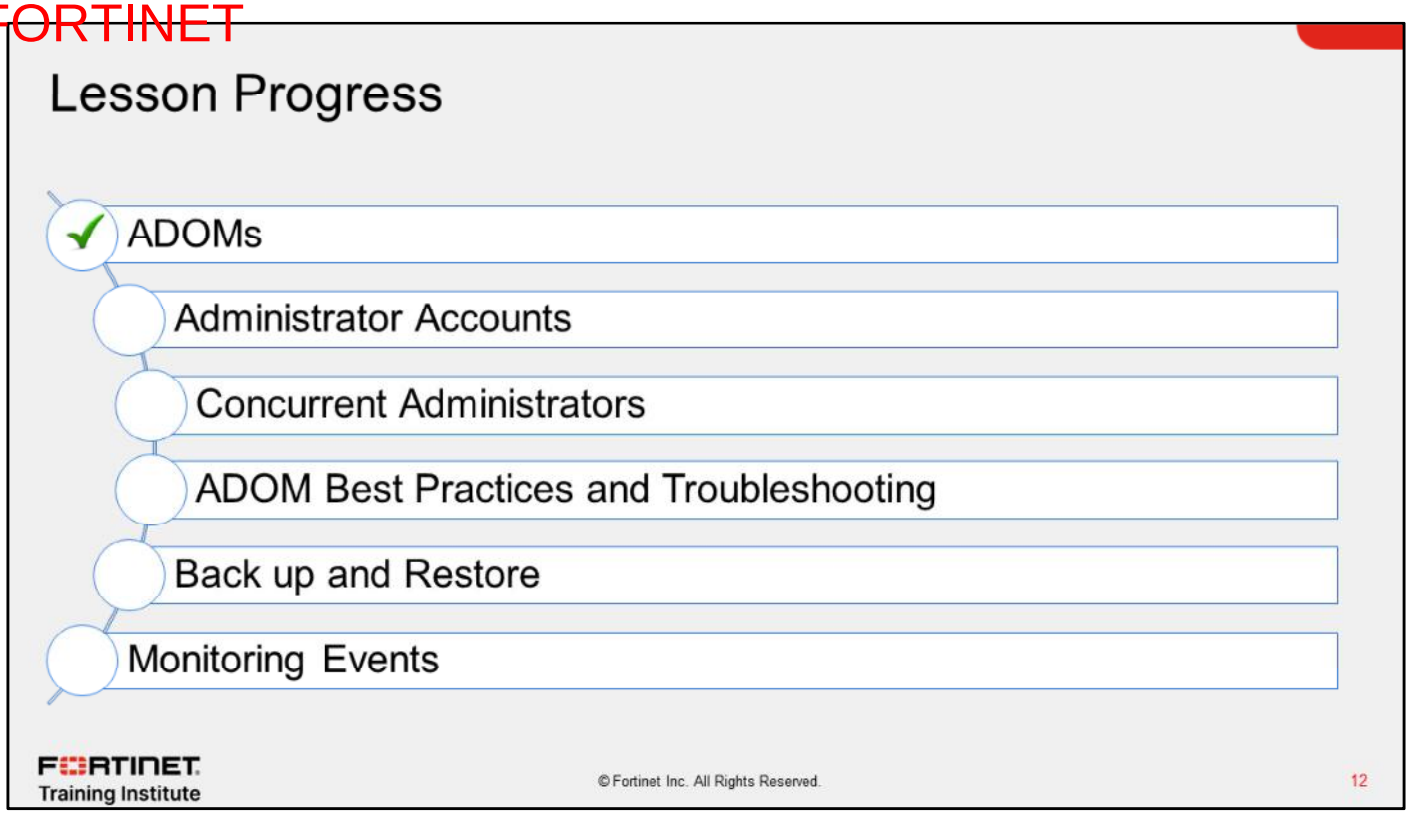
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

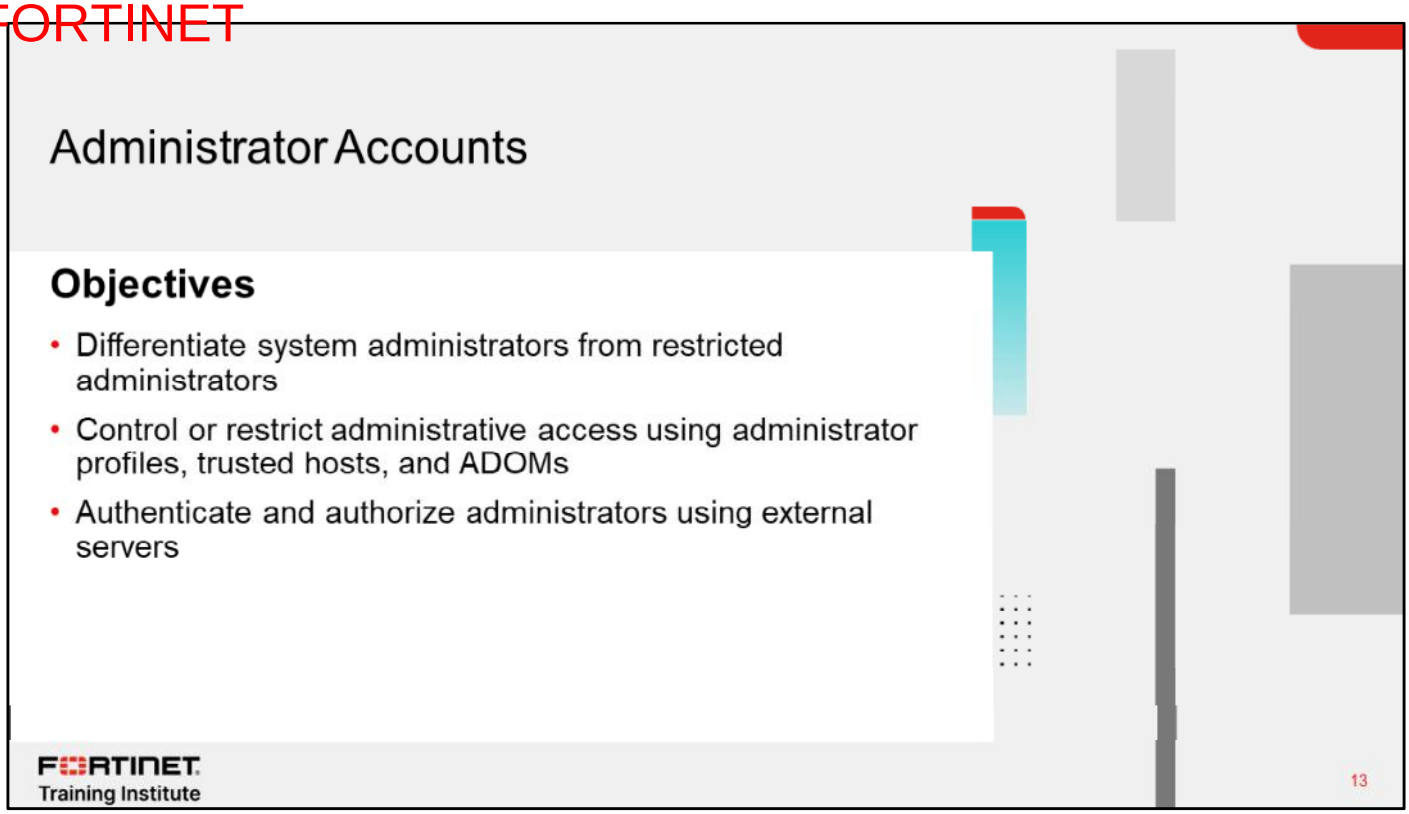


Good job! You now understand ADOMs.

Now, you will examine administrator accounts on FortiManager.

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 using administrative access controls, you will be able to better safeguard the administration and management of FortiManager and the managed devices.

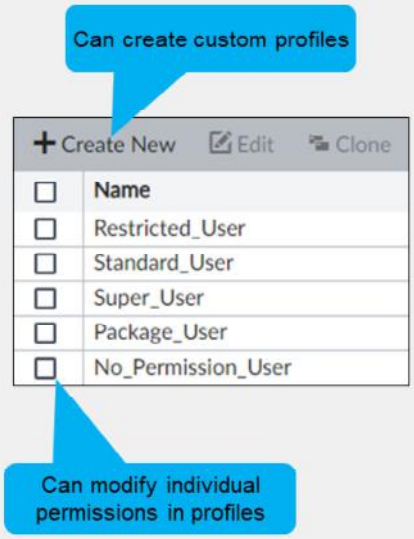
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuring Administrator Profiles

- Access profiles define administrator permissions

Profile Name	Administrator permissions
Package_User	• Read/write access to policy packages and object permissions • Read-only access for system and other permissions
Restricted_User	• No system permissions • Read-only access for all device permissions
Standard_User	• No system permissions • Read/write access for all device permissions
Super_User	• All system permissions enabled • All device permissions enabled
No_Permission_User	• No system or device privileges enabled



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

In order to efficiently administer your system, FortiManager comes with five pre-installed default profiles that you can assign to other administrative users. Administrator profiles define administrator permissions and are required for each administrative account. The five default profiles are:

- Package_User: provides read/write access to policy package and objects permissions, but read-only access for system and other permissions
- Restricted_User: provides read-only access to device permissions, but not system permissions
- Standard_User: provides read/write access to device permissions, but no system permissions
- Super_User: provides access to all device and system permissions, such as FortiGate
- No_Permission_User: no system or device privileges enabled

You can assign the default profiles to administrative accounts, or you can modify the individual permissions associated with each default profile. Alternatively, you can create your own custom profile.

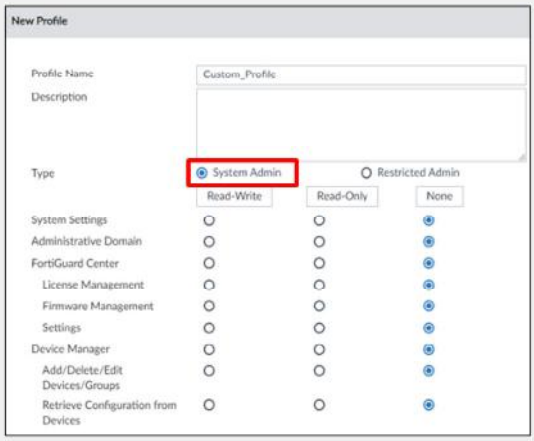
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Types of Administrator Profiles

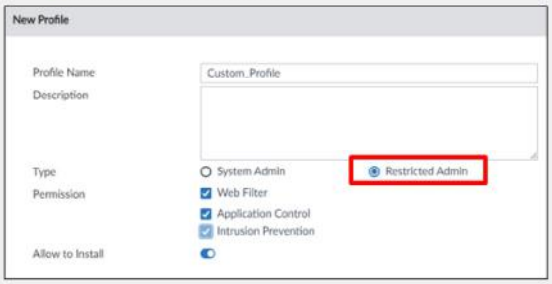
System Admin

- Wider scope and granularity
- Custom profile options control administrator access



Restricted Admin

- Restricts administrator accounts
- Delegated management of specific security profiles for each ADOM
- Scope is only three security profiles
  - Intrusion protection system (IPS) sensors
  - Web filter profiles
  - Application sensors



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

You can customize both administrator profile types: **System Admin** and **Restricted Admin**.

For the **System Admin** type, you can modify one of the predefined profiles, or create a custom profile. Only administrators with full system permissions can modify administrator profiles. Depending on the nature of the administrator's work, access level, or seniority, you can allow them to view and configure as much, or as little, as required.

For the **Restricted Admin** type, you can create a new restricted administrator profile to allow the delegated administrator to make changes to the web filtering profile, IPS sensor, and application sensor associated with their ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Types of Administrator Profiles (Contd)

IPS Admin

- New firewall administrator role on IPS objects
- CLI only configuration

```
config system admin profile
edit <profile_name>
set ips-objects {none | read | read-write}
next
end
```

- If set to `read`, administrators with this profile can:
  - Read but not edit or install IPS objects
  - Install firewall policies without installing IPS-related objects
  - Assign IPS profiles in the policy package
- If set to `read-write`, administrators with this profile can:
  - Edit and install IPS objects in addition to having *read-only* privileges
- If set to `none`, administrators with this profile cannot see IPS objects

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

A new firewall administrator role *IPS admin* has been added. The IPS administrator, depending on permissions, can have read or read-write access on the IPS objects. You can configure this administrator profile only from the CLI. You can set none, read, and read-write permissions. If permissions are set to `read`, the IPS administrator can:

- Read but not edit or install IPS objects
- Install firewall policies without installing IPS-related objects
- Assign IPS profiles in the policy package

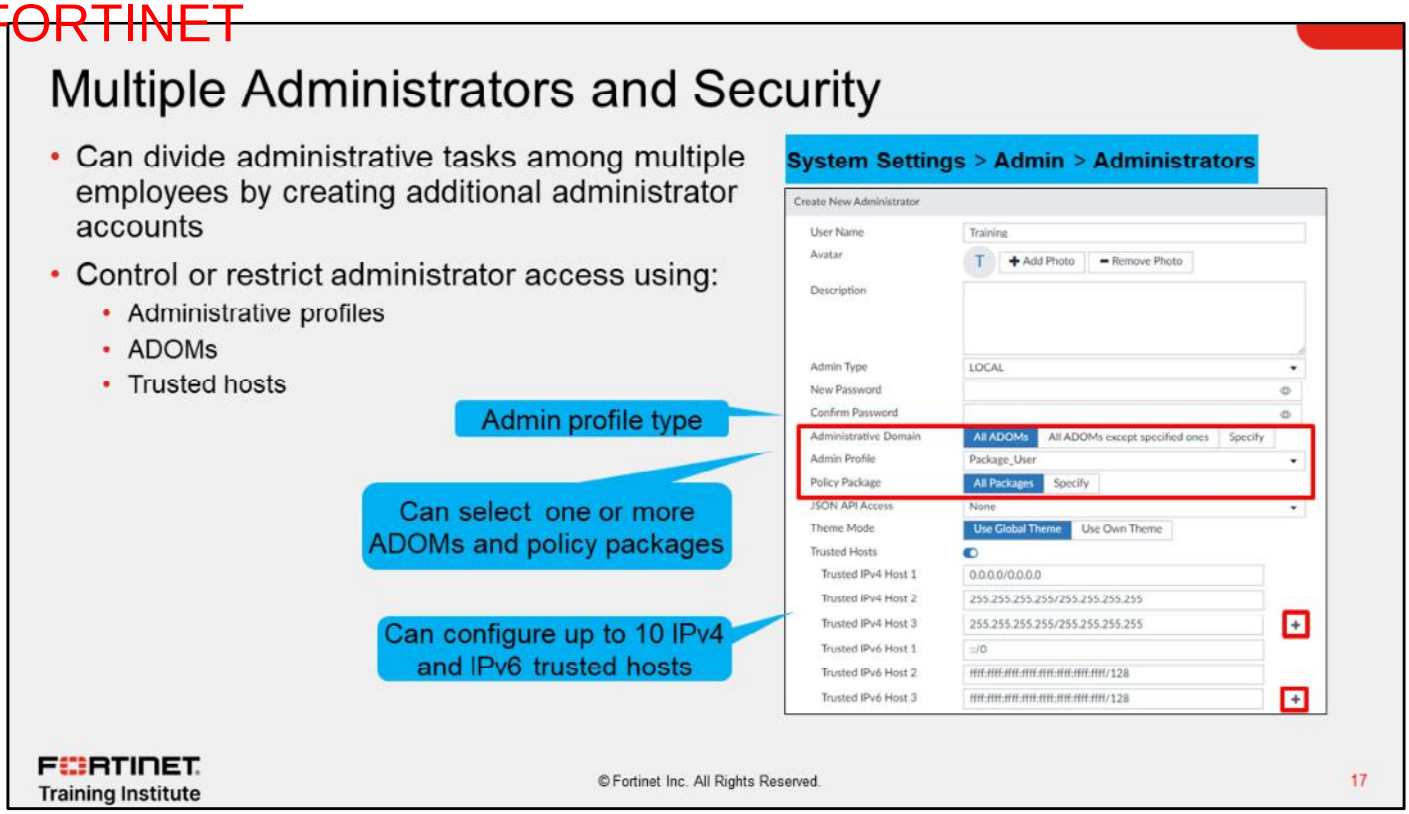
An administrator with a `read-write` profile can also edit and install IPS objects in addition to having the read-only privileges.

The IPS admin profile has visibility on each IPS profile on FortiManager, including usage, status, installed versus modify, and configuration differences, as compared to the *Restricted Admin* profile that has visibility only to the IPS profile associated with their ADOM. This enables the administrator to assign multiple ADOMs to the IPS administrator, including the global ADOM.

This feature is very useful for large enterprises or financial institutions that have dedicated IPS administrators for IPS management.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Depending on your deployment, you may want to divide FortiManager administrative tasks among multiple employees by creating additional administrator accounts.

In order to protect your network, you can control and restrict administrator access using the following methods:

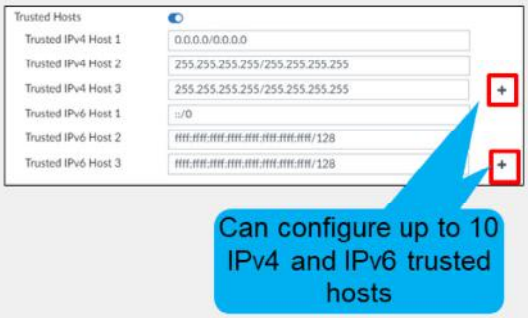
- Administrative profiles
- ADOMs
- Trusted hosts

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access Control for Administrative Users

- Trusted hosts restrict login access to specific IP addresses or subnets
- Configure up to ten IPv4 and IPv6 trusted hosts
- Applies to both GUI and CLI (when accessed through SSH)



- Local-in policy control traffic
- Only available on the CLI
- Support both IPv4 and IPv6

```
# config system local-in-policy
(local-in-policy)# config system local-in-
policy
    edit 1
        set action accept
        set src 10.0.1.10 255.255.255.0
    next
End
```

```
Additional settings:
set
action: Action performed on traffic matching this policy.
dport: Destination port number (0 for all).
dst: Destination IP and mask.
intf: Incoming interface name.
protocal: Traffic protocal.
src: Source IP and mask.
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

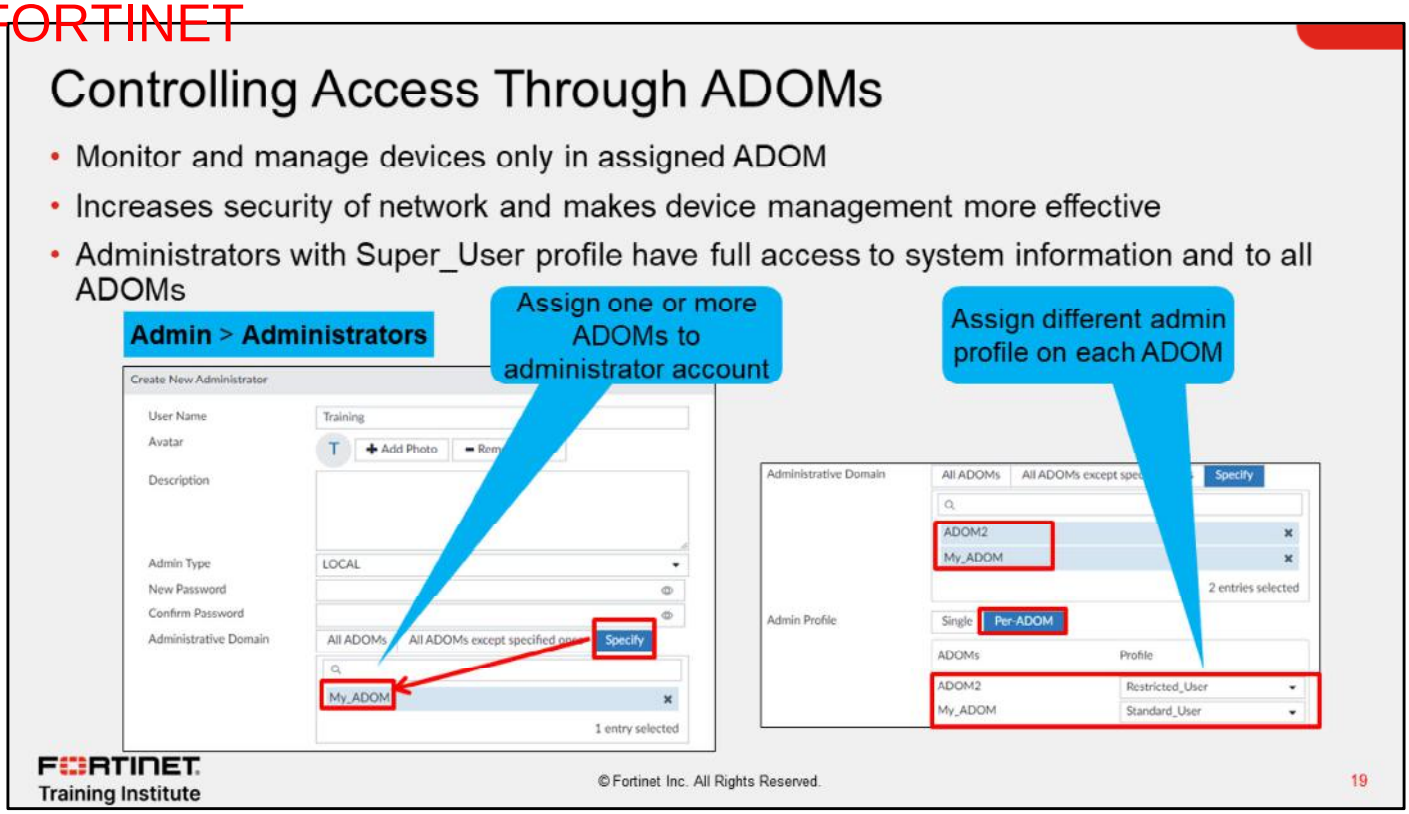
In addition to controlling administrative access through administrator profiles, you can further control access by setting up trusted hosts for each administrative user and/or local-in policy to control traffic to a FortiManager.

The trusted host restricts administrators to logins from specific IP addresses or subnets only. You can even restrict an administrator to a single IP address if you define only one trusted host IP address. The trusted hosts you define apply to both the GUI and the CLI when accessed through SSH.

A local-in policy controls traffic to a FortiManager interface and can be used to restrict administrative access. This policy allows you to define settings such as action, destination port, destination IP, incoming interface, protocol and source IP address. This feature can only be configured using the FortiManager CLI and supported for both IPv4 and IPv6 traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Another way you can control administrative access is through ADOMs. This makes device management more effective, because administrators need to monitor and manage devices only in their assigned ADOM. It also makes the network more secure, because administrators are restricted to only those devices to which they should have access.

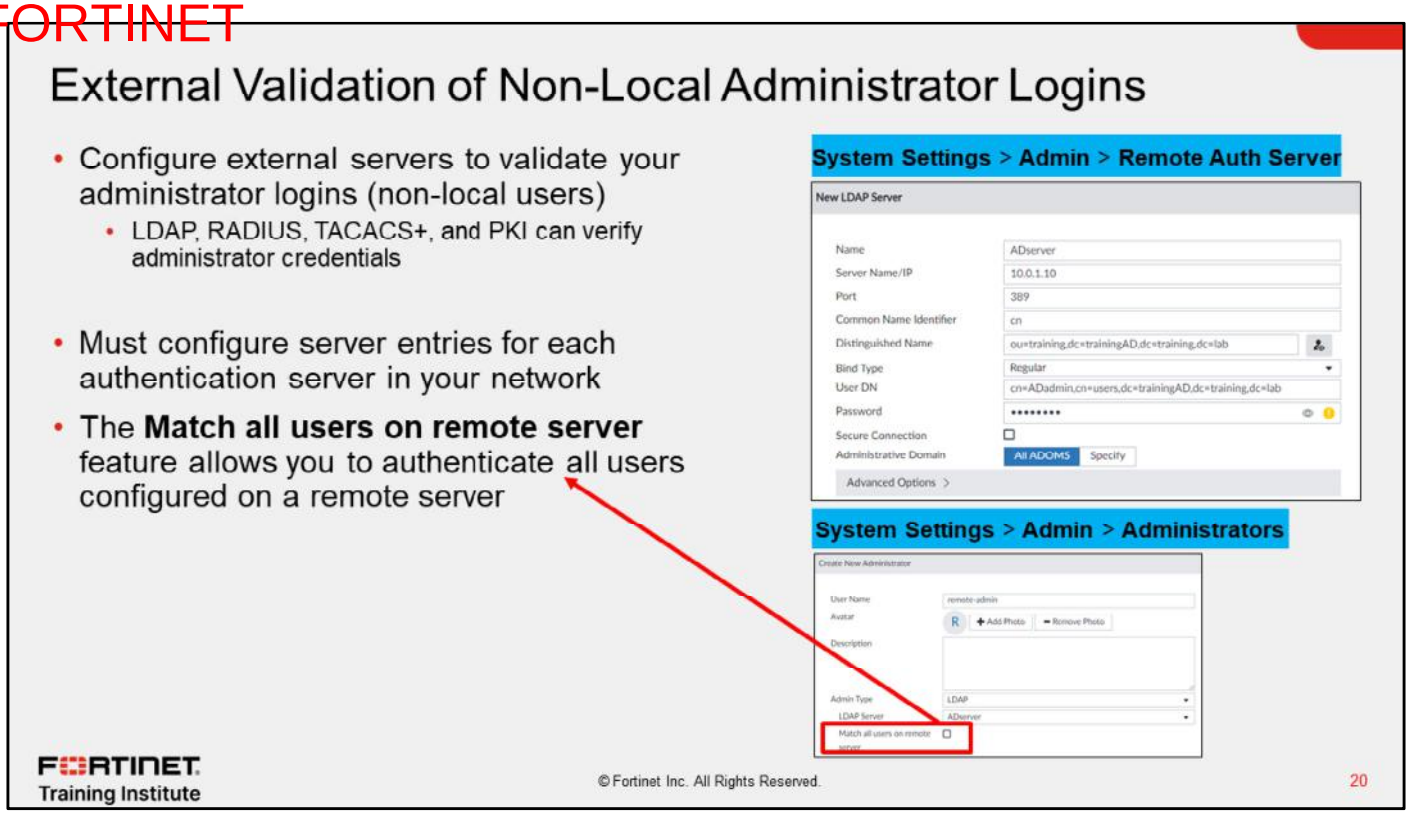
Administrators who have the Super_User profile have full access to all ADOMs, whereas administrators with any other profile have access only to those ADOMs to which they are assigned—this can be one or more.

You can also assign different admin profiles to same administrator for each ADOMs. As shown on this slide, an administrator **Training** is assigned two ADOMS and for profile **Per-ADOM** is selected. The Admin Profile setting displays the list of ADOMs that you specified access to for the administrator with a different profile you selects for each ADOM.

If **Single** is selected, the administrator will only have one admin profile for all ADOMs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

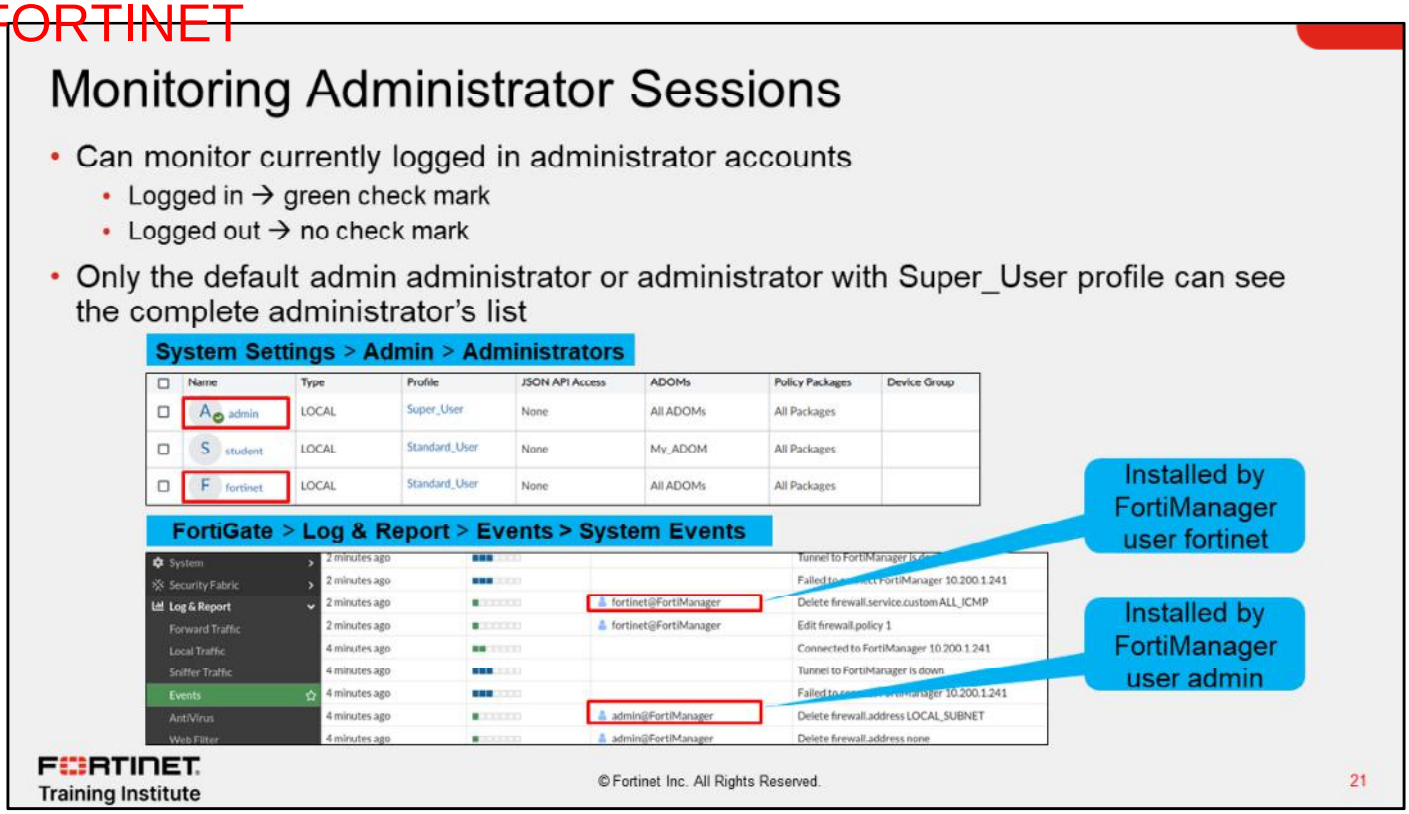


Instead of creating local administrators, where logins are validated by FortiManager, you can configure external servers to validate your administrator logins. You can use RADIUS, LDAP, TACACS+, and PKI as means of verifying the administrator credentials.

To configure two-factor authentication, you also need FortiAuthenticator and FortiToken. See the *FortiManager Administration Guide* for more details.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To track administrator user sessions, including who is currently logged in and through what trusted host, click **System Settings** > **Admin** > **Administrator**. Only the default admin administrator or administrator with the **Super_User** profile can see the complete administrator's list.

To track installation changes from the FortiManager user, click **Log & Report** > **Events** on the managed FortiGate device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. How can you restrict an administrator's access to only a few ADOMs on FortiManager?
   A. By disabling concurrent access to ADOMs
   ✓ B. By assigning ADOMs to the administrator account

2. Which feature is available in the Restricted Admin profile?
   A. Device registration
   ✓ B. IPS sensor

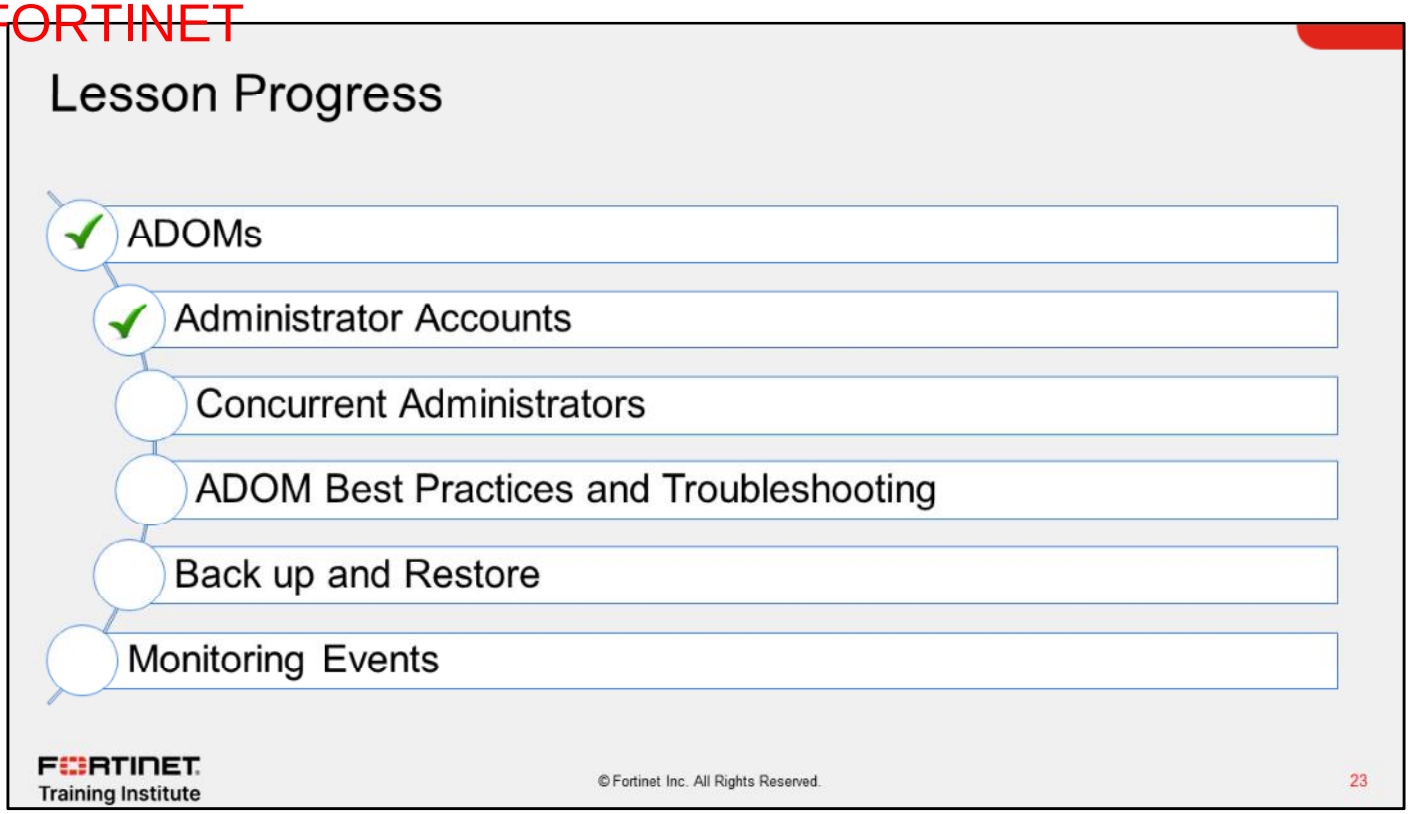
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

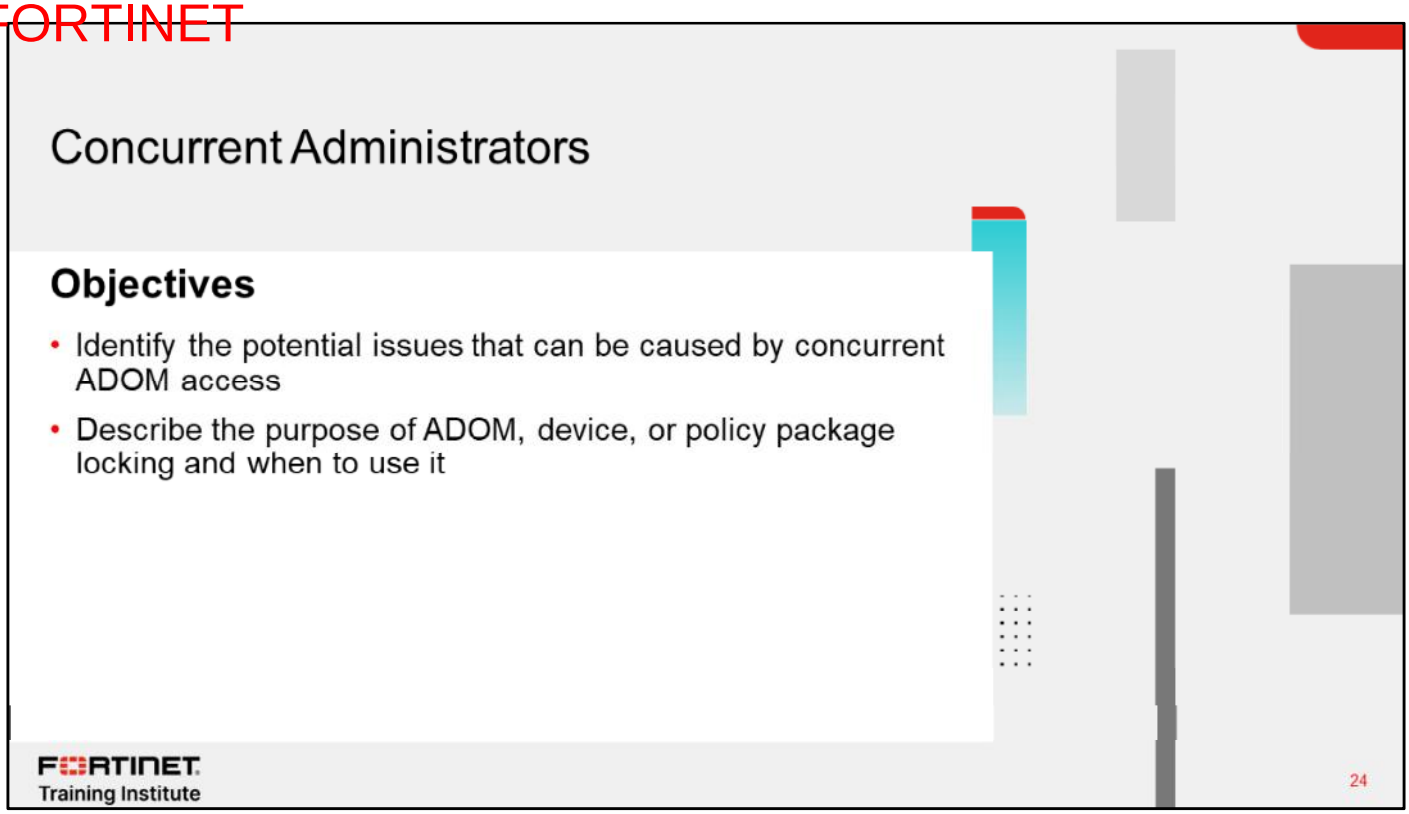


Good job! You now understand administrator accounts.

Now, you will examine concurrent administrators on FortiManager.

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 using ADOMs, device, or policy package locking, you will be able to better safeguard the administration and management of FortiManager and the managed devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Concurrent ADOM Access

- By default, multiple administrators can log in to same ADOM, at same time

```
config system global
set workspace-mode disabled
end
```

Default disabled

- Allows concurrent access
- Causes conflicts if two or more administrators try to change same ADOM, at same time

System Settings > Admin > Administrators

Name	Type	Profile	JSON API Access		Packages
A admin	LOCAL	Super_User	None		ages
S student	LOCAL	Standard_User	None	My_ADOM	All Packages
F fortinet	LOCAL	Super_User	None	All ADOMs	All Packages

= logged in

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

By default, multiple administrators can access the same ADOM concurrently because `workspace-mode` is set to `disabled`.

Usually this is OK, especially if you've used administrator profiles with non-overlapping permissions. The probability of two people changing the same setting in a network with hundreds of complex devices is small, but it is still possible.

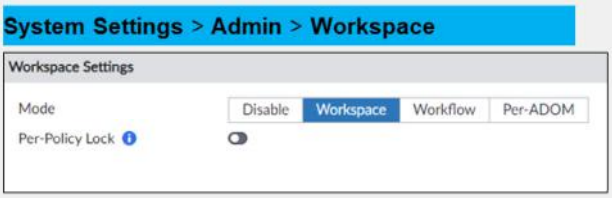
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Workspace Mode

- Disables concurrent ADOM access, adds ADOM locking
- You must lock an ADOM, a device, or a policy package
- Read/write access for only *one* administrator—all other administrators have read-only access

```
config system global
set workspace-mode normal
end
```



- Must notify other administrators before enabling workspace mode to save their work
  - May cause some login users to lose their unsaved data

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

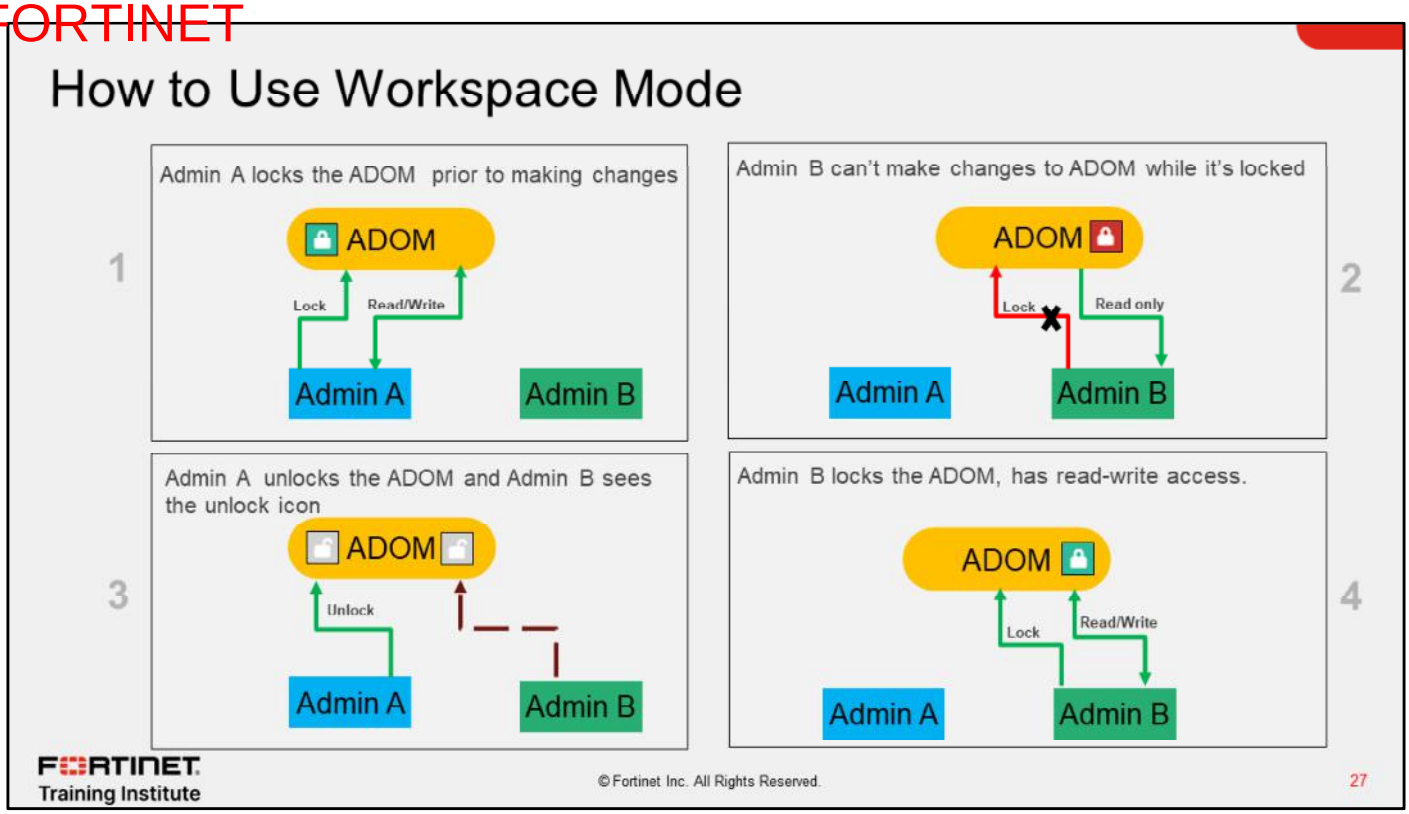
What if multiple administrators try to change the same devices, at the same time, but make different changes?

This can cause conflicts: one administrator's changes will be overwritten by the other administrator's changes. If conflicts are likely to occur for you, you can use both CLI or GUI to enable workspace mode and prevent concurrent ADOM access.

This allows administrators to lock their ADOM, a device, or a policy package. Furthermore, only a single administrator has read/write access to the ADOM, while all other administrators have read-only access. Locking an ADOM automatically removes locks on devices and policy packages that you have locked within that ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

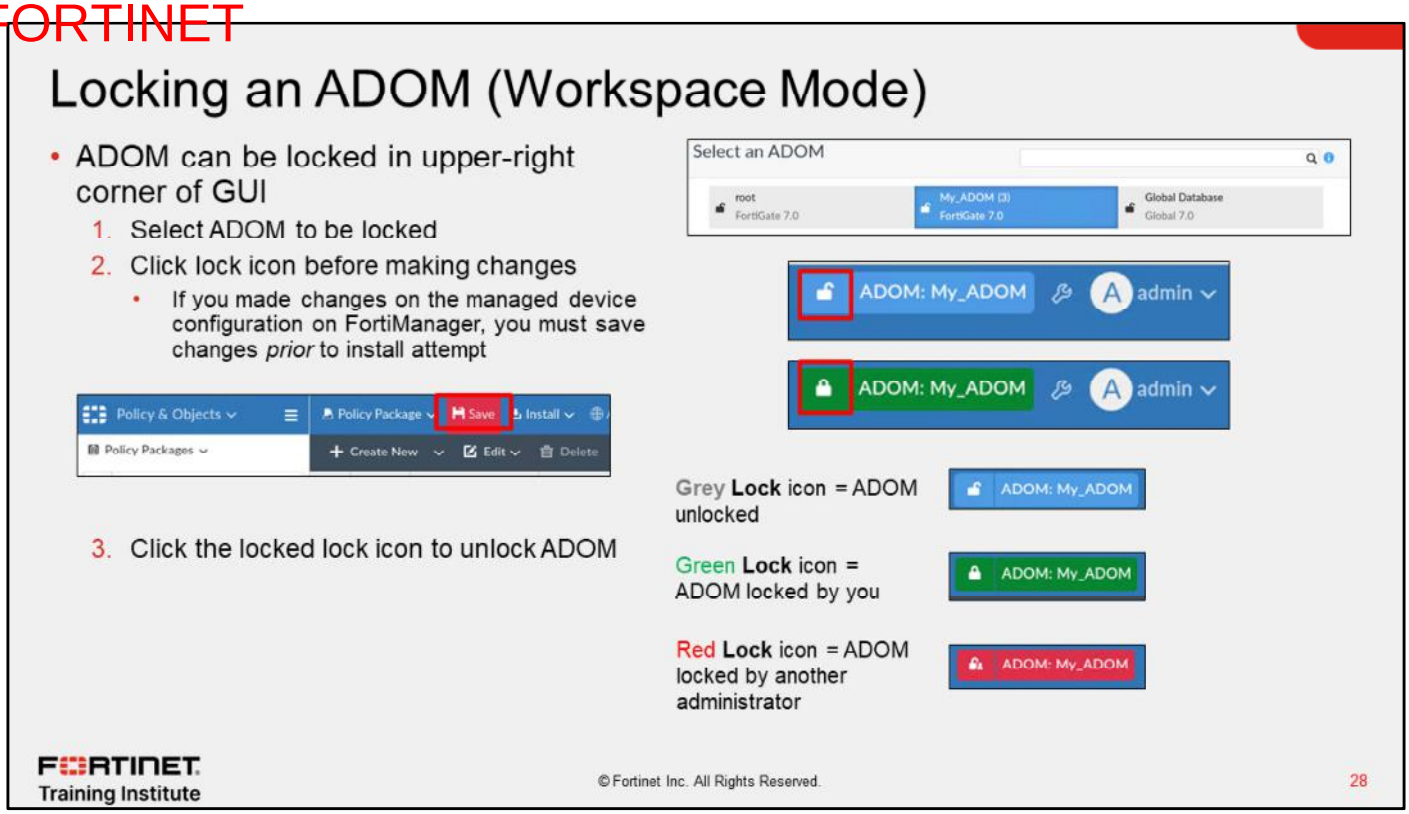


When workspace mode is enabled, how do you use it?

1. Prior to making changes, Admin A locks the ADOM. A green lock icon appears. Admin A now has read/write access and can make changes to the managed devices in that ADOM.
2. During this time, Admin B sees a red lock icon on the ADOM. Admin B has read-only access to that ADOM, and cannot make changes.
3. When Admin A finishes making changes, they save the changes and then unlock the ADOM. The icon changes to a grey unlocked icon. Admin B sees that the ADOM is now available for use.
4. Now, Admin B locks the ADOM, and again the lock icon changes to green. Admin B now has read-write access, and can safely make changes without risk of conflicts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When workspace is enabled, the ADOM is initially read-only. To enable read/write permission, and make changes to the ADOM, you *must* lock the ADOM, device, or policy package.

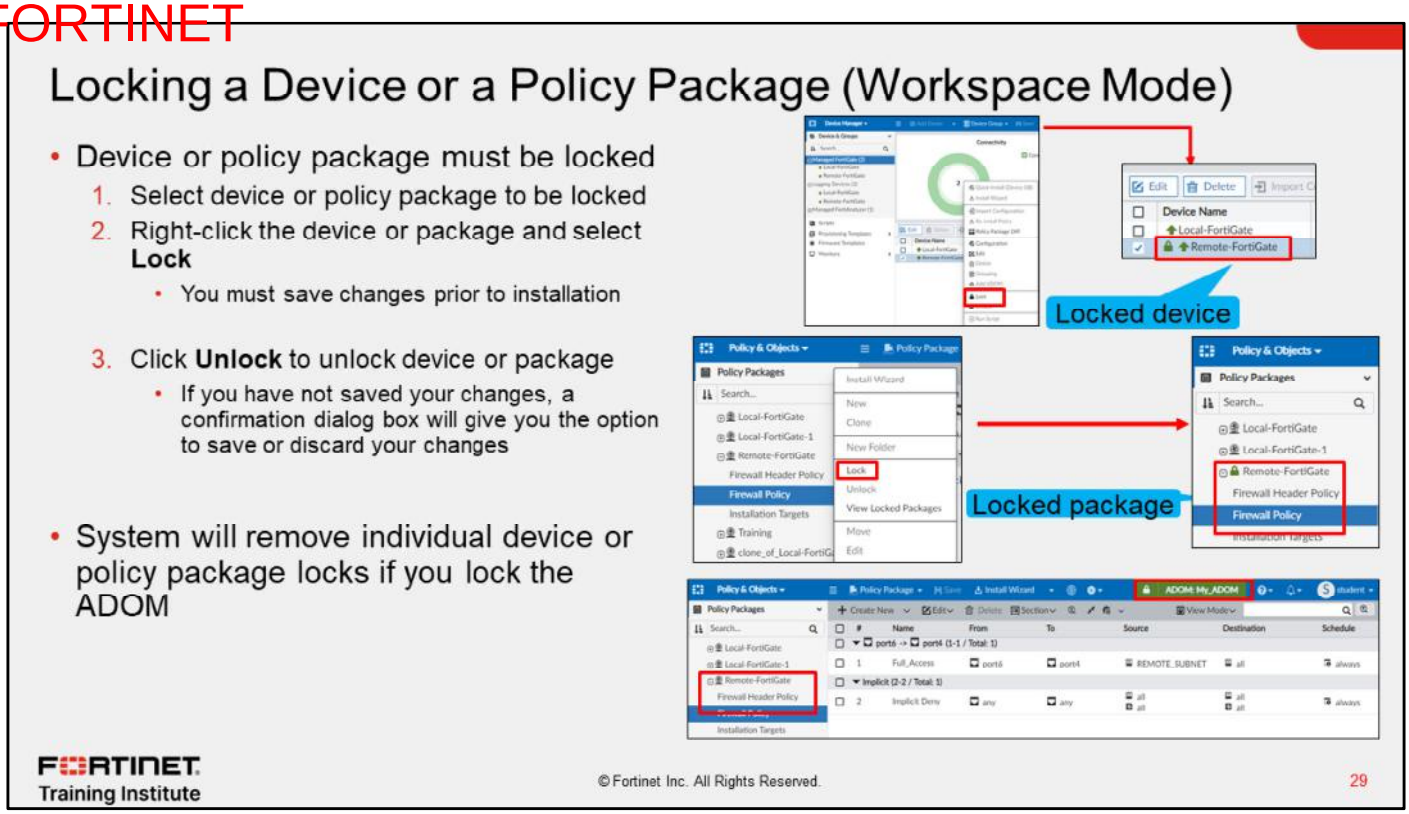
You can lock the ADOM in the upper-right corner of the GUI. After you lock the ADOM, you can safely make changes to the managed device settings, in that ADOM, without worrying about conflicts. If you make changes to the managed device configuration or policy packages, the changes *must* be saved prior to attempting to install them. Other administrators can't make changes to the ADOM because they have read-only permissions.

There are three lock status icons:

- Grey lock icon: The ADOM is currently unlocked. To make changes, you must first lock the ADOM.
- Green lock icon: The ADOM is locked by you. You can make changes in that ADOM.
- Red lock icon: The ADOM is locked by another administrator. You must wait for them to finish and unlock the ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In **Normal** workspace mode, you must lock a device or a policy package before you can make changes to it. Other administrators will be unable to make changes to that device or policy package until you unlock it, log out of FortiManager, or are forcibly disconnected when another administrator locks the ADOM that the device or package is in.

Locking an ADOM automatically removes locks on devices and policy packages that you have locked within that ADOM.

You cannot lock individual devices if ADOMs are in **Advanced** mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When should an administrator consider using workspace mode?
   - ✓A. When multiple administrators require concurrent access
   - B. When multiple managed FortiGate devices have a single administrator

2. Which statement about locking an ADOM is true?
   - ✓A. It automatically removes locks on devices and policy packages.
   - B. Other administrators have read/write access.

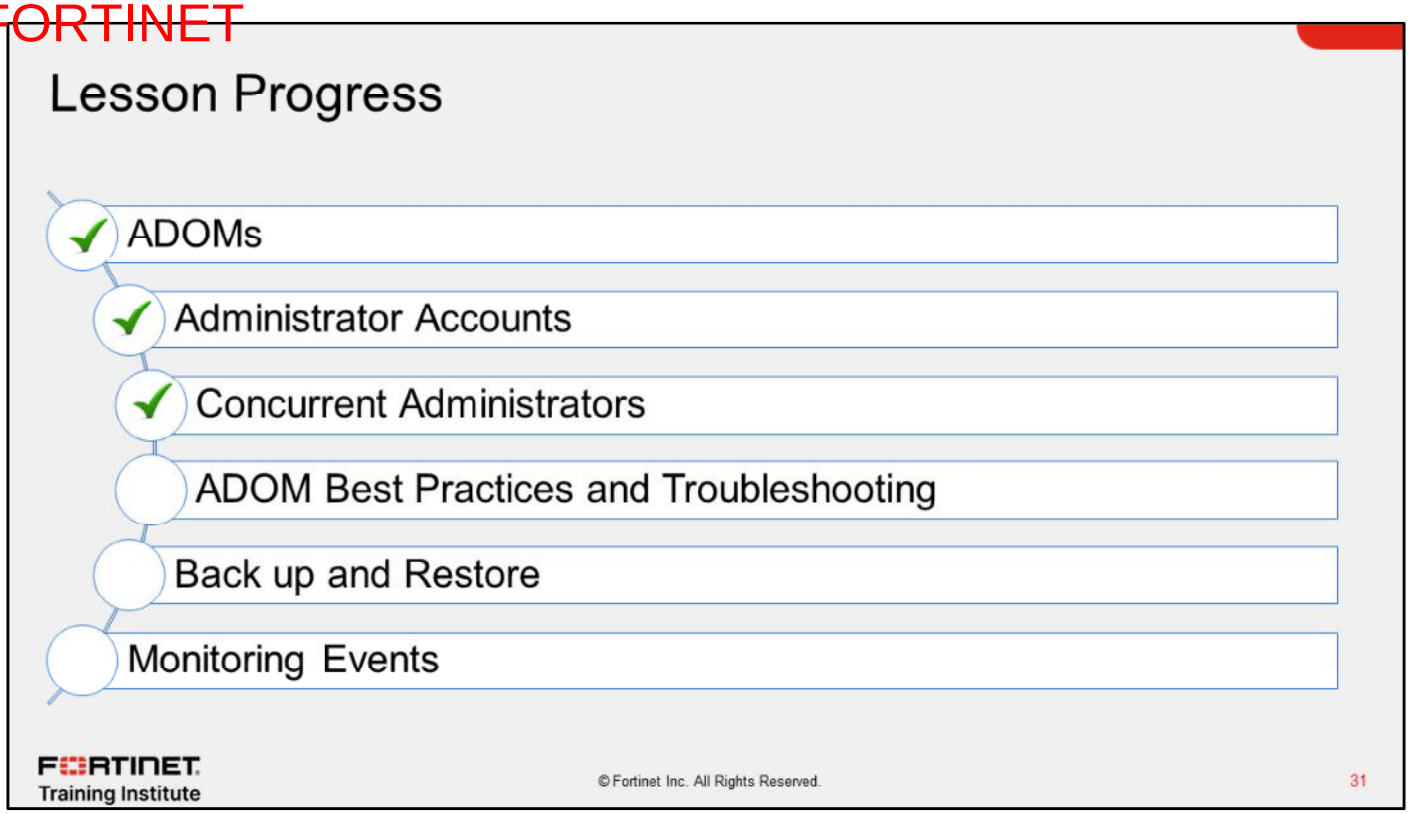
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

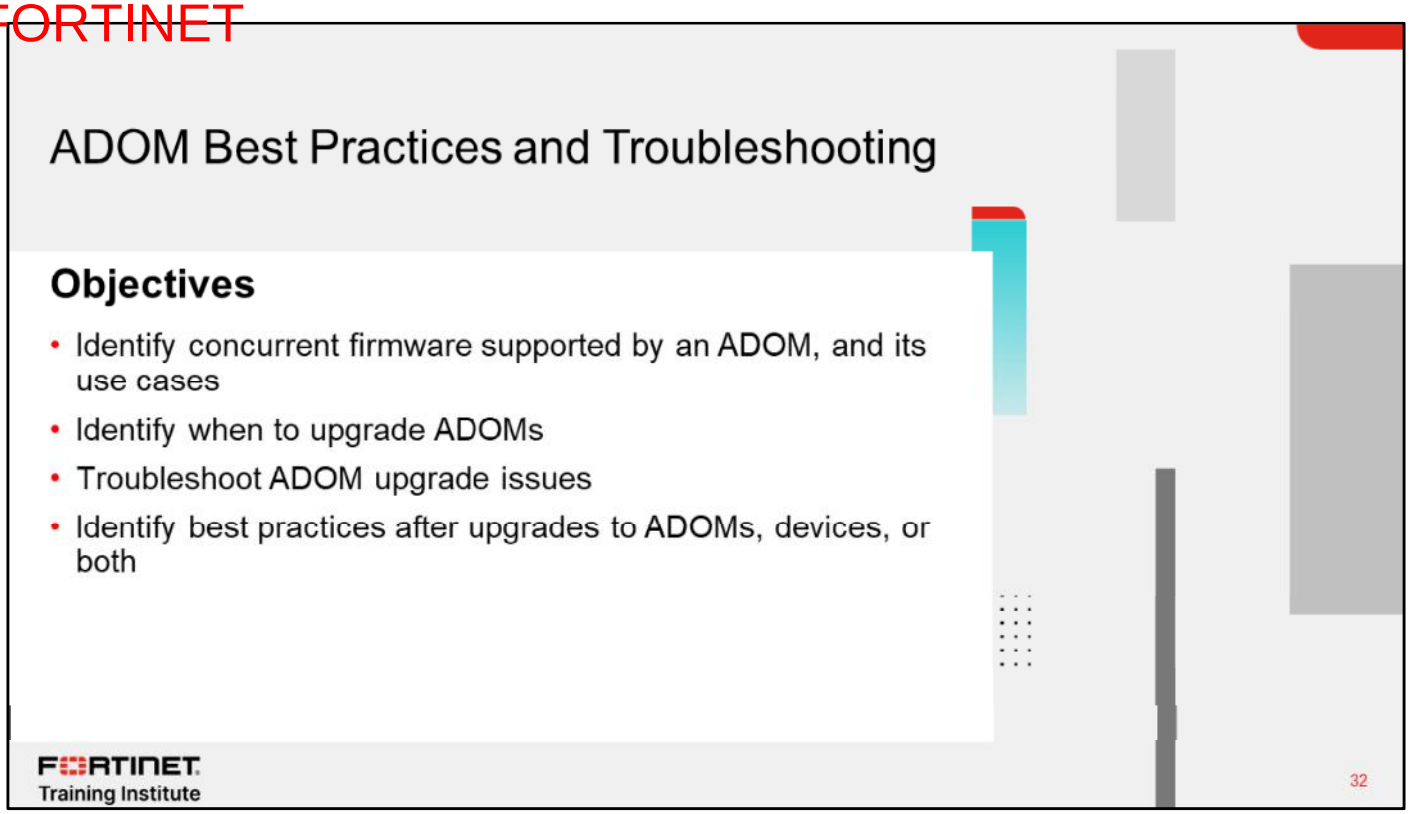


Good job! You now understand concurrent administrators.

Now, you will examine ADOM best practices and troubleshooting.

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 ADOM best practices and troubleshooting, you will be able to organize and manage your FortiGate device more effectively within FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Supported ADOM Versions

- Each ADOM is associated with a specific firmware version
  - The same ADOM can manage different firmware versions, if FortiGate devices run:
    - 7.0 and 7.2
    - But *not* 5.x with 7.2
  - Allows devices to share a common database
- FortiManager 7.2, supported ADOM versions are 6.4, 7.0, and 7.2

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

33

In the FortiManager database, each ADOM is associated with a specific FortiGate firmware version, based on the firmware version of the devices that are in that ADOM. The firmware version determines the appropriate database schema.

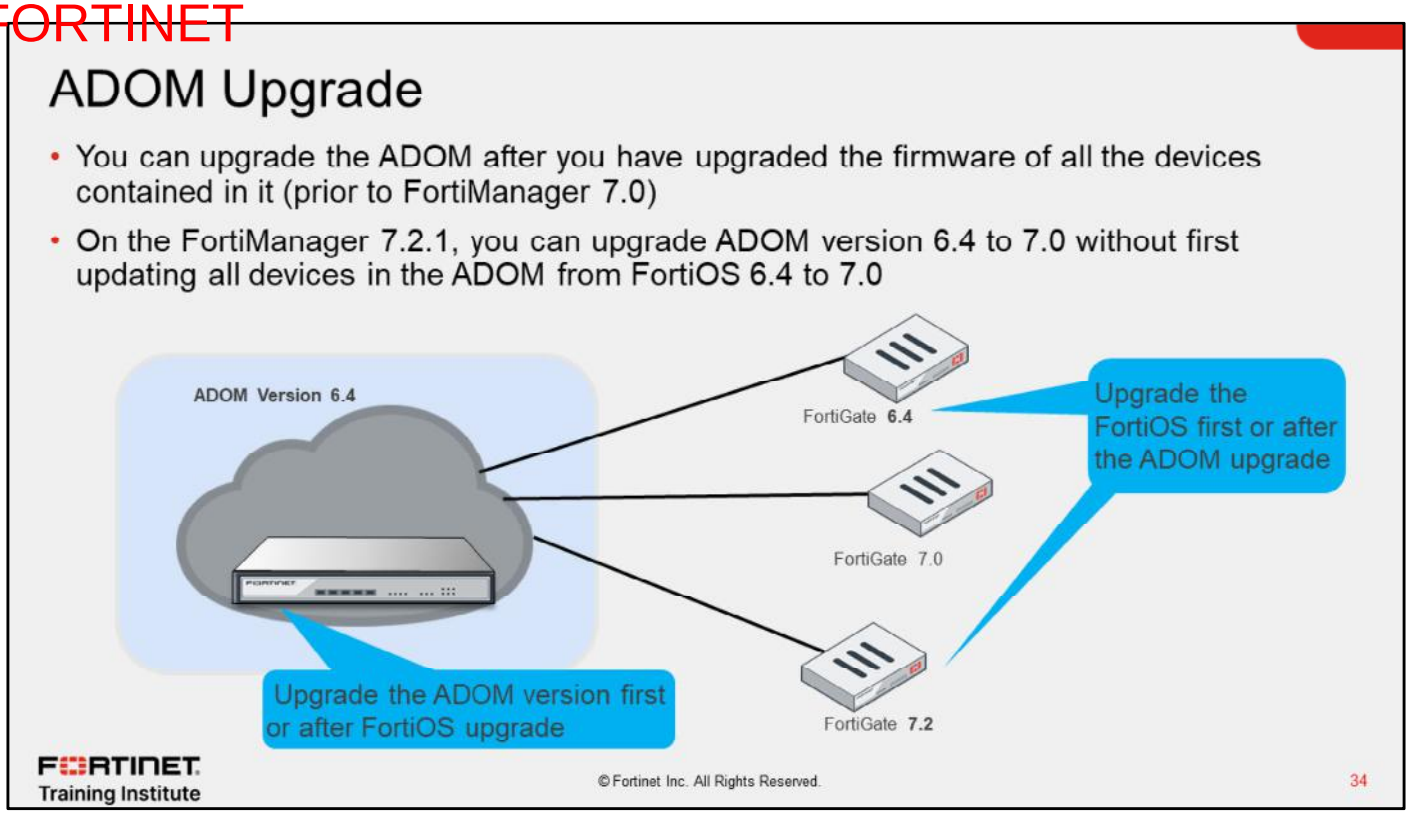
What if you created an ADOM using version 7.0, added FortiGate devices running FortiOS 7.0, but then needed to upgrade the FortiGate devices to FortiOS 7.2? An ADOM can concurrently manage FortiGate devices running two FortiGate firmware versions; for example, FortiOS 7.0 and 7.2. Therefore, the devices running firmware versions 7.0 and 7.2 can share a common FortiManager database.

Although multiple FortiOS versions can exist in the same ADOM, some of the features of the newer firmware version may be restricted if you are using an older ADOM version. This is because the CLI command syntax for the newer firmware version might have changed because of new features and is, therefore, configured differently. It is very important to make sure you add FortiGate to an ADOM that is based on its FortiOS firmware version. You should not add a higher version FortiGate to a lower version ADOM. Also, keep in mind that upgrading the FortiManager firmware version will not upgrade the ADOM version.

You should use this feature only to facilitate upgrading to new firmware. ADOMs are not usually run with mixed firmware. In that case, use separate ADOMs instead.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

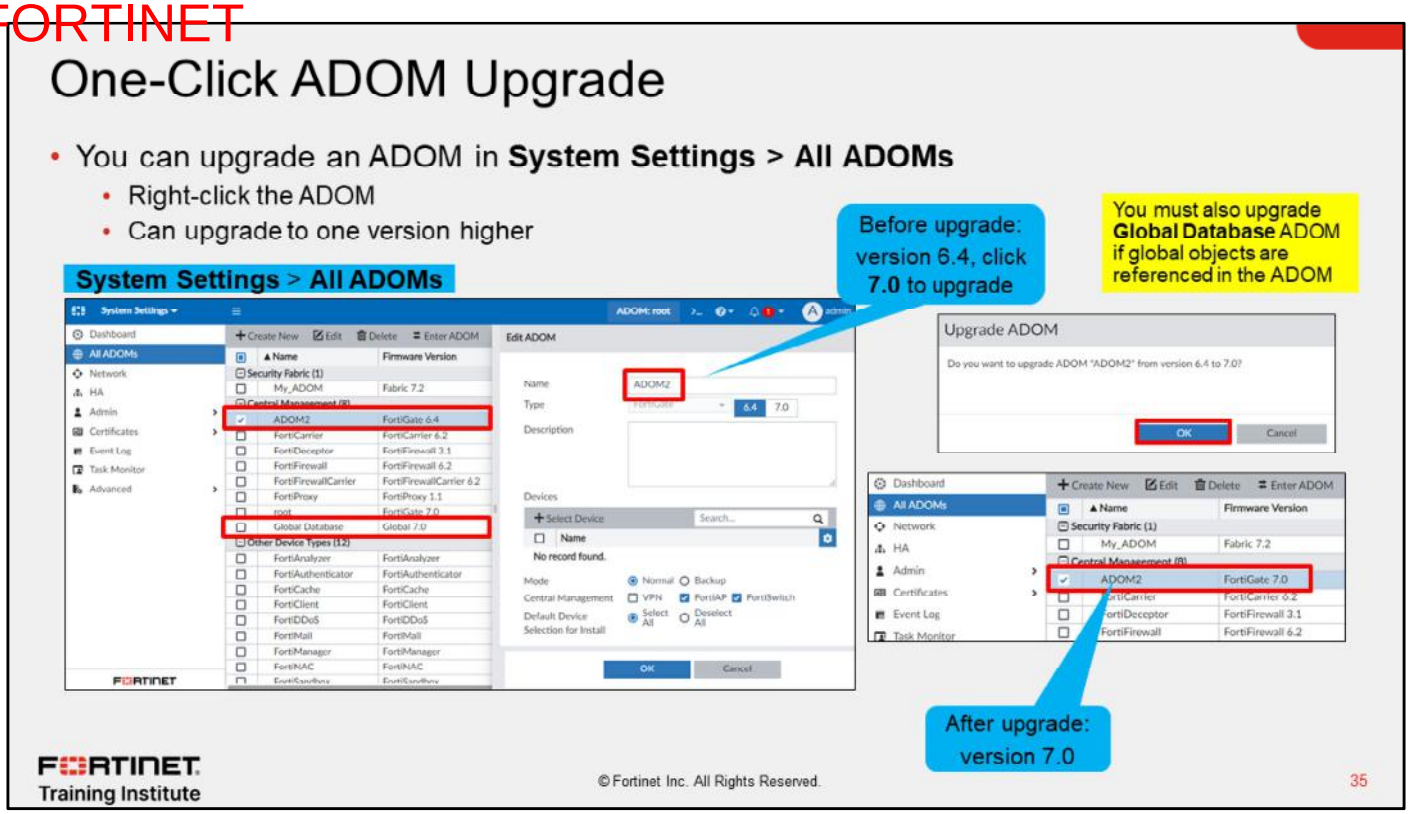


On the FortiManager 7.2.1, you can upgrade ADOM version 6.4 to 7.0 without first updating all devices in the ADOM from FortiOS 6.4 to 7.0. In the older version ADOM, upgrade ForiGate devices first and then the ADOM version.

Note: If there are many ADOM revisions, FortiManager requires more system resources and the ADOM upgrade can take more time to complete.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can upgrade the ADOM in **System Settings** > **All ADOMs**. You can upgrade an ADOM to one version higher by selecting the version. For example, you can upgrade an ADOM running 6.4 to 7.0 first, then to 7.2.

Note that if ADOM is using Global ADOM objects then you must also upgrade **Global Database** ADOM to same version, otherwise you will lose configuration. Upgrade process only updates the selected ADOM's database. For example, if FortiGate configuration is using SDN connector then you must upgrade global ADOM as connectors are global settings. You'll learn more about global ADOM later in the course.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

ADOM Upgrade Debugging

- ADOM upgrade debugging commands:

```
diagnose debug enable
diagnose debug service cdb 255
```

- The following event log entry is generated during the ADOM upgrade:

```
2022-08-18 18:25:07 log_id=0001010065 type=event subtype=system pri=information desc="Adom
upgrade successful" user="admin" userfrom="GUI(10.0.1.10)" msg="Upgrade adom (ADOM2) oid
(263) from version 6.4.0 to version 7.0.0 successfully" session_id=33077
upgrade_adom="ADOM2" upgrade_from="version 6.4.0" upgrade_to="version 7.0.0"
```

Task monitor entry for ADOM upgrade:

+ Group Error Devices | Delete | View Details | Show Status

☐	ID	Source	Description	User	Status	Time Used	ADOM
☐	26	Device Manager	dvmdb adom ADOM2 object member	A admin	Success: 1	2s	ADOM2
☐	25	Copy Global Object	Upgrade	A admin	Success: 1	7s	ADOM2

FORTINET Training Institute

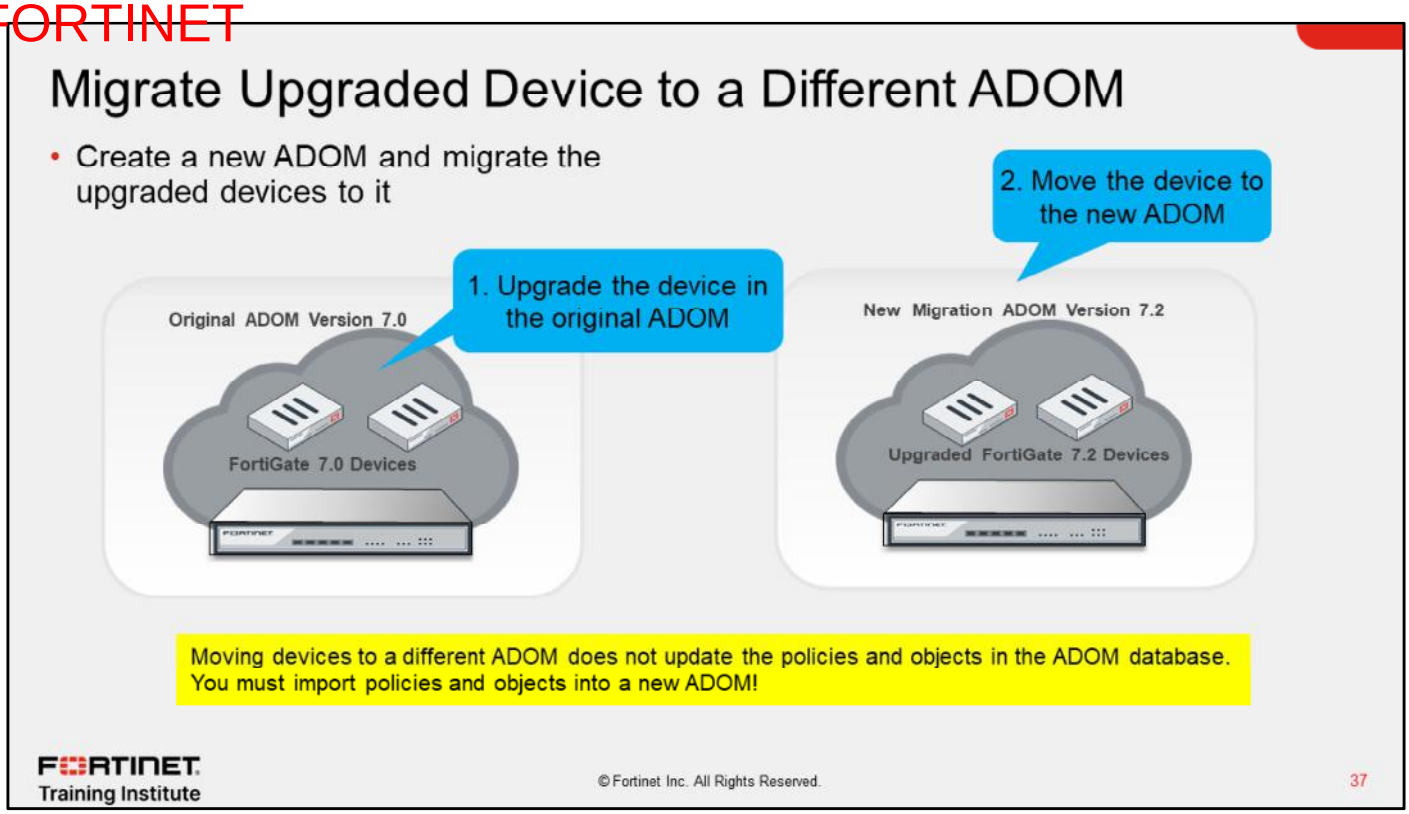
© Fortinet Inc. All Rights Reserved.

36

You can perform real-time ADOM upgrade debugging using the CLI commands shown on this slide. When you upgrade the ADOM, the system generates an event log stating that the ADOM upgrade was successful. The task monitor also generates an entry for the ADOM upgrade.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



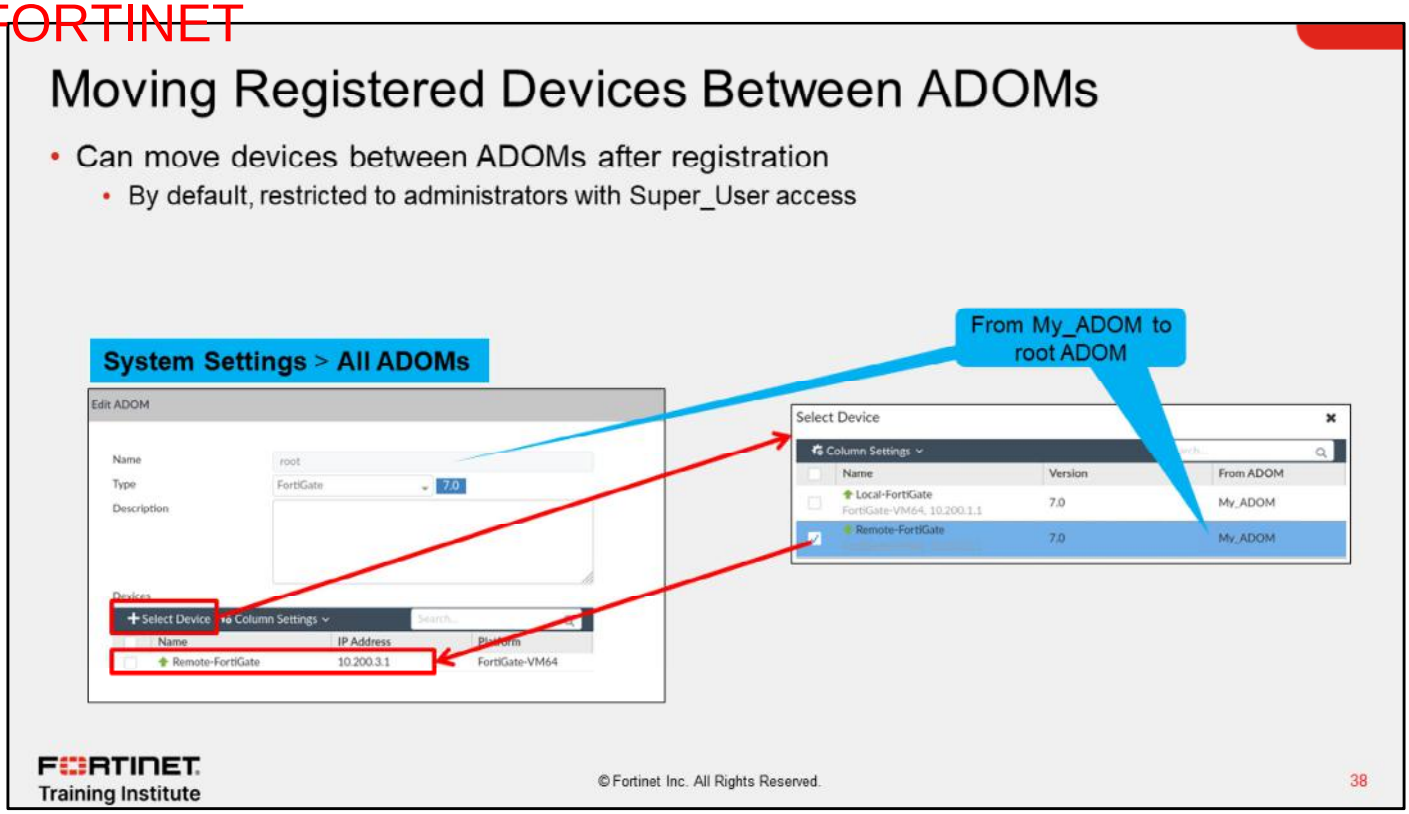
What if you need to upgrade a few FortiGate devices, but not all of them are contained in the same ADOM?

Another way to handle mixed FortiGate versions in the ADOMs is to first upgrade the devices in the original ADOM, then move them to a new ADOM that uses a matching firmware version.

If you move a device from one ADOM to another, policies and objects are *not* imported into the ADOM database. You must run the **Import Policy** wizard to import policies and objects into the ADOM database. Moving devices from one ADOM to another is not a recommended practice. For example, if you have configured complex IPsec VPNs with VPN Manager, you will need to reconfigure the VPN settings after you move the IPsec VPNs from one ADOM to another.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can move devices between ADOMs after registering on the **All ADOMs** page. You can move devices between ADOMs by editing the custom ADOM to which you want to add the device, and then selecting the device to add to it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

ADOM Best Practices—Before and After Upgrades

Before upgrades

- Install any pending device settings or policy package changes
- After installation, make sure policy packages and device configurations are all synchronized

After upgrades—devices and ADOMs

- Check installation preview to identify any changes caused by the upgrade
- Check if the to-be-installed changes are acceptable

Device migrated to different ADOM

- Shared policy package and objects will not move to the new ADOM
- Can perform import policy

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

39

Before an ADOM upgrade, you should install any pending device settings or policy package changes to the managed devices and get all devices and policy packages synchronized.

Once you have upgraded the devices and the ADOM, you should perform the installation preview. The **Install preview** shows you any changes that occurred during the upgrade process. You will need to check that all the to-be-installed changes occurred during the upgrade process, and make corrections if required.

When you move devices from one ADOM to another ADOM, shared policy packages and objects do not move to the new ADOM. You will need to import policy packages from managed devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which step should you take as a best practice after a FortiGate firmware upgrade?
   A. Push the policy package and run a script to update the objects.
   ✓B. Upgrade the ADOM and retrieve the configuration.

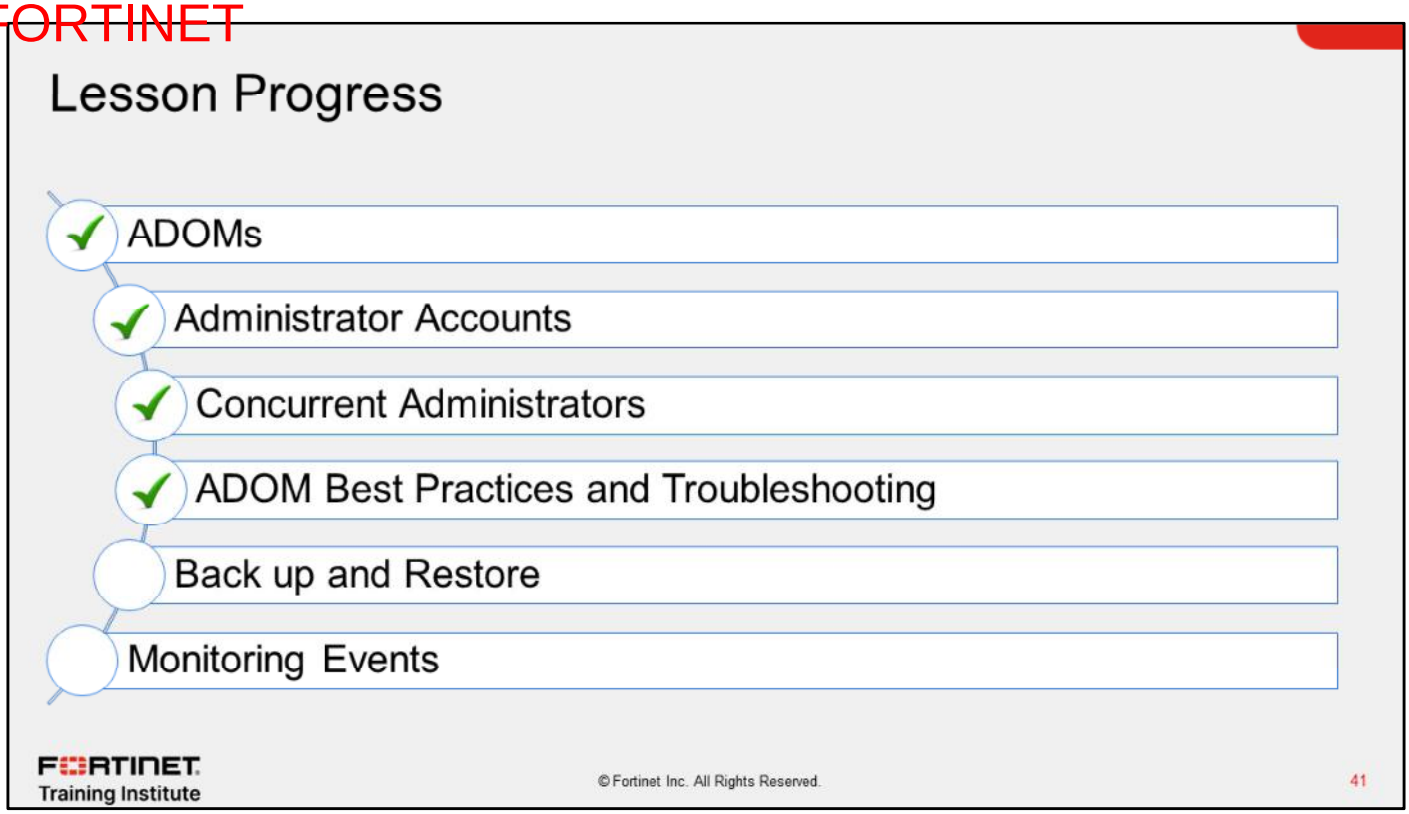
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

40

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

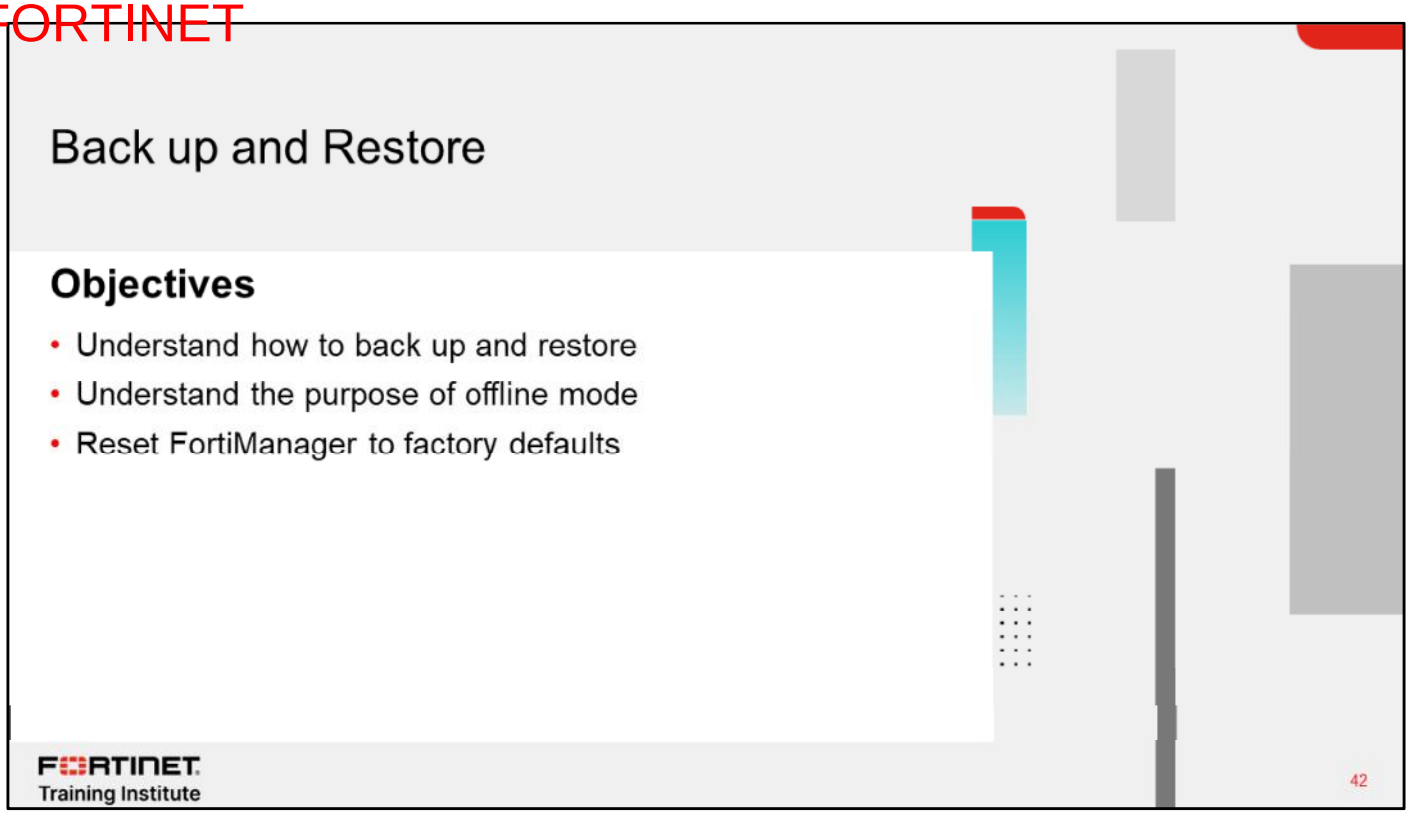


Good job! You now understand ADOM best practices and troubleshooting.

Now, you will examine backup and restore on FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

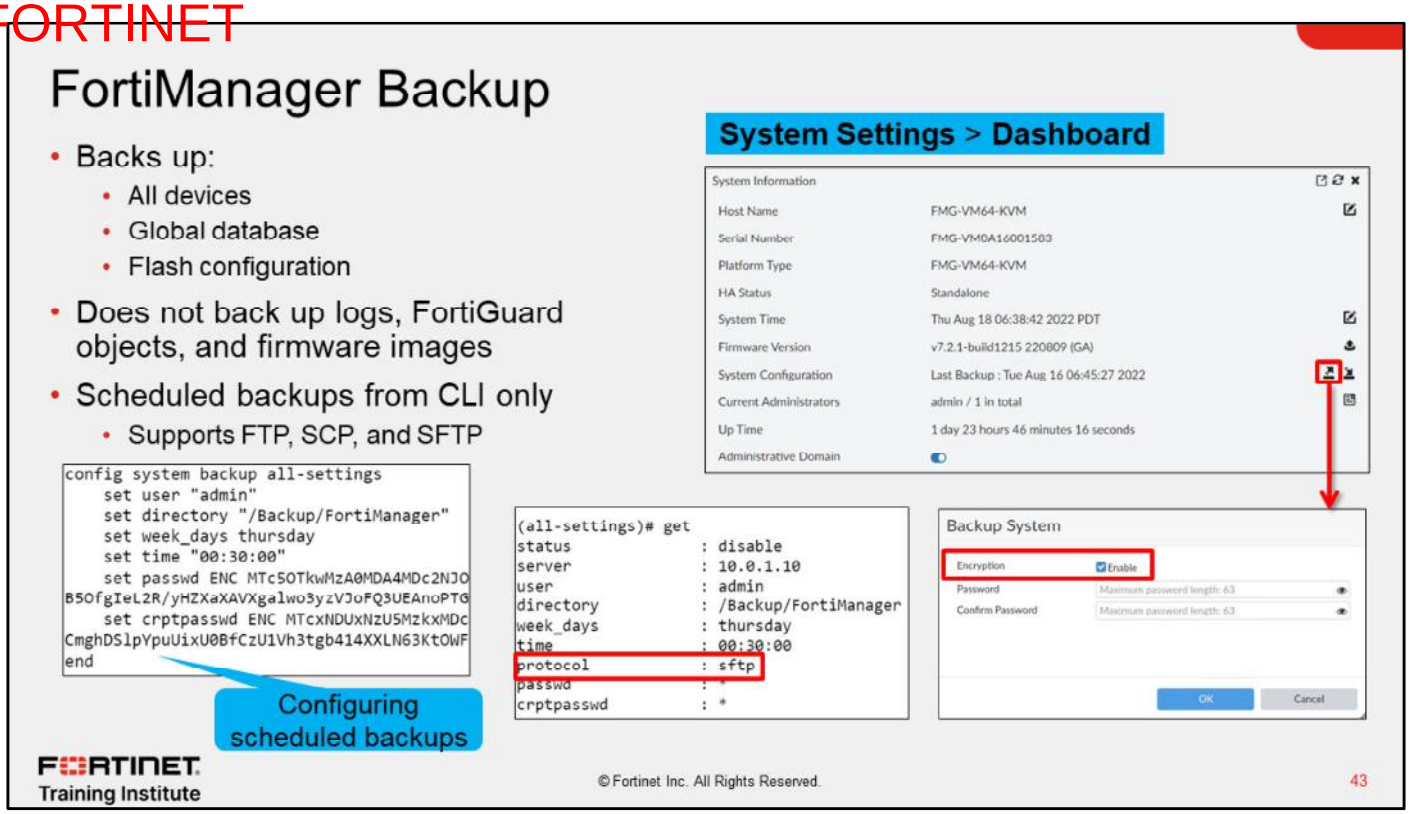


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in backup and restore, you will be able to ensure that if there is a severe hardware failure, you can quickly restore FortiManager to its original state without affecting the network. This is, after all, your central network management system, and you will probably be investing considerable time and resources in building and maintaining your firewall policies. So, you will learn how to keep the data safe.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



At any time, you can back up the FortiManager configuration in the **System Information** widget on the GUI. By default, encryption is enabled when you use the GUI for backups. If you use encryption, you must set a password that is used to encrypt the backup file. The backup file can't be restored unless you provide the same password. Fortinet Technical Support usually requests the FortiManager backup in unencrypted format.

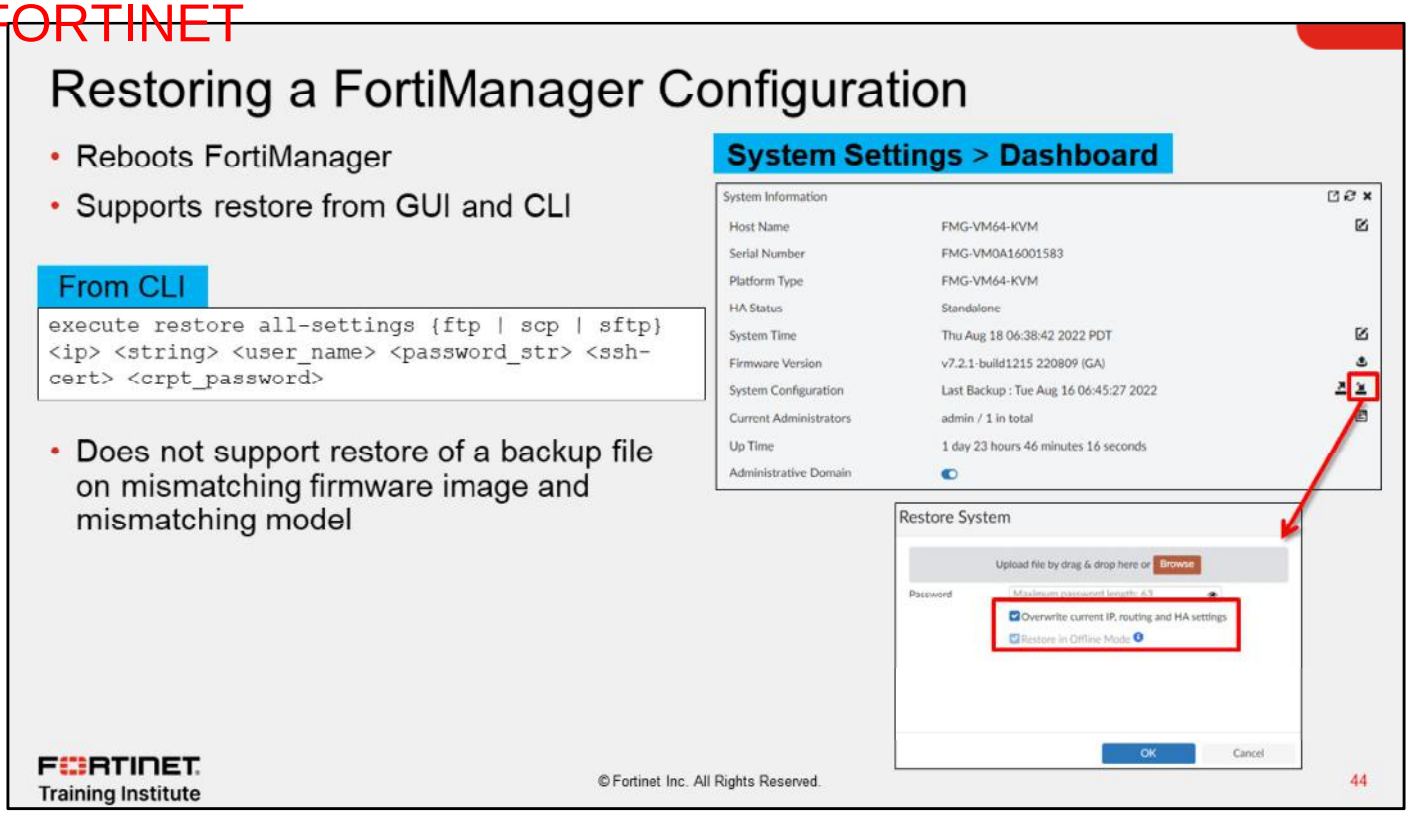
The backup contains everything except the logs, FortiGuard cache, and firmware images saved on FortiManager.

You can also use the CLI to schedule backups at regular intervals.

If changes are made to FortiManager that end up negatively affecting your network, you can restore the configuration from any of the backups you performed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can restore the FortiManager configuration using the GUI or CLI. When you perform a restore, FortiManager reboots and the changes take effect. When you are restoring a backup file, make sure the FortiManager's firmware version and model matches the backup file.

There are a few other options in the **Restore System** pop-up that are worth learning about:

- **Overwrite current IP, routing, and HA settings**: by default, this option is enabled. If FortiManager has an existing configuration, restoring a backup will overwrite everything, including the current IP address, routing, and HA settings. If you disable this option, FortiManager will still restore the configurations related to device information and global database information, but will preserve the basic HA and network settings.
- **Restore in Offline Mode**: by default, this is enabled and grayed out—you cannot disable it. While restoring, FortiManager temporarily disables the communication channel between FortiManager and all managed devices. This is a safety measure in case any devices are being managed by another FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Migrating a FortiManager Configuration

Can migrate a configuration from one FortiManager model to another FortiManager model

1. Back up the FortiManager configuration on the first FortiManager
2. On the CLI of the second FortiManager, run the following commands:

```
exec migrate all-settings < ftp | scp | sftp > <server> <filepath> <user> <password>
[cryptpasswd]
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

45

You can back up the configuration on one FortiManager model and restore this configuration on a different FortiManager model. This can be useful for:

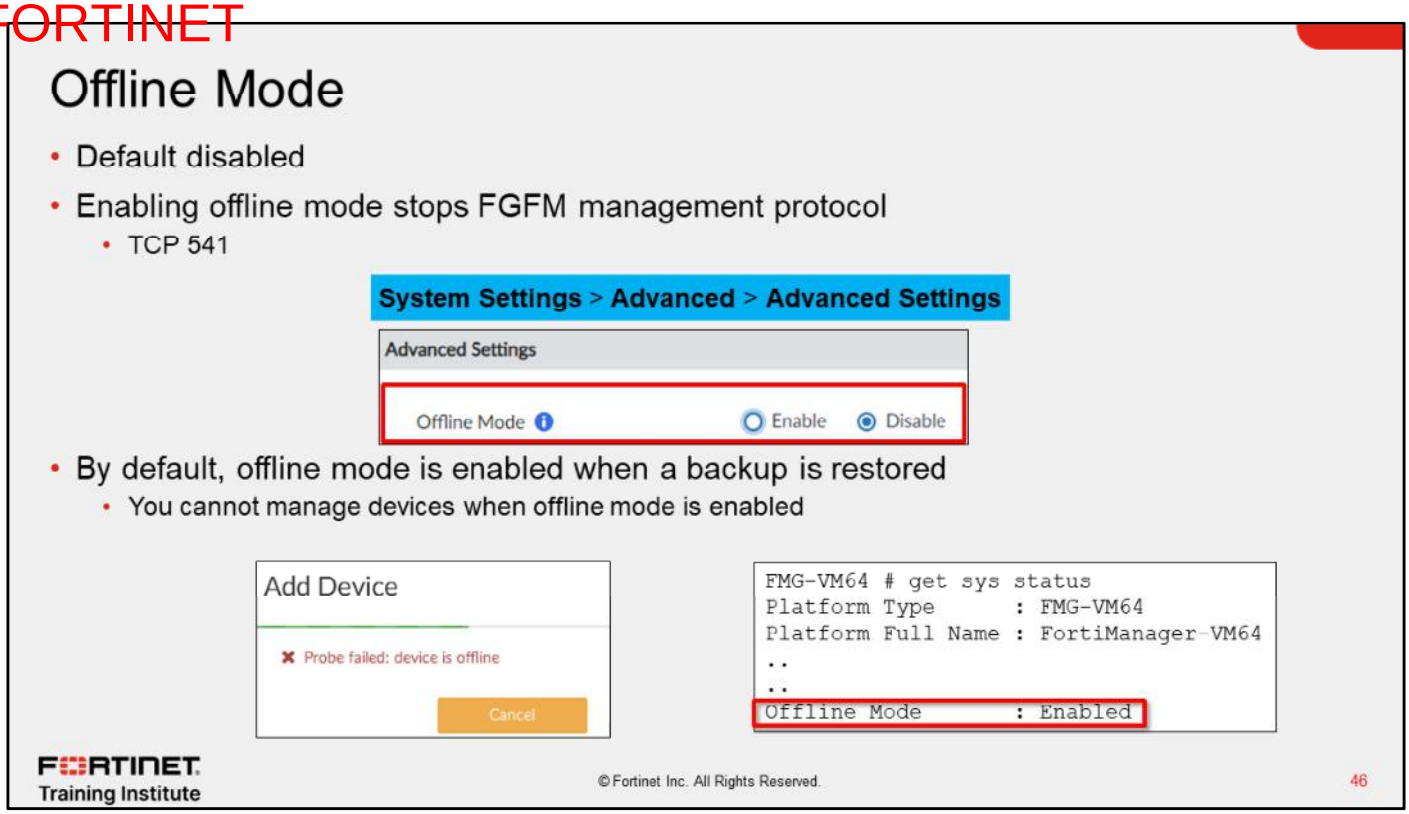
- Troubleshooting purposes, by restoring the configuration to a different FortiManager model.
- Upgrading FortiManager to a bigger model, because it will preserve your already-configured devices and task manager database. System settings are not preserved.

The steps required to migrate a configuration are simple. You need to back up the configuration on one FortiManager model, and then run the CLI migrate command on the second FortiManager.

FortiManager supports FTP, SCP, and SFTP protocols to migrate a configuration from one FortiManager model to another FortiManager model.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



By default, offline mode is disabled, allowing FortiManager to manage the devices. When you perform a configuration restore, FortiManager disables the FGFM protocol. This protocol uses TCP port 541 for communication between FortiManager and FortiGate devices. You can manually enable or disable in **System Settings** > **Advanced** > **Advanced Settings**.

When should you enable offline mode? You can enable offline mode to troubleshoot problems. Offline mode allows you to change FortiManager device settings without affecting managed devices, or to load a backup on a second FortiManager for testing. That way, the second FortiManager cannot automatically connect to your FortiGate devices and start managing them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

How to Reset Settings

- Back up, then reset using the local console

```
execute reset all-settings
execute reset all-except-ip
```

  - Reset all configuration except interface and routing configuration

```
execute format {disk | disk-ext3 | disk-ext4} <RAID-level> deep-erase <erase-times>
```

- Reset all settings will
  - Reset FortiManager to factory default settings
  - Erase the configuration on flash, including IP address and routes
  - Disconnect all the sessions and reboot FortiManager
- Format command will
  - Delete all databases and logs, and repartitions hard disk

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

47

If you need to factory reset FortiManager, connect using the console port.

The `reset all-settings` command returns FortiManager to its factory default settings and reboots FortiManager.

The format disk command erases all device settings and images, FortiGuard databases, and log data on the FortiManager hard drive.

To completely erase all configuration databases, reset all settings, then format the disk using the CLI.

Even if you format your disks, this only destroys the file system tables. Files remain, and attackers could use forensic tools to recover the data. Failure to overwrite your configuration databases jeopardizes the security of your entire network. So, if you will be replacing or selling your FortiManager, or replacing the hard disk, you should use a secure (deep-erase) disk reformat, to overwrite the hard disk with random data. Usually, the deep-erase feature takes longer to complete and is not necessary in most cases.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is included in the FortiManager backup?
   A. Logs and firmware images
   ✓B. Global database and all devices

2. Which statement about scheduled backups of FortiManager is true?
   ✓A. It supports FTP, SCP, and SFTP.
   B. It can be configured using the CLI and GUI.

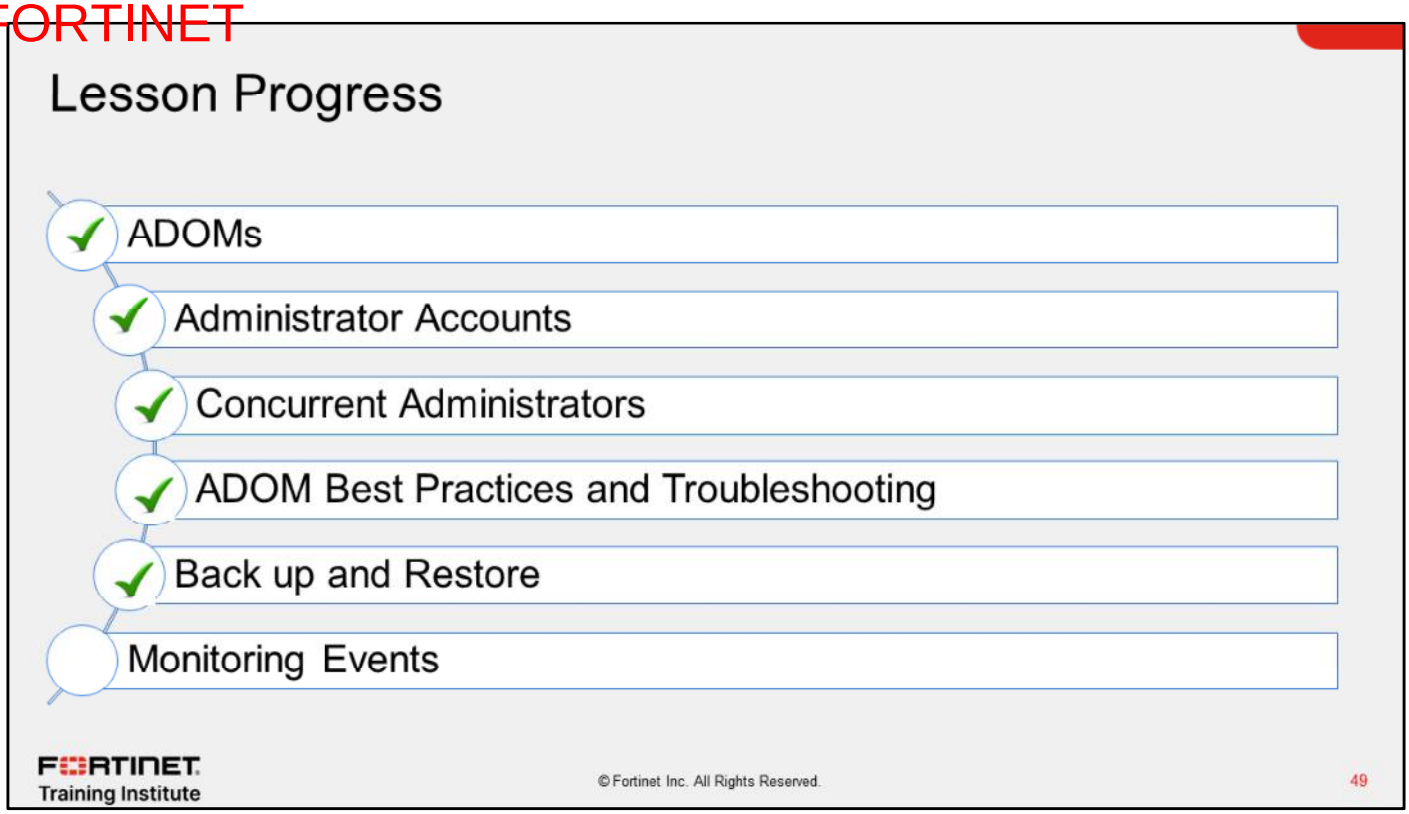
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

48

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

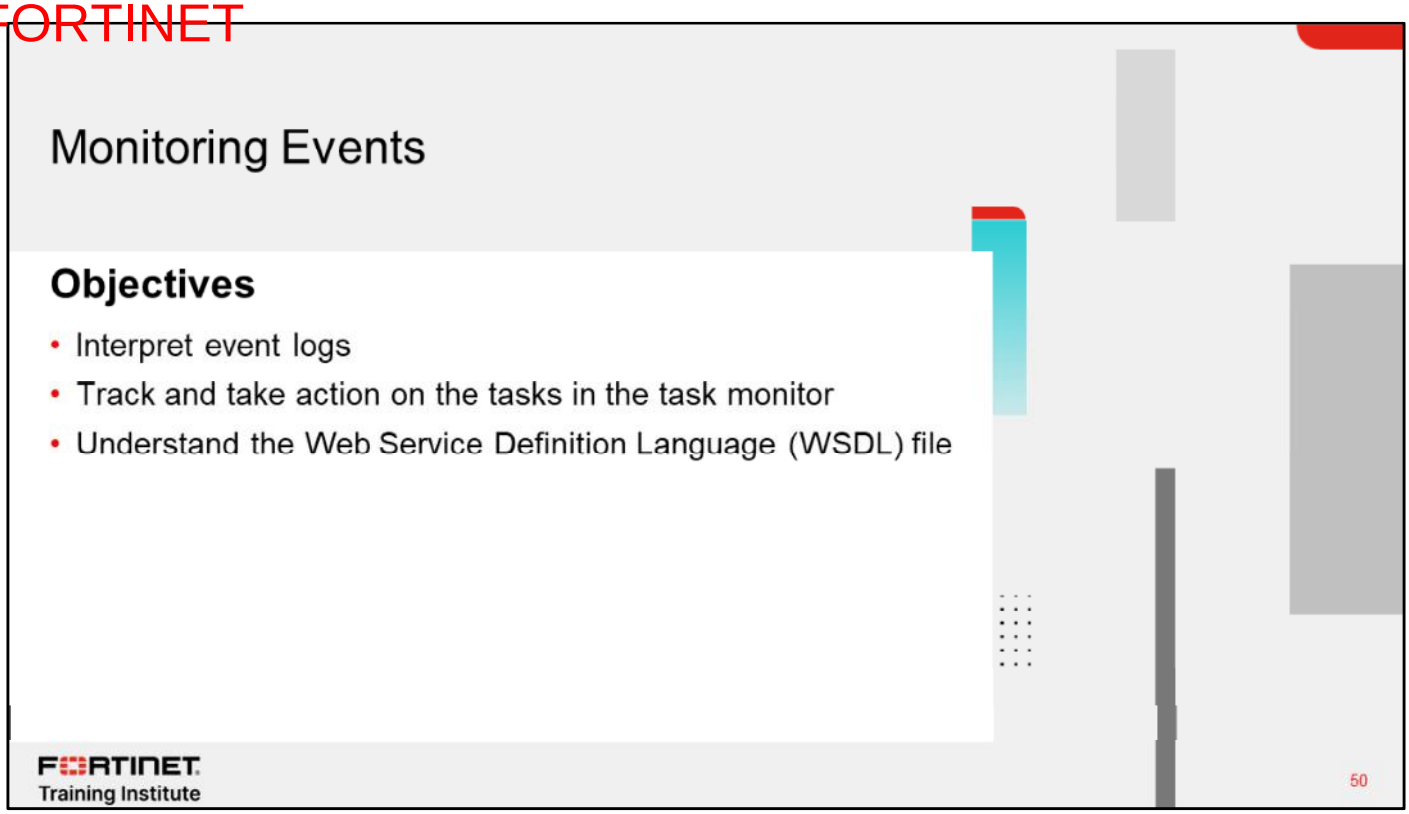


Good job! You now understand backup and restore.

Now, you will examine monitoring events.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

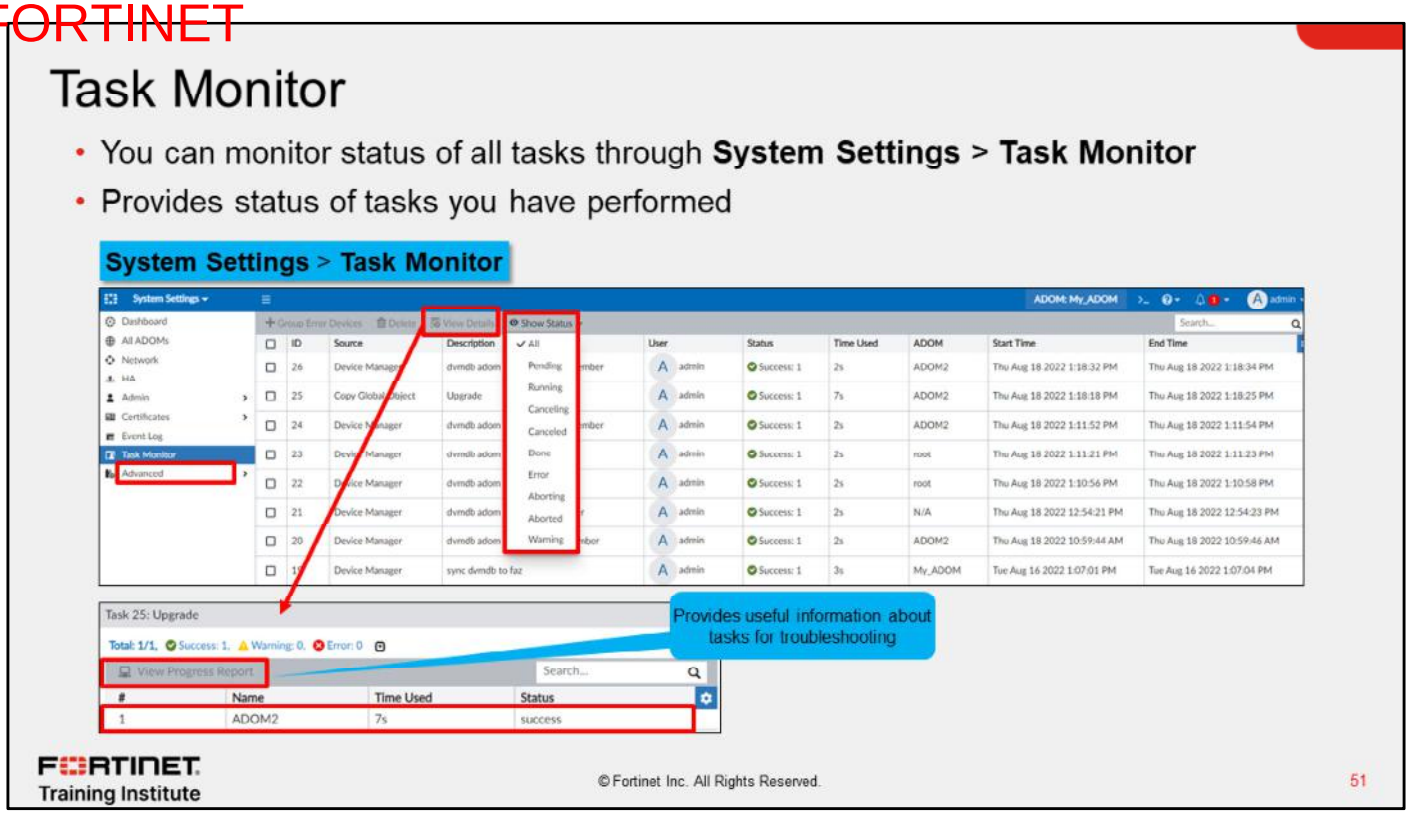


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in monitoring FortiManager events, you will be able to diagnose and troubleshoot issues related to FortiManager and managed devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To monitor the status of all tasks, such as imports and device upgrade status, click **System Settings** > **Task Monitor**. You can filter a task category in the **Show Status** drop-down list, or leave the default **All**.

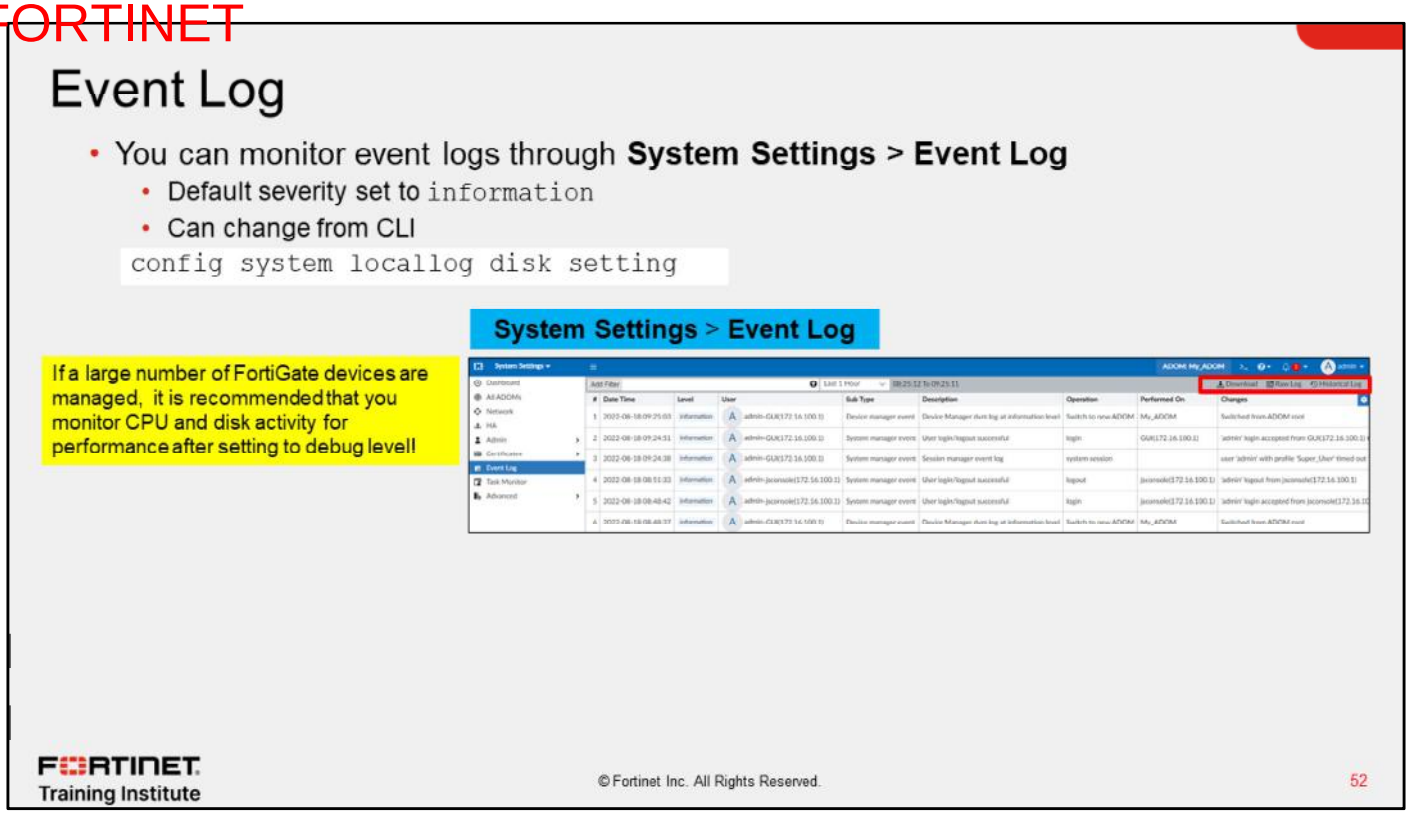
For example, you can filter by running, pending, canceling, or aborting tasks, and can identify if the tasks have been in that stuck state for long time. You can cancel or delete the tasks that are stuck for a long time and have stopped progressing, because they might prevent other pending tasks from being processed.

The system stores tasks in a separate task database. Under special circumstances, it is possible to reset this database (thus clearing all task entries). The system includes these tasks in the configuration backup and are visible when you perform a configuration restore.

The **View Progress Report** on the task details page is very useful to troubleshoot FortiManager task issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Logs provide important troubleshooting information about events that happen on FortiManager.

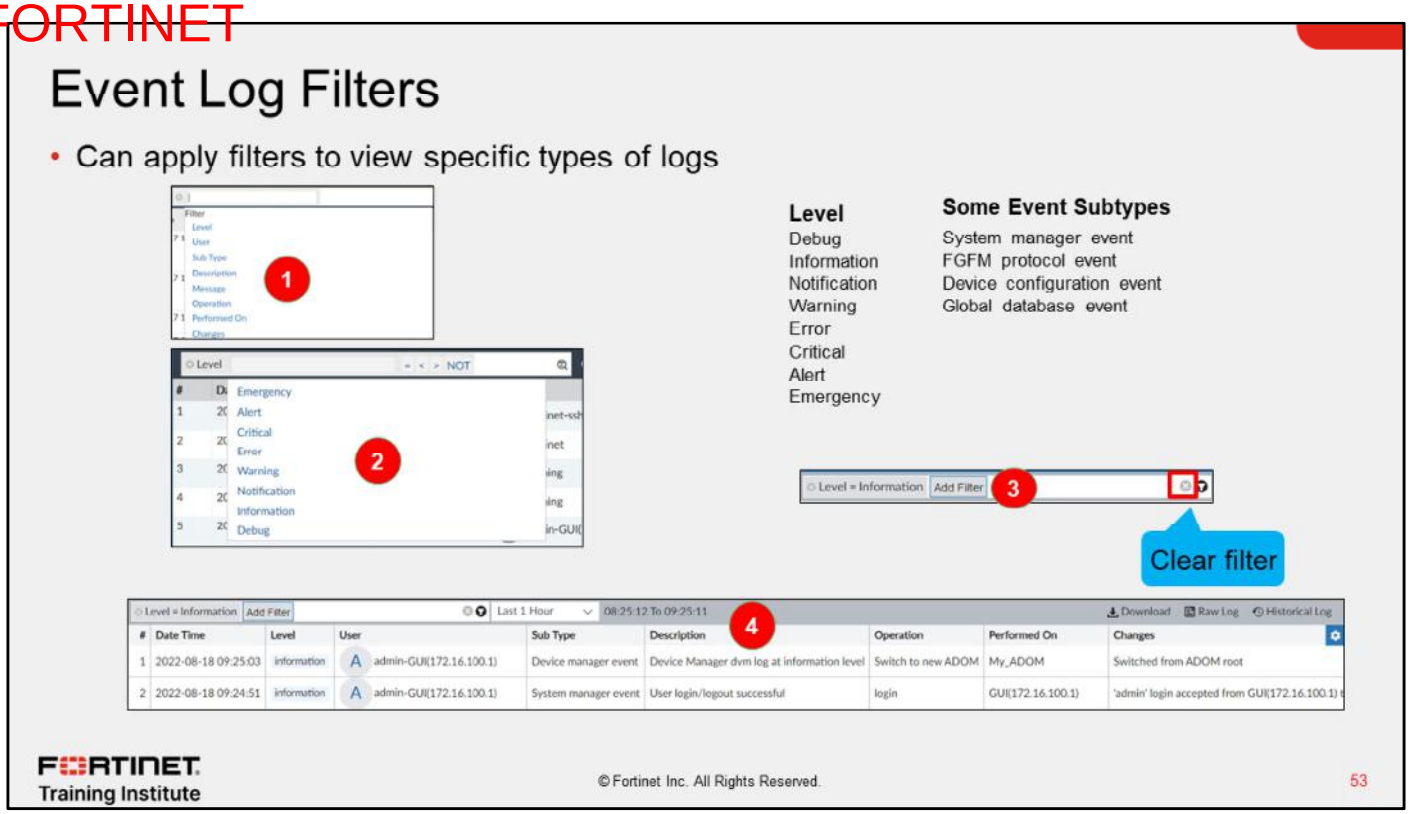
You can view logs, download, view logs in raw format, or view historical logs by clicking **System Settings** > **Event Log**.

By default, event log severity is set to the `information` level. You can change the level (increase or decrease) using the CLI. Information-level log severity provides enough details about the log messages to investigate an issue. If you need to work with Fortinet Technical Support, you can increase the log severity to debug level to get more details on the event logs.

Depending upon the number and type of FortiGate devices managed and amount of daily activity, you should monitor disk (input and output wait states) and CPU activity after increasing it to debug level, to ensure that there are no significant increases in CPU or disk usage.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



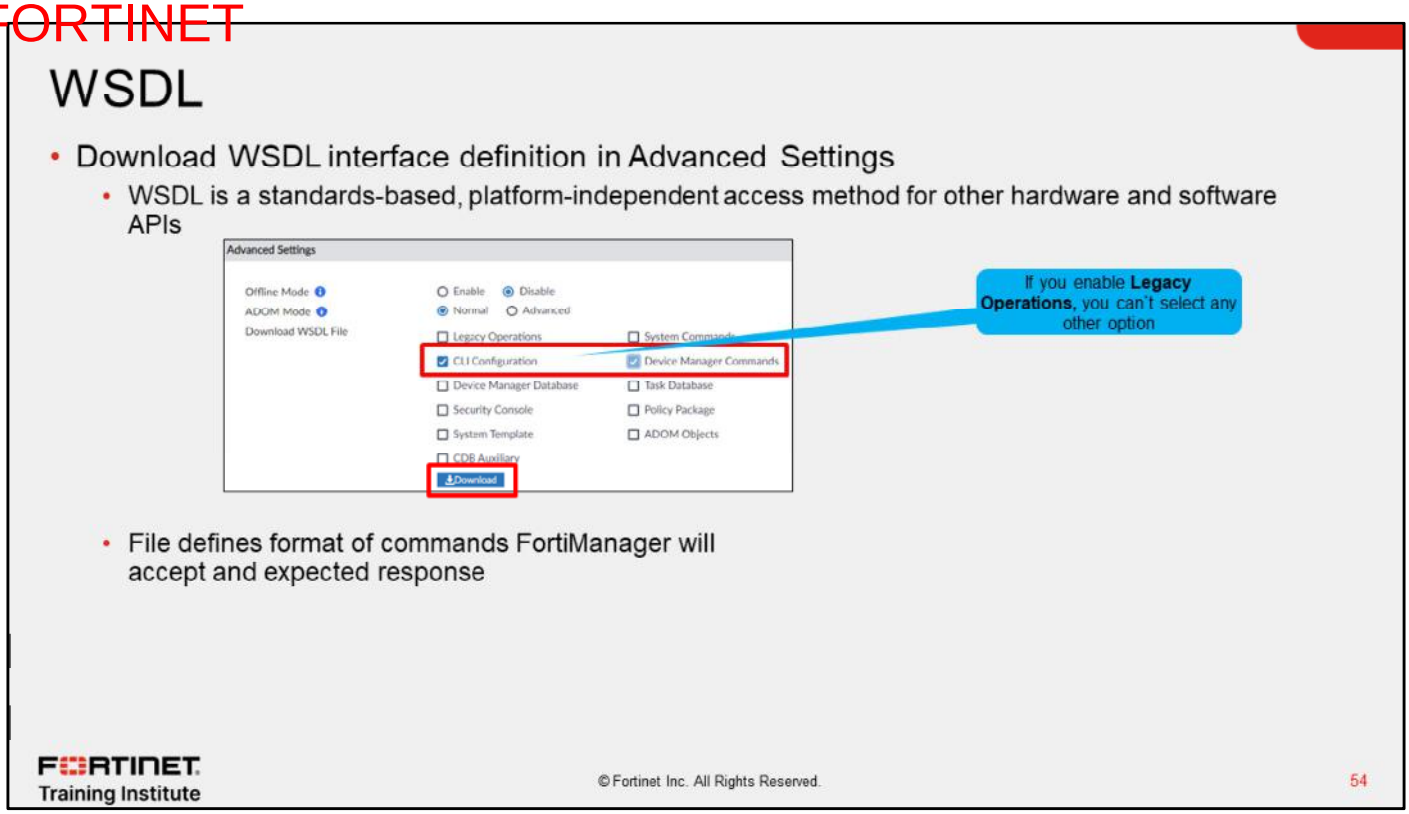
If you need to focus on specific types of log messages, use filters. For example, you can filter by level, administrator, subtype, and messages. To apply a filter, click **Add Filter**, then select which parameter you would like to refine.

Next, pick a level and, if required, select an event subtype. NOT and OR operators are also available in the dynamic list. You can click **Add Filter** to add and combine additional filters.

Event logging for FortiManager has several subtypes. For additional details, refer to the *FortiManager Log Message Reference Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



If you want to use APIs to monitor your system, or to set or get data using third-party devices, you can use the JSON API. The FortiManager APIs are a very powerful tools that offer administrative web portals to customers, automated deployment, and provisioning systems.

If you want to use web services to monitor your system, you can download the WSDL interface definition from FortiManager in **Advanced Settings**.

Web services is a standards-based, platform-independent access method. The file itself defines the format of commands FortiManager will accept, as well as the response to expect.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. When should an administrator use event logs at the debug level?
   - ✓ A. When investigating a FortiManager issue with technical support
   - B. When searching for an administrator login event

2. What is the main purpose of using APIs on FortiManager?
   - ✓ A. To manage FortiManager device using third-party hardware and software
   - B. To manage many devices without a FortiManager license

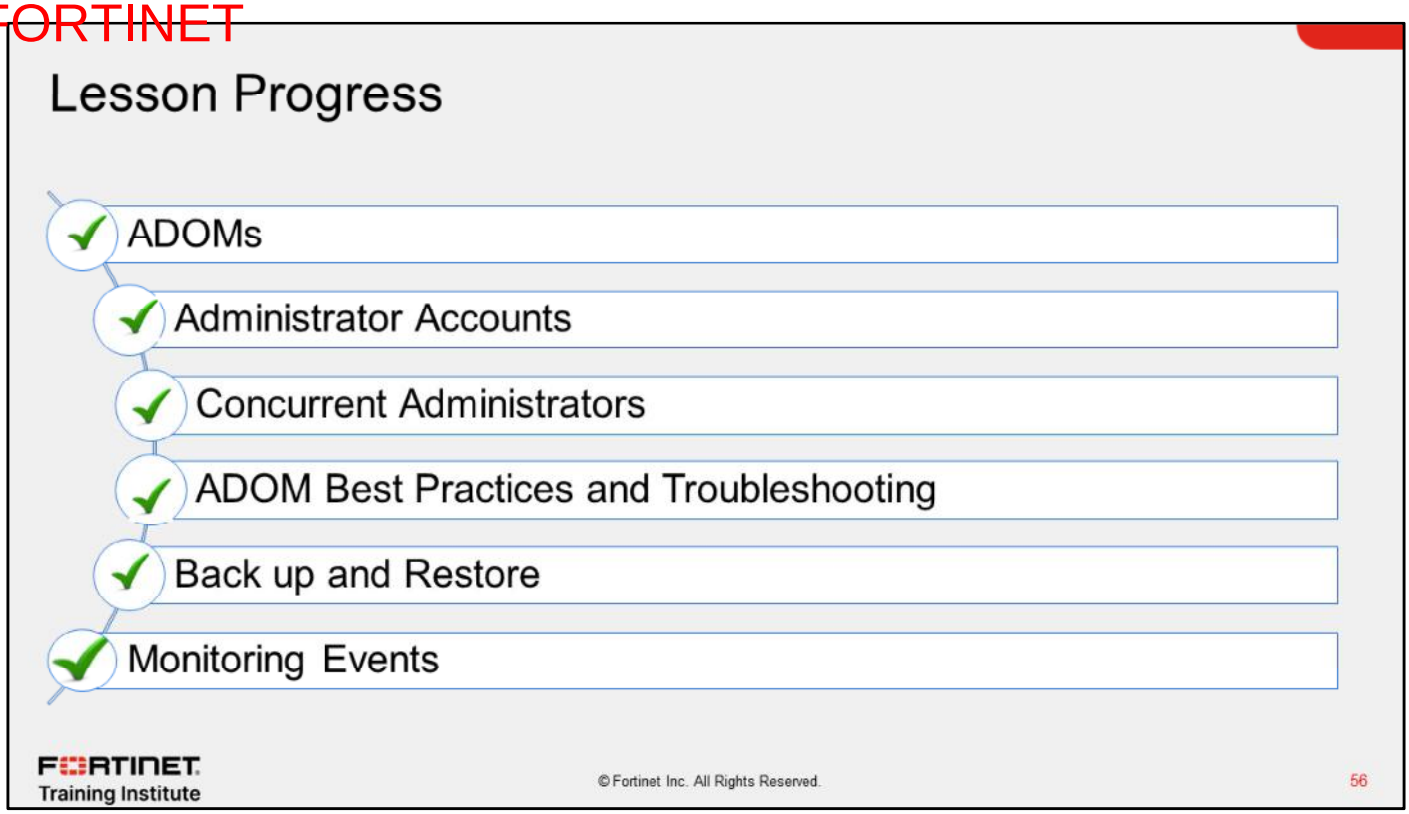
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

55

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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

Review

- ✓ Identify the purpose of ADOMs
- ✓ Describe ADOM modes
- ✓ Configure ADOMs
- ✓ Create administrator accounts and permissions
- ✓ Understand concurrent access
- ✓ Know when and how to use the workspace
- ✓ When to upgrade an ADOM and how to troubleshoot
- ✓ Back up and restore the configuration
- ✓ Use offline mode for testing
- ✓ Read event logs
- ✓ Monitor tasks

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

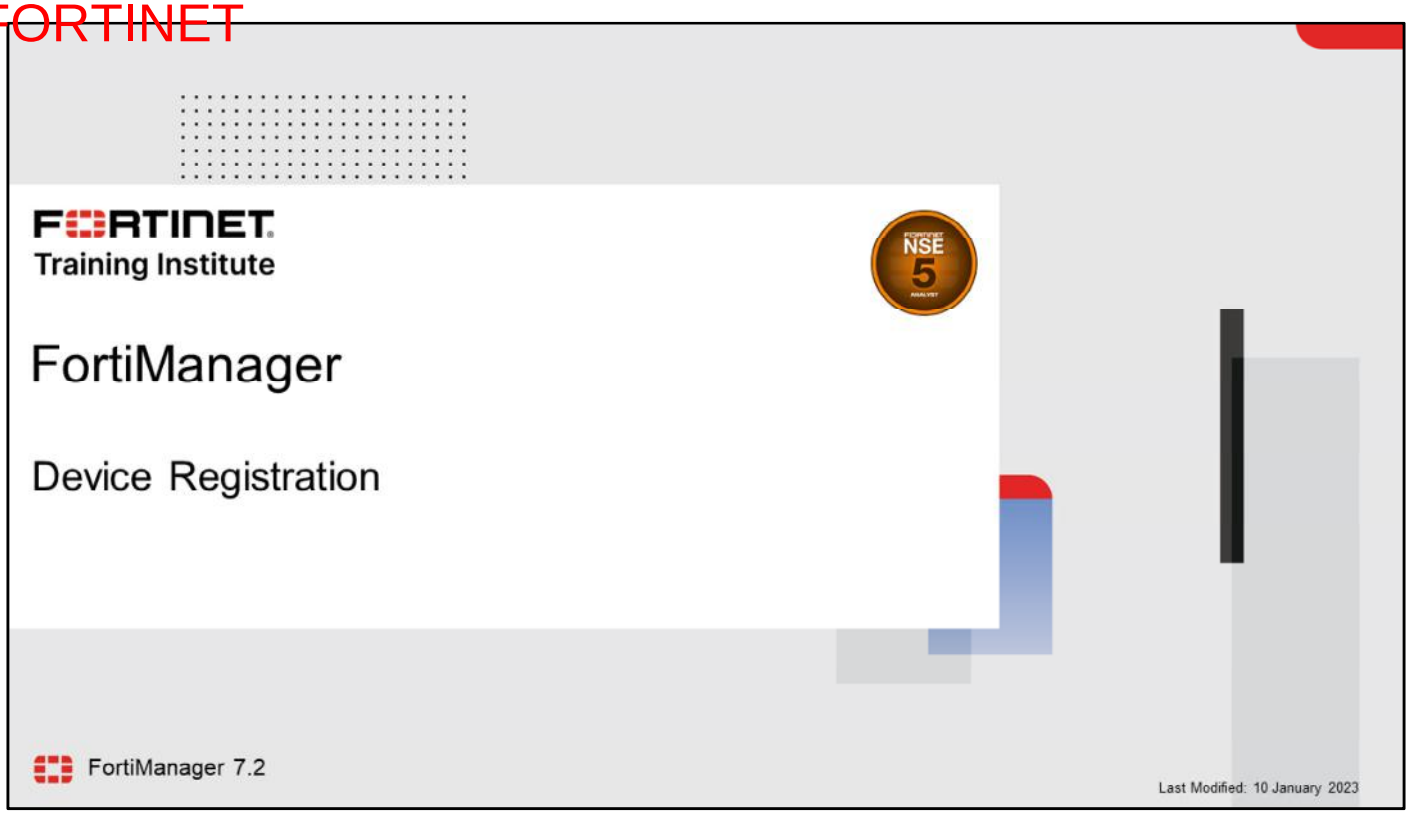
57

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

By mastering the objectives covered in this lesson, you learned how to set up and administer FortiManager. You also learned how to use features that are critical to day-to-day use, such as ADOMs, event monitoring, back up, and restore.

Vouchers & Dumps are Available | WhatsApp +201224560923

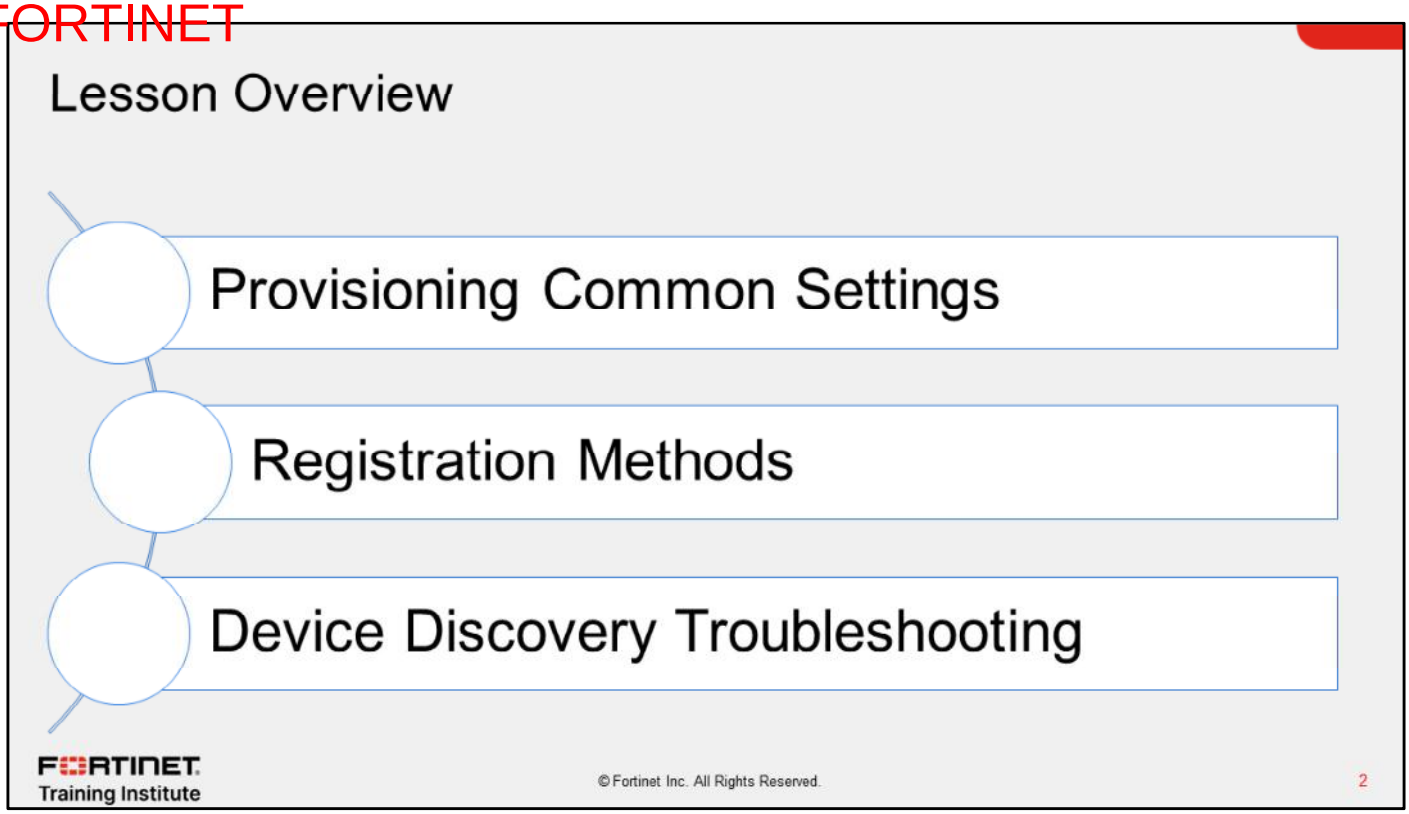
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the primary functions of the device manager pane, and how to manage FortiGate using FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

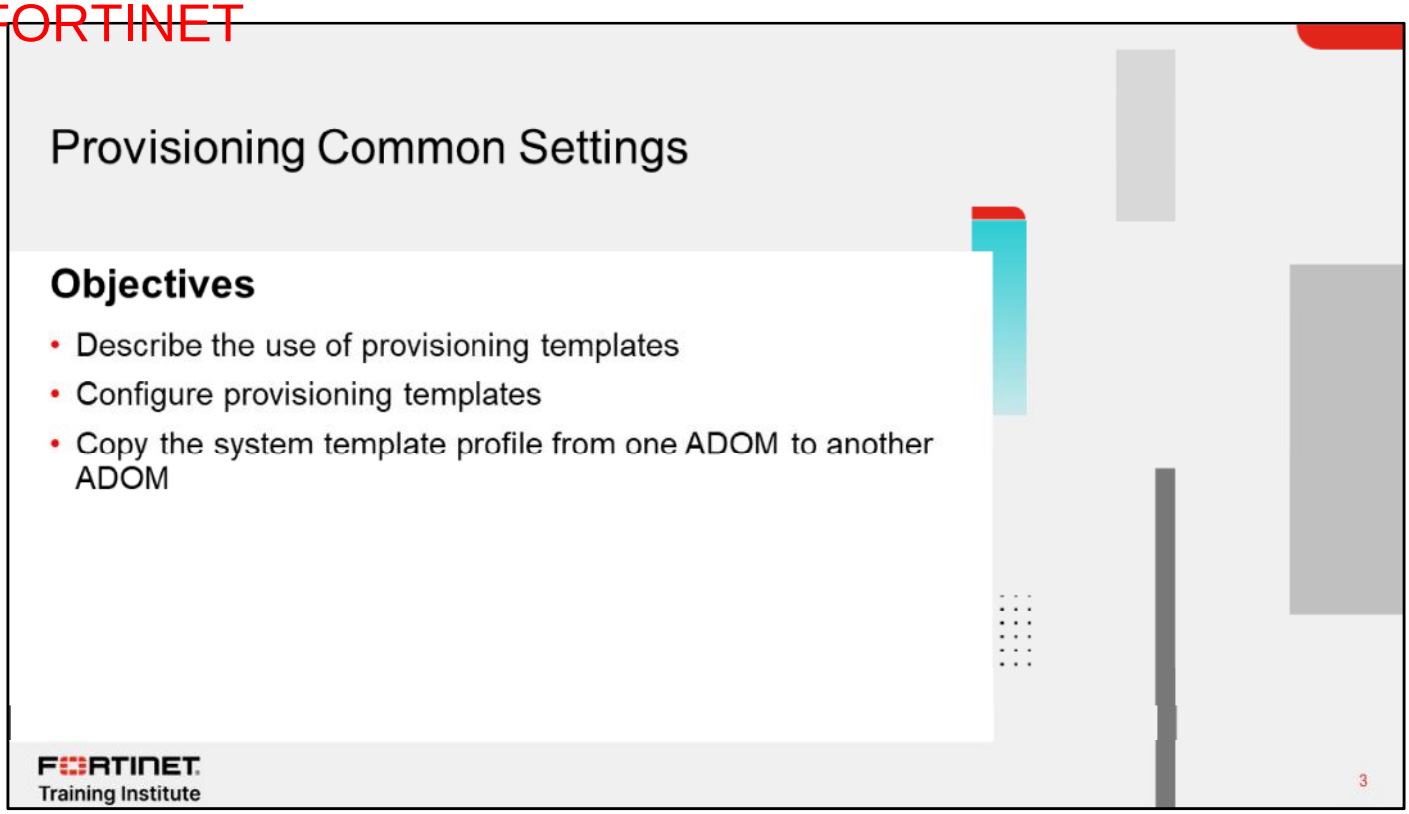
DO NOT REPRINT
© FORTINET
Brave-dumps.com



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

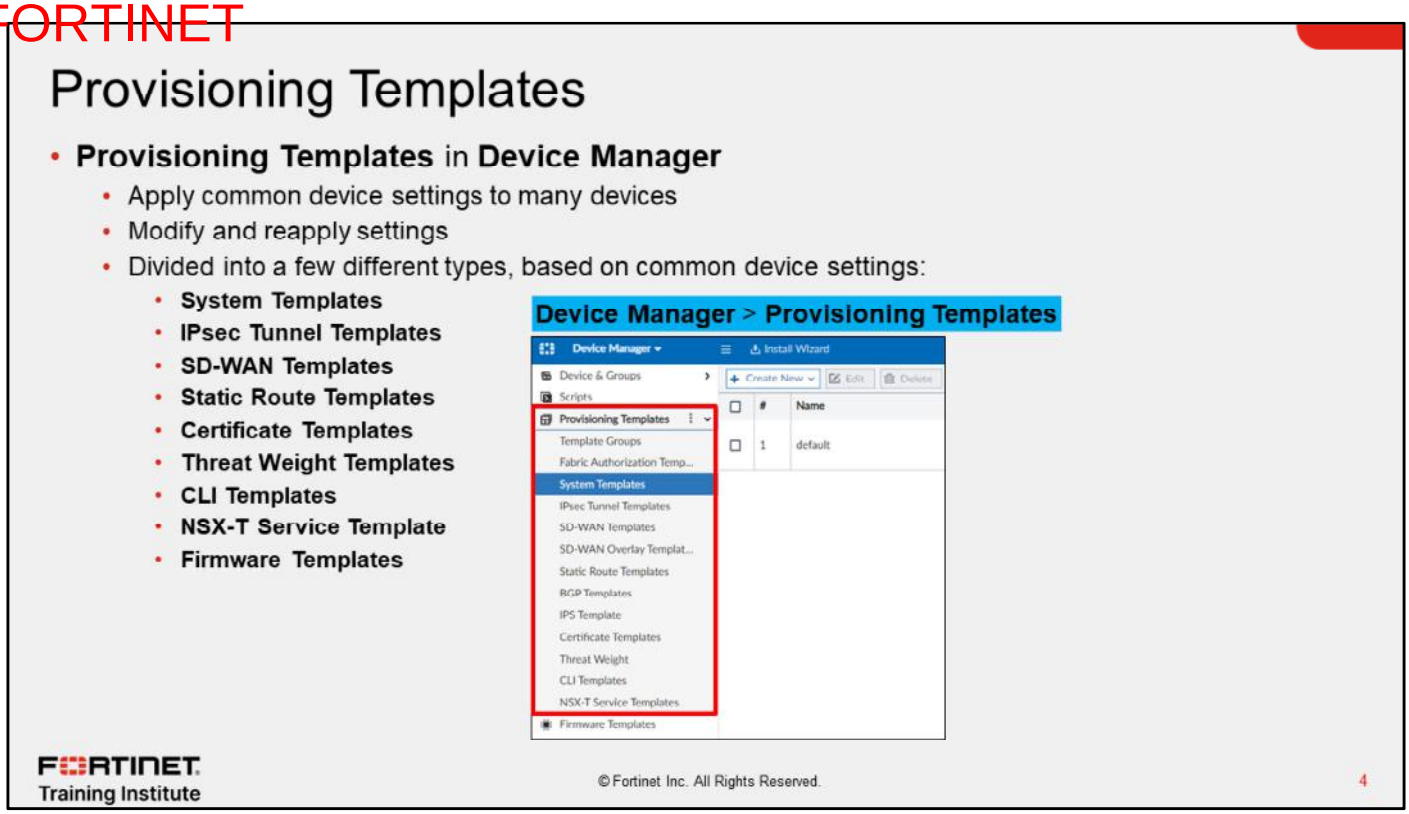


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in provisioning common settings, you will be able to use FortiManager to configure common settings for many FortiGate devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



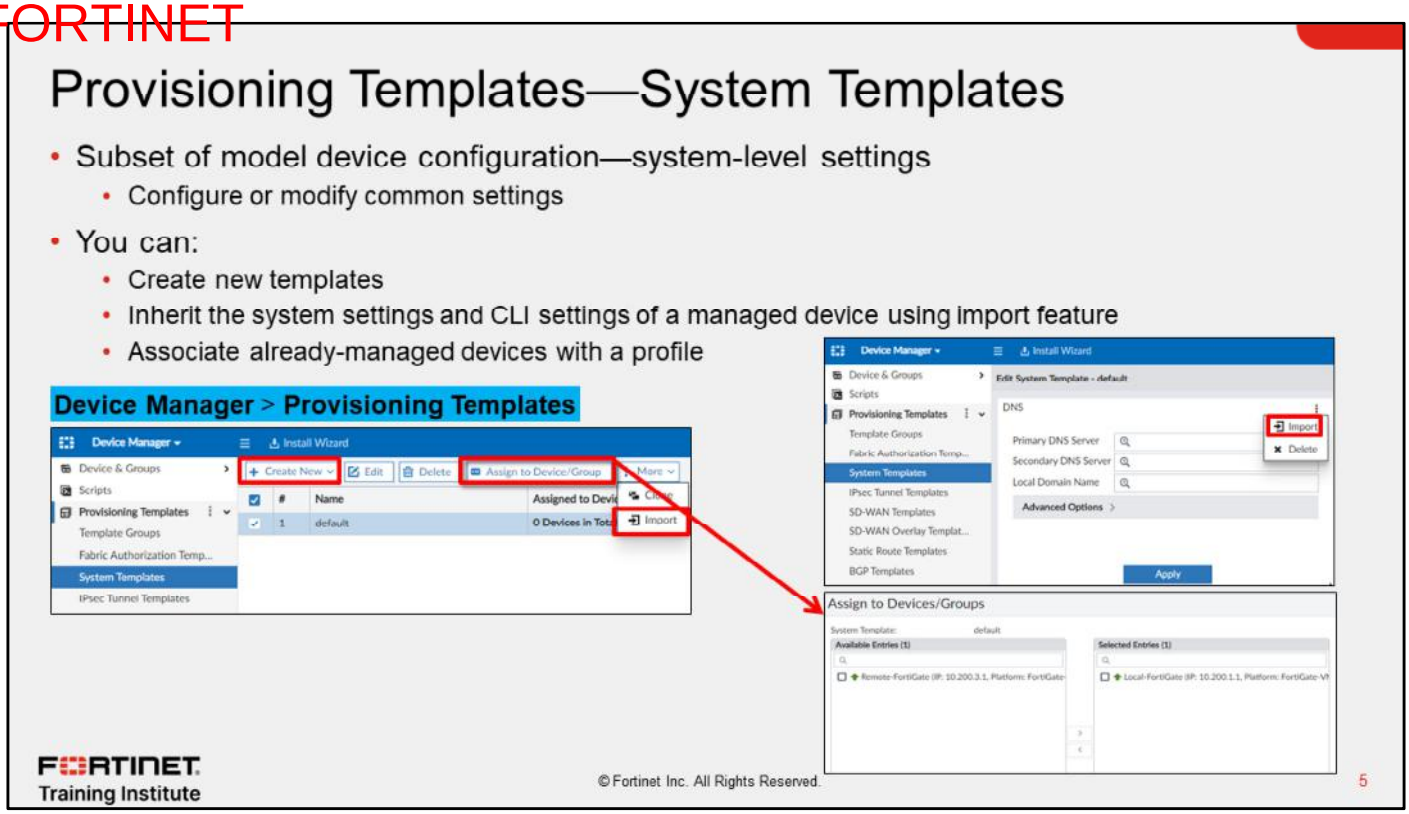
Provisioning templates allow you to create profiles that contain device-level settings. These templates facilitate identical device-level settings across many devices. You can edit and reapply the templates. There are few types of templates, based on common device settings. They are as follows:

- **System Templates**: allow you to create and manage common system-level settings for the managed device.
- **IPsec tunnel Templates**: You can provision IPsec tunnels to FortiGate branch devices using an IPsec template.
- **SD-WAN Templates**: allow you to configure SD-WAN for one or more devices.
- **Static Route Templates**: You can provision static routes to FortiGate devices by using a static route template.
- **Certificate Templates:** allow you to create certification authority (CA) certificate templates, add devices to them, and generate certificates for selected devices. After you generate and sign the CA certificates, you can install them using the install wizard.
- **Threat Weight Templates:** allow you to create threat weights, which can provide information by tracking client behavior and reporting on activities that you determine risky or otherwise worth tracking
- **CLI Templates**: allow you to create CLI script templates or CLI script template groups that you can assign to managed devices.
- **NSX-T Service Template**: allow you to manage multiple FortiGate VMs running on NSX-T by automatically applying VDOM, policy, and configuration settings to each VM that belongs on the same registered service.
- **Firmware Templates**: Firmware templates define what firmware version should be installed on FortiGate devices and all access devices, such as FortiAP, FortiSwitch, and FortiExtender.

Note that the provisioning templates are based on specific ADOM versions, so some settings may not be available.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **System Templates** page contains one generic profile named **default**, which is a subset of the model device configurations and contains the widgets such as **DNS**, **Alert Email**, **Admin Settings**, and others.

You can create a new device profile and configure the settings in the widgets in that profile. You can use the **Import** icon or **Import Template** to import the settings from a specific managed device, which inherits the system-level settings and CLI settings of that managed device.

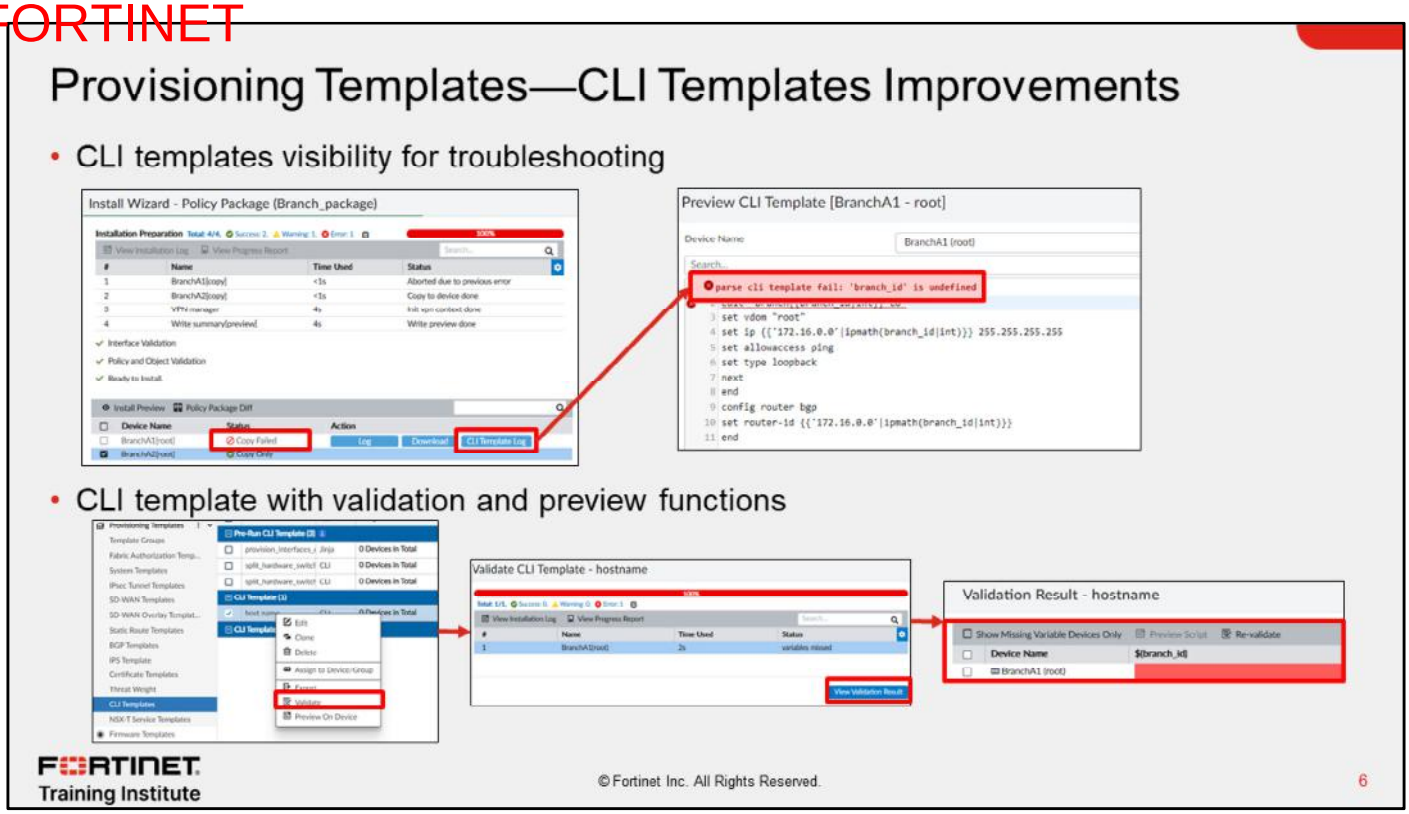
You can use the **Assign to Device** tab to associate devices with a profile, or to view the list of devices already assigned to a profile.

You can apply these configured profiles to multiple devices within the same ADOM, which facilitates identical device-level settings across many devices.

You will apply the **default** profile in **System Templates** when you add FortiGate to FortiManager later in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



As you know **CLI Templates** allows you to create CLI script templates or CLI script template groups that you can assign to managed devices. In FortiManager 7.2, CLI templates have increased visibility for troubleshooting including: line numbering, detailed error report with line number, template name, and reason for the installation failure. The example on this slide shows a policy package for two devices that encountered the error **Copy Failed** for a FortiGate device named “Branch A1”.

To preview the error, click **CLI Template Log** to display the CLI content. If you hover the mouse over the red x that indicates an error, you can view information about the error.

CLI templates also include validation and preview functions to perform verification of the template before installation. You can validate the template by clicking **Validate**. After the template validation finishes, detected errors are displayed, and you can check the errors for details. For example, this slide shows variables that are missing from the template. You can now click **View Validation Result** to type the missing variable in the dialog box. When the CLI template passes validation, you can preview the script by clicking **View Validation Result** again.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Moving System Template Profiles Between ADOMs

- Each ADOM has its own system templates
- Can export profile from one ADOM to another ADOM
  - Useful when same set of profiles required by devices in different ADOMs
- Steps
  - Export profile from first ADOM to dump to file system

```
execute fmprofile export-profile <ADOM name> <profile name> <output file name>
```

  - Import profile to second ADOM from file system

```
execute fmprofile import-profile <ADOM name> <profile name> <full path of exported file>
```

- Example: coping system template from ADOM1 to ADOM2

```
execute fmprofile export-profile ADOM1 1020 Training
output dump to file: [/tmp/Training]

execute  fmprofile import-profile ADOM2 1020 /tmp/Training
Successfully import from file [/tmp/Training] to profile [default]
```

Named file as Training
File copied in FortiManager tmp folder
Full path of exported file
Imported profile in other ADOM

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

What if you need to apply the same system-level settings to many FortiGate devices in different ADOMs?

Remember, each ADOM has a unique object database, which also includes the templates. You can, however, export and import system templates from one ADOM to another ADOM. The ADOMs must be running the same firmware version. First, you need to export the system template from the original ADOM to the FortiManager file system, then you can import that profile into the other ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about system templates is true?
   - ✓ A. They facilitate identical device-level settings across many devices.
   - B. You can use them to install a common policy package across multiple devices.

2. What is the main benefit of exporting a template from one ADOM to another?
   - A. All policy packages also get exported along with the template.
   - ✓ B. You can use the same template across devices in multiple ADOMs without much effort.

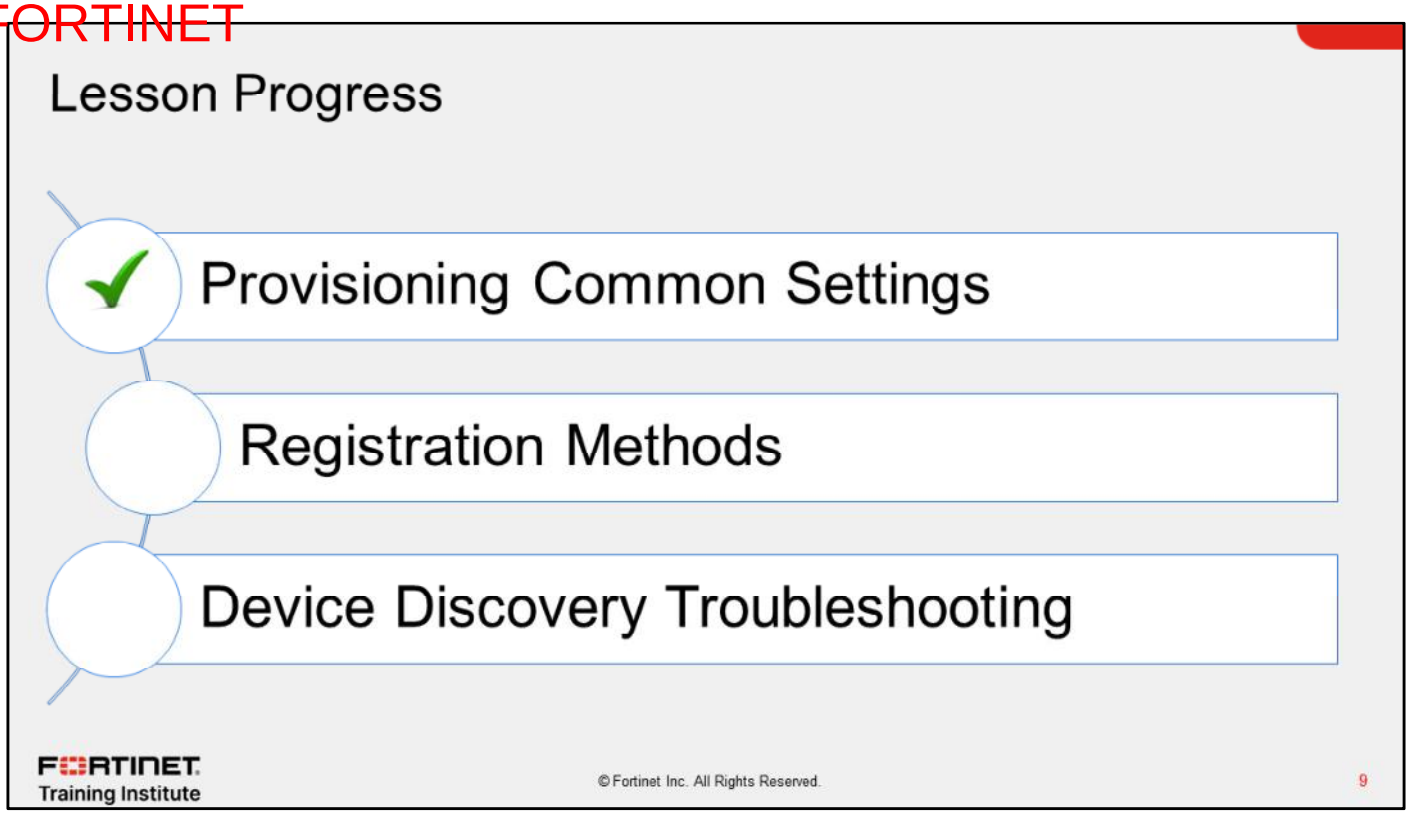
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

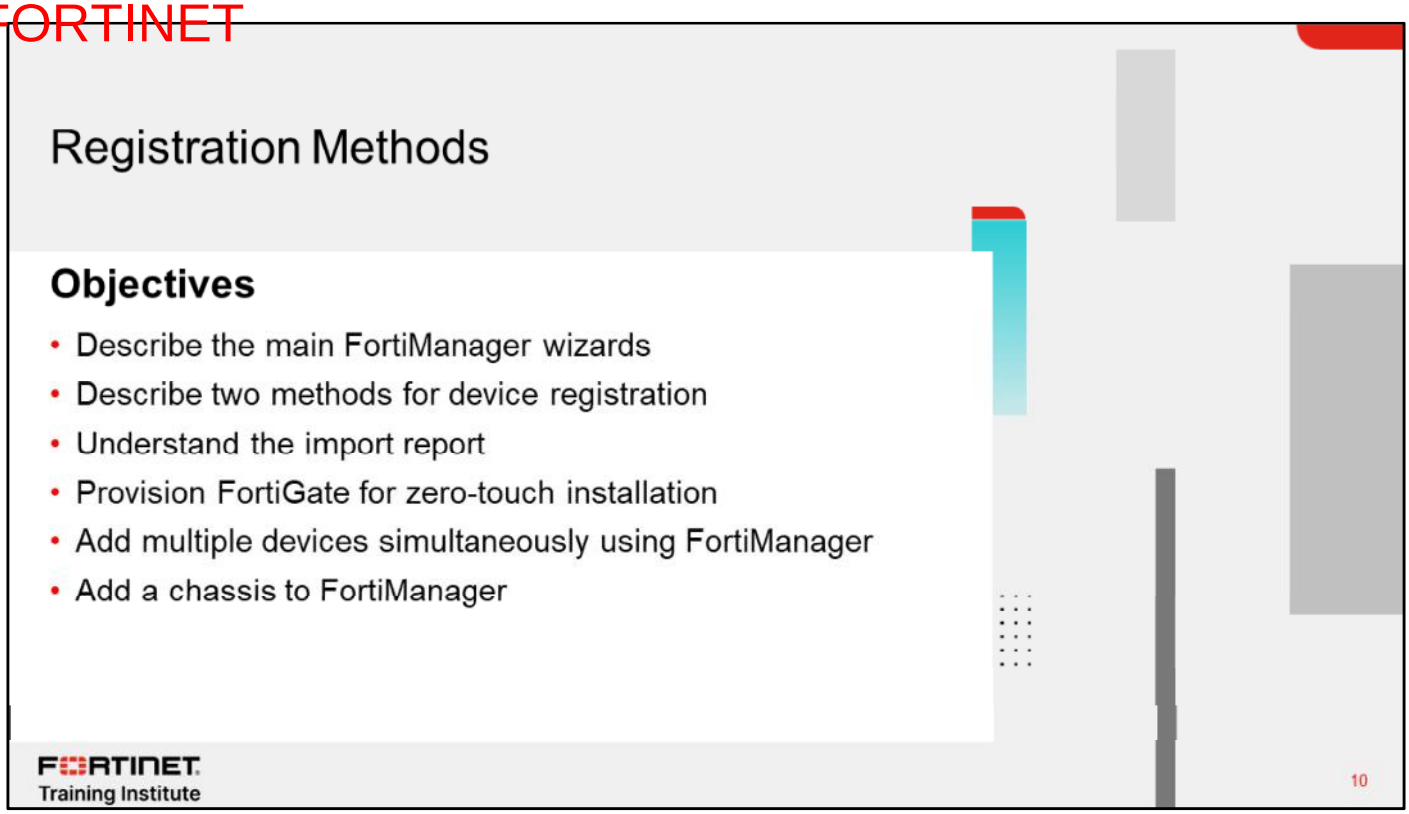


Good job! You now understand provisioning common settings.

Now, you will learn about registration methods.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

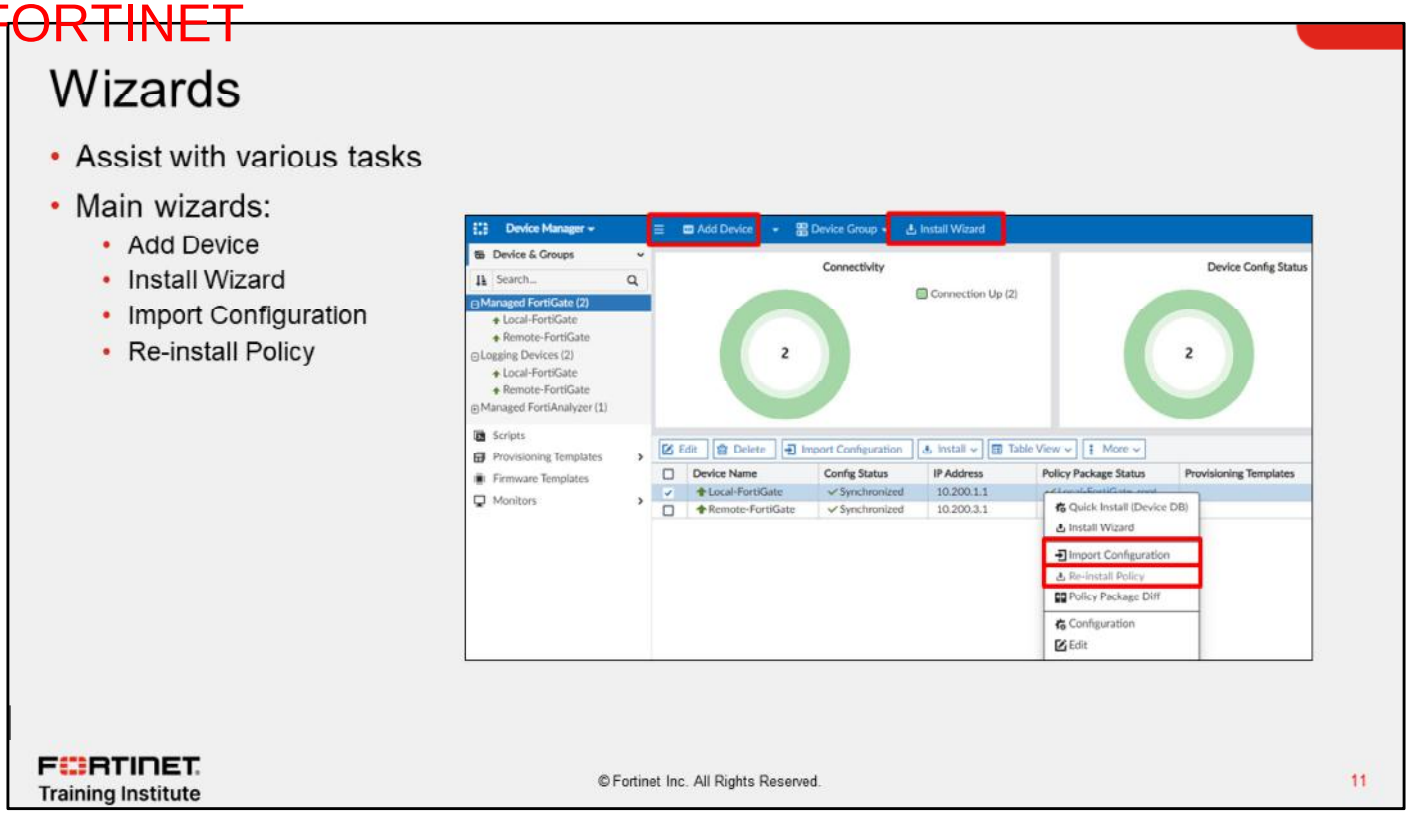


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in device registration, you will be able to add devices into FortiManager for managing and administering these devices from FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Device Manager** provides device and installation wizards to help you perform administrative and maintenance tasks. Using these tools can help you shorten the amount of time it takes to do many common tasks.

There are four main wizards:

- **Add Device**: Add devices to central management and import their configurations.
- **Install Wizard**: Install configuration changes from **Device Manager** or **Policies & Objects** to the managed devices. It allows you to preview the changes and, if the administrator doesn't agree with the changes, cancel and modify them.
- **Import Configuration***:* Import interface mapping, policy database, and objects associated with the managed devices into a policy package under the **Policy & Object** pane. You can run it with the **Add Device** wizard, and run it at any time from the managed device list.
- **Re-install Policy***:* Install the policy package quickly. It also allows you to preview the changes that are installed on the managed device.

You can access the **Import policy** and **Re-install Policy** wizards by right-clicking your managed device on the **Device Manager** tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Methods of Device Registration

Method 1: Device registration wizard

1. The FortiManager administrator uses the device registration wizard to register the device
2. If the device is supported and the details are correct, FortiManager registers the device

Method 2: Request from supported device

1. The administrator of the supported device requests registration
2. The FortiManager administrator accepts (or denies) the request

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

There are two ways you can register a device using FortiManager.

The first method involves the FortiManager device registration wizard. If the device is supported and all the details of the device are correct, FortiManager registers the device.

The second method involves a request for registration from a supported device. When the FortiManager administrator receives that request, the request is accepted (though it can be denied).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Method 1: Add Device Wizard

- Allows you to:
  - Add devices to be centrally managed by your FortiManager
  - Import all the policies and their dependent objects, or all objects from a device into the **Policy & Objects** database
  - Add devices that are not yet online (add model device)
- Performs multiple checks on items being imported
  - Prevents potential problems, such as duplicate names and conflicts
- Often new devices are added with a minimal call home configuration (model device)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

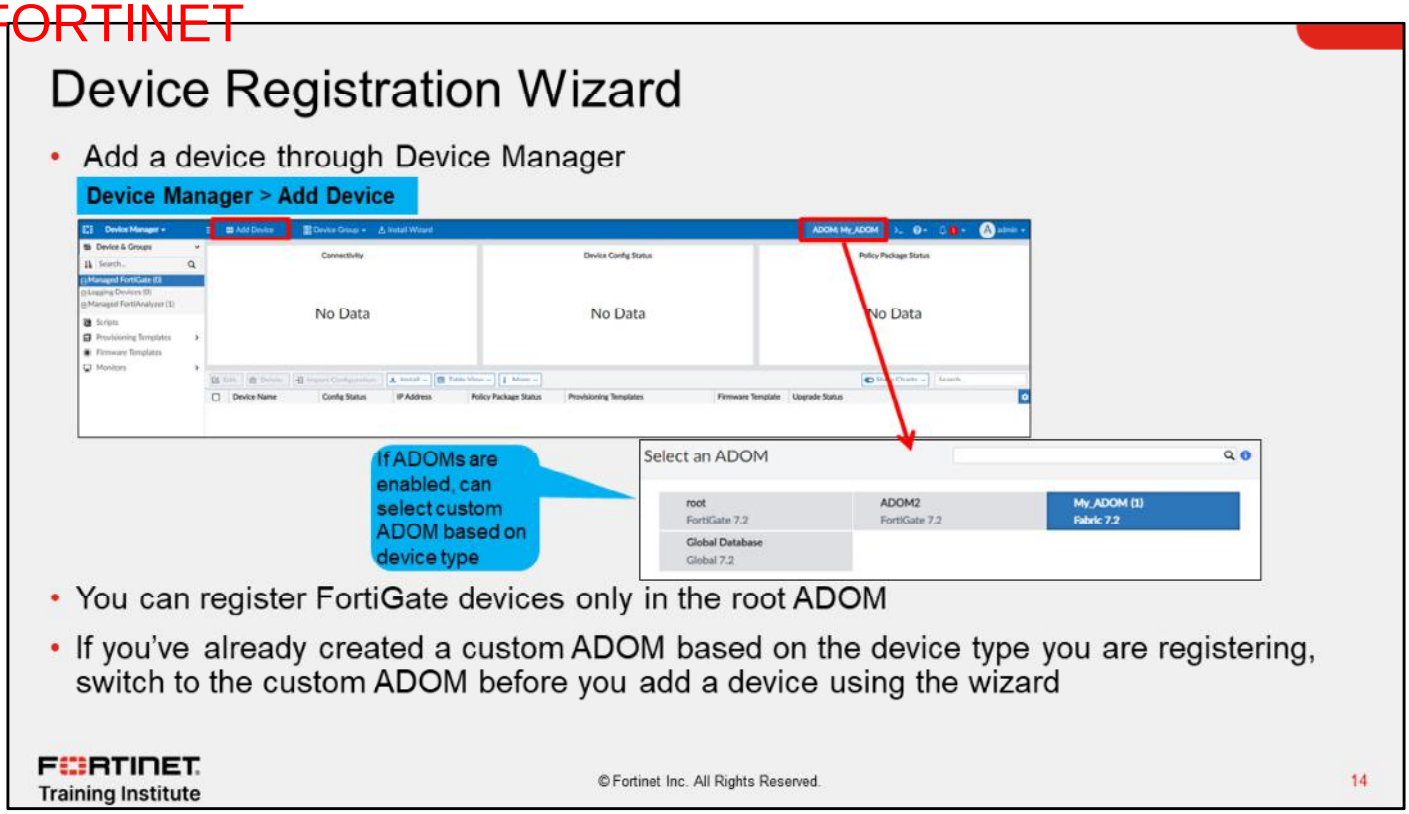
13

Using the **Add Device** wizard, you can add a FortiGate device with an existing configuration (which includes its firewall policies) or add a new FortiGate device. FortiGate is usually provisioned with a *call home* configuration, which is the minimum configuration needed to reach FortiManager (the central management server). Such configurations are typically installed by a technician and the actual firewall configuration is done by the administrator in the security/network operations center where FortiManager resides.

When you import a device that has an existing configuration, FortiManager imports the device firewall policies into a new policy package (which you can rename). Objects share the common object database per ADOM. FortiManager saves the objects in the ADOM database, which you can share or use among different managed FortiGate devices in the same ADOM. FortiManager also checks for duplicate or conflicting objects.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

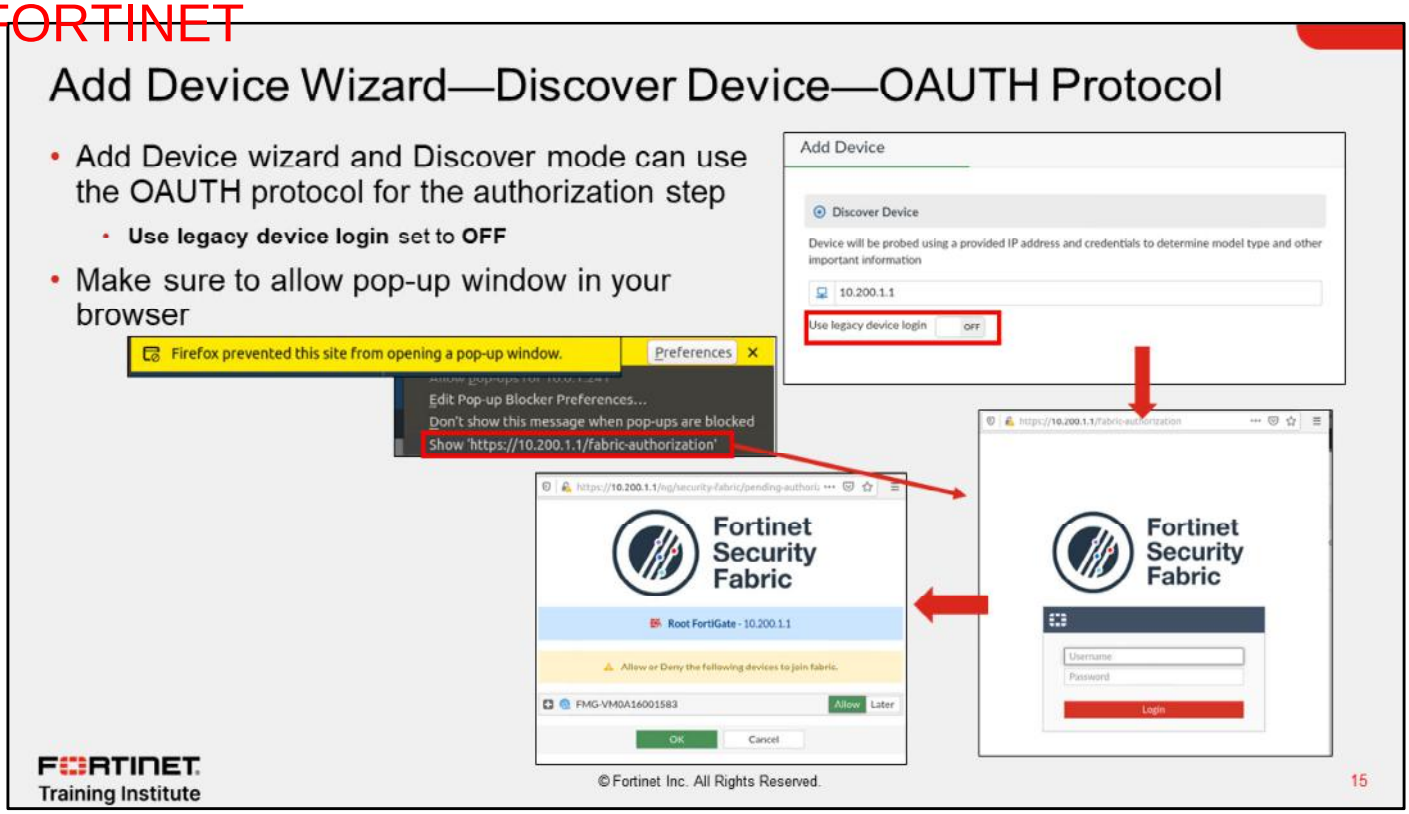


The first registration method you will learn about is the device registration wizard on FortiManager. When this method is used, the FortiManager administrator proactively initiates and, ultimately, performs the registration. When this method is used, the administrator must have specific details about the device that they are registering.

You can launch the wizard from the **Device Manager** pane by clicking **Add Device** on the menu bar. If you have enabled ADOMs and want to add the device to a specific ADOM, select the ADOM from the ADOM list before clicking **Add Device**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can add an online device to FortiManager using the **Add Device** wizard and discover mode with the OAUTH protocol. You type in the IP address of the FortiGate management port, keep the **Use legacy device login** setting at the default **OFF** position, and then click **Next** to continue. At this stage of the wizard, the following actions occur:

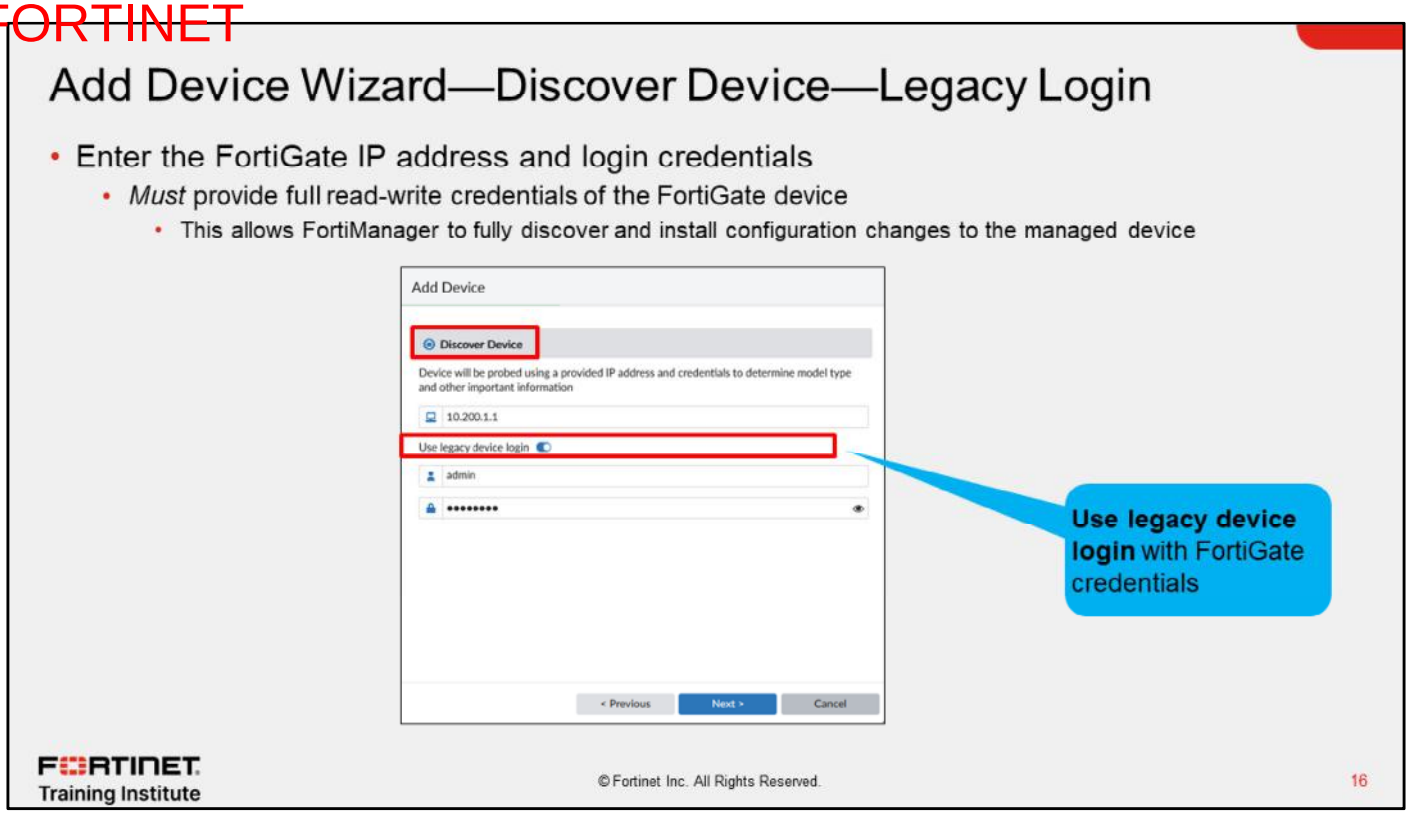
1. FortiManager connects to the online FortiGate.
2. A browser popup window opens to let you log in to FortiGate as part of the authorization process.
3. When FortiManager connects to FortiGate, it retrieves the FortiOS management IP address and management port.

In some cases, FortiManager can access FortiGate, but the browser pop-up window cannot. For example, if FortiGate uses NAT, FortiManager can access the internal IP address for FortiGate and establish the connection. However the browser pop-up window cannot access the internal IP address for the FortiGate device, and the authentication connection fails. You can work around this problem by specifying an accessible management IP address and port on FortiOS.

As an alternate to specifying the accessible management IP and port for FortiOS, you can use the legacy login for the **Add Device wizard** with **Discover** mode. If you are adding a FortiGate running FortiOS 6.4.x, you must use the legacy login.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



For FortiGate devices running FortiOS 7.0.0 and later, you can use the legacy login method instead of using the new authorization method. The legacy login method is useful for certain topologies where the browser pop-up window used by the new authorization method cannot connect to online FortiGate devices.

You use the **Discover Device** and **Use legacy device login** option to add an existing device. Here, you *must* enter the login credentials for the FortiGate device—IP address, user name, and password.

In order to fully discover the device and add the full configuration, the login credentials that you enter when you use the **Discover Device** option *must* have *full read-write access* on FortiGate. This also allows FortiManager to install the configuration on the managed FortiGate. If you are adding a FortiGate running FortiOS 6.4.x and earlier, you must use the legacy login.

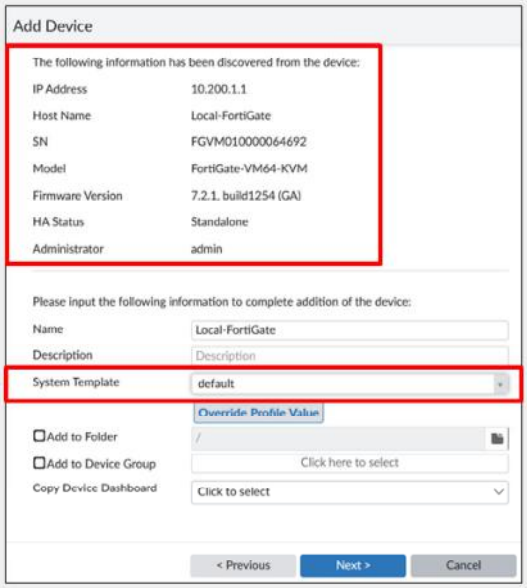
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Add Device Wizard—Discover Device—Legacy Login (Contd)

- FortiManager discovers the information about the device:
  - IP address
  - Host Name
  - Serial number
  - Model
  - Firmware version
  - HA status
  - Administrator user name
- You can apply system templates for specific common device-level settings

Applying preconfigured system template



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

In this step, FortiManager determines whether the FortiGate device is reachable and also discovers basic information about the device, including IP address, administrative user name, device model, firmware version (build), serial number, and high-availability mode.

Administrators can configure the system template in advance and apply it to new devices as they are being added to FortiManager. Templates save time by removing the need to repeat common configuration settings multiple times.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Add Device Wizard—Discover

- This FortiManager CLI command provides the same information

```
# diagnose debug application depmanager 255
# diagnose debug enable
```

FMG-VM64 # Request:
{ "client": "dvm\/cmd:dvm\/cmd\/discover\/device ...:5907", "id": 2, "method": "
exec", "params": [{ "data": { "host": "10.200.1.1", "passwd": "******", "usr": "
admin"},
Response:
{ "id": 168, "result": [{ "data": { "branch_pt": 1254, "build": 1254, "managed_serial": "FMG-
VM0A16001583" "platform_str": "FortiGate-VM64-KVM", "serialno": "FGVM010000064692", "version":
700}, "status": { "code": 0, "message": "ok"},
"url": "start\/probe\/session"}]}.....

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

You can run the `diagnose debug application depmanager 255` and `diagnose debug enable` CLI commands on FortiManager to obtain real-time status of the FortiGate device being added.

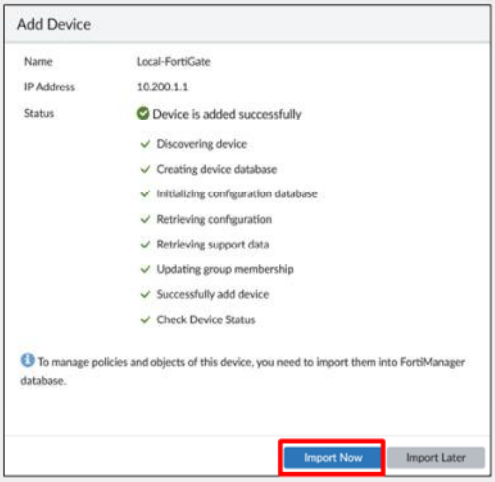
Note that the output of this command is verbose and shows the output from other managed devices too.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Add Device Wizard—Import Options

- Discovers and creates the initial configuration
  - Retrieves support contract and IPS signatures
- Choose to import policies and objects
  - **Import Now**
    - Policy package created
    - Objects added in common ADOM database
  - **Import Later**
    - No policy package and objects added
    - Can be imported later using the **Import policy** wizard



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

In the next step, FortiManager checks the addition of the FortiGate device and creates the initial configuration file in the revision history. This is the full configuration that contains all used and orphaned objects along with the firewall policies on FortiGate. It also checks the support contract, which is useful in the event FortiManager is used as the local FortiGuard server for the managed FortiGate.

There are two options for importing policies and objects:

- Clicking **Import Now** adds the policies to the policy package and objects in the common shared ADOM database. These objects can be used by multiple FortiGate devices in the same ADOM.
- Clicking **Import Later** adds only the device-level settings to the device database, but the firewall policy and objects are not imported into **Policy & Objects**. You can import these later using the **Import policy** wizard.

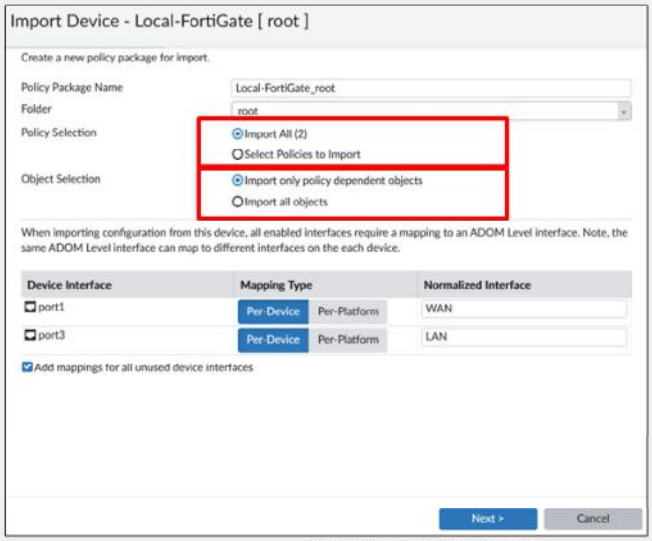
In the example shown on this slide, the **Import Now** option is selected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Add Device Wizard—Policy and Objects

- Allows administrators to import policies and objects
- Creates policy package under the **Policy & Object** pane



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

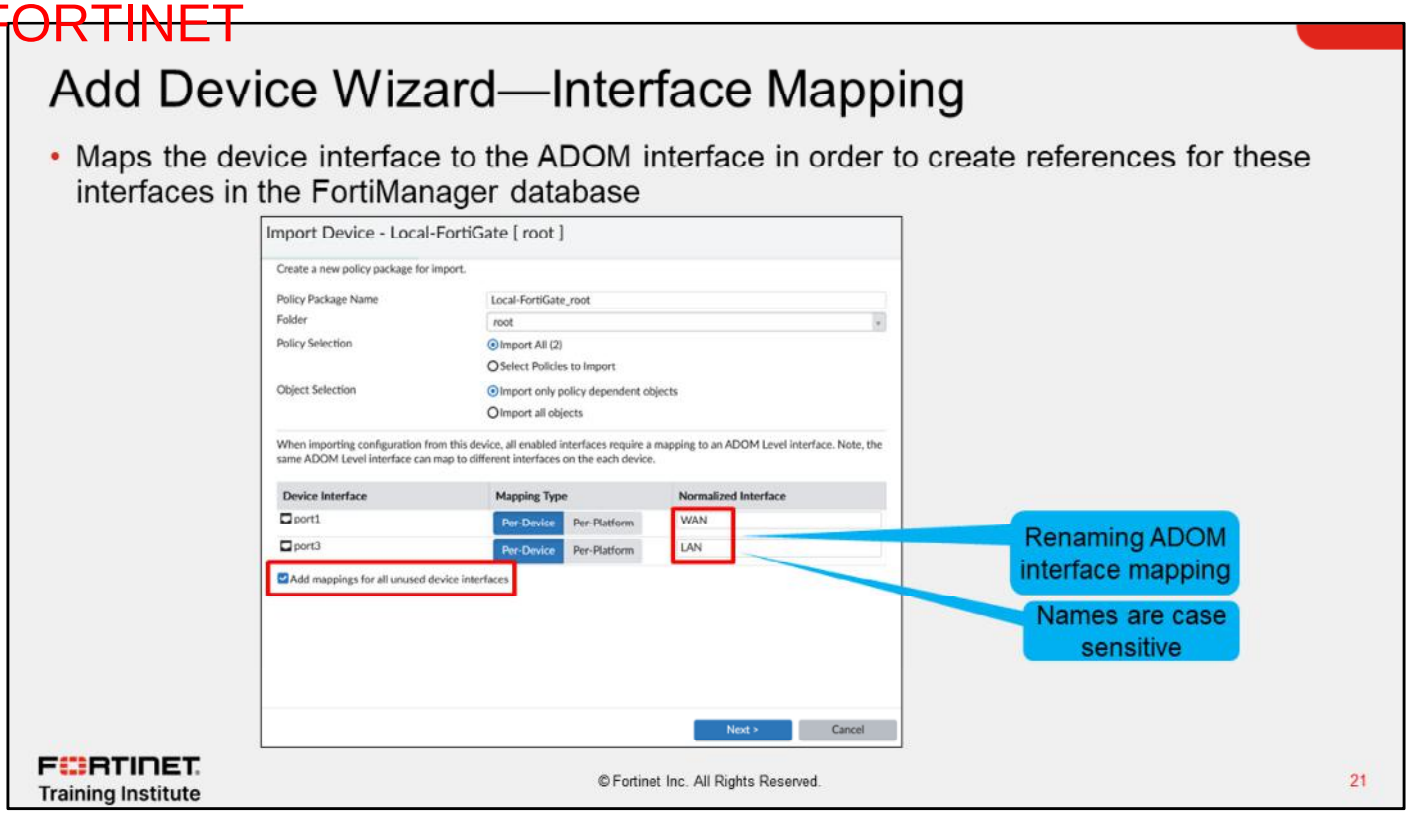
20

The wizard searches for all policies to import into the FortiManager database. In this step, policies are imported into a new policy package under the **Policy & Objects** pane.

At this point, you can choose whether to import all policies or selected policies, and whether to import only referenced objects or all objects. By default, the **Import All** and **Import only policy dependent objects** options are selected when adding a device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



If virtual domains (VDOMs) are configured, you are prompted to select the VDOMs you want to import. The majority of a firewall configuration is specific to the VDOM, therefore each VDOM counts as one managed device.

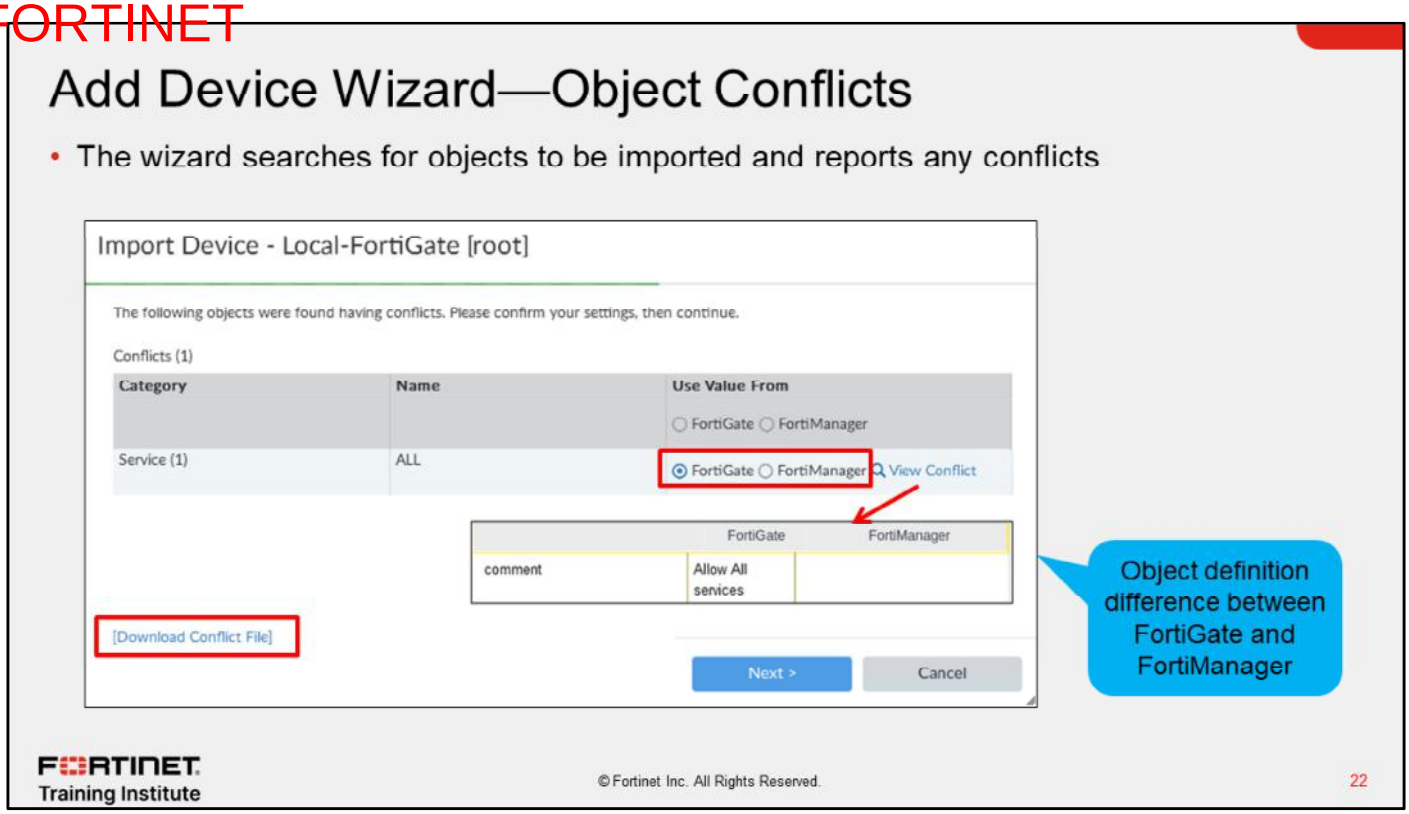
FortiManager probes FortiGate and creates an interface mapping in the ADOM database. You can also rename the ADOM interface mapping. The FortiGate device has interfaces port1 and port3, which are renamed to WAN and LAN respectively. This mapping is local to the FortiManager database and you can view policies on FortiManager as from LAN and WAN interfaces. You can use local ADOM interface mappings for multiple FortiGate devices. Keep in mind that ADOM interface names are case sensitive. For example, if you have an existing device with an interface WAN and you rename the interface to wan, you will see two interfaces named WAN and wan in your interface lists.

Correct interface mappings are useful in large deployments, where administrators can use common names for ADOM interfaces. You can also use the same name for the FortiGate device interfaces at the ADOM level. It also helps administrators view and track firewall policies easily on FortiManager.

By default, the **Add mappings for all unused device interfaces** setting is enabled. Enabling this setting creates an automatic mapping for the new interface. As such, the FortiManager administrator does not need to create a manual mapping.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

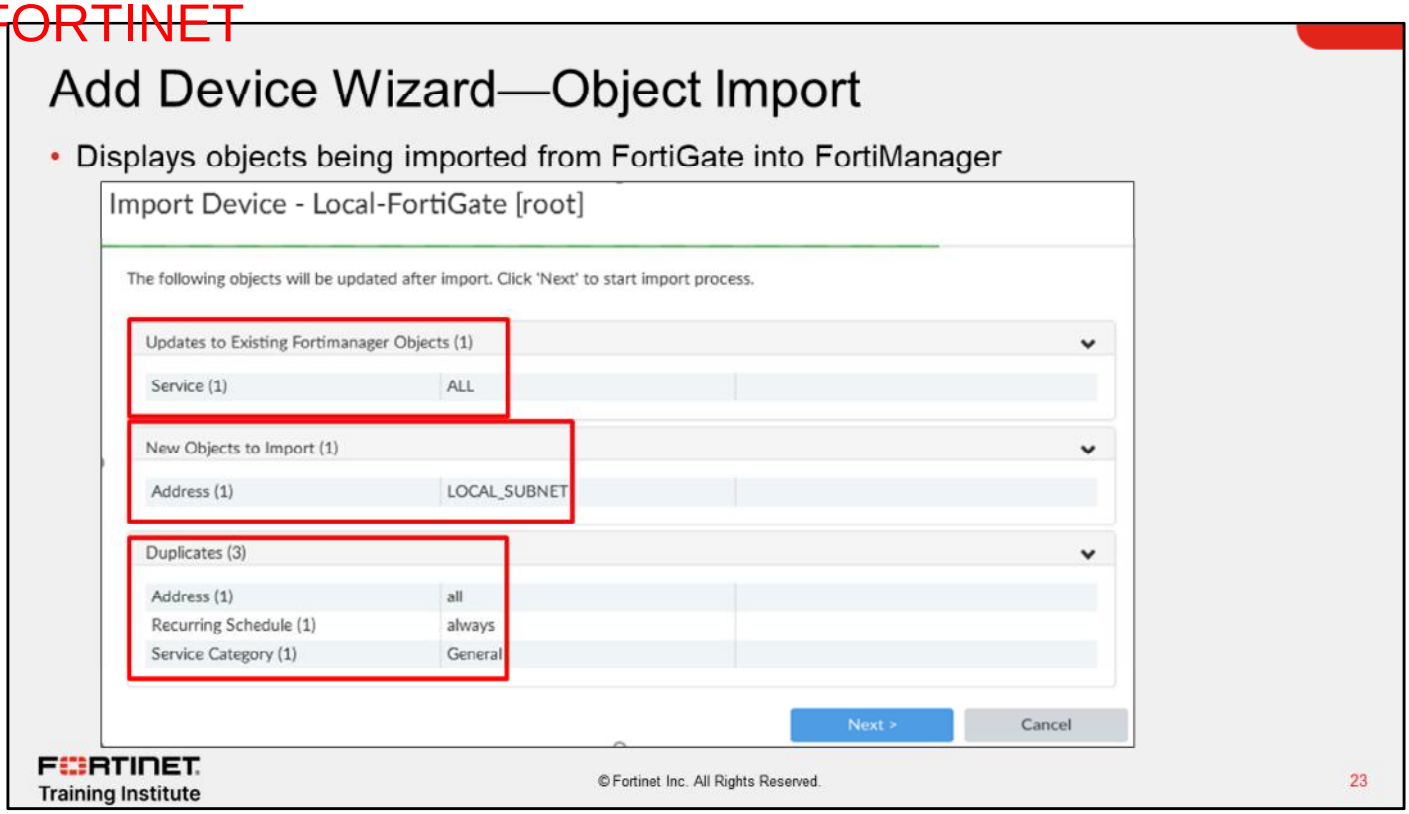


Next, the wizard searches the FortiGate device for objects to import and, if any conflicts exist, they appear here. You can view additional details, as well as download the conflicts in HTML format.

If you select **FortiGate** from the **Use Value From** column, the FortiManager database gets updated with that value. If you select **FortiManager**, the next time you install the configuration from FortiManager to FortiGate it makes those changes to the FortiGate firewall. By default, **FortiGate** is selected.

Vouchers & Dumps are Available | WhatsApp +201224560923

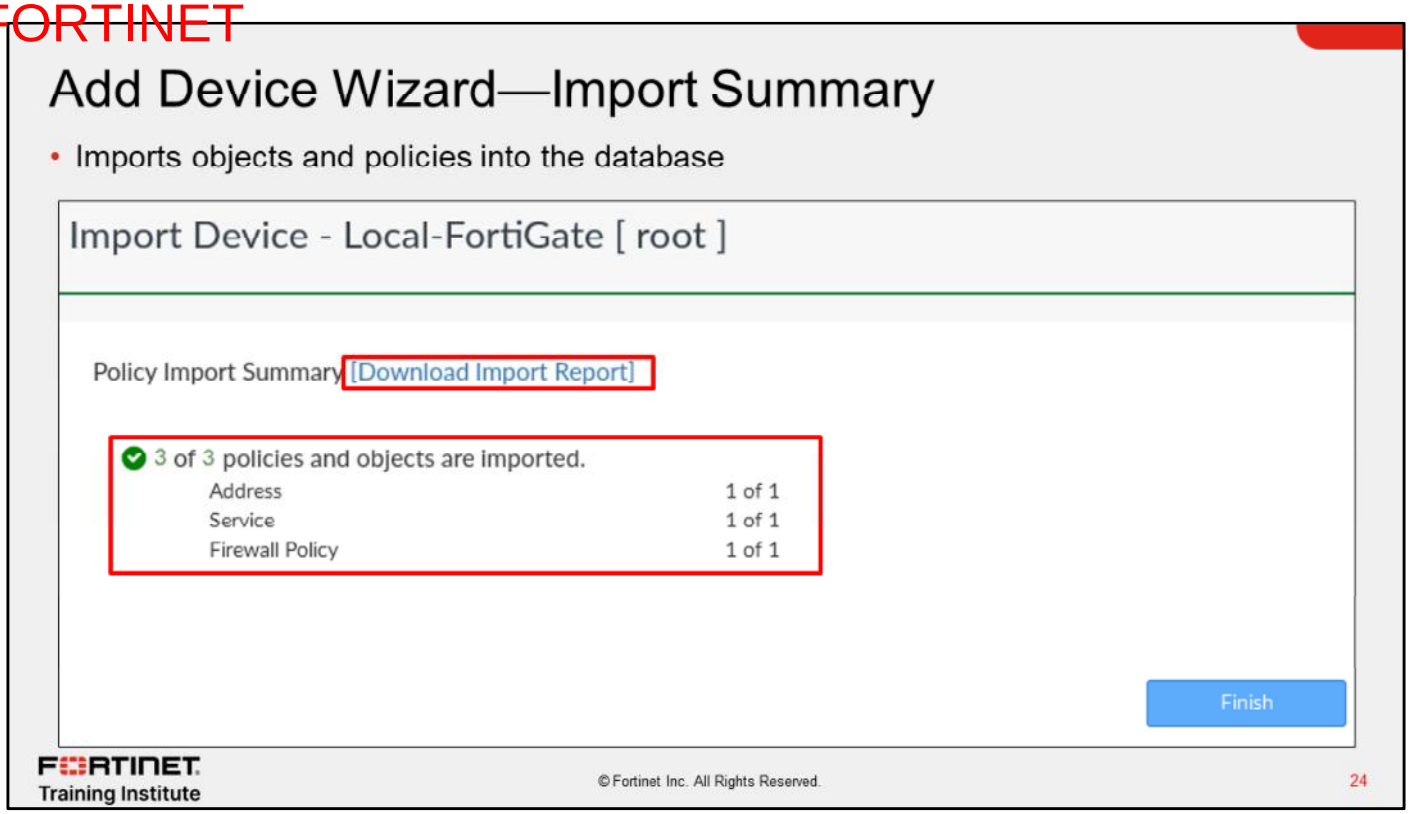
DO NOT REPRINT Brave-dumps.com
© FORTINET



Once the object conflicts are noted and resolved, the wizard searches for the objects to import. FortiManager adds new objects and updates the existing FortiManager objects. FortiManager does not import duplicate entries in the ADOM database, because those objects already exist in the database.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

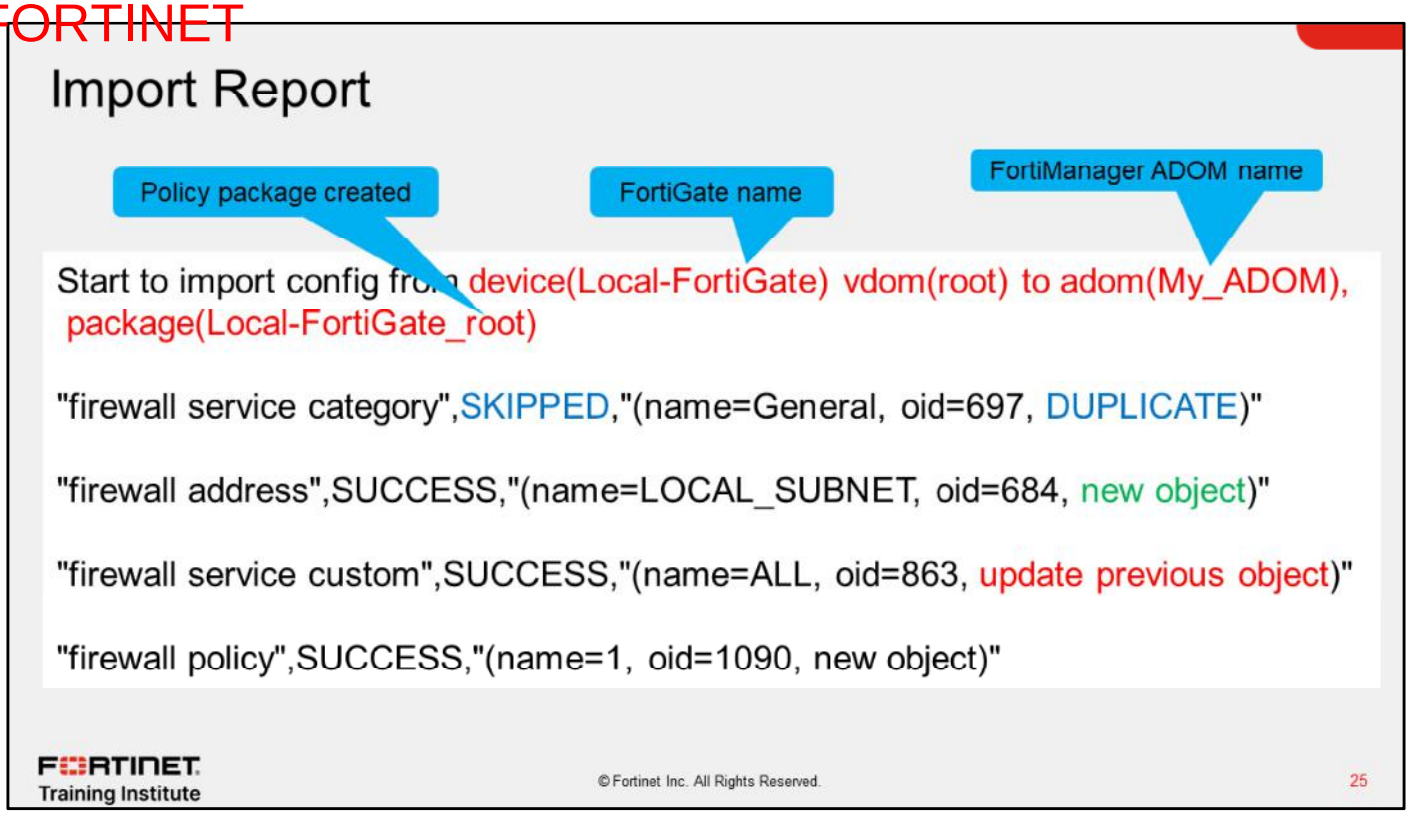


The final page of the wizard is **Import Summary**. On this page of the wizard, the firewall policies and objects are imported into FortiManager.

You can also download the import report, which is only available on this page. As a best practice, it is recommended that you download the report. The next slide shows the downloaded import report.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The import report provides important information, such as which device is imported into which ADOM, as well as the name of the policy package created along with objects imported. These objects and policies are created in the **Policy & Objects** pane for that ADOM.

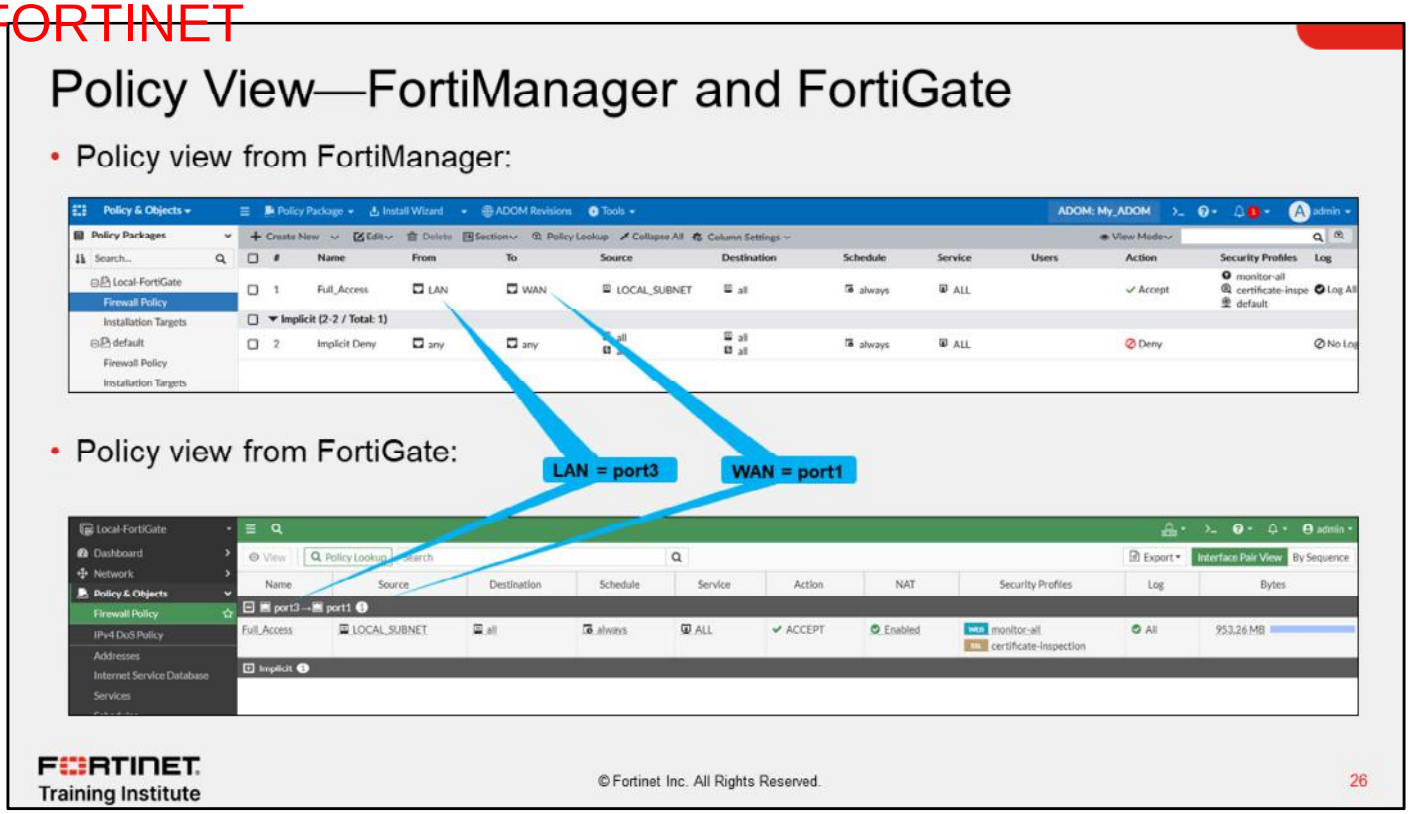
FortiManager imports new objects. FortiManager does not import already existing, or duplicate, entries into the ADOM database. If a conflict is detected, FortiManager updates the object associated with the selected device in the **Objects Conflict** step of the wizard. In the import report, the object is referred to as *update previous object.*

As the example on this slide shows, when you import the configuration from FortiGate to FortiManager, a comment is associated with the address object named ALL in the device configuration. However, there is *no* comment associated with the address object ALL in the FortiManager database. When you choose the FortiGate device value and import the address object ALL, an entry named *update previous object* is added to the import report.

Dynamic objects can also be created, whereby a single object name has different values, depending on which device it is installed on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Because you renamed port3 to LAN and port1 to WAN in the interface mapping step of the wizard, on FortiManager, the policy shows as being imported from LAN and WAN interfaces. However, on FortiGate the policy shows port1 and port3. This is called *dynamic mapping*: firewall policies created in policy packages refer to these mappings. When the policy packages are installed, the interface mapping is translated to the local interfaces on the managed device.

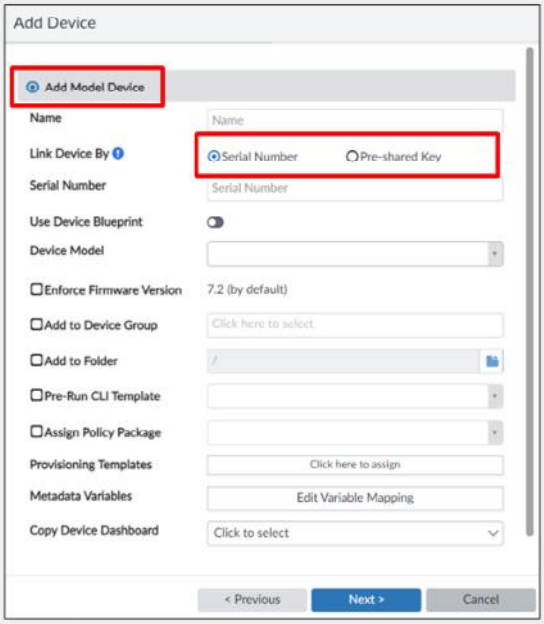
Dynamic mapping is useful when installing the same policy package to multiple managed FortiGate devices, where interface mapping is translated to the local interfaces on the managed device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Add Device Wizard—Model Device

- Supports zero-touch, on-site FortiGate deployment by automatically promoting a model device to a managed device
- Provisions a device in FortiManager, that is not yet online
- Can link device by either:
  - FortiGate serial number
  - Pre-shared key
    - Must be unique if adding multiple model devices



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

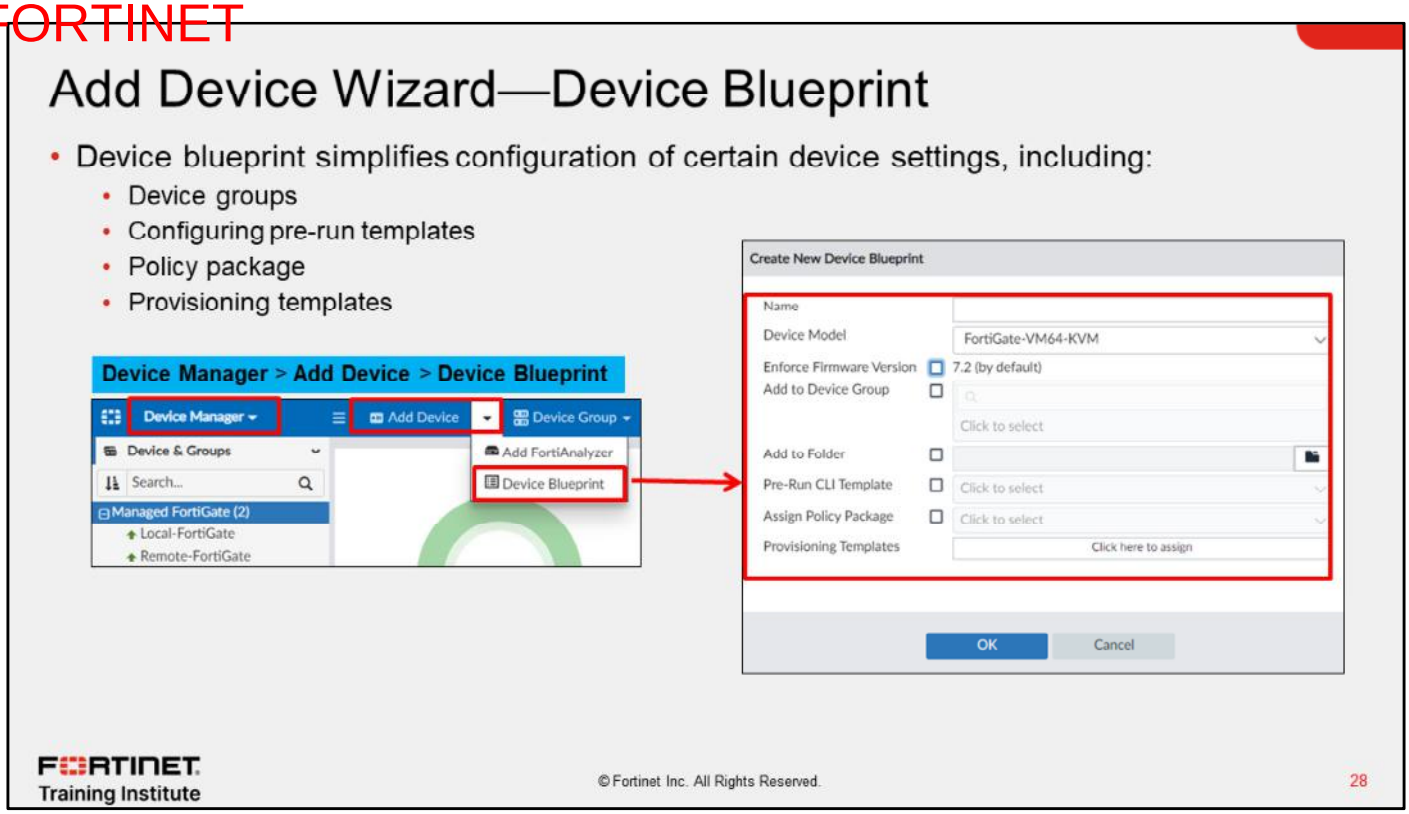
27

The second option in the **Add Device** wizard is **Add Model Device**, which allows you to add a device that is not yet online. Using this option, you can create the configuration in advance.

You can link to the real device using either of the following two methods:
- FortiGate serial number, which is mandatory when adding FortiGate as a model device
- Pre-shared key, a unique pre-shared key if adding multiple model devices

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In FortiManager 7.2, you can now create device blueprints to simplify configuration of certain device settings, including device groups, configuring pre-run templates, policy packages, provisioning templates, and so on. Once a device blueprint has been created, it can be selected when adding a model device or when importing multiple model devices from a CSV file.

You can see it as a package which simplifies the zero touch provisioning process. Per device model, you will be able to select which firmware version should be used, to what device group or folder the FortiGate needs to be added, assign pre-run CLI templates, provisioning templates and a policy package as shown on this slide.

Devices that are assigned the blueprint are automatically configured with the settings specified by the blueprint when they are added to FortiManager.
As an example, device blueprints can simplify the onboarding of branch devices in an SD-WAN configuration when using SD-WAN Overlay Templates by configuring the default device group to which the devices are added.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Model Device—FortiGate Configuration

- Configuration on FortiGate
  - If serial number is used when adding model device

```
config system central-management
set type fortimanager
set fmg <FortiManager IP>
end
```

Configure FortiManager IP address on FortiGate central management

  - If pre-shared key is used when adding model device

```
config system central-management
set type fortimanager
set fmg <FortiManager IP>
end
```

Configure FortiManager IP address on FortiGate central management

```
execute central-mgmt register-device
<fmg-serial-no> <fmg-register-password>
```

Run to link model device to real device

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

On the FortiGate side, you need to configure FortiGate to point to FortiManager. This is important for minimal touch deployments, such as when using FortiDeploy.

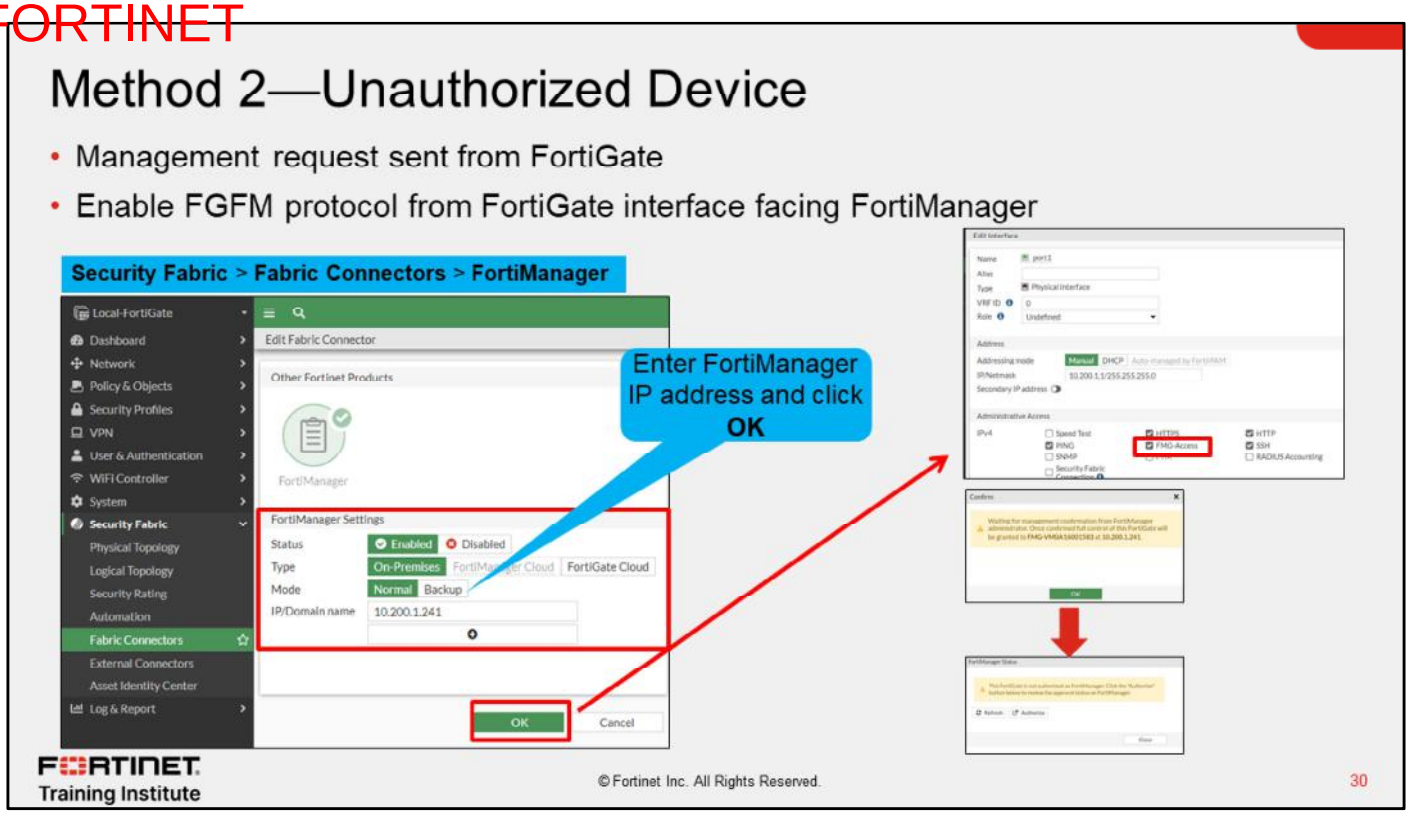
If you are using a serial number to add FortiGate as a model device, you must configure the FortiManager IP address on FortiGate under the central management configuration.

If you are using a pre-shared key to add a model device, you must perform the central management configuration, plus you must run a `register device` command on the FortiGate CLI. This command requires a FortiManager serial number, along with a pre-shared key to use when adding a model device.

The FortiGate device is automatically promoted as a registered device after FortiGate is deployed with its basic IP address and routing configuration to reach FortiManager. You can then install the preconfigured configuration from FortiManager to FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



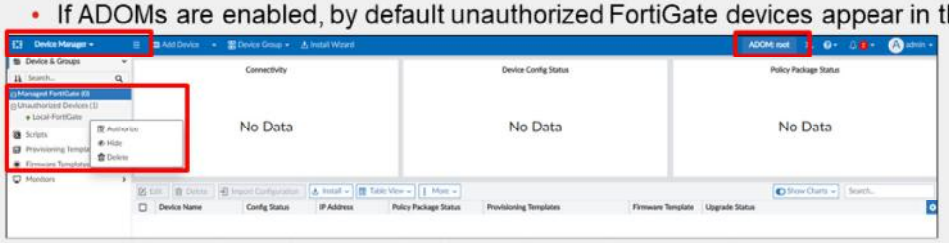
The FortiGate administrator must configure the FortiManager IP address and apply the settings. A pop-up window opens stating that the management request has been sent to FortiManager. Click **OK** to open the **FortiManager Status** window, and then you can authorize the FortiGate device. Also, you must ensure that **FMG-Access** is enabled on the FortiGate interface that is facing the FortiManager device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

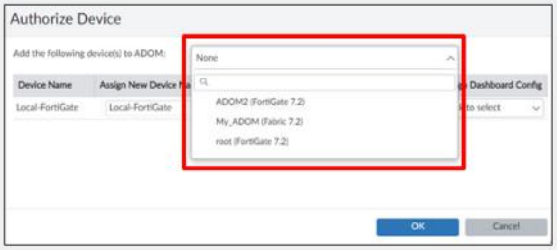
Method 2—Unauthorized Device (Contd)

- Unauthorized devices requesting registration appear under Device Manager
  - If ADOMs are enabled, by default unauthorized FortiGate devices appear in the root ADOM



- Can enable automatic registration—the default is disabled

```
config system admin setting
set allow_register {enable | disable}
```



- Can add FortiGate in a different ADOM,
- if ADOMs are enabled

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

31

So how does FortiGate move from an unauthorized device to a managed device? This happens on the FortiManager side. After the request is made from the supported device, the request appears under **Device Manager** > **Unauthorized Devices** on the FortiManager GUI.

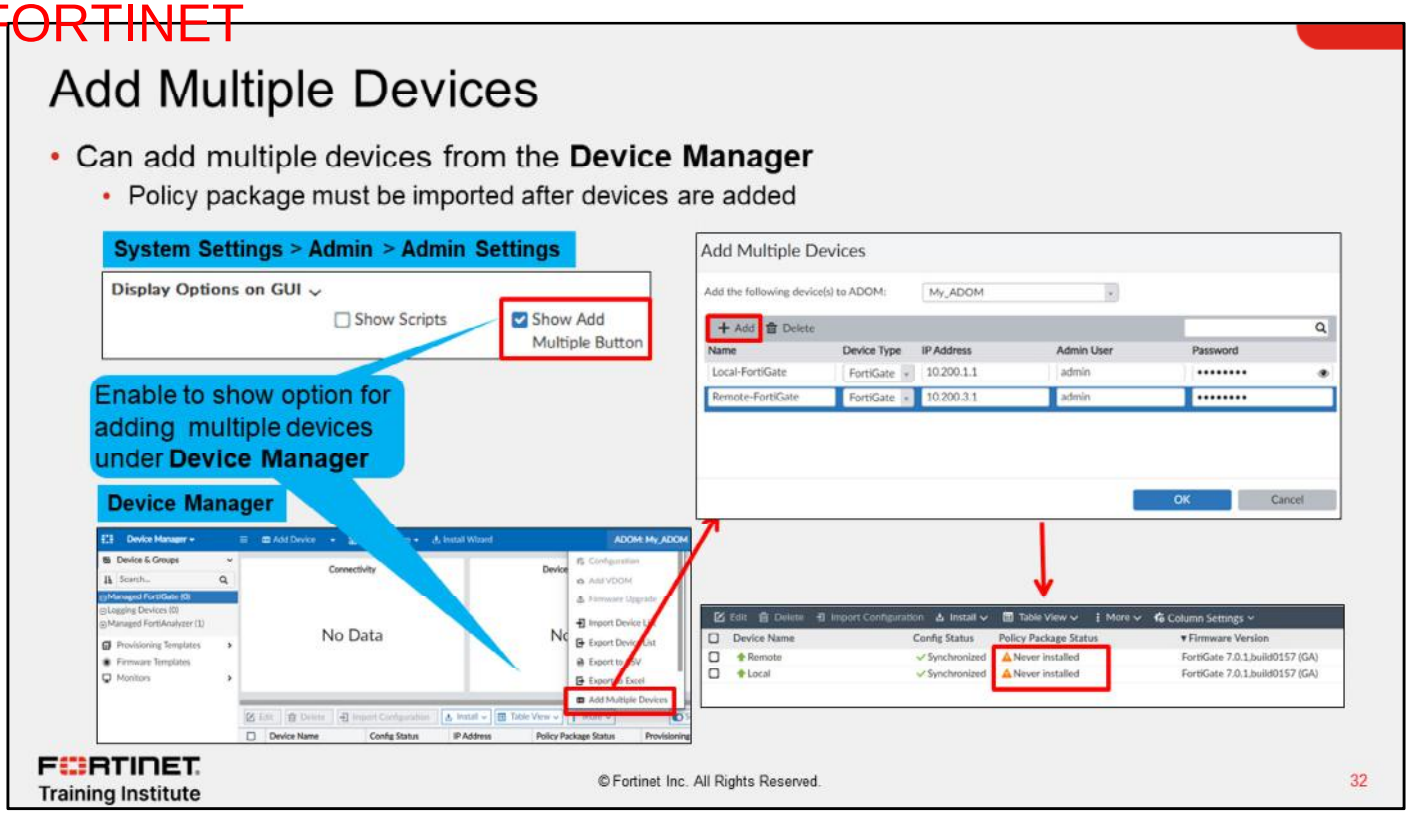
The FortiManager administrator should review the details of the unauthorized device and, if satisfied, authorize the device. If you authorize an unauthorized device, then you must run the **Import Policy** wizard to import the device firewall policy into a new policy package.

If ADOMs are enabled, the device appears in the root ADOM, which is the management ADOM of FortiManager. The root ADOM is based on the FortiGate ADOM type, so you can authorize only FortiGate devices to join the root ADOM. Alternatively, if you've created a custom ADOM based on the FortiGate ADOM type, you can authorize FortiGate to join the custom ADOM instead.

On the FortiManager CLI, you can enable automatic authorization of unauthorized devices. But, you still need to run the **Import Policy** wizard to import the device firewall policy into a new policy package.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



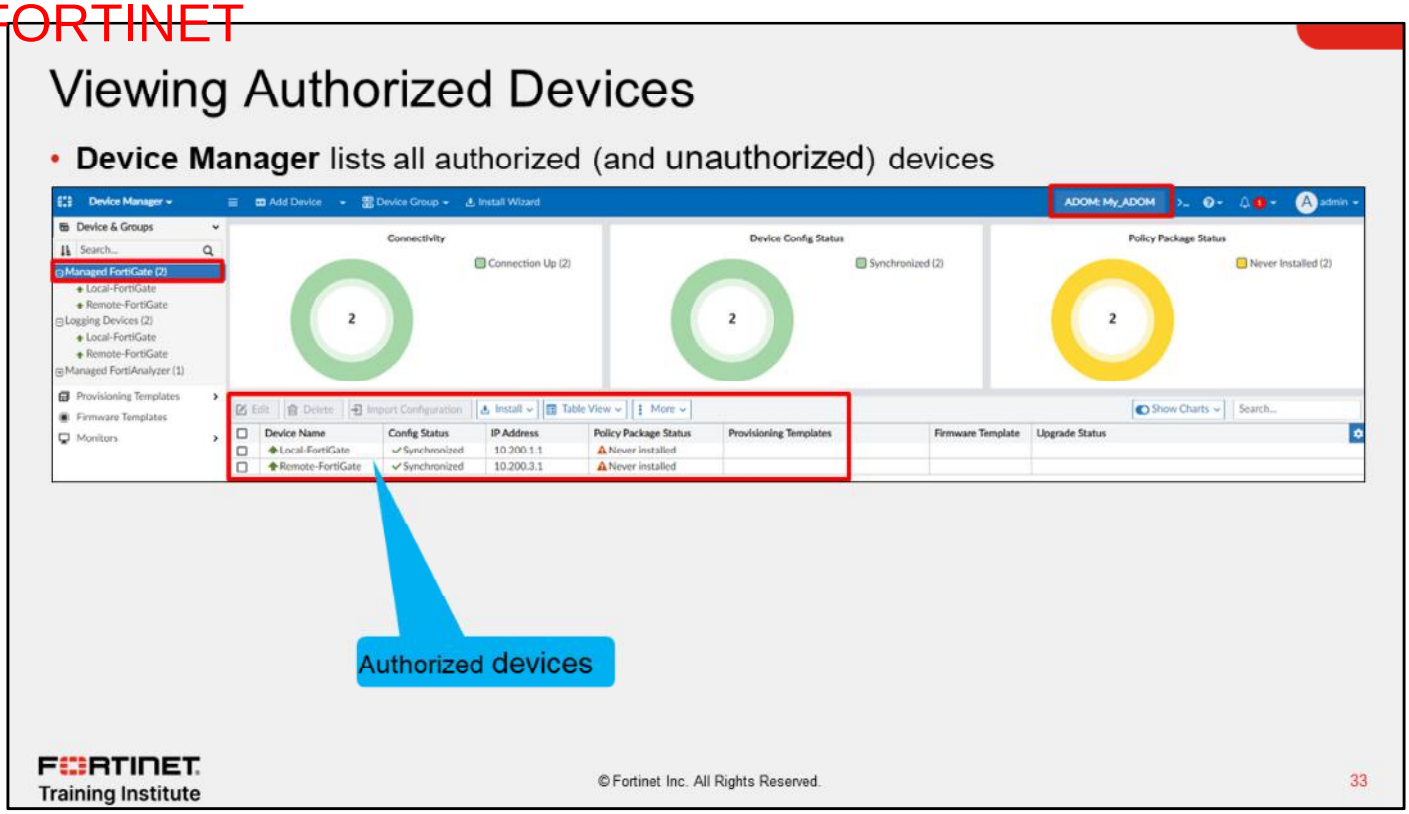
What if you need to add multiple FortiGate devices at the same time?

You can enable **Show Add Multiple Button** under **Admin Settings**, which enables the option for adding multiple devices under **Device Manager**. You can click **Add** and enter the FortiGate IP address, user name, and password.

Similar to adding an unauthorized device, policy packages are not automatically created. You must run the **Import Policy** wizard to import the device firewall policy to a new policy package.

Vouchers & Dumps are Available | WhatsApp +201224560923

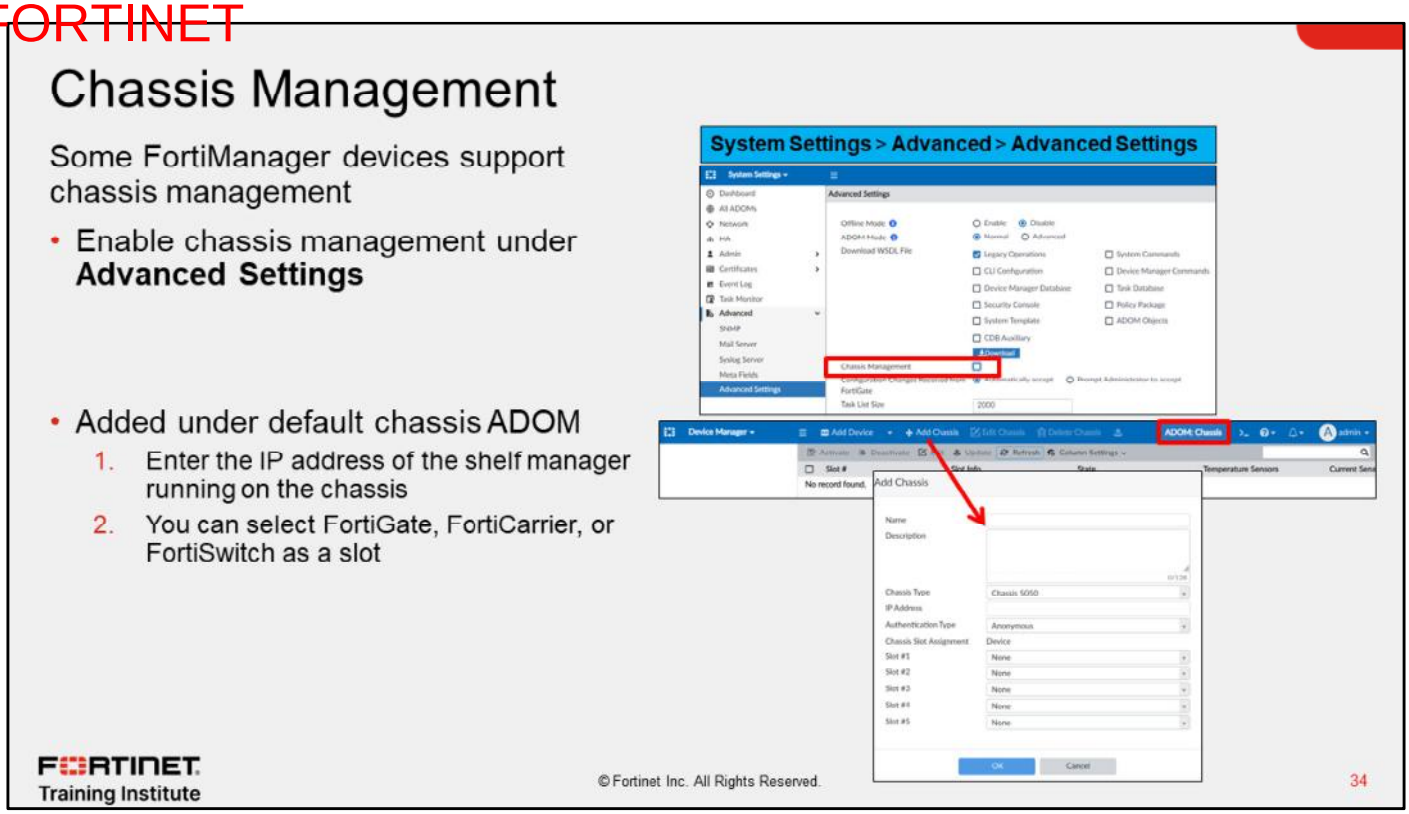
DO NOT REPRINT Brave-dumps.com
© FORTINET



After you register FortiGate devices, they appear on the **Device Manager** in the ADOM to which they were added.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

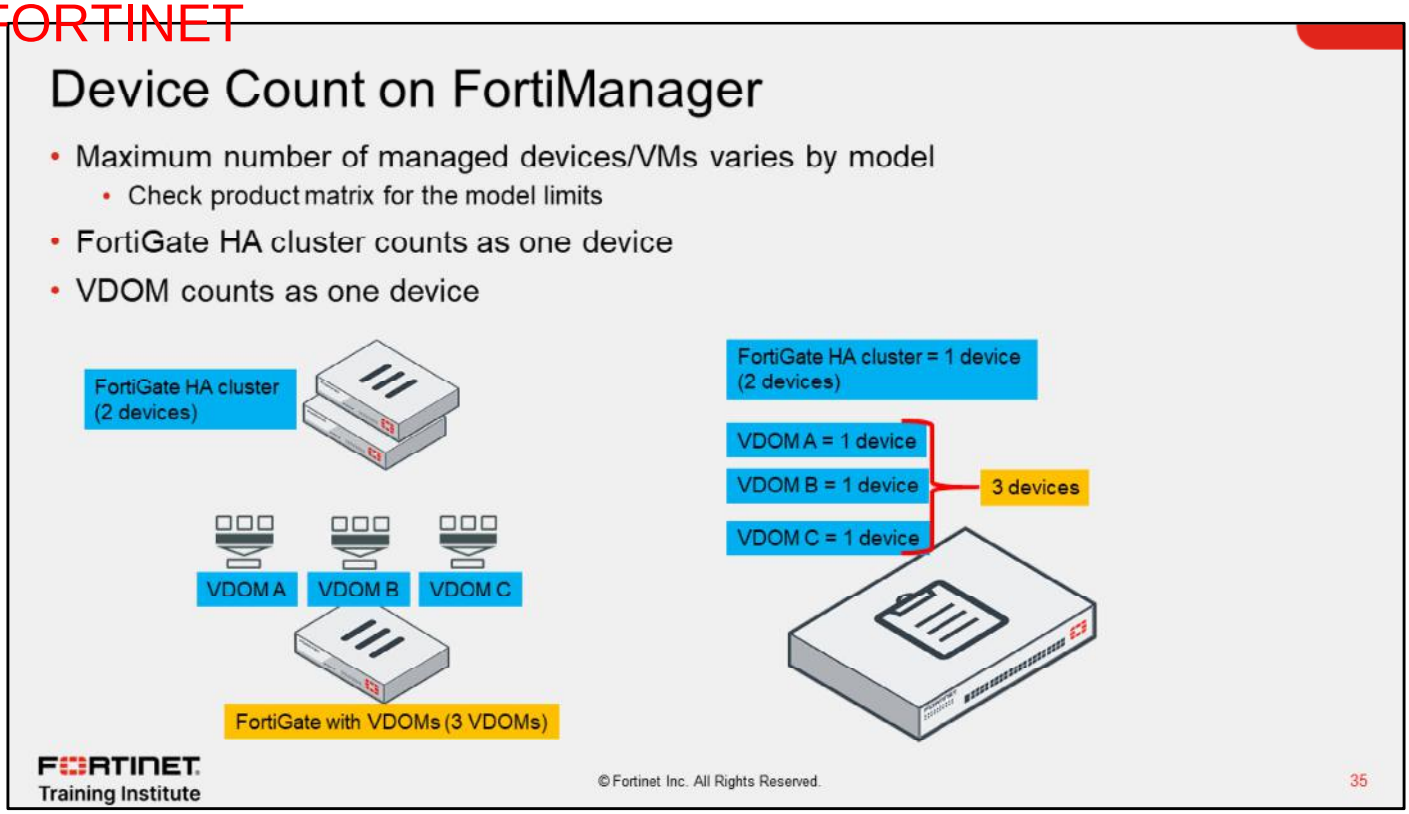


Some FortiManager devices can work with the shelf manager to manage the FortiGate 5000 series chassis. First, you must enable chassis management on the **System Settings** > **Advanced** > **Advanced Settings** pane. After you enable it, you can add the chassis in the default chassis ADOM.

The dashboard for the chassis provides the information related to slot number, slot information, current state of blade, and various other parameters. On the dashboard, you can view or configure information related to the blades, PEM, fan tray, shelf manager, and SAP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiManager physical devices or virtual machine (VM) licenses support a limited number of devices, depending on the device size or license type. A FortiGate high availability (HA) cluster counts as a single device, as does a virtual domain (VDOM). This is because the bulk of the configuration relates to the firewall policies and objects, and a device that is in a cluster does not increase the size of that configuration, because devices in the cluster are running the same configuration. The use of VDOMs increases the size of the configuration.

For example, if there are two FortiGate devices in an HA cluster (active-active or active-passive), both FortiGate devices have the same configuration and are counted as one device. However, enabling a VDOM increases the size of the configuration, because each VDOM is logically a separate firewall.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate HA Cluster

- Managed as a single device
- Use `diagnose dvm device list` to see cluster members
- FortiManager is unaware of the FortiGate HA sync status
- HA per device management interface is for SNMP monitoring only for the secondary FortiGate
- Device serial number is automatically updated when there is a new primary FortiGate
- FortiGate HA configuration is read-only in FortiManager (GUI only)
  - HA failover operations are possible on FortiManager
- Local changes to the FortiGate HA configuration do not cause an out-of-sync state

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

36

A FortiGate HA cluster is managed as a single device from FortiManager, and has a unique ID. You can use the `diagnose dvm device list` command on the CLI to view the device members. FortiManager is unaware of—and will not verify—FortiGate HA synchronization status. The optional, dedicated HA per device management interface is for SNMP monitoring only and must not be used for FGFM management.

FortiGate HA configuration on FortiManager is read-only using the GUI only. It is retrievable and visible, but cannot be modified. FortiGate HA configuration is also not applied to FortiGate during installations. This is to avoid overwriting the HA configuration. However, if FortiGate HA roles have changed, you can force an HA failover using FortiManager. FortiGate configuration changes concerning HA parameters do not modify the checksum (`get system mgmt-csum`) and do not cause an out-of-sync situation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When you link the model device to the real device, what are the two methods you could use?
   A. IP address and serial number
   ✓B. Serial number and preshared key

2. What is the `# diagnose dvm device list` command used for?
   ✓A. To view individual cluster members of the FortiGate HA cluster
   B. To install all the pending device configuration changes using the CLI

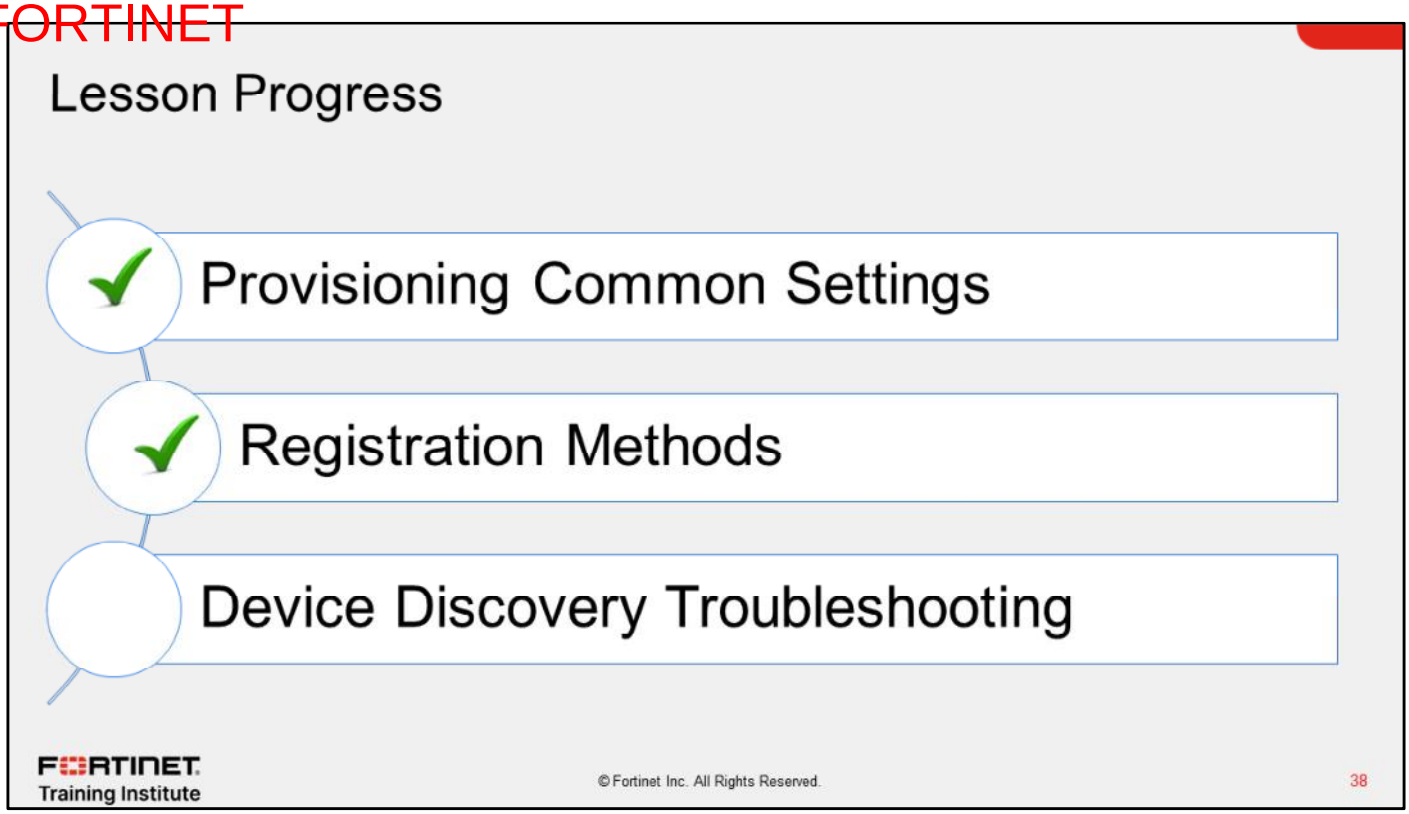
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

37

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

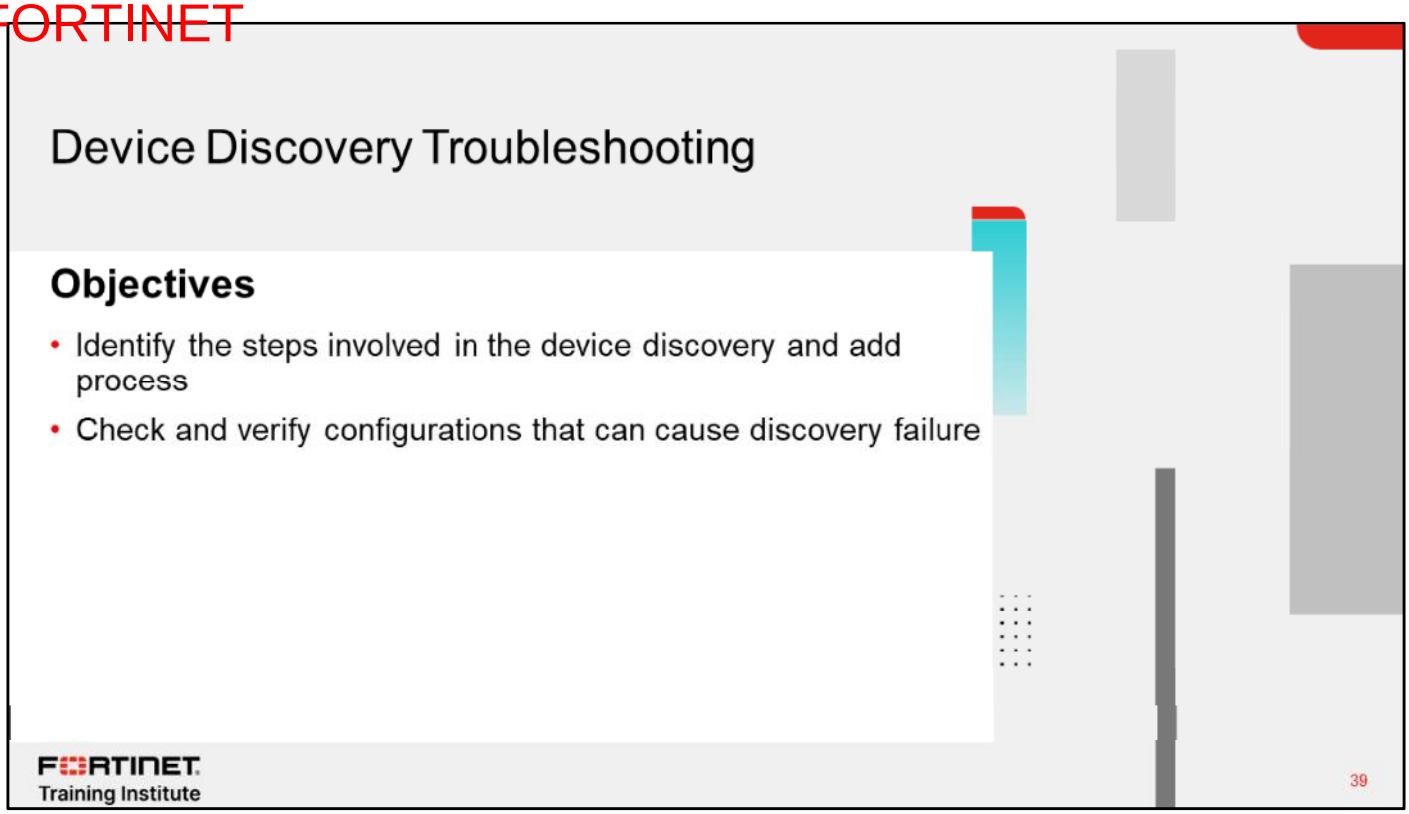


Good job! You now understand registration methods.

Now, you will examine common device discovery issues and how to resolve them.

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 device discovery troubleshooting, you will be able to diagnose and resolve issues related to device discovery.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FGFM Management Protocol

- An FGFM daemon runs on both:
  - FortiGate `fgfmd`
  - FortiManager `fgfmsd`
- Secure communication tunnel using port TCP 541 between:
  - FortiManager and all managed FortiGate devices
  - TCP-based, therefore supports port-based NAT
- Protocol is enabled for each interface on FortiGate (FMG-Access)
- Link-level addresses are used for the management traffic tunneled over the secure connections
- Once FortiGate is managed, the FGFM tunnel is authenticated and established using the serial number verification of the FortiGate in the FGFM tunnel

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

40

The management protocol FGFM runs on both FortiGate (`fgfmd`) and FortiManager (`fgfmsd`). FortiManager and FortiGate create a secure tunnel on port TCP 541. Being TCP-based, the connection works with port-based NAT, which allows both FortiGate and FortiManager to be behind a NAT device. On the FortiGate side, you can enable the **FMG-Access** setting for each interface and for the interface facing FortiManager.

Once you have configured the management tunnel, it can be established in either direction—by FortiManager or the managed FortiGate device. FortiManager reserves link-level addressing using the `169.254.0.0/16` subnet. The `169.254.0.1` IP address is reserved for FortiManager and managed devices are allocated to other IP addresses in the `169.254.0.0/16` range.

A keepalive message is sent from the FortiGate device. The keep-alive message includes the checksum of the FortiGate configuration, which calculates the synchronization status.

FortiGate login credentials are required when discovering the device for the first time or reclaiming the tunnel. The login credentials are to set the serial number. After the login credentials have been entered, the serial number becomes the basis of authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Device Discovery and Add Process

- When FortiGate is added to FortiManager, it goes through two steps:
  1. Discovery
     - Secure tunnel established and a `get system status` is collected to obtain minimal information to start modeling the device
  2. Adding
     - Various other configuration details are obtained through CLI commands and the configuration is retrieved and stored in the device database
- The FGFM tunnel is initiated by either of the following:
  - FortiManager, during add and discovery process
  - FortiGate, if a management request is sent by FortiGate

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

41

There are two steps involved when FortiGate is registering on FortiManager:

1. Discovery: In this step, FortiManager sends a CLI command to obtain the minimum information for FortiGate.
2. Adding: During this step, complete configuration details of FortiGate are obtained by FortiManager and FortiGate configuration is stored in the revision history.

There are two methods to register FortiGate on FortiManager. The secure FGFM tunnel can be initiated by either device: FortiGate or FortiManager.

If the tunnel is initiated by FortiGate, the device is added to the FortiManager unauthorized device list in the root ADOM. At this point, it has not been discovered. The complete discovery and add process starts once the device is promoted to being a authorized device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Device Discovery and Add Process (Contd)

- Commands sent by FortiManager during discovery and add device process

```
get sys status

get system interface
get system interface physical
get hardware status

get mgmt-data status

config system central-management
set type fortimanager
unset serial-number
set serial-number "FMG-VM0A16001583"
set fmg "10.200.1.241"
end
..
get ips rule status
get ips decoder status
get application name status
```

Device discovery

Add process starts here

Command to check hard disk changes on FortiGate

Setting FortiManager serial number

Retrieving IPS signature information

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

42

When FortiManager is discovering and adding FortiGate, it sends commands to FortiGate to get complete information on FortiGate.

You can also run the following CLI command on FortiGate, while discovering and adding it:

```
diagnose debug cli 8
diagnose debug enable
```


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Discovery Failure Checklist

What to Investigate	Common Solutions
Are the devices able to contact each other?	# execute ping
Does the FortiManager administrator have sufficient privileges to add the FortiGate?	Check the FortiManager administrator profile.
Is FortiManager in offline mode? (Can be due to configuration restore.)	Disable offline mode on the **System Settings** pane
Is TCP port 541, between FortiManager and FortiGate, blocked? (Used for communication between FortiGate and FortiManager.)	Use the following command to run packet sniffer on both devices on TCP port 541: `# diagnose sniff packet <interface> <filter> <level>`
Are the IP address and credentials (super_admin access) of the FortiGate correct in the add device wizard?	Confirm the FortiGate IP address and credentials
Is FGFM access on FortiGate interface disabled?	Enable FGFM access on the FortiGate interface facing FortiManager
Is FortiGate already in an unauthorized device list?	Check under the root ADOM or run the CLI `# diagnose dvm device list` If appearing as unauthorized device, add it from root ADOM.
Are the date and time correct on both devices? (Incorrect date or time can result in expired certificates being used in tunnel negotiation between the two devices.)	Check the date and time on both devices
Are incorrect or excessive debug levels set on FortiGate? (May prevent FortiGate from discovery.)	Run the following CLI command on FortiGate to reset the debug levels: `diagnose debug reset`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

43

If you are experiencing communication issues between FortiGate and FortiManager, first ensure that the two devices can reach each other. Use the `execute ping` CLI command from either device to verify that the devices are capable of routing to each other. (Ping must be enabled and allowed by all intermediate firewalls.)

If you are having issues with discovering FortiGate from FortiManager, check the following:

- FortiManager has sufficient administrator privileges. Sufficient privileges are required to add a FortiGate.
- Offline mode is disabled (disabled by default). Enabling offline mode disables the FGFM protocol (TCP port 541) used to communicate with managed devices.
- Packets from FortiGate are reaching FortiManager and packets from FortiManager are reaching FortiGate. Run sniffers on both devices to confirm.
- FortiGate credentials are correct in the **Add Device** wizard.
- FGFM access is enabled on the FortiGate interface facing FortiManager.
- FortiGate is in an unauthorized device list. You can check from the root ADOM on the GUI or from the CLI using the following command:
  `diagnose dvm device list`
- The date and time are synchronized between FortiManager and FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. How do you enable FGFM access on FortiGate?
   - ✓ A. Through FortiGate interfaces
   - B. Through FortiGate adminstrative settings

2. Which FGFM process runs on FortiGate?
   - A. fgfmsd
   - ✓ B. fgfmd

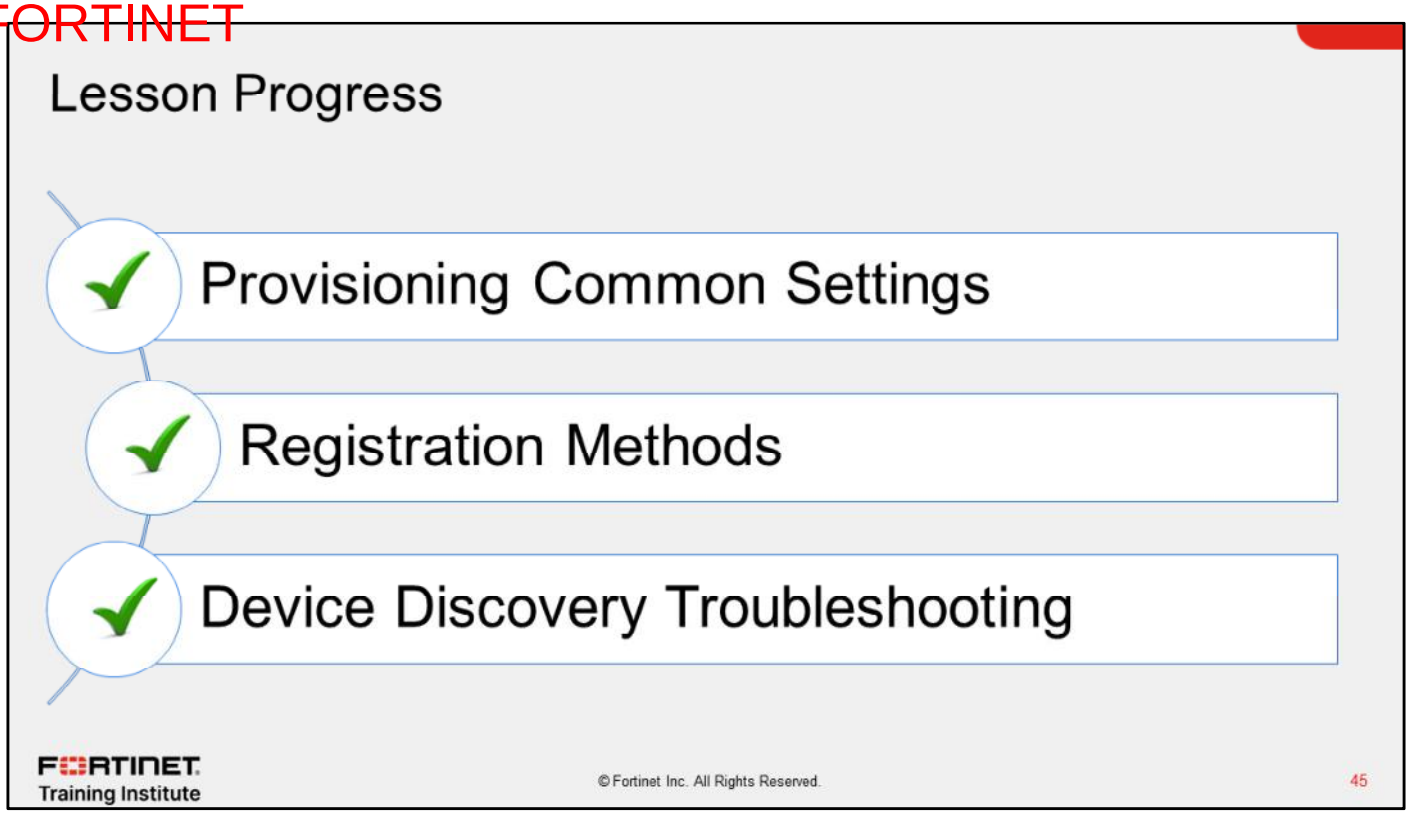
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

44

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

Review

- ✓ Configure and apply provisioning profiles to your managed devices
- ✓ Add FortiGate to FortiManager
- ✓ Understand the import report
- ✓ Add multiple FortiGate devices to FortiManager at the same time
- ✓ Add a chassis to FortiManager
- ✓ Manage a FortiGate HA cluster using FortiManager
- ✓ Troubleshoot device discovery issues

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

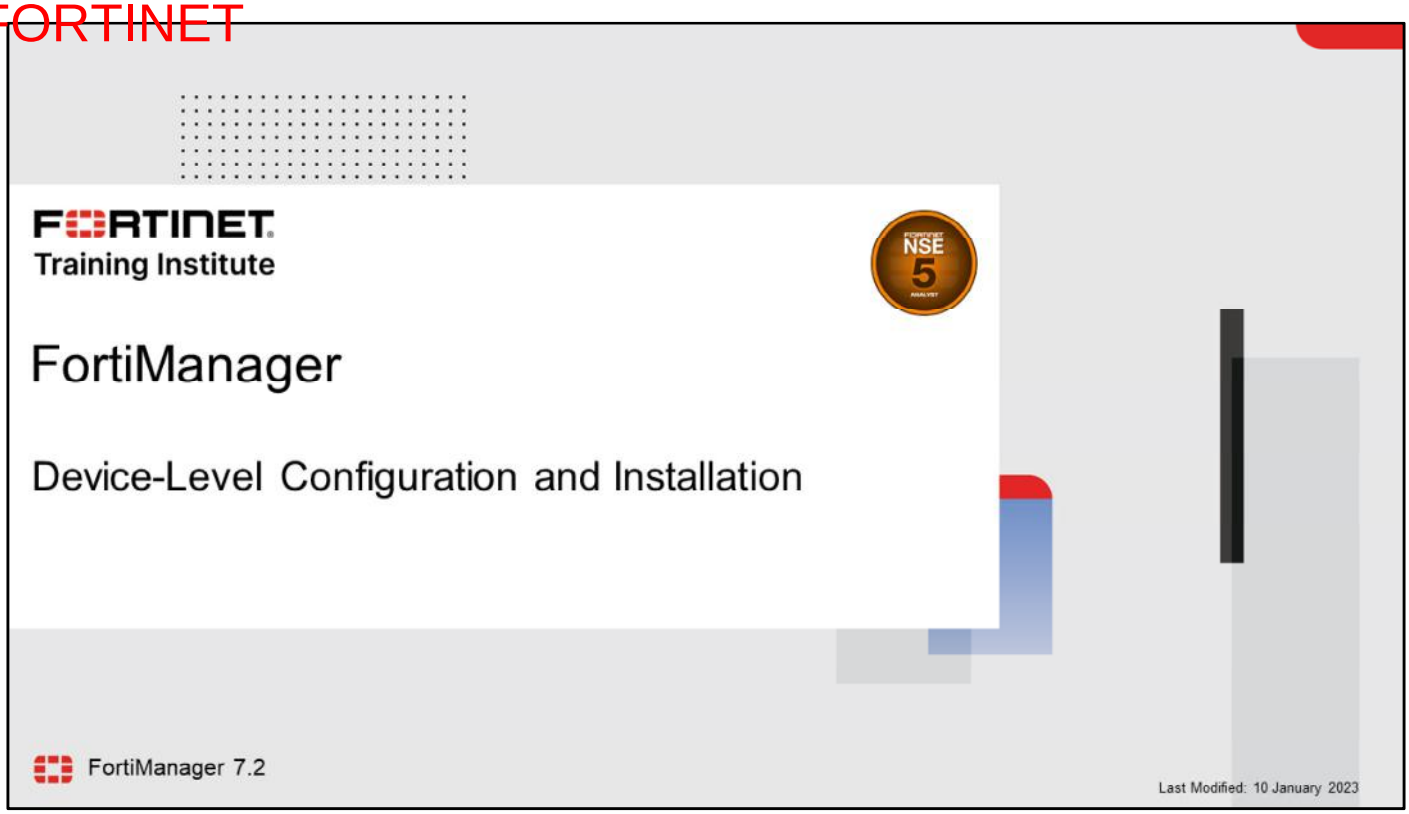
46

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

By mastering the objectives covered in this lesson, you learned about the primary functions of the device manager pane, and how to manage FortiGate using FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to configure device-level changes, understand the status of a managed FortiGate on FortiManager, and install changes to the managed FortiGate devices. You will also learn how to use the revision history for troubleshooting, and you will learn about the capabilities of scripts and device groups.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Device-Level Settings and Managed Device Status
- Installing Configuration Changes
- Revision History
- Scripts and Device Groups

FORTINET Training Institute

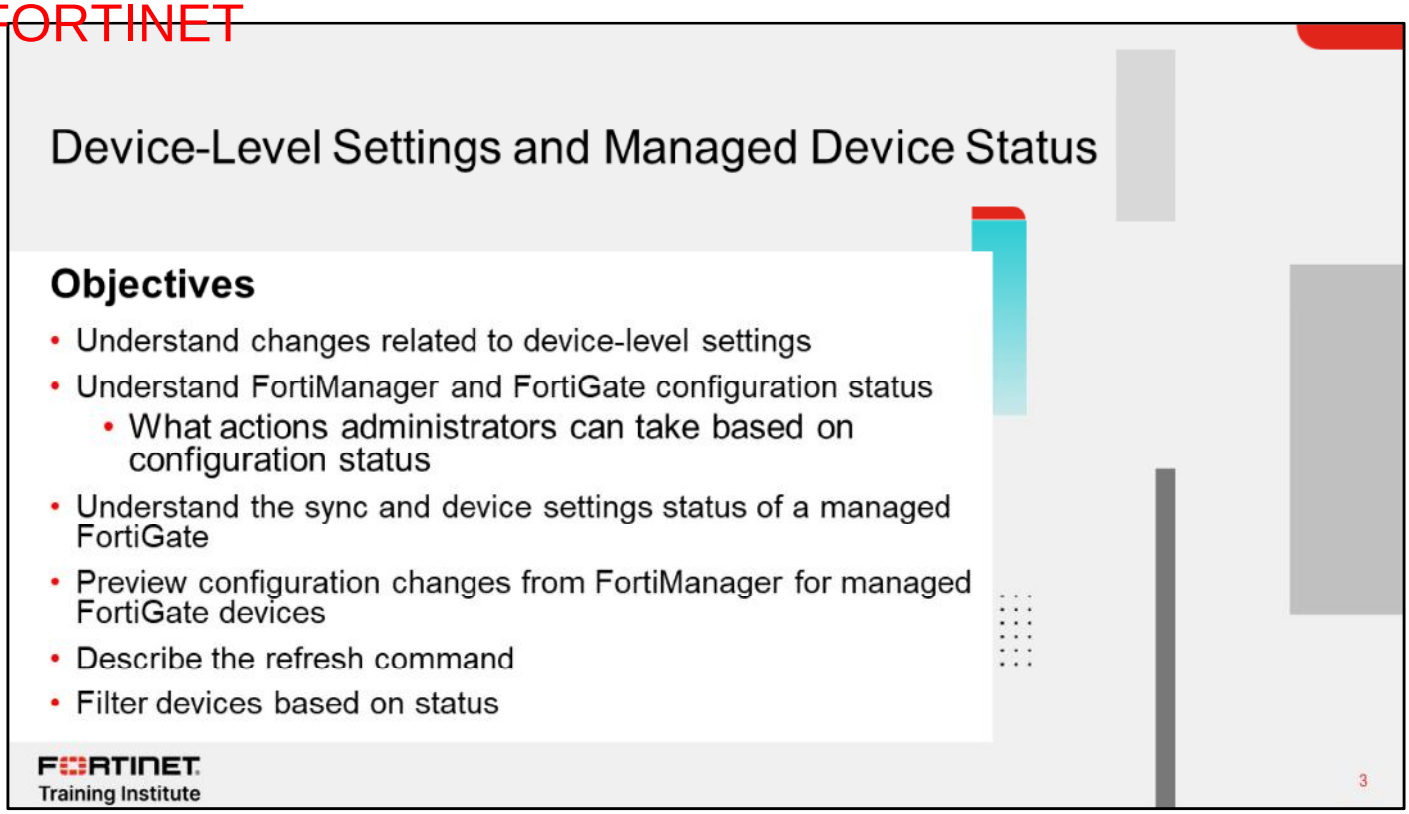
© Fortinet Inc. All Rights Reserved.

2

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

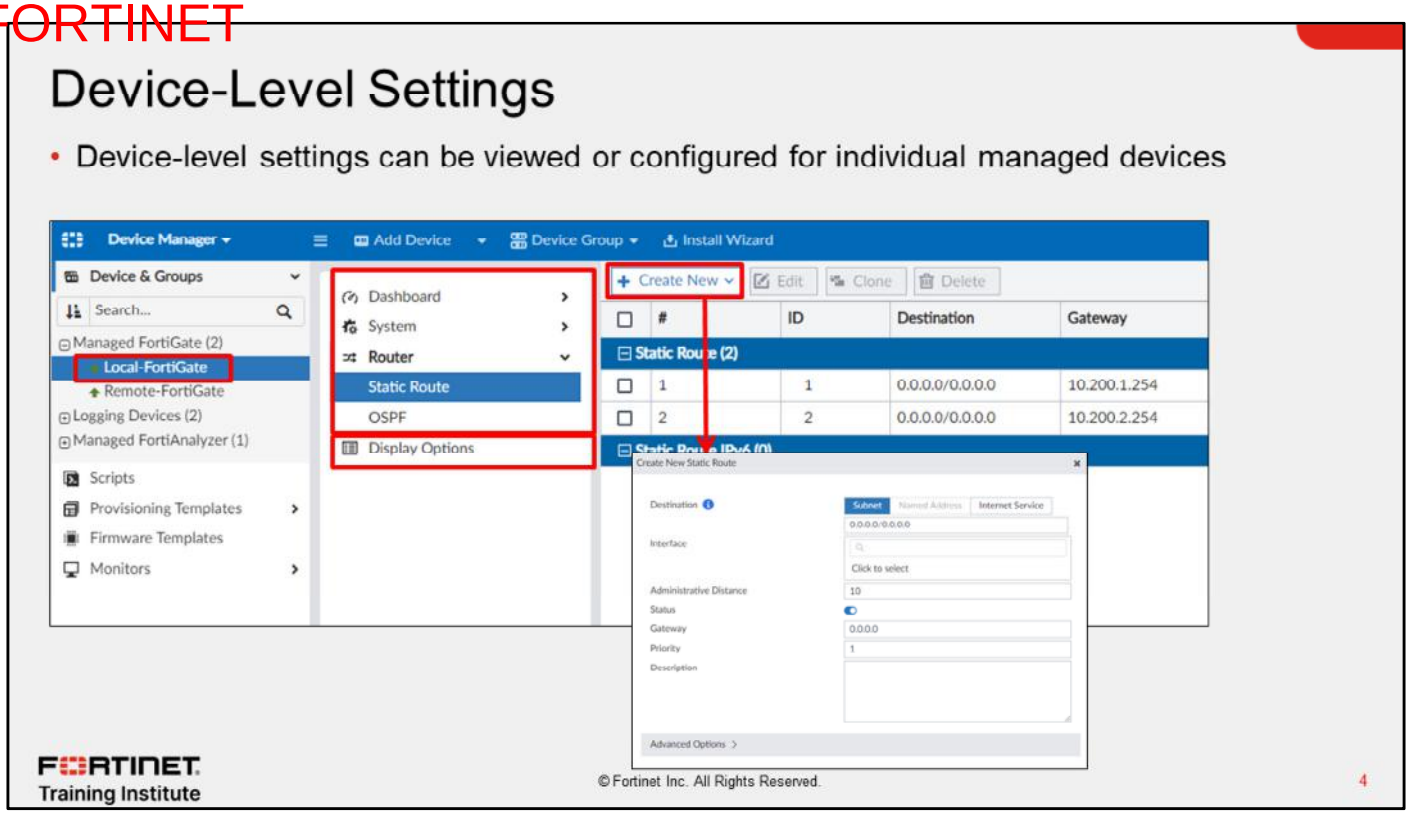


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding FortiGate configuration status and synchronization behavior, you will be able to diagnose and take action based on the status of FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To configure registered devices, select the device or VDOM in the **Device Manager**. In this example, the FortiGate device named **Local** is selected.

The device-level settings of a managed FortiGate can be viewed and configured from the toolbar at the top of the **Dashboard**. You can view or configure interfaces, HA, DNS, and so on. To configure or view routes, select the **Router** tab.

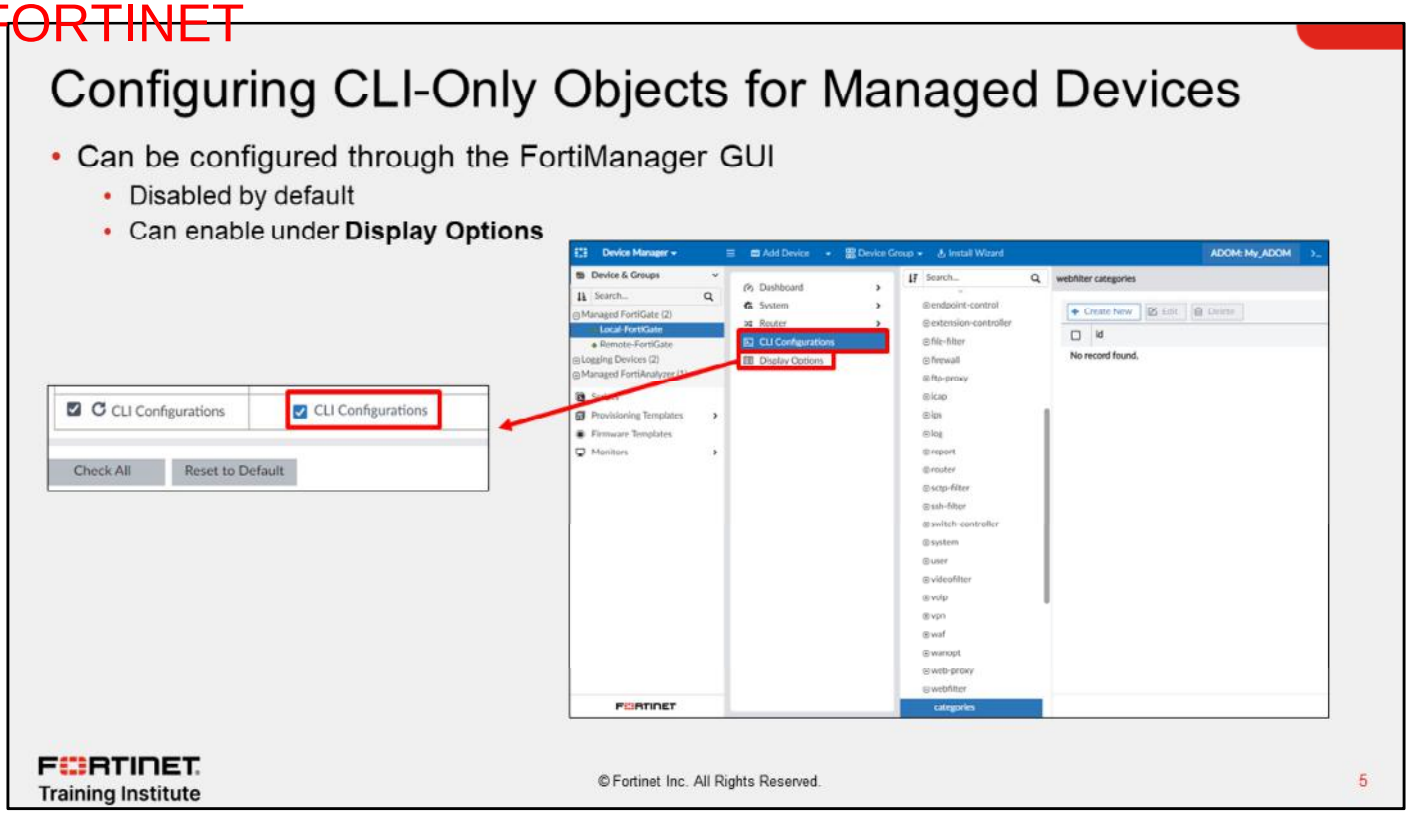
In this example, a new static route is created.

Most of the settings that you see in this example have a one-to-one correlation with the device configuration that you would see if you logged in locally using the FortiGate GUI or CLI.

Note that there are only a few options in the toolbar (**Dashboard** and **Router**). You can click **Display Options** to customize device tabs at the device level.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



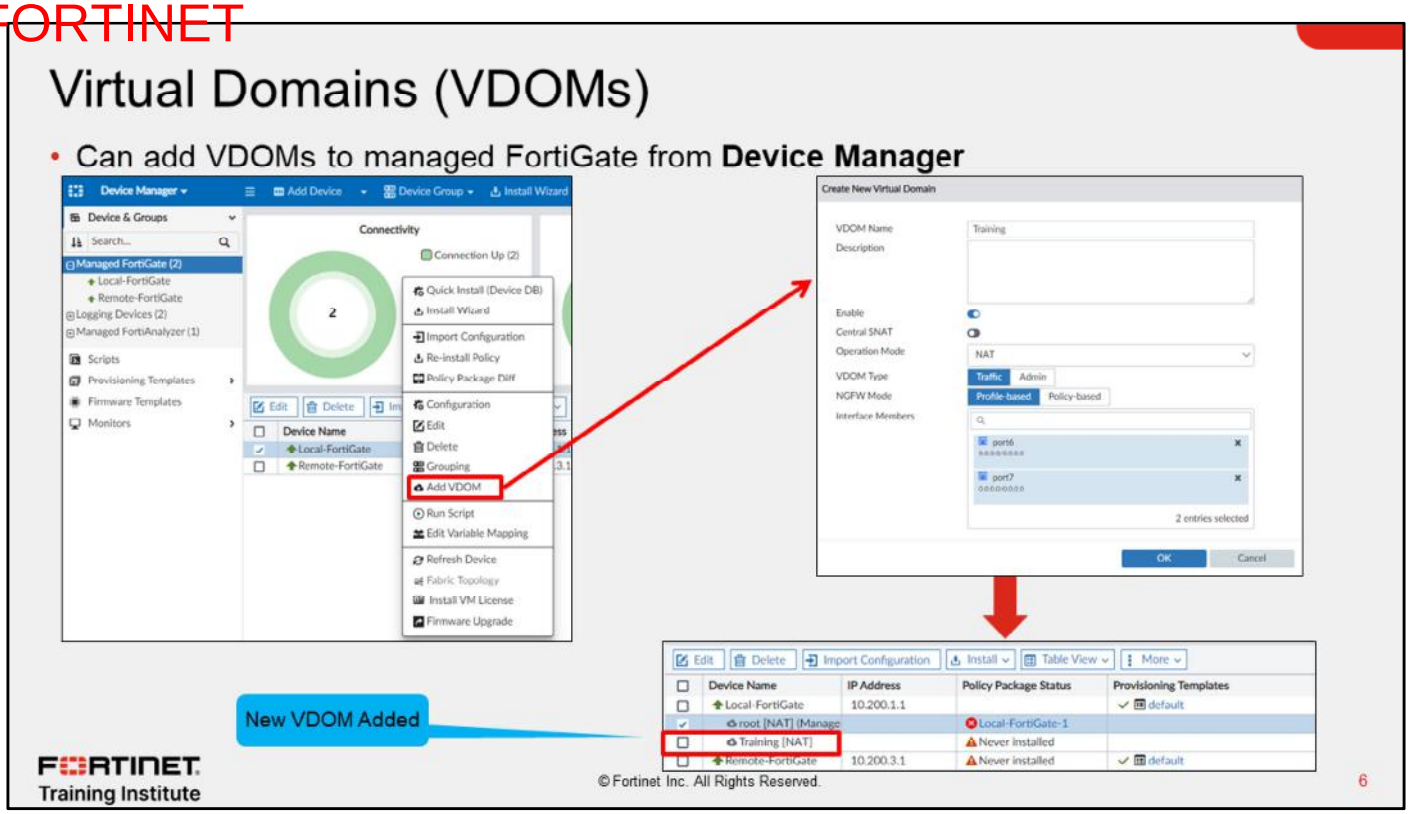
The **CLI-Only Objects** menu allows you to configure device settings that are normally available and configured only through the FortiGate CLI.

Note that the available options vary according to device, supported features, and firmware version. Hidden by default, this menu can be enabled in **Display Options**.

The **CLI-Only Objects** menu is available in the **Device Manager** and **Policy & Objects** panes.

Vouchers & Dumps are Available | WhatsApp +201224560923

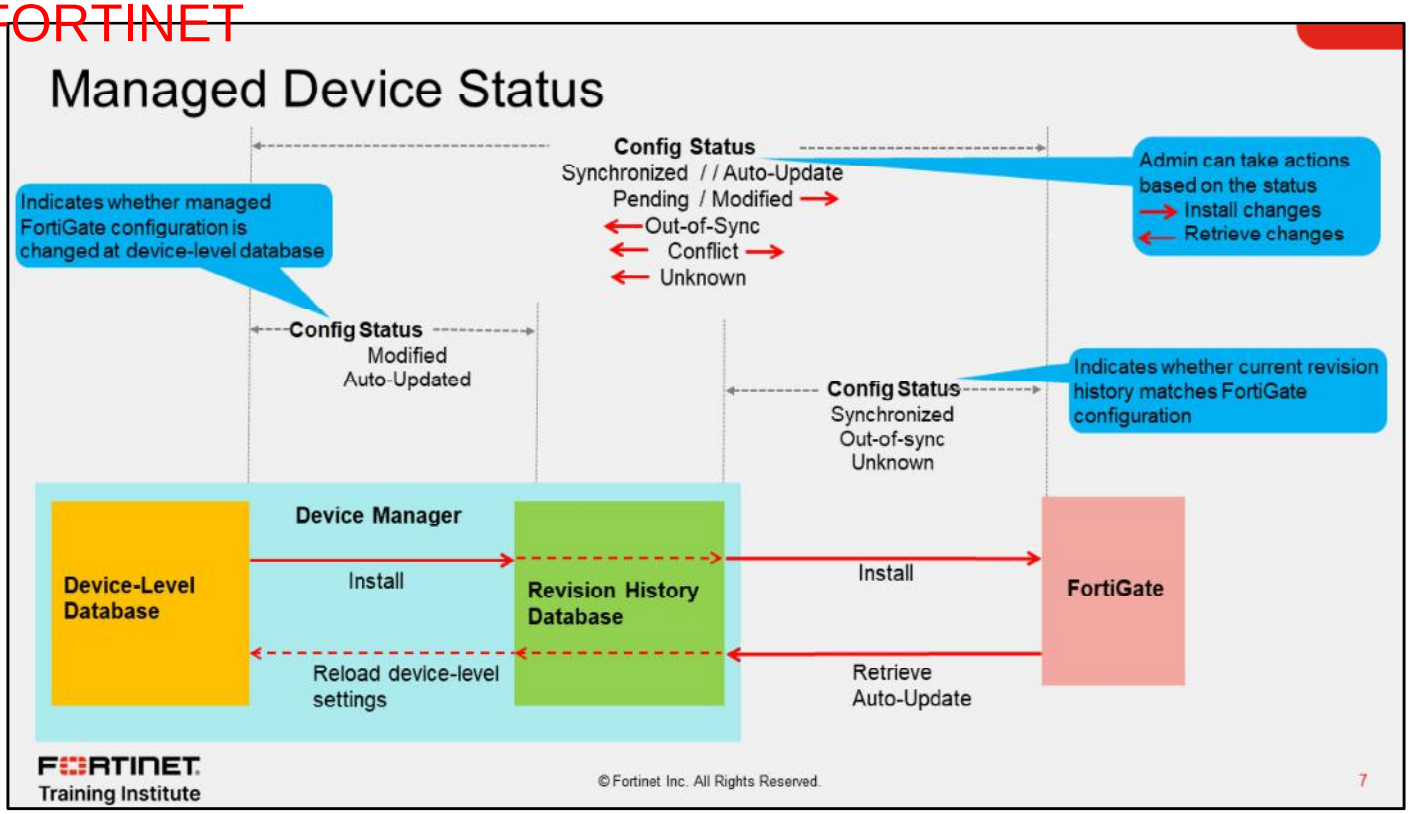
DO NOT REPRINT Brave-dumps.com
© FORTINET



You can add a VDOM to the managed device from the **Device Manager** pane. Adding a VDOM is a configuration change, so you need to install these changes on the managed device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



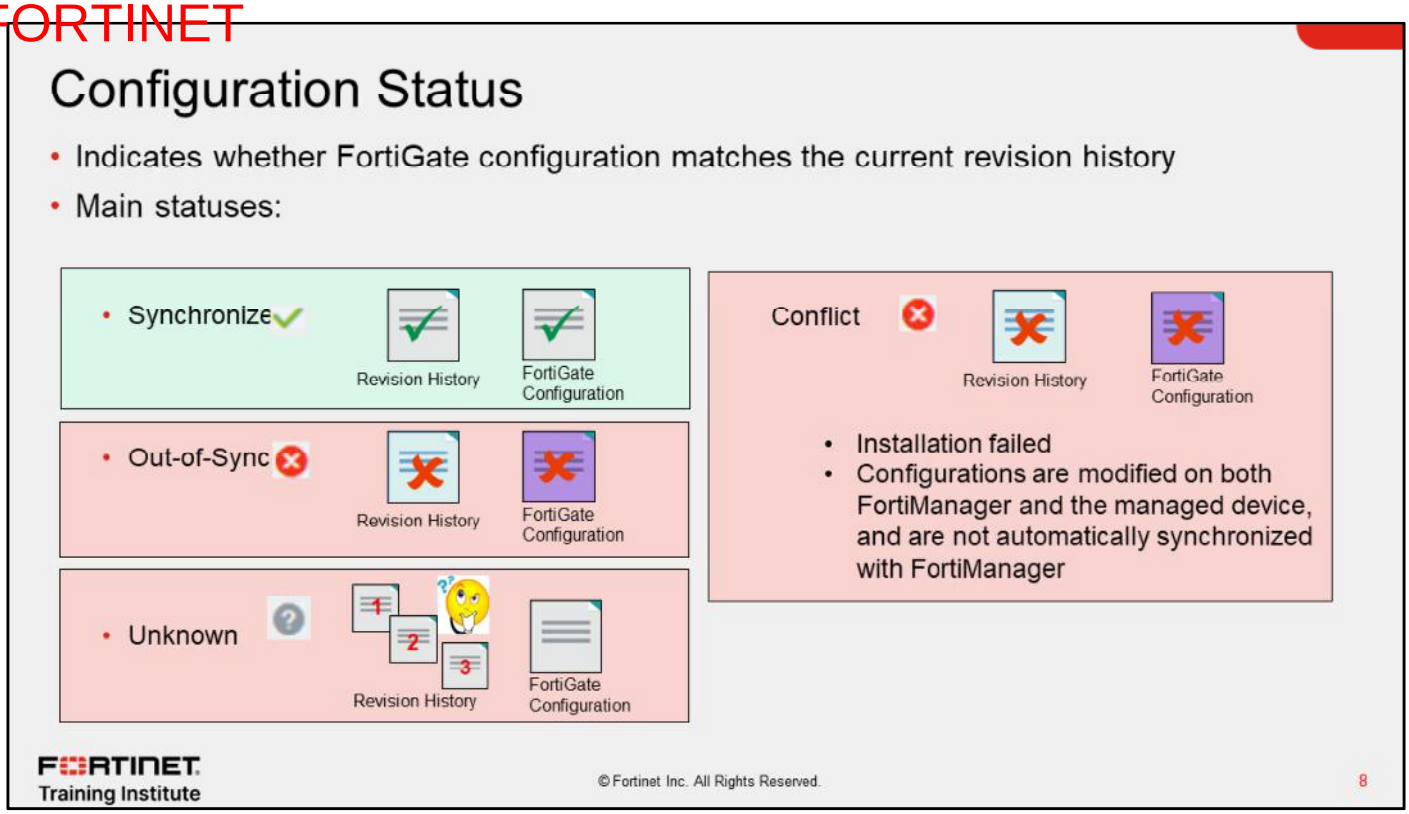
This diagram shows the status of a managed FortiGate. FortiManager keeps FortiGate configurations in the revision history. The latest revision history is compared with the FortiGate configuration to provide the configuration statuses. The latest revision history is also compared with the device-level database of the FortiGate, which indicates if FortiGate configuration has changed on the FortiManager.

Knowing the overall configuration status of a managed device helps the administrator identify issues and take appropriate actions from FortiManager:

- **Synchronized / Auto-Update**: The latest revision history configuration entry (whether an install, retrieve, or auto-update) is aligned with the configuration on FortiGate.
- **Modified**: Configurations are modified on FortiManager and not synchronized between FortiManager and the managed device.
- **Out-of-Sync**: The latest revision history configuration entry does not match the configuration on the FortiGate due to configuration changes made locally on FortiGate or a previous partial install failure. It is recommended that you perform a retrieve from the FortiManager.
- **Conflict**: If the changes are made locally on the FortiGate and are not retrieved, but changes are also made from FortiManager, the status goes in conflict state. Depending on the configuration changes, you can either retrieve the configuration or install the changes from FortiManager. The Conflict status can also indicate a failed installation.
- **Unknown**: The FortiManager is unable to determine the synchronization status because the FortiGate is not reachable, or due to a partial install failure. It is recommended that you perform a retrieve from the FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

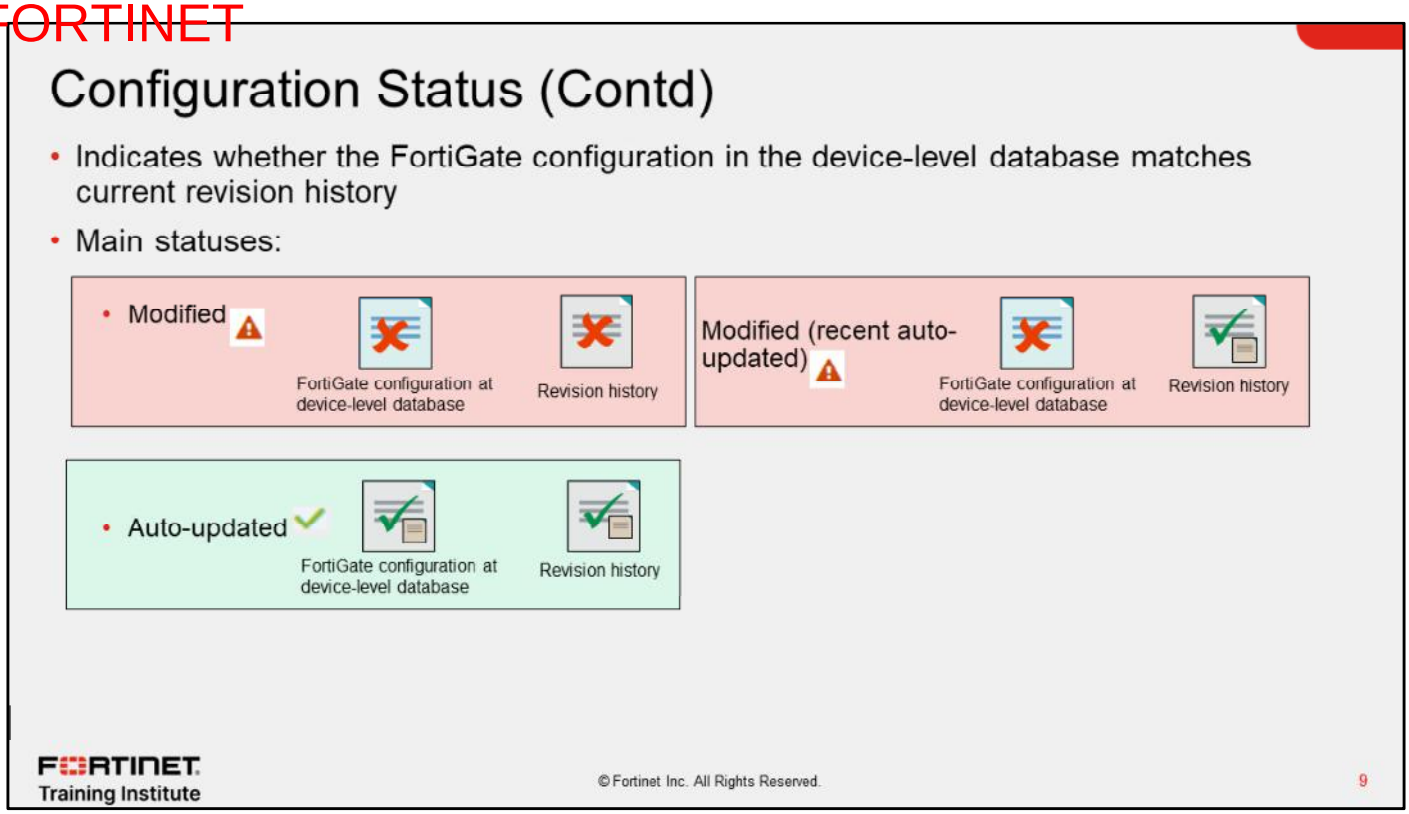


On the **Device Manager** pane, click a managed FortiGate to select it and view its dashboard. You can see the **Config Status** field under the **Configuration and Installation** widget.
The **Config Status** compares the running device configuration with the current version in the revision history. There are few possible sync statuses:

- **Synchronized**: The current revision history configuration entry (whether an install or retrieve) is synchronized with the running configuration on the FortiGate.
- **Out-of-Sync**: The current revision history configuration entry does not match the running configuration on the FortiGate. It can be caused by failed installation or direct changes made on FortiGate that were not auto-updated.
- **Unknown**: The FortiManager system is unable to detect which revision (in the revision history) is currently running on the device due to a connection issue. The Unknown status can also indicate that you added a model device, which does not generate a revision.
- **Conflict**: When install failed or configuration are modified on both FortiManager and the managed device, and not automatically synchronized with FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

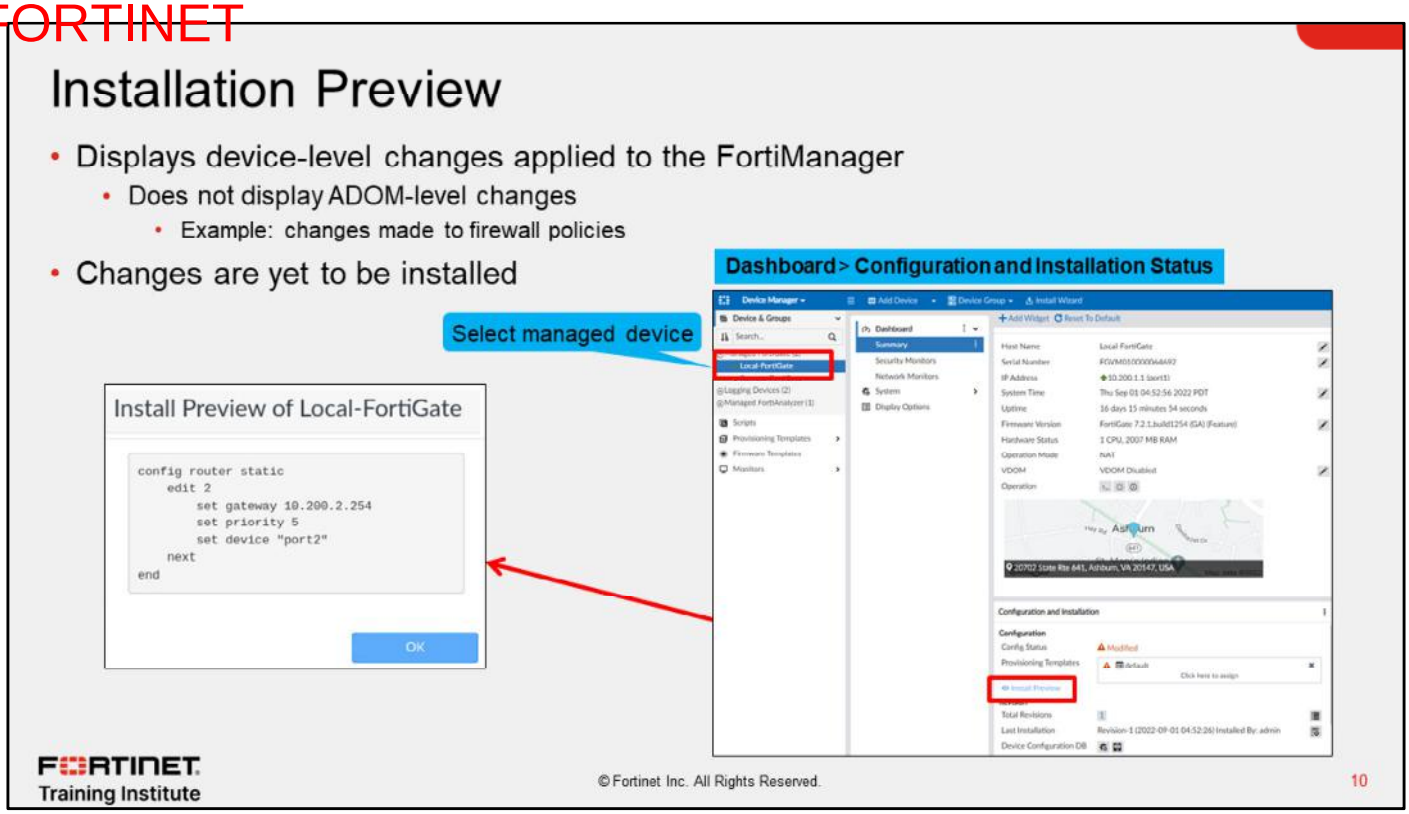


The **Config Status** indicates the status of the device settings on FortiManager. There are three configuration statuses:

- **Modified**: If the device is configured from the **Device Manager**, the device database is changed and the device settings status is tagged as **Modified**, because it doesn't match the running configuration or latest revision history for that device. If changes are installed, it puts the device back into the synchronized state.
- **Auto-Updated**: The configuration changes are made directly on FortiGate and the device database is updated automatically.
- **Modified (recent auto-updated)**: Configurations are modified on FortiManager and configurations modified on the managed device are automatically synchronized with FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Under the **Configuration and Installation** widget, click **Install Preview** to view the changes made to the device database on FortiManager. These are the exact commands that will be installed on this FortiGate when the next install is performed.

Previously, we configured a new static route. That is why the **Config Status** is tagged as **Modified**. In this example, the static route configuration will be pushed to FortiGate on the next install.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Device List

- diagnose dvm device list
  - Provides details of all managed and unregistered devices
  - Each FortiGate configuration is stored in its own device-level database
    - This is represented by an object ID (OID)

Object ID is used to reference the managed device for various CLI commands

HA: Blank if in standalone mode, otherwise FGT HA mode is displayed

FortiGate connecting IP address

Name of the ADOM

Firmware version running on FortiGate

```
FMG-VM64# diagnose dvm device list
--- There are currently 2 devices/vdoms managed ---
TYPE     OID     SN        HA        IP          NAME            ADOM      IPS        FIRMWARE
fmg      270     FGVM01..  -    10.200.1.1  Local-FortiGate     root    6.0..  7.0 MR2 (1254)
faz-managed                                                              (extended)
        |- STATUS: dev-db: modified; conf: in sync; cond: modified; dm: autoupdated; conn: up

        |- vdom:[3]root flags:0 adom:root pkg:[imported]Local-FortiGate_root
```

FORTINET Training Institute

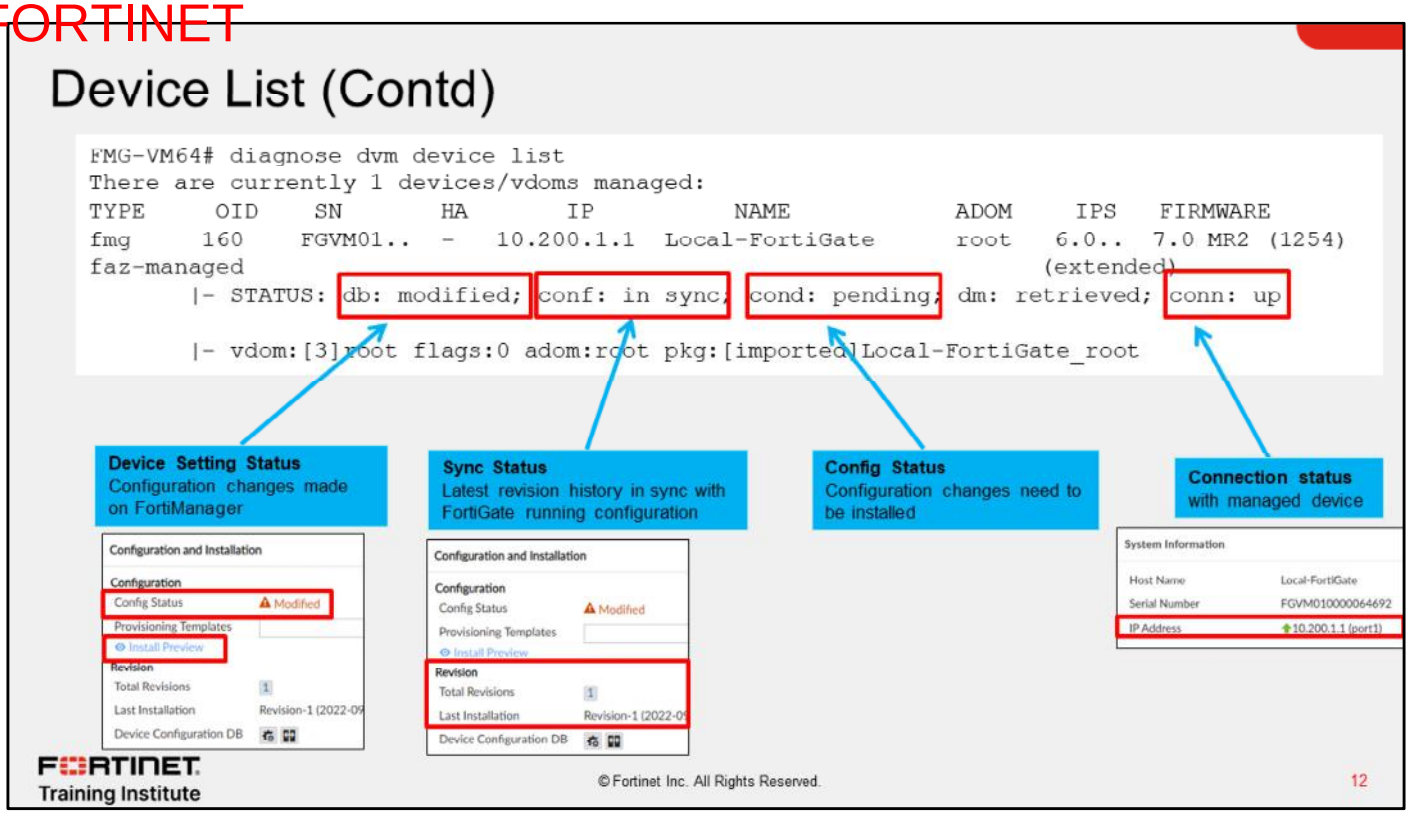
© Fortinet Inc. All Rights Reserved.

11

The `diagnose dvm device list command` provides the list of all devices or VDOMs for managed and unregistered devices. It also provides information, such as serial number, connecting IP, firmware, HA mode, and status for device-level settings and policy packages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The example on this slide shows that the FortiGate configuration is in sync with the latest running revision history. However, changes have been made to the device-level settings. That is why the CLI output is showing `db:modified` and the `cond` is showing as `pending`. After you install the changes on FortiGate, it will show `db: not modified` and `cond:OK`.

You can also check whether the FGFM tunnel between FortiGate and FortiManager is up or down.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

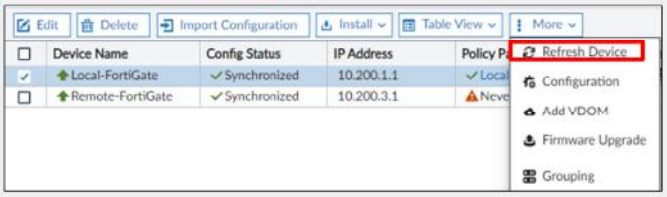
FGFM Session List and Refresh Connection

- Lists the status of FGFM tunnels for all managed devices
  - Connecting IP address
  - Uptime
  - Link-level addresses

```
# diagnose fgfm session-list
  Session count = 1
  Local-FortiGate(270) sn(FGVM010000064692) ip(10.200.1.1)
  state(3) tunnel(169.254.0.7) uptime:Mon Aug 29 13:12:04 2022
```

- Re-establish the connection using the Refresh button
  - Recovers basic information about the managed device

More > Refresh Device



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

You can use the `diagnose fgfm session-list` command to verify the FGFM tunnel uptime between FortiManager and FortiGate devices, display the connecting IP addresses of all managed devices, and show the link-level addresses assigned by FortiManager to FortiGate devices for management traffic.

When you refresh a device, you attempt to establish the connection between the selected device and FortiManager. This operation retrieves basic information about the managed device, such as serial number, firmware version, support contracts, and FortiGate HA cluster member information.

You can refresh the connection by clicking the **Refresh** icon in the **Connection Summary** widget, or by selecting the device in the **Device Manager** and then selecting **Refresh Device** from the **More** drop-down list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. How does FortiManager determine if the configuration status of a managed device is **Out-of-Sync**?
   - ✓A. It compares the current revision history with the FortiGate configuration
   - B. It compares the device-level database with the FortiGate configuration
2. What does **Config Status Modified** indicate?
   - A. Configuration changes made directly on FortiGate are automatically updated on FortiManager and tagged as **Modified**
   - ✓B. Device-level configuration changes are made on FortiManager for the managed device

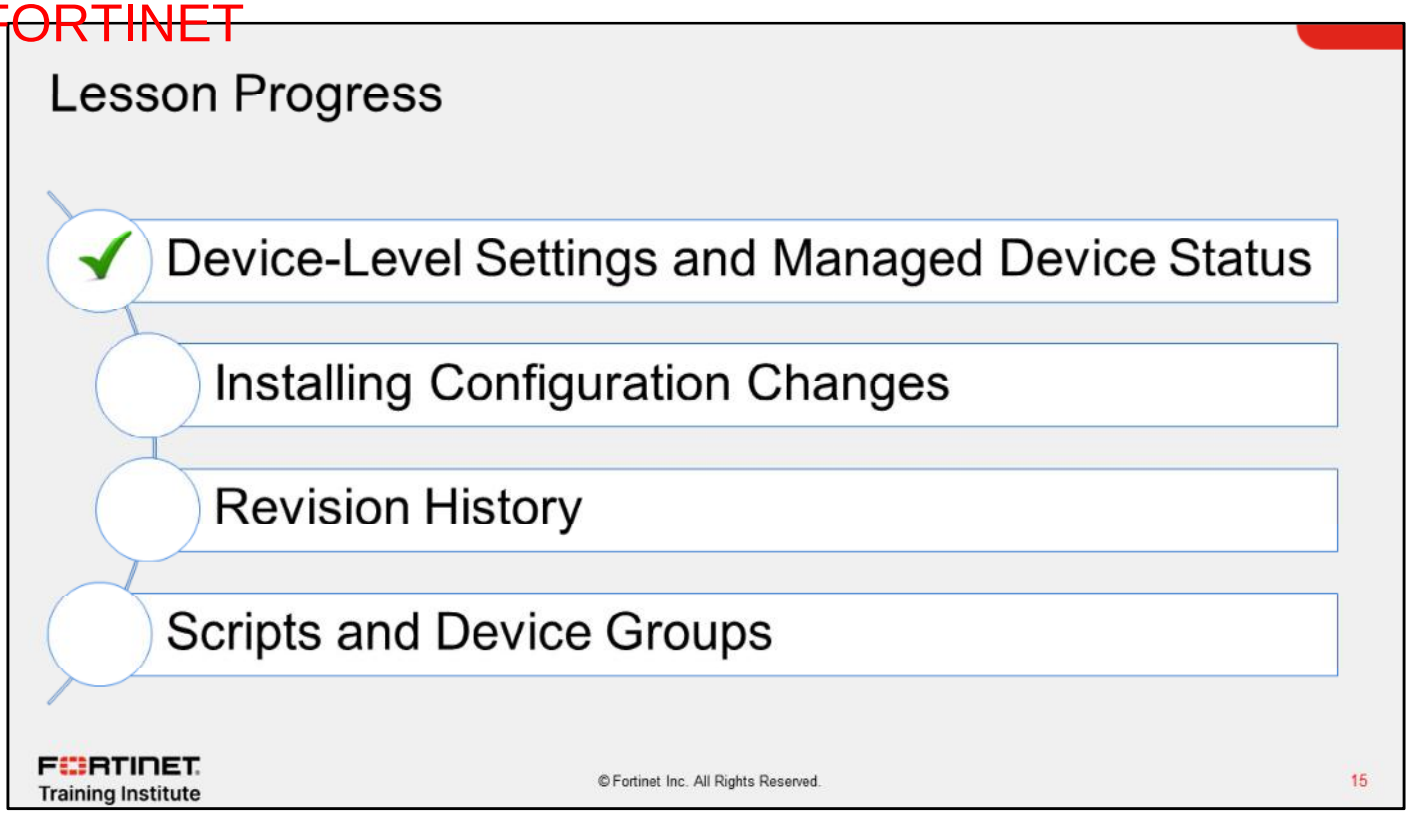
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

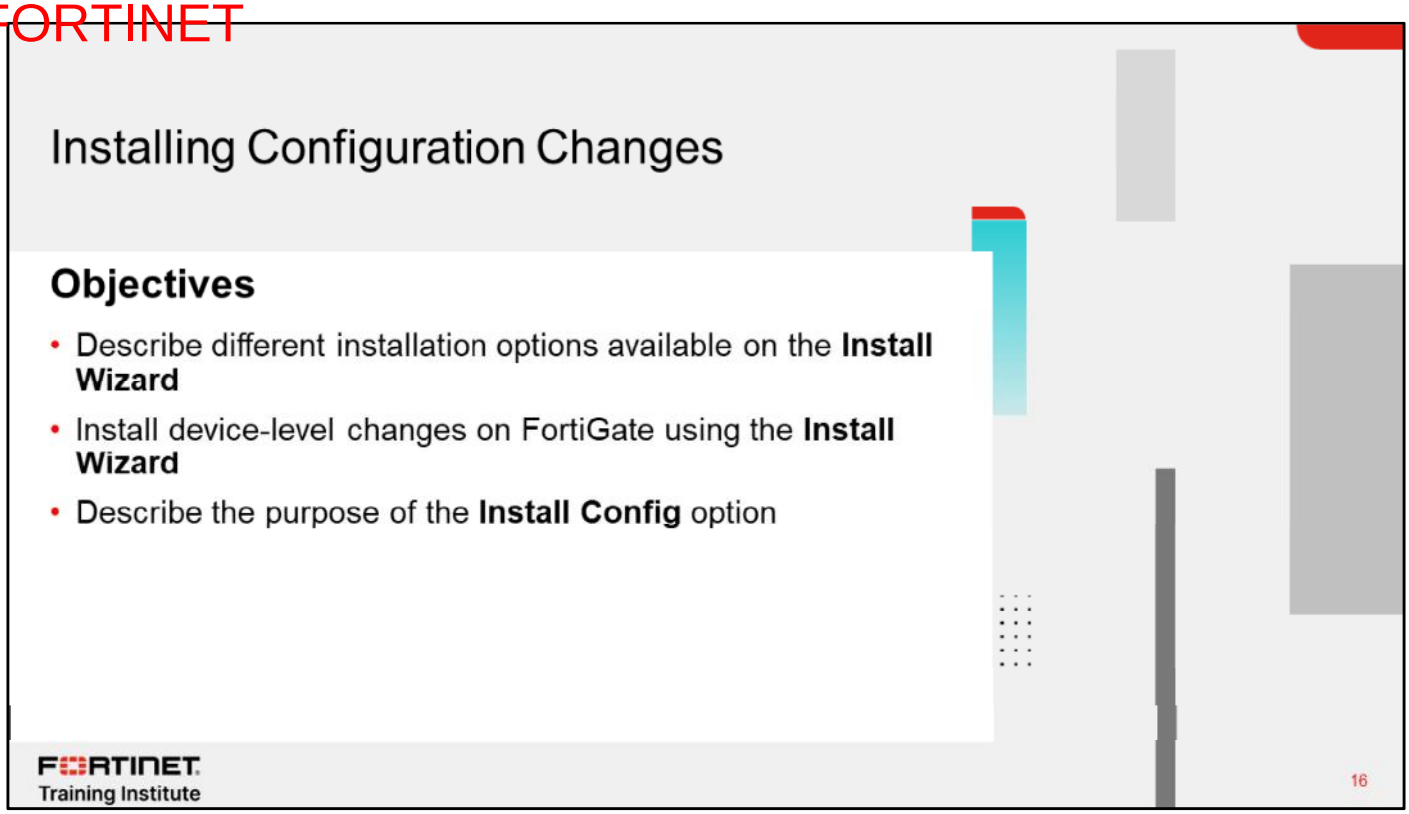


Good job! You now understand the device-level settings and status of the managed device on FortiManager.

Now, you will learn how to install configuration changes from FortiManager.

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.

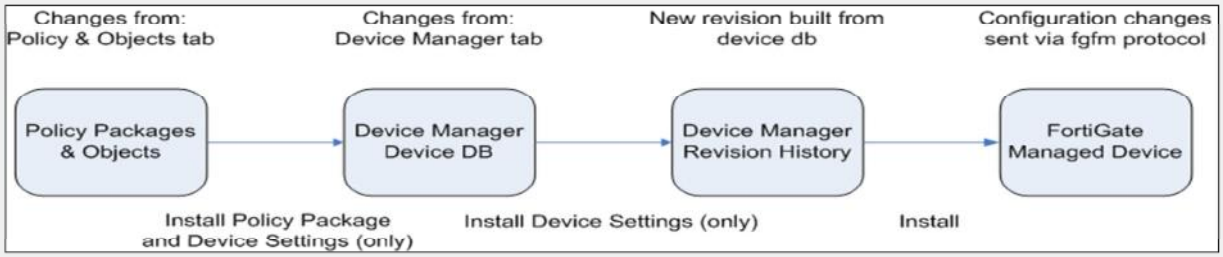
By demonstrating competence in installing configuration changes, you will successfully make changes to managed devices through FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Installation Process

- Changes made from the **Device Manager** pane are made to the device database
  - A new revision is generated and the changes are installed
- Changes from the **Policy & Object** pane are made to the device database



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

This diagram illustrates the installation process that pushes changes from the **Device Manager** pane to a device. For completeness, the **Policy & Objects** pane is also included in this illustration.

When a new configuration is installed, FortiManager compares the latest revision history running on the device with the changes made on FortiManager. FortiManager then creates a new revision in the revision history and installs these changes on the managed device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

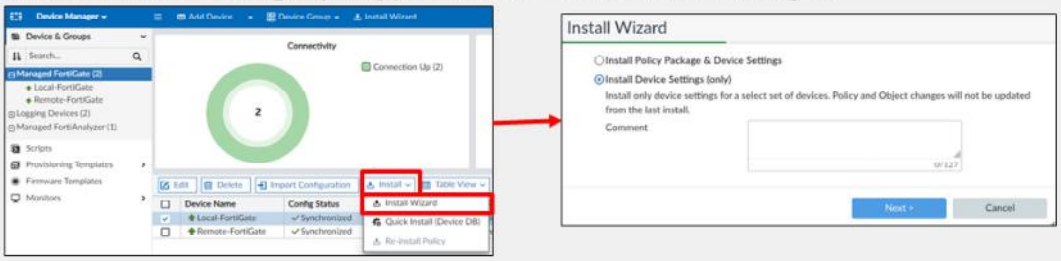
Install Wizard

- Installs settings on one or more FortiGate devices
- Two options in **Install Wizard**

Install Device Settings (only)
- Install only device settings for a select set of devices
- Policy and object changes are not installed

Install Policy Package & Device Settings
- Install a selected policy package
- Any device-specific settings for devices associated with the package are also installed

- Launch the **Install Wizard** from **Device Manager**
- Select **Install Device Settings (only)** to install device-level changes



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

The installation process involves the FortiManager **Install Wizard**. Configuration changes made from the **Device Manager** do not take immediate effect—they have to be *installed*. Until they are installed, the **Device Setting Status** remains as **Modified**.

During installation, you are asked to choose between two different installation types.

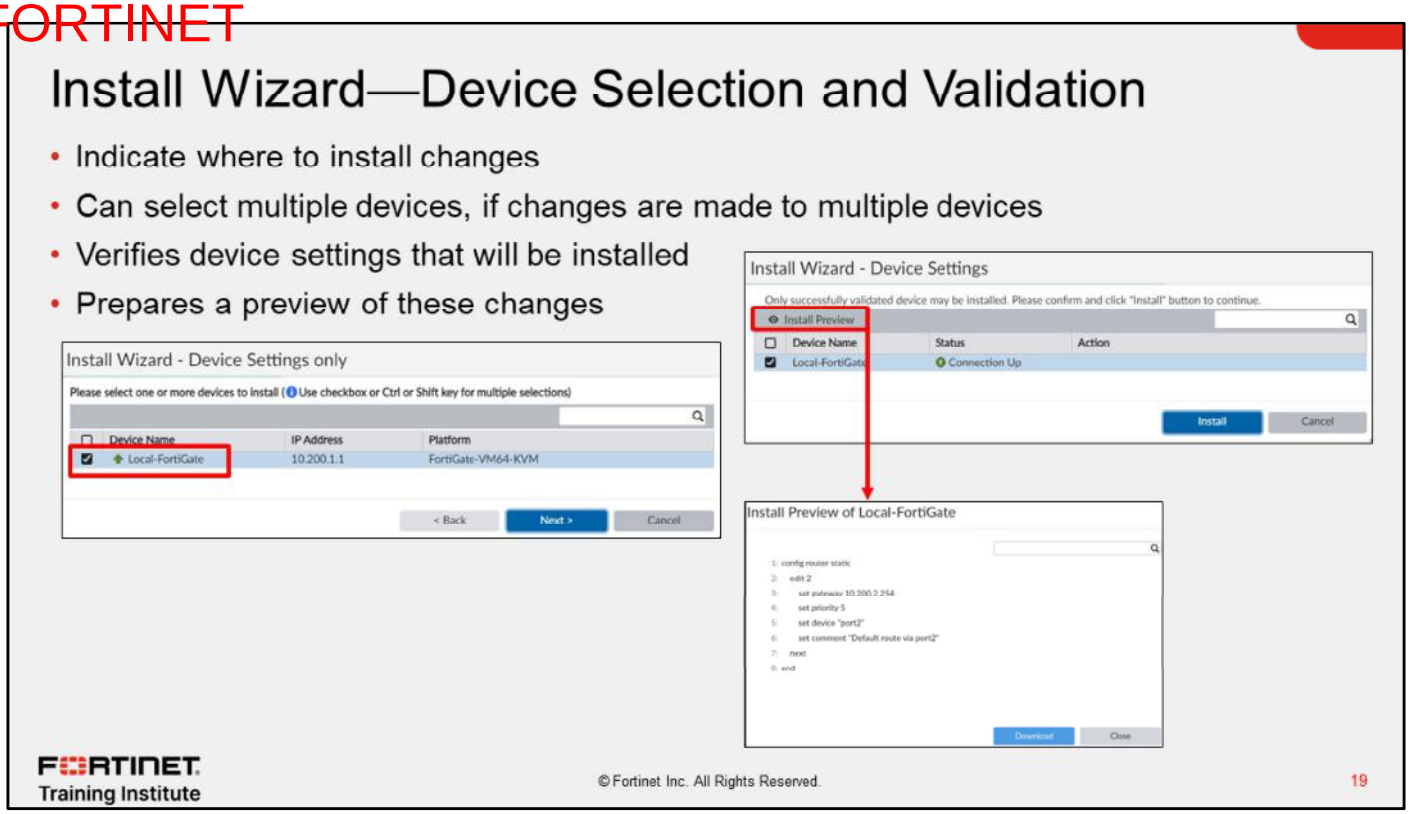
If you choose **Install Device Settings (only)**, the wizard installs only device-level configuration changes made from FortiManager. If you have made changes to the device-level configuration and policies in the policy packages, you can choose **Install Policy Package & Device Settings**, which installs policy package changes and any device-specific settings.

To launch the install wizard, click **Install Wizard** on the toolbar, or click In**stall** and choose **Install Wizard**.

When the **Install Wizard** opens, you need to choose which option you want to use to install your settings. In this example, we select **Install Device Settings (only)**. This option installs only the configuration changes that are related to device-level settings. Because we previously added a new route to the managed FortiGate, the **Config Status** is showing as **Modified**. During this installation process, the device configuration items are installed on the managed device. Once complete, the FortiManager and FortiGate are in sync, and the **Config Status** changes from **Modified** to **Synchronized**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In the next step, you need to select the device you want to install the changes on. If you've made device-level changes to multiple devices under the **Device Manager**, you can select multiple devices on which to install those changes.

The next step is validation. The **Install Wizard** checks the device settings and compares them with the latest running revision history.

Click **Install Preview** to view the configuration changes that will be installed on the managed FortiGate. You can download the preview by clicking **Download**. The file is saved in a .txt format.

As a best practice, you should always preview and verify the changes that will be committed to FortiGate. In the case of a conflict, you can cancel the installation. Then, you can review and correct the conflicting configuration under **Device Manager** and relaunch the **Install Wizard**.

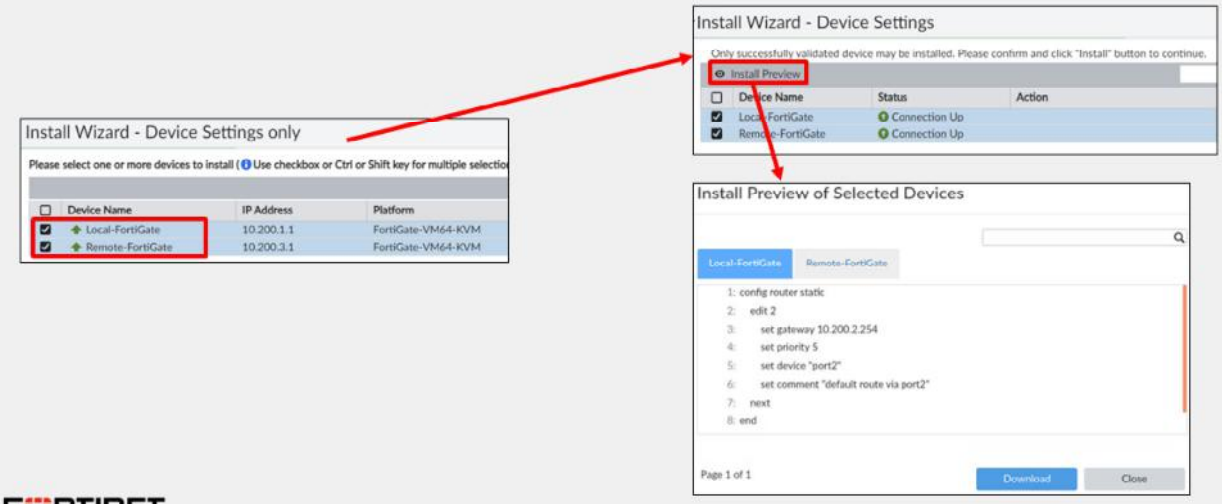
In the example shown on this slide, a new static route has been added.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Install Wizard—Multiple Device Selection and Preview

- Can select multiple devices, if changes are made to multiple devices
- Consolidated install preview for up to 10 devices



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

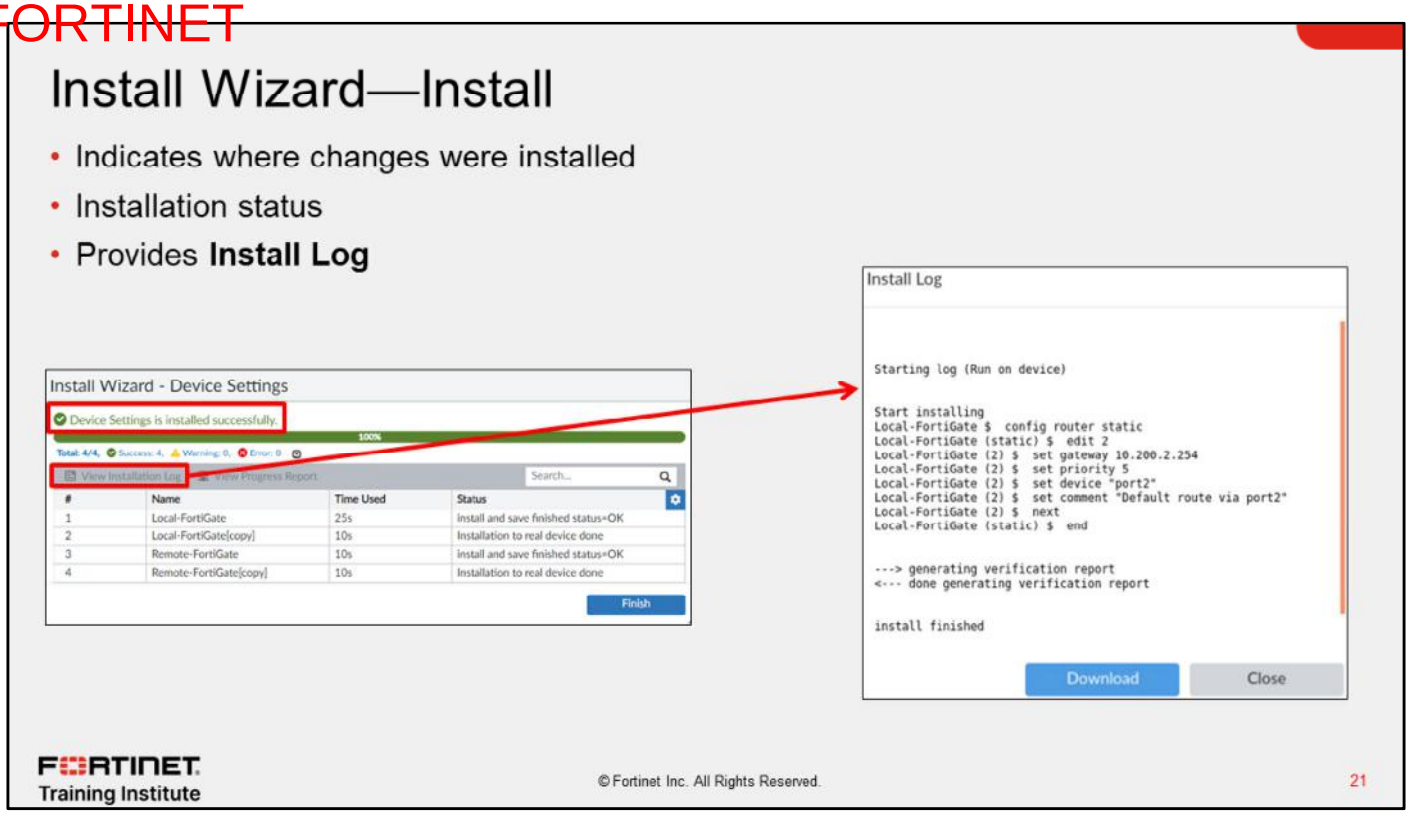
20

You can now preview device settings and policy packages on up to 10 devices when using the **Install Wizard**. Multiple device selection is available in the **Device Manager** and **Policy & Objects** tiles.

In the example shown on this slide, you can see a preview for both selected FortiGate devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



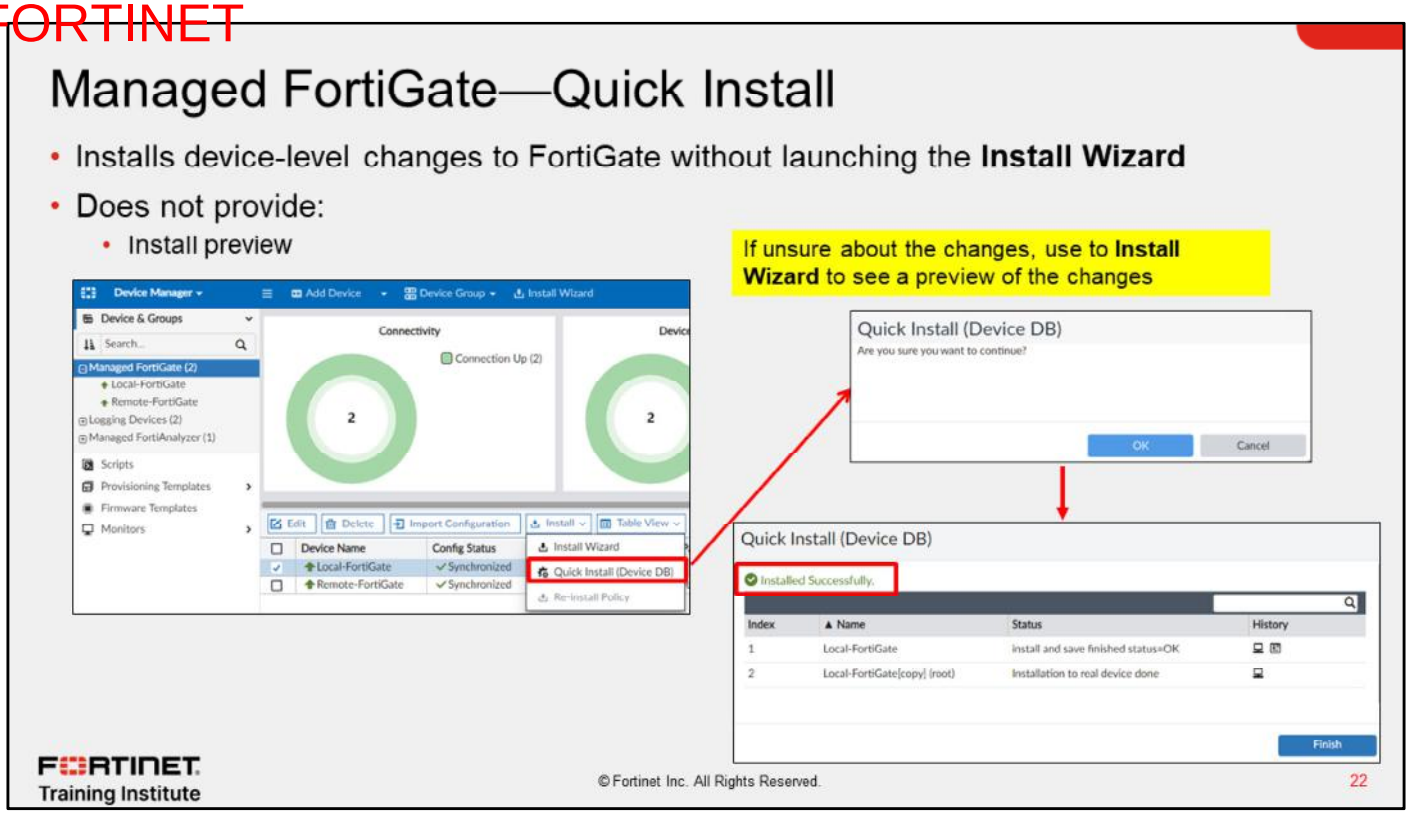
The final step performed using the **Install Wizard** is the installation. After the installation is complete, you can view the **Install Log** to see the list of devices on which the configuration changes were installed.

The log also shows any errors or warnings that occurred during the installation process. Click **View Installation Log** to view the configuration changes installed on the managed FortiGate. If the installation fails, the install log provides an indication of the stage where the failure occurred.

In the example shown on this slide, the installation was successful and FortiManager created a new revision history for the installation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Quick Install** option allows you to perform a quick installation of device-level settings without launching the **Install Wizard**. When you use this option, you cannot preview the changes prior to committing. Administrators should be certain of the changes before using this install option, because the install can't be cancelled after the process is initiated.

If unsure about the changes, administrators are encouraged to use the **Install Wizard**, so that they can preview the changes before committing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which option should you select when installing policy package changes?
   A. Install **Device Settings only**
   ✓ B. Install **Policy Package and Device Settings**

2. Which installation option allows you to preview all the changes before the installation?
   ✓ A. The **Install Wizard**
   B. The **Quick Install**

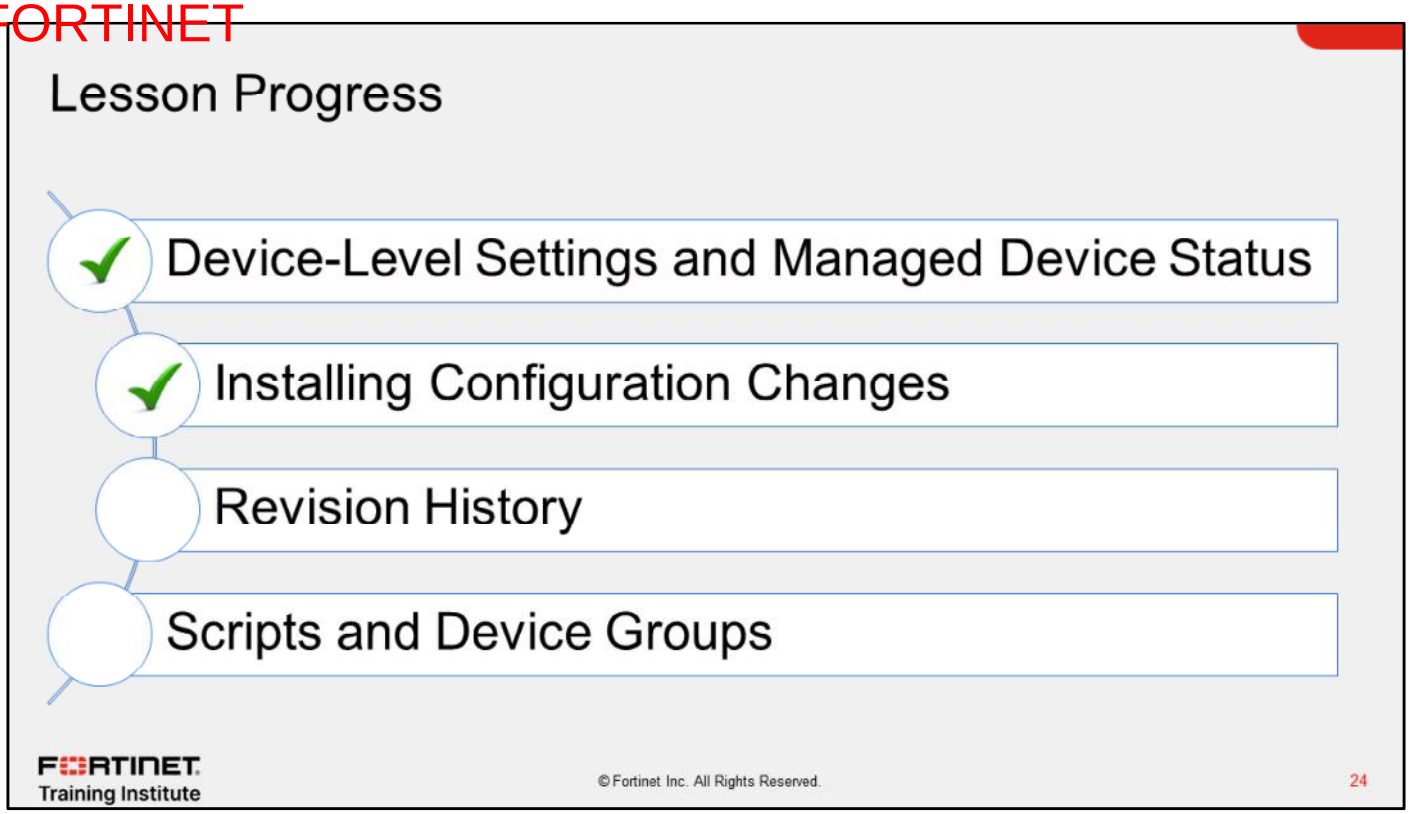
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

23

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

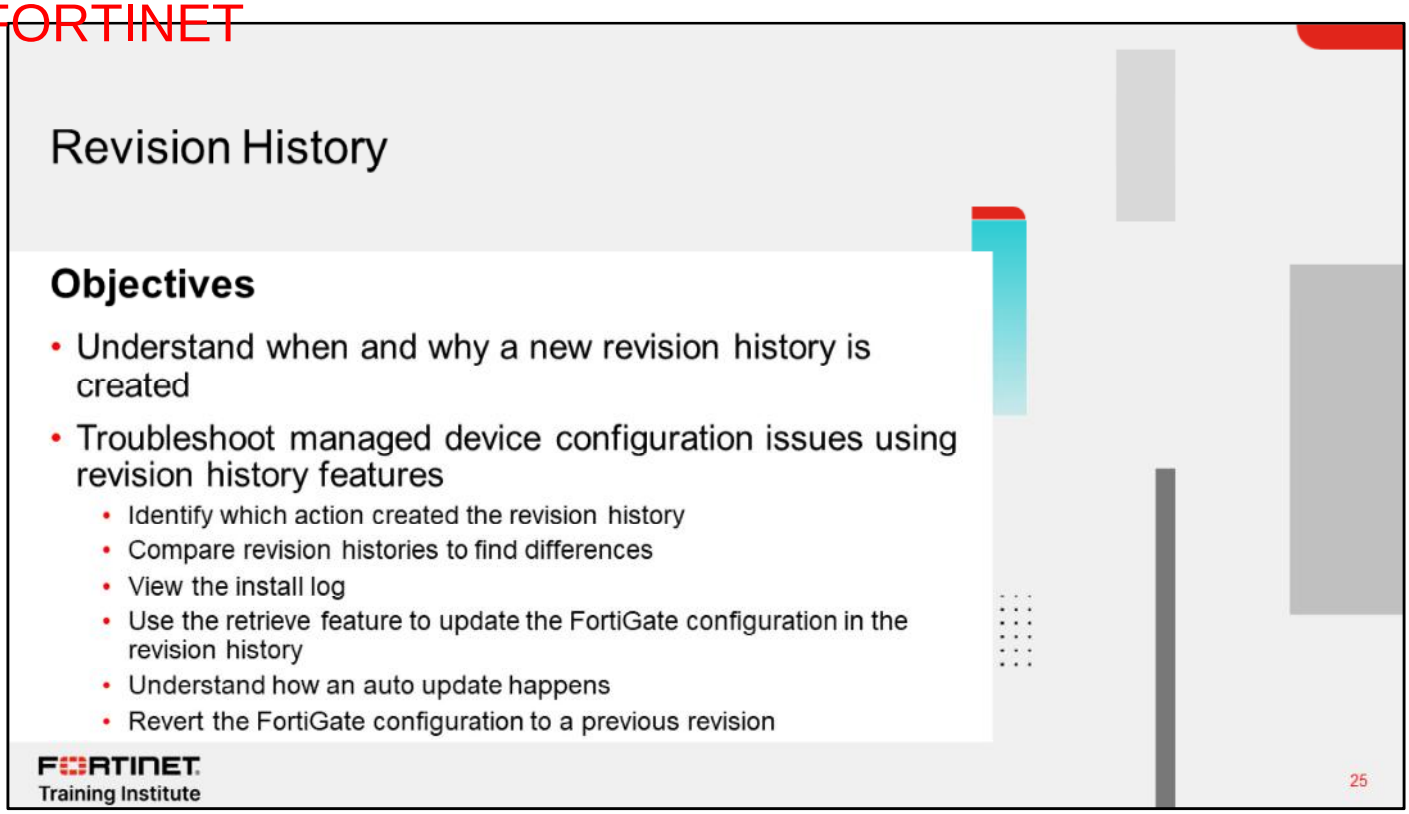


Good job! You now understand the steps involved in installing device-level configuration changes.

Now, you will learn about the revision history repository for the managed FortiGate on FortiManager.

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 using revision history features, you will be able to diagnose and troubleshoot common issues related to FortiGate configuration changes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Conditions for Revision History and Troubleshooting

- FortiManager creates a revision history when:
  - FortiGate is added to FortiManager
  - Device changes are installed
  - FortiGate configuration is retrieved from FortiManager
  - A local change on FortiGate causes an automatic update
    - Scripts run directly on remote devices also cause automatic updates and create a revision history
  - You revert to a previous revision and install the changes
- How to check managed FortiGate configuration issues:
  - View and download FortiGate configuration revision
    - Compare differences between revisions
  - View who made the changes
  - View what has been installed on the managed device

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

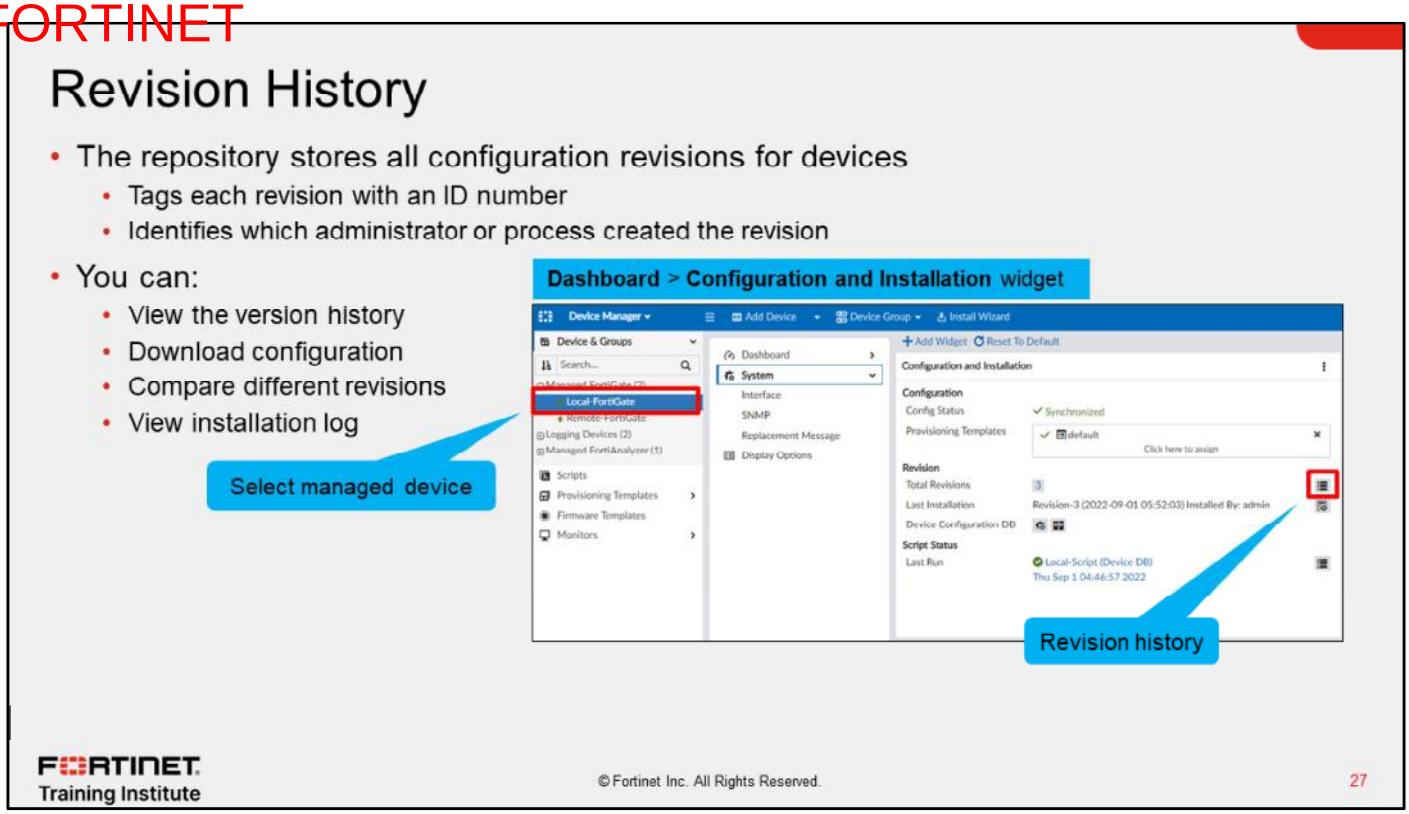
A revision history is created by many different operations, such as adding a device, installing changes, retrieving a configuration, or the occurrence of an automatic update.

FortiManager maintains a repository of the configuration revisions made to managed devices.

This allows the FortiManager administrator to view and download the configuration revisions for a managed device, inspect configuration changes between configuration revisions, view installation history, and view which administrator or process created the new configuration revision.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



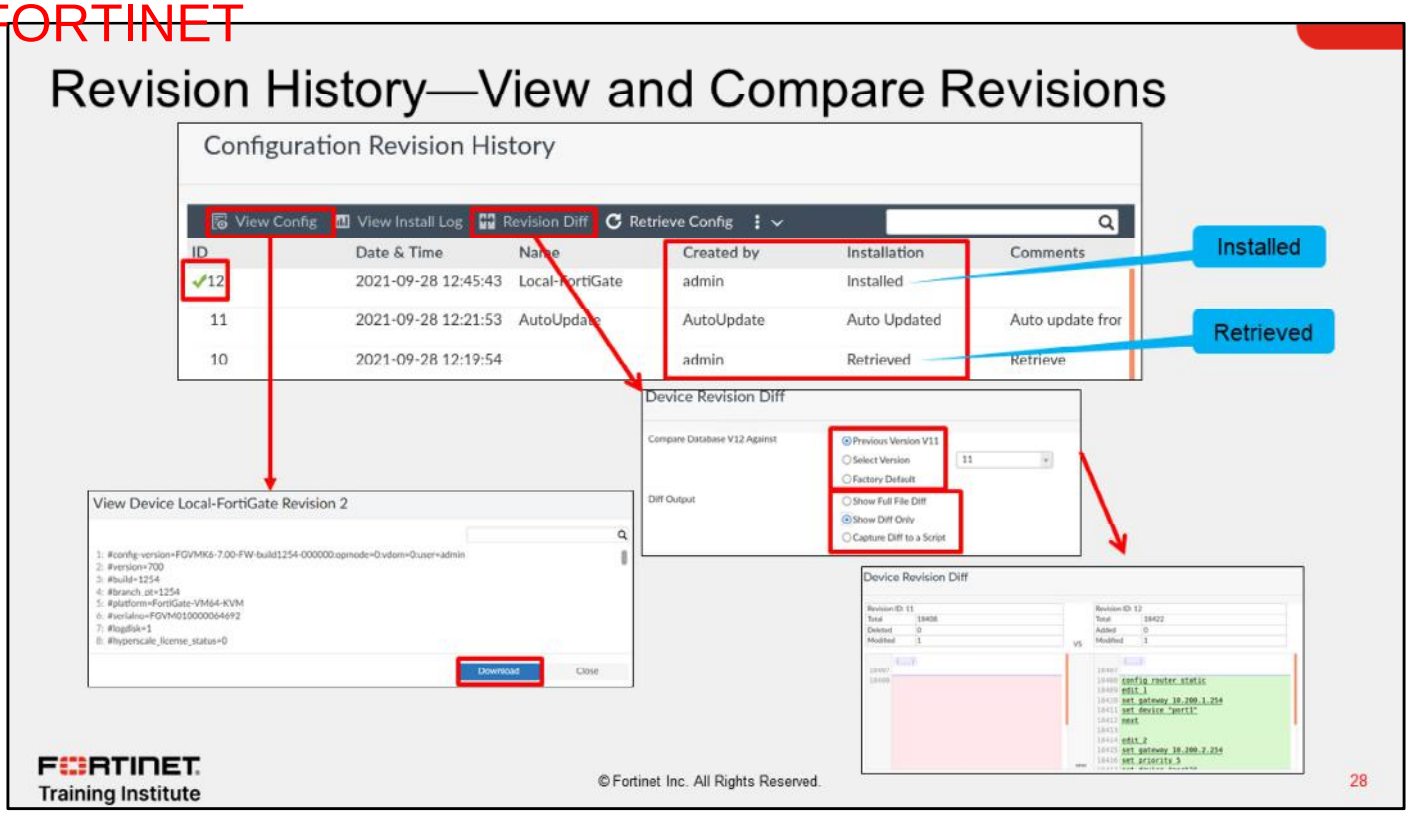
If the managed FortiGate device configuration is modified directly from the FortiGate, FortiManager compares the checksum with the latest revision history to the running configuration on the FortiGate, and creates a new revision history in its repository. It then updates the FortiManager database, which includes device-level settings only. The policy and objects are updated using the **Import Policy** wizard.

If the changes are made from FortiManager to the managed device, when performing the install, it will compare the checksum with the latest revision history to the FortiManager database and create a new revision history.

So, when a change in the configuration is detected, FortiManager creates a new revision history and tags it with a version or ID number. Select the device and, in the **Configuration and Installation** widget**,** you can view, download, or compare the differences between revisions. Revision history also allows you to view the installation performed from FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Revision History** repository stores all configuration revisions for the devices and tags each revision with a version or ID number. The **Installation** and **Created by** columns provide details about the action, process, or administrator that created the revision.

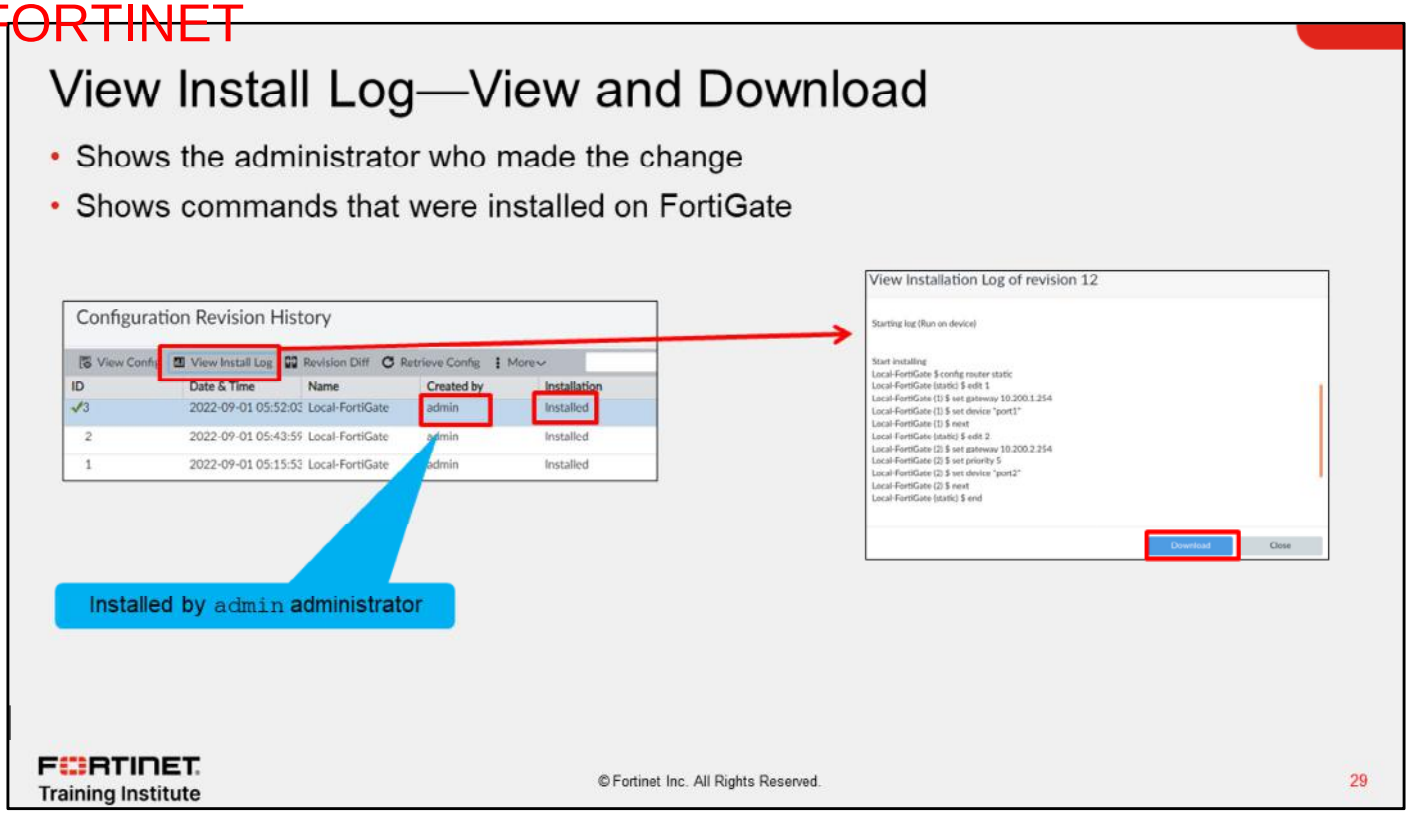
You can select the revision ID to view or download the configuration revision. This is the complete configuration of the managed device, including device-level, policy, and object configuration.

After every retrieval and installation operation, FortiManager stores the FortiGate configuration checksum output with the revision history. This is how the out-of-sync condition is calculated.

You can also compare the differences between the revision histories by clicking **Revision Diff**. You can compare the revision history to a previous version, select a specific version, or compare it to the factory default configuration. In terms of the output, you can choose to show the full configuration with differences, differences only, or you can capture the differences to a script.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When the installation is done from FortiManager, the installation log shows the name of the administrator who made the change. When an install is performed, the **Installation** column is automatically filled with the **Installed** entry. These are the revisions for which you can view install logs.

You can view the commands sent for that revision ID by selecting the revision ID and clicking **View Install Log**. If an installation fails because there is no rollback, this history is useful because it shows which commands were sent to and accepted by the device, as well as the commands that were not accepted.

You can also click **Download** to download this file in .txt format.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Resolving Configuration Issues

- Retrieve the configuration of a managed device
- Automatic update
  - Modify the configuration locally on a managed device
- Install configuration changes to FortiGate after modifying on FortiManager
- Revert to previous working configuration
- Import configuration from a local computer
  - Can import *only* configuration files that are downloaded from FortiManager; otherwise, the import will fail

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

30

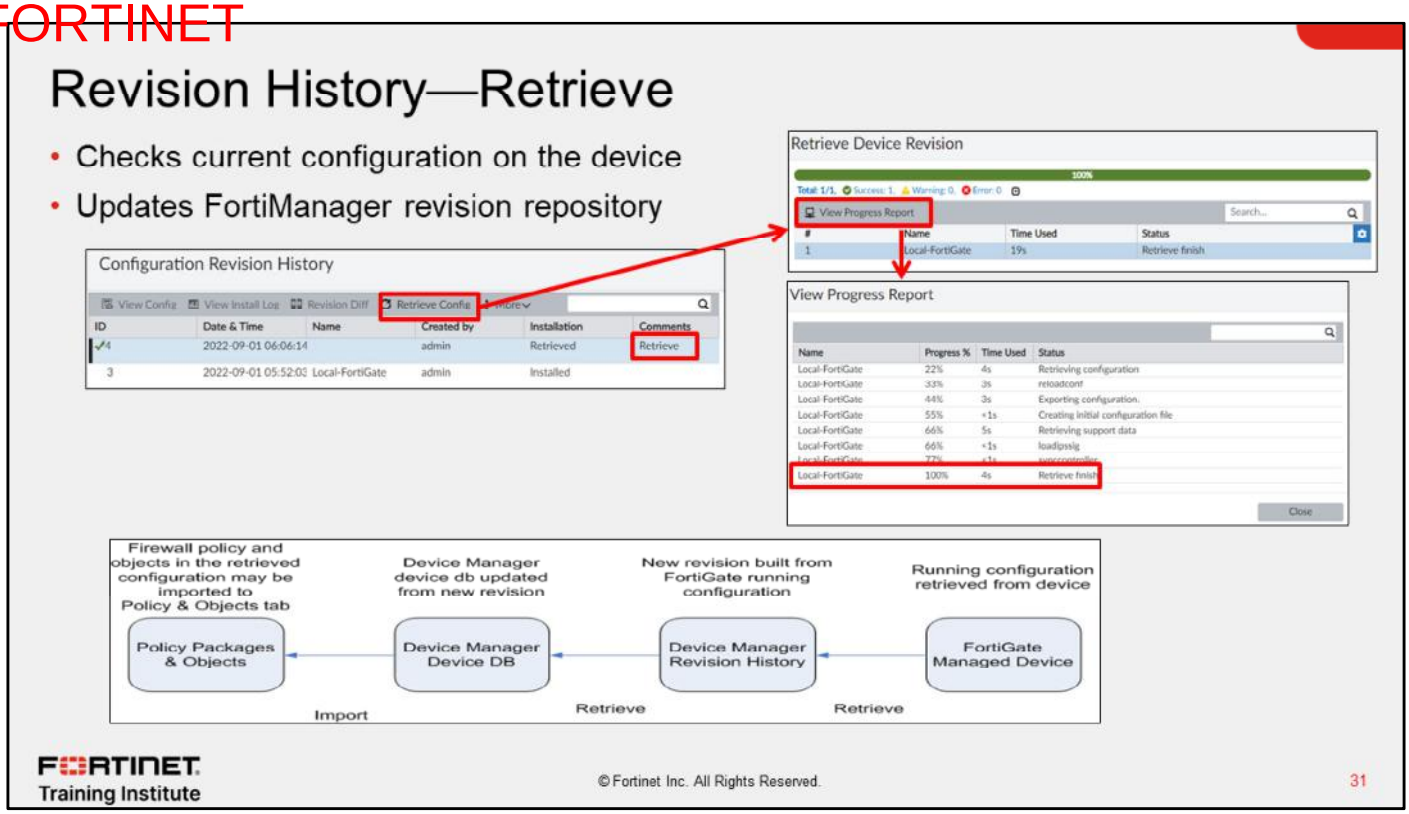
If you are not satisfied with the running configuration there are multiple ways to resolve the configuration issues. You can:

- Modify the configuration on FortiManager and then install it to the managed device
- Modify the configuration directly on the managed device
- Retrieve the configuration
- Revert to a previous configuration
- Import the FortiGate configuration from a local computer

Note that FortiManager supports importing only configuration files that are downloaded from FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The revision history also allows you to create a new revision from the device's running configuration. Click **Retrieve Config**. FortiManager checks and compares the configuration on the managed device and current revision history on FortiManager. If there is a difference, FortiManager creates a new revision history with a new ID number.

This option can be used to resync the FortiGate device with the FortiManager device database. However, when retrieving a configuration, firewall policy changes need to be imported to the **Policy & Objects** pane.

The **Comments** column automatically generates a comment if a retrieve operation is performed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

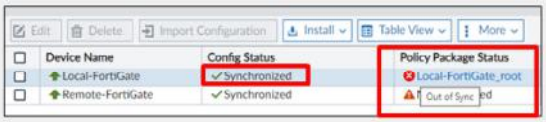
Revision History—Automatic Update

- Modifying configuration directly on a managed device automatically creates a new revision

- Can disable automatic update behavior from FortiManager CLI
  - Default enabled
  - If disabled–can accept or reject the changes

```
config system admin settings
set auto-update disable
end
```

- Config Status is updated automatically under the Device Manager



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

32

By default, all changes made directly on the FortiGate device are automatically updated (retrieved) by FortiManager and reflected in **Revision History** and **Config Status** for that device in the **Device Manager**.

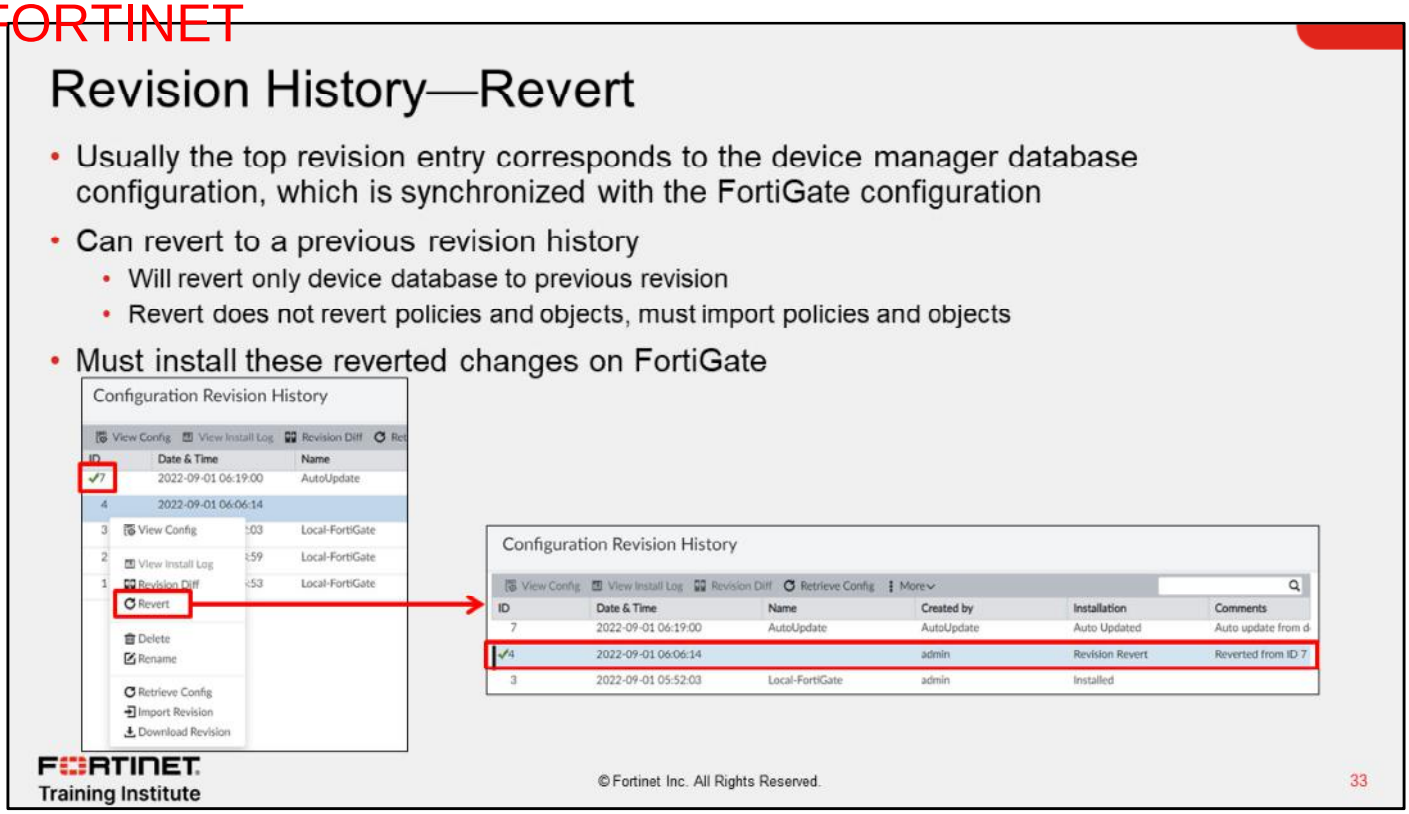
You can disable the automatic update behavior, which allows the FortiManager administrator a choice to accept or refuse the automatic update.

If an automatic update occurs, it is no longer possible for FortiManager to be sure the selected policy package is the same as the running firewall policy. As such, **Policy Package Status** returns an **Out-of-Sync** error.

You must run the **Import Policy** wizard on FortiManager to sync the policy package.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The green checkmark in the revision history indicates which revision history configuration corresponds to the device manager database configuration. It is usually the top entry, which is synchronized with the FortiGate configuration.

A revert operation within the revision history changes the device database configuration to a previous configuration state. You must install these reverted changes on FortiGate, which then creates a new revision entry. This new revision is a copy of the reverted one and in sync with the FortiGate configuration. Revert followed by installation would only revert device-level changes. Keep in mind that revert does not revert policy packages; you will need to import policies and objects.

You can revert to any previous revision by right-clicking that entry and then clicking **Revert**. The selected previous entry for revert will automatically updates the **Installation** column to **Revision Revert**. FortiManager also updates the **Comments** column with the number of the revision revision it is reverted from, and that installation is required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is one of the main ways that you can take advantage of the revision history?
   A. To modify FortiManager system settings
   ✓B. To view and download a FortiGate configuration revision

2. What is the main benefit of the FortiManager revert feature?
   ✓A. The administrator can revert the device database to a previous revision
   B. The administrator can perform a factory reset on FortiManager

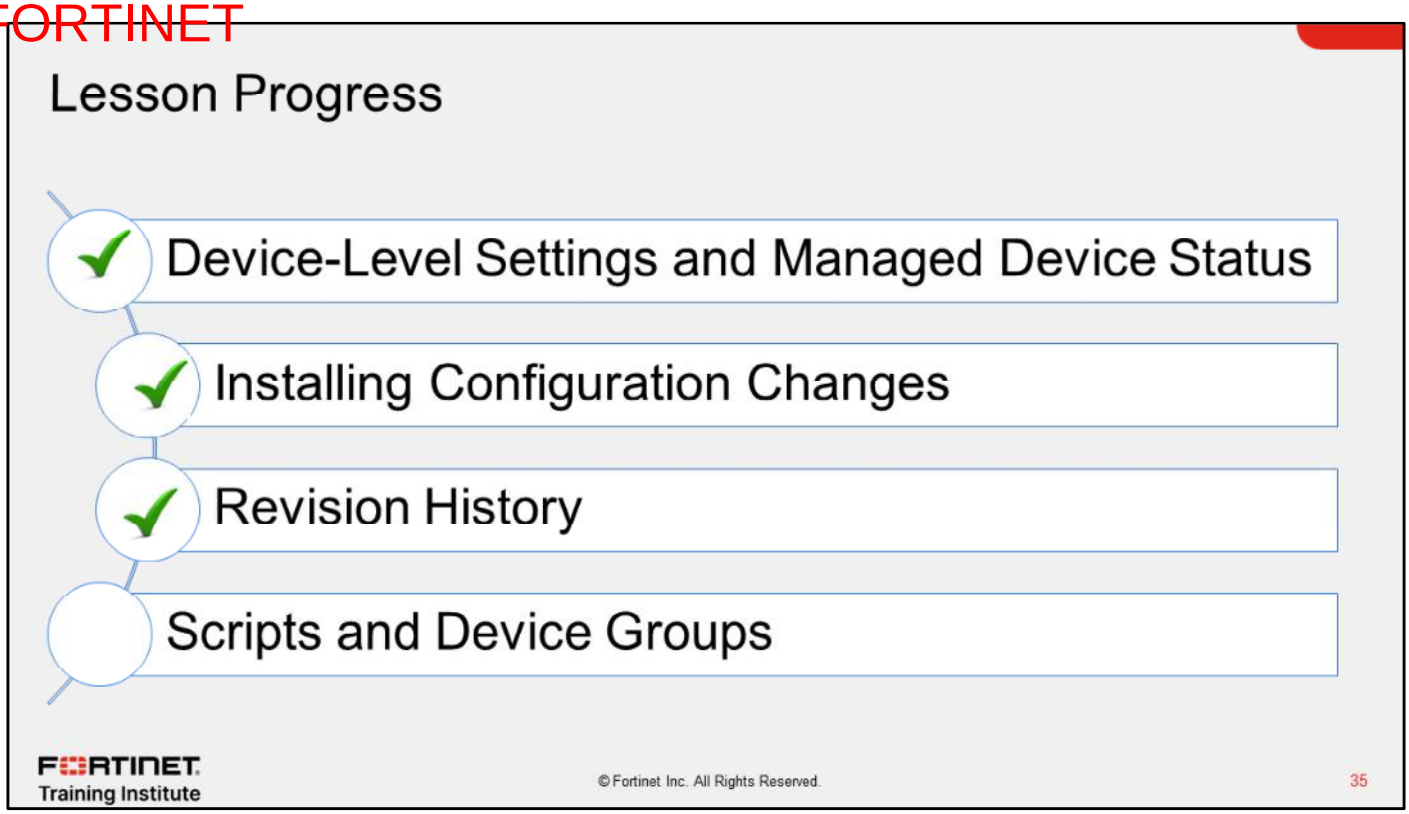
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

34

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

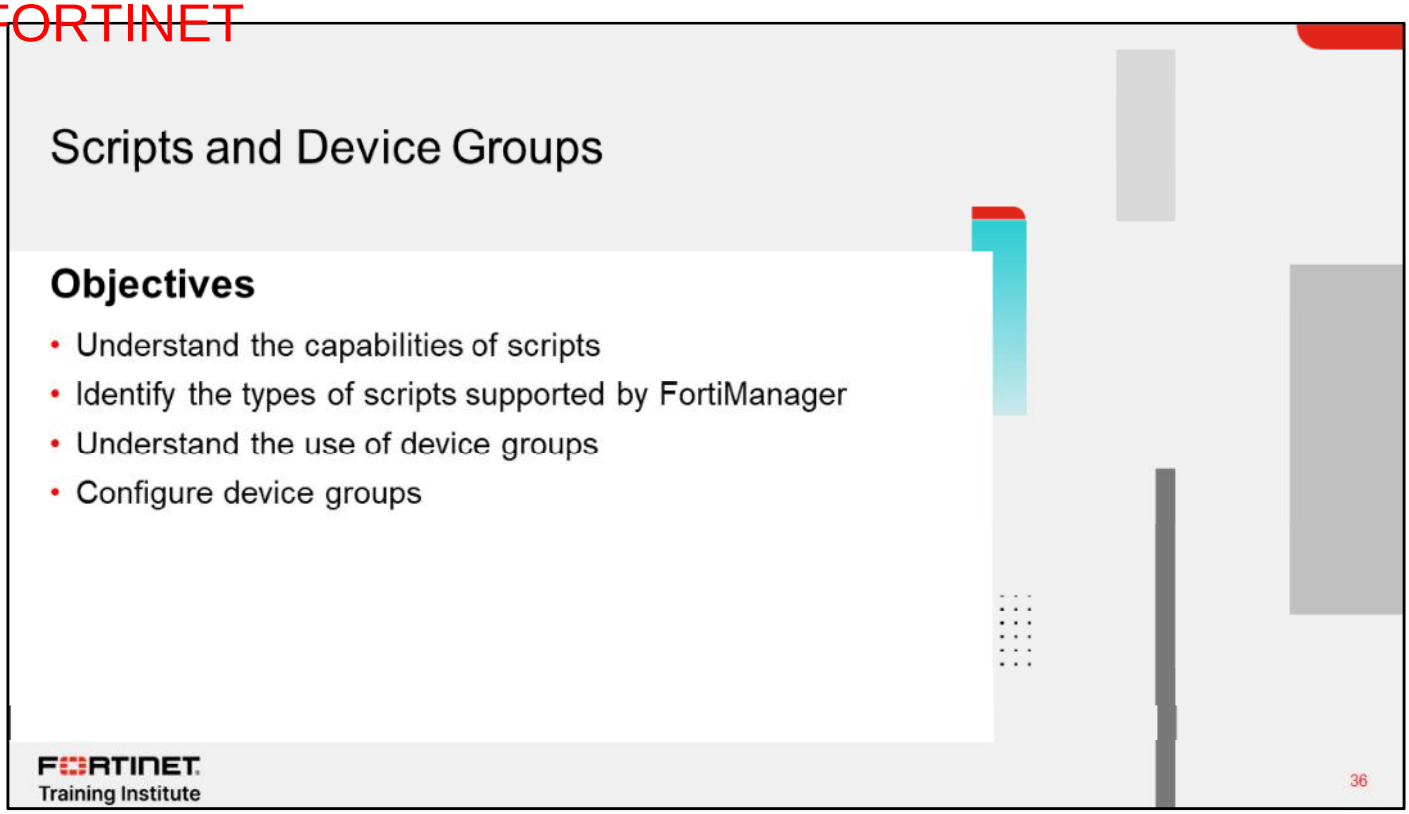


Good job! You now understand the purpose of the revision history and how it can be used.

Now, you will learn about scripts and device 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 objectives shown on this slide.

By demonstrating competence in using scripts, you will be able to use scripts to make many changes to managed FortiGate devices. Using device groups, you will be able to administer and manage your FortiGate devices more effectively and efficiently.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scripts

- Can make many changes to many managed devices
  - Can be used to provision FortiGate devices
  - Can be used to automate configuration changes
- Help to simplify bulk configuration changes and maintain consistency
- There are two types of scripts:
  - Command Line Interface (CLI)
    - A sequence of FortiGate CLI commands, as you would type on the FortiGate CLI
  - Tool Command Language (TCL)
    - A dynamic scripting language that provides more functionality to your scripts, including global variables and decision structures
- Scripts are enabled by default
- TCL scripts can be enabled on the FortiManager CLI

```
config system admin setting
set show_tcl_script enable
end
```

TCL scripts enabled on FortiManager CLI

TCL scripts are not run through the FGFM tunnel like CLI scripts. They use SSH and require SSH authentication to work.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

37

Scripts can make many changes to a managed device and are useful for bulk configuration changes and consistency across multiple managed devices.

FortiManager supports two types of scripts:

- CLI: CLI scripts include only FortiOS CLI commands as they are entered at the command line prompt on a FortiGate device.
- TCL: TCL is a dynamic scripting language that extends the functionality of CLI scripting. In FortiManager TCL scripts, the first line of the script is a number sign (#) plus an exclamation mark (!), which are for standard TCL scripts. Do not include the exit command that normally ends TCL scripts; it will prevent the script from running. You must be familiar with the TCL language and regular expressions. For more information about TCL scripts, visit the official TCL website: http://www.tcl.tk

By default, scripts are enabled. For TCL scripts, you also need to enable the `show_tcl_script` command from the FortiManager CLI.

Note that TCL scripts do not run through the FGFM tunnel like CLI scripts do. TCL scripts use SSH to tunnel through FGFM and they require SSH authentication to do so. If FortiManager does not use the correct administrative credentials in the device manager, the TCL script fails. CLI scripts use the FGFM tunnel, and the FGFM tunnel is authenticated using the FortiManager and FortiGate serial numbers.

In this lesson, you will learn about CLI scripts only.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Best Practices for CLI Scripts

- Use complete FortiOS CLI commands
  - Incomplete syntax may cause the script to fail

✓ `config router static`

✗ `con rou stat`

- A comment line that starts with the number sign (#) will not execute

```
#config system dns
```

- Ensure console output on FortiGate CLI is set to standard, otherwise scripts and other output longer than a screen length will not execute or display correctly

```
config system console
set output standard
end
```

Set to standard on FortiGate CLI

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

38

When creating CLI scripts, follow these best practices:

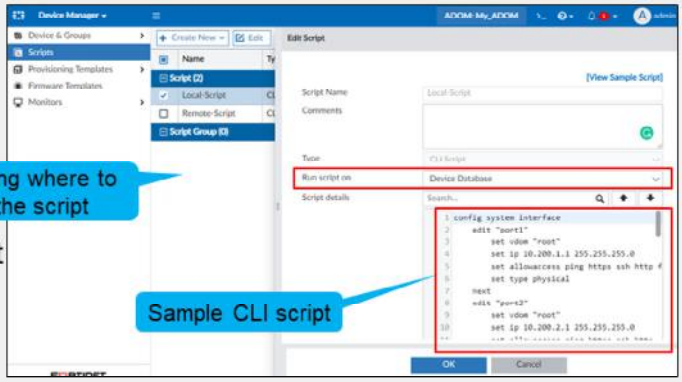
- Use complete FortiOS CLI commands. Partial syntax can be used; however, it may cause the script to fail.
- A comment line that starts with the number sign (#) will not execute.
- In the FortiGate CLI, ensure the console output is set to `standard`. Otherwise, scripts and other output longer than a screen in length will not execute or display correctly.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuring Scripts

- Scripts can be run on:
  - Device database
  - Policy package, ADOM database
  - Remote FortiGate directly (through the CLI)
- By default, scripts run on the device database
- Can select advanced filters to restrict the script to be executed on devices matching the set criteria



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

39

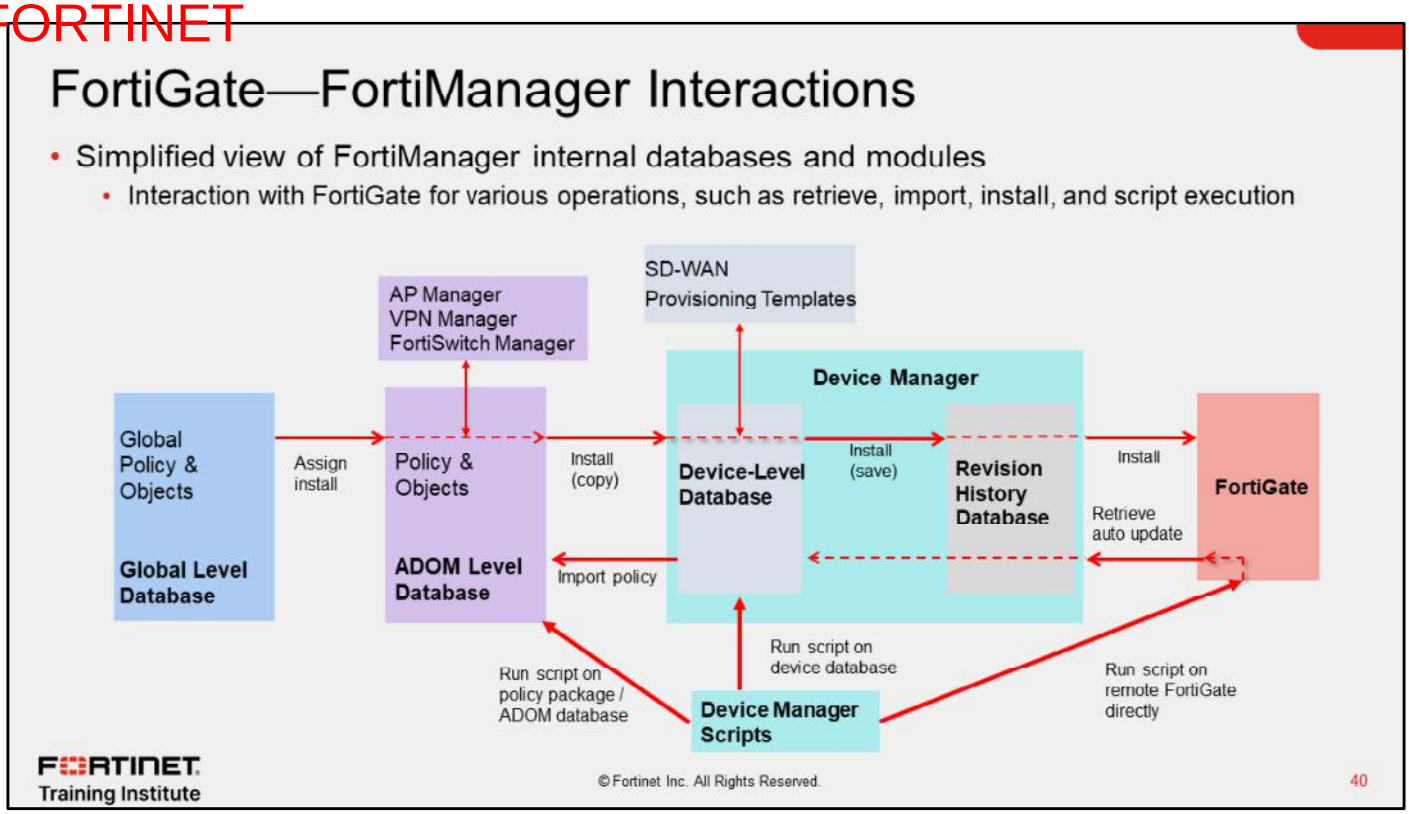
Scripts can be run in three different ways:

- **Device Database**: By default, a script is executed on the device database. It is recommended that you run the changes on the device database (default setting), because this allows you to check what configuration changes you will send to the managed device. Once scripts are run on the device database, you can then install the changes on a managed device using the installation wizard.
- **Policy Package**, **ADOM Database**: If a script contains changes related to ADOM-level objects and policies, you can change the default selection to run on **Policy Package**, **ADOM Database** and can then install the changes using the installation wizard.
- **Remote FortiGate Directly (through the CLI)**: A script can be executed directly on the device and you don't need to install the changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

You can also apply options in **Advanced Device Filters**, which you can use to restrict the scripts to running on managed devices only if the device matches the set criteria.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The diagram on this slide shows FortiManager-FortiGate interactions. As this slide shows, when you perform an installation from FortiManager to FortiGate, FortiGate creates a new revision history.

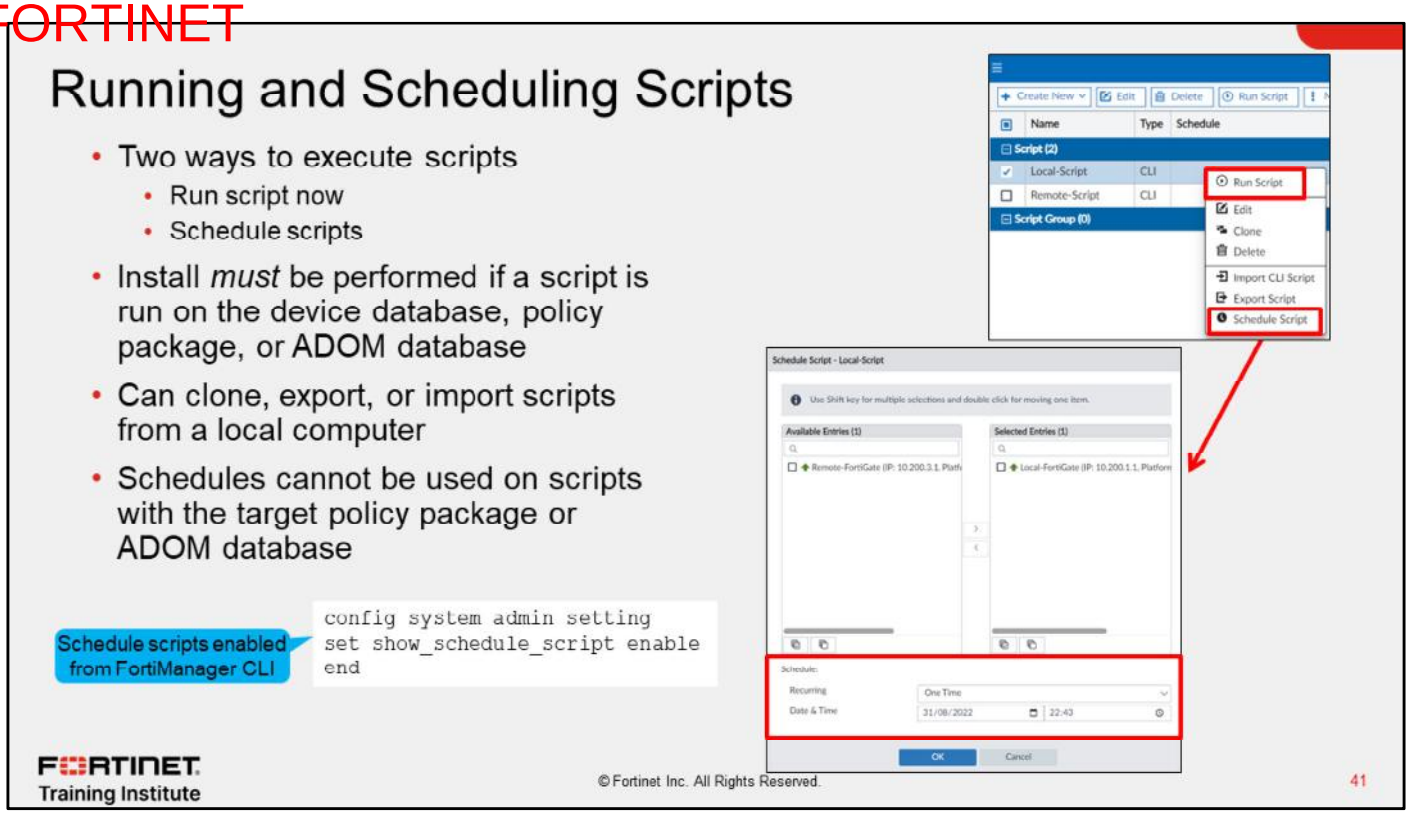
If you run a script on a device database or on a policy package, you must perform an installation on the managed devices.

If you run a script directly on a remote device, an automatic update occurs, creates a new revision, and updates the device-level database.

If you perform a retrieval from FortiManager, or an automatic update occurs, FortiManager creates a new revision history. If the changes are related to policies or objects, you *must* run the **Import Policy** wizard to import policies and objects into the ADOM database.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Once you've configured the script, you can browse the ADOM script list for the ADOM that contains the script you would like to run.

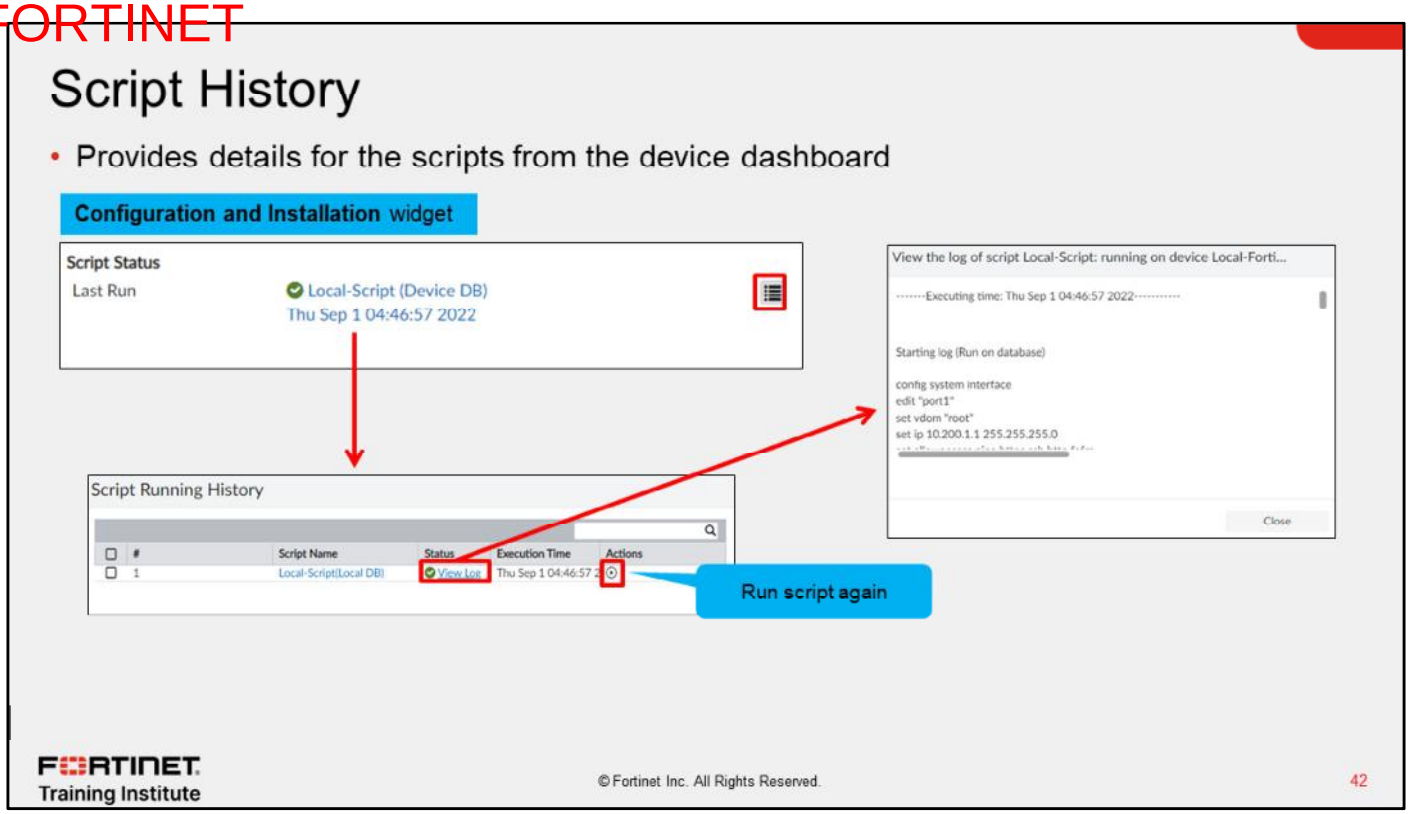
To run the script now, select the script and click **Run Scripts Now**.

You can also schedule the script to run at a specific time; for example, outside of business hours. This is useful when you don't want to interfere with the production network in the business hours. To open the window where you can schedule the script to run, right-click the script and click **Schedule Scripts**. Schedules cannot be used on scripts with the target policy package or ADOM database.

The right-click menu also provides other options, such as create new script, edit, clone, and delete the existing script. You can also export the script by clicking **Export**. The exported script can be saved on your local computer in .txt format. Scripts can also be imported as text files from your local computer by clicking **Import**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

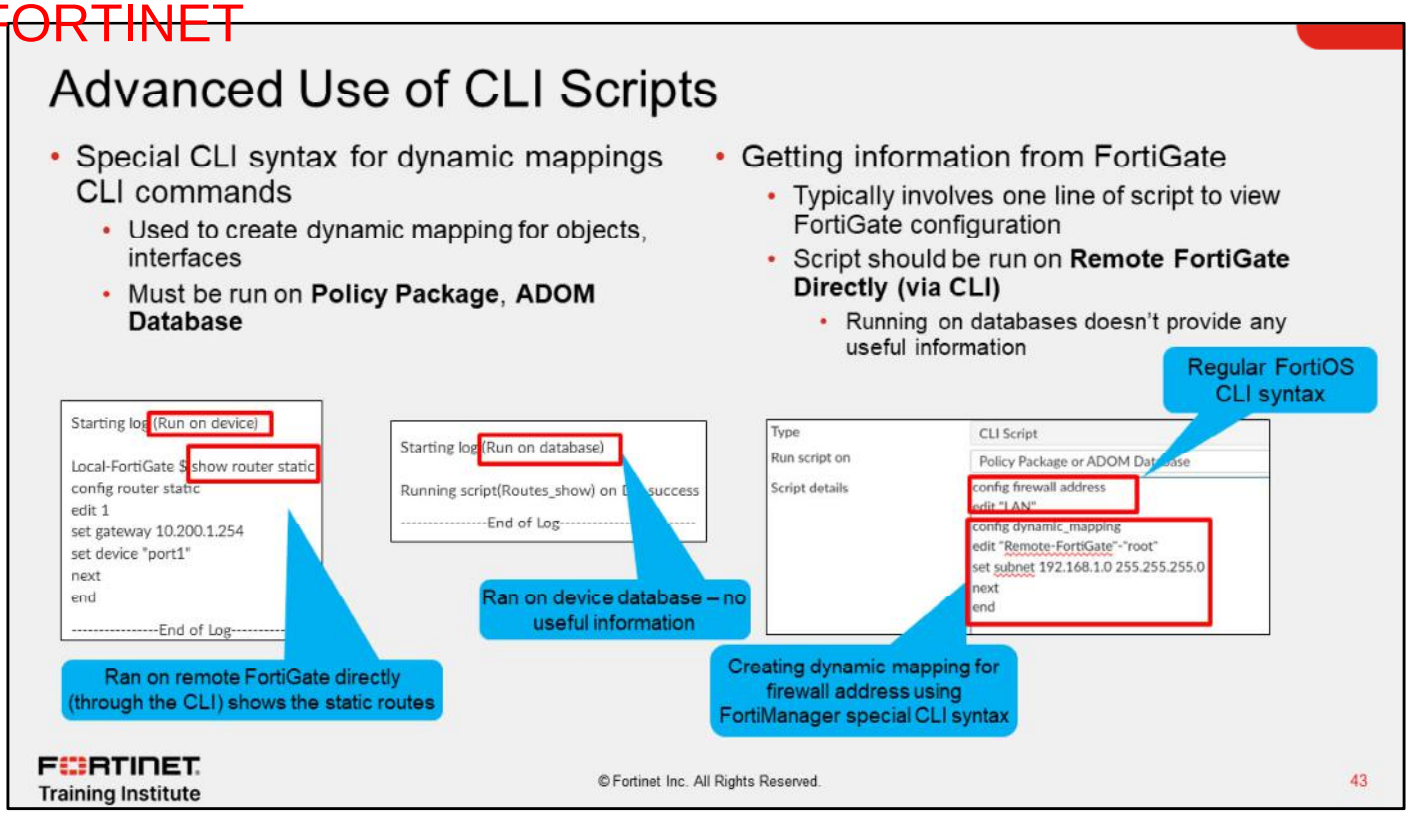


To view the script history, go to the device dashboard. Under the **Configuration and Installation Status** widget, click **View History** to open the **Running Script History** table. This table provides additional information, such as name, execution time, and status of the script. Click the **Execution Log** icon to view the execution log of that particular script and confirm that the script ran without any issues.

The **Script Executing History** table also allows you to rerun the script. Click the **Run Again** icon in the far right column of the table to rerun the script.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can also use scripts to get information from the FortiGate device. These types of scripts are usually one-line scripts that use `show` commands and should be chosen to run on **Remote FortiGate Directly (via CLI)**. Running a script on the device or on the ADOM database does not provide any useful information.

FortiManager supports dynamic mapping of interfaces and objects so that they can be used with multiple policy packages. You can configure these dynamic mappings from the FortiManager GUI under the **Policy & Object** pane.

But what if you need to configure dynamic mapping for hundreds of FortiGate devices for an address object or interface?
You can use scripts that requires special CLI syntax that is applicable to FortiManager internally and is used for creating dynamic mapping. It is two-part script:

- The top part is the regular FortiOS CLI syntax defining the object.
- The bottom part is special FortiManager CLI syntax to create dynamic mapping for the object or interface defined in top part.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Real-Time Debugs

- Can debug script execution in real time

```
# diagnose debug application depmanager 255
# diagnose debug enable

Request:
{ "id":,.... "scope": [ { "name": "Local-FortiGate", "vdom": "global" } ], "script": 204...
startInstallScript_ ==> Inst-Tcl/Ondb-Script (scriptid=204, CLI script, OnDb)
==INST SCRIPT==>init state: start to run-on-db
..
.... "script-name": "Static Routes", "target": 295 },
Response:
{ "id": 1034, "result": [{ "status": { "code": 0, "message": "OK"}, "url": "install\/script"}]}
==INST SCRIPT==>running on_db script succeeded
==INST SCRIPT==>Script Static Routes executed on local db of Local-FortiGate.
View Script Execution History log file for result.
```

CLI script run on device database

Name of the script

Results of script execution

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

44

You can also run a real-time debug on FortiManager when executing scripts that shows the request performed and the outcome of the request.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Common Script Execution Errors

Common errors	Common causes	Common solution
command parse error	Misspelled keyword or incorrect command format*	Check the script output
unknown action	Previous line of the script was not executed	Check the script output
Device <name> failed-1	Problem with the end of the script. Usually script has no end statement FortiGate not in sync with FortiManager	Check the script output Add an end statement Resync FortiGate by retrieving configuration

*There should be no punctuation at the start or end of the lines.

*Only whitespace is allowed on the same line as the command. This is useful in lining up `end` and `next` commands for quick and easy debugging of the script.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

45

These are the common errors and common causes for the scripts to fail. You can use these to diagnose and troubleshoot script failure issues and can use common solutions to fix the issue.

The common errors and common causes for the scripts to fail are:

- `command parse error`: It was not possible to parse this line of your script into a valid FortiGate CLI command. This is usually caused by misspelled keywords or an incorrect command format.
- `unknown action`: Generally this message indicates the previous line of the script was not executed, causing the following CLI commands to fail to execute properly.
- `Device <name> failed-1`: This usually means there is a problem with the end of the script. The `<name>` is the name of the FortiGate on which the script is executed. If a script has no end statement or that line has an error in it, you may see this error message. You may also see this message if the FortiGate unit has not been synchronized by deploying its current configuration.

To resolve the script failure issues, use the script history that shows which CLI commands are executed and which commands it is failing to execute.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Troubleshooting Scripts

- Can view the details of script from script history
  - Useful to view whether script was run successfully or with errors
- Task monitor
  - Can click on **View Details** > **View Script Execution History** icon to view the script run

- From event logs–if debug level set to `debug`

```
config system locallogs disk settings
```

```
type=event subtype=dm pri=information desc="Script install status" user="admin" msg="script Static Routes install on Local-FortiGate succeed"
device="Local-FortiGate" adom="root" status="successfully" script="Static Routes"

type=event subtype=dm pri=information desc="Script install status" user="admin" msg="Install script failed:
Script Training executed on local db of Local-FortiGate failed. Reason: invalid value ...
device="Local-FortiGate" adom="root" status="failed" script="Training"
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

46

When troubleshooting scripts, you can check the **Script History** to see details about the script. The task monitor also provides the same information along with other tasks performed. You can also change the logging level to debug for event logs, which creates the log for the actions performed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Useful CLI Commands

- You can use the `execute fmscript` command tree on FortiManager for scripts

CLI Command	Used for
clean-sched	• Unable to delete scheduled scripts if an associated device has been deleted • Cleans script schedule table for all non-existent devices
copy	• Copy scripts between ADOMs
import	• Import a script to FortiManager
list <adom name>	• List scripts in ADOMs
showlog <devicename>	• Show a run script log for a device

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

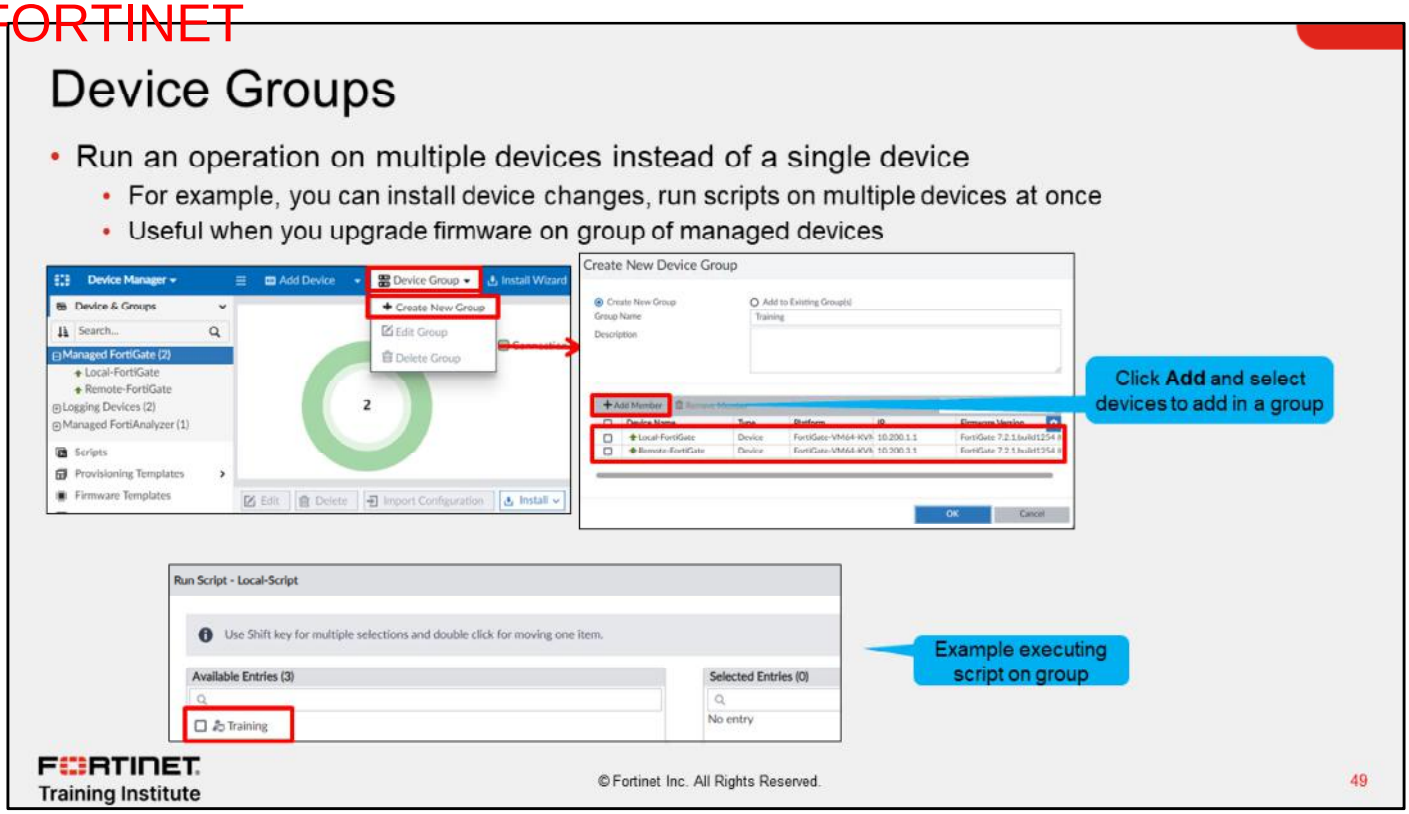
47

You can use the `execute fmscript` command tree on FortiManager for scripts.

The `execute fmscript` command tree on FortiManager provides various commands for scripts, such as deleting scheduled scripts, copying scripts between ADOMs, importing scripts, listing all the configured scripts in an ADOM, or showing the script log for a device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can create device groups in an ADOM. You can use device groups to simplify a management action by providing a target that represents multiple devices for scripts, firmware upgrades, and configuration changes.

You can create a new device group by clicking **Device Group** > **Create New Group** and selecting the devices to be added to this group.

Note that to delete a device group, you *must* delete all devices from the device group first. Similarly, to delete an ADOM, you must delete all device groups from the ADOM first.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which type of scripts are supported on FortiManager?
   - ✓A. CLI and TCL scripts
   - B. Bash and Linux Shell scripts

2. What happens to the **Device Settings Status** if you execute a script using the **Remote FortiGate Directly (via CLI)** option?
   - ✓A. It will be tagged as **Auto-Updated**
   - B. It will be tagged as **Modified**

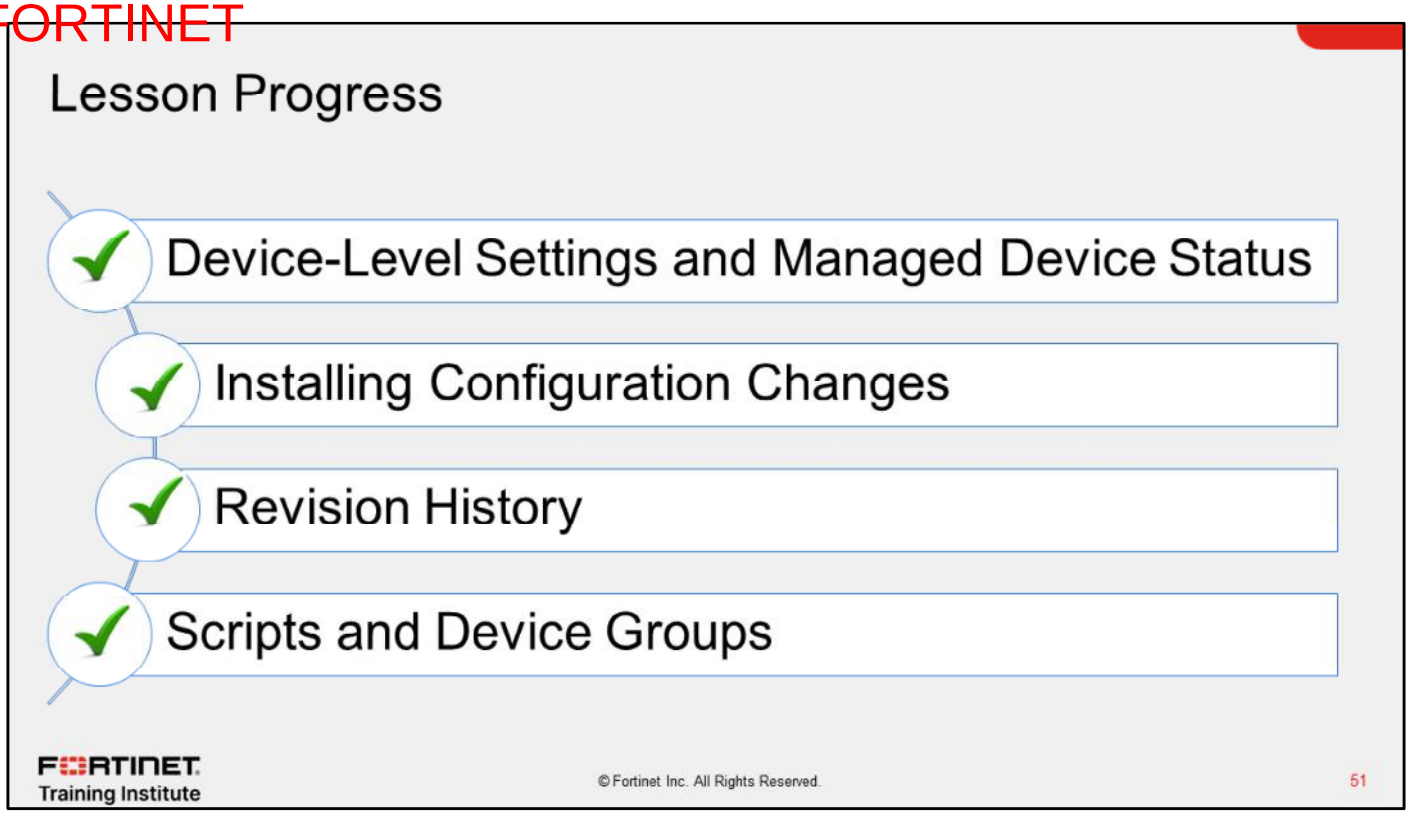
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

50

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

Review

- ✓ Configure device-level settings
- ✓ Understand FortiGate configuration status and synchronization behavior
- ✓ Push configuration changes to FortiGate
- ✓ Use revision history for diagnosing and troubleshooting
- ✓ Configure and install scripts on managed devices
- ✓ Use device groups for simplifying management of FortiGate devices

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

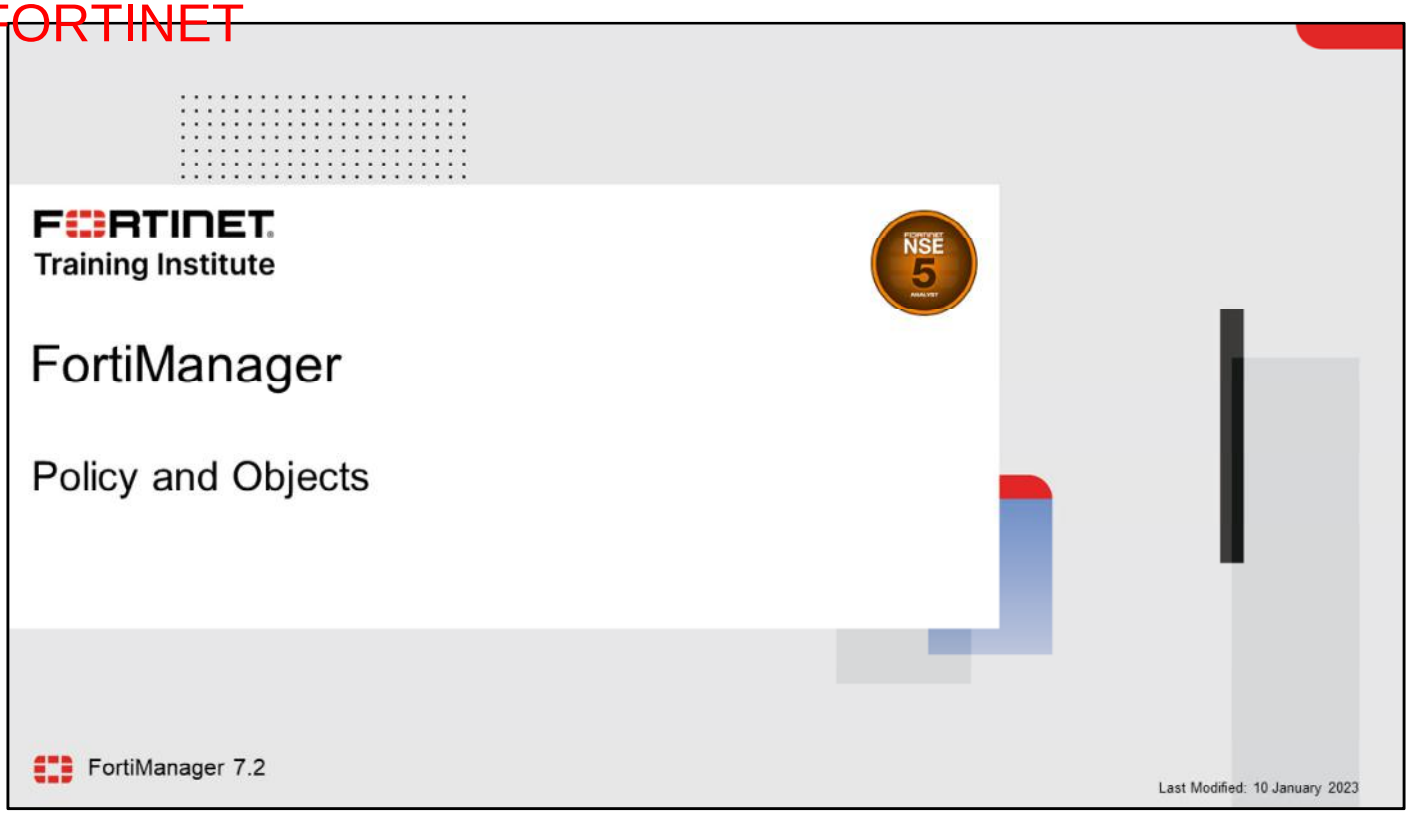
52

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

By mastering the objectives covered in this lesson, you learned how to configure device-level changes, understand the status of a managed FortiGate on FortiManager, and install changes to the managed FortiGates. You also learned how to use the revision history for troubleshooting and about the capabilities of scripts and device groups.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn how to manage policy and objects on FortiManager for FortiGate. You will also learn how to configure policy and objects on FortiManager, and then install them on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Overview

- Policy and Objects Management
- Import and Install Wizards
- ADOM Revision and Database Versions
- Policy Locking and Workflow Mode

FORTINET Training Institute

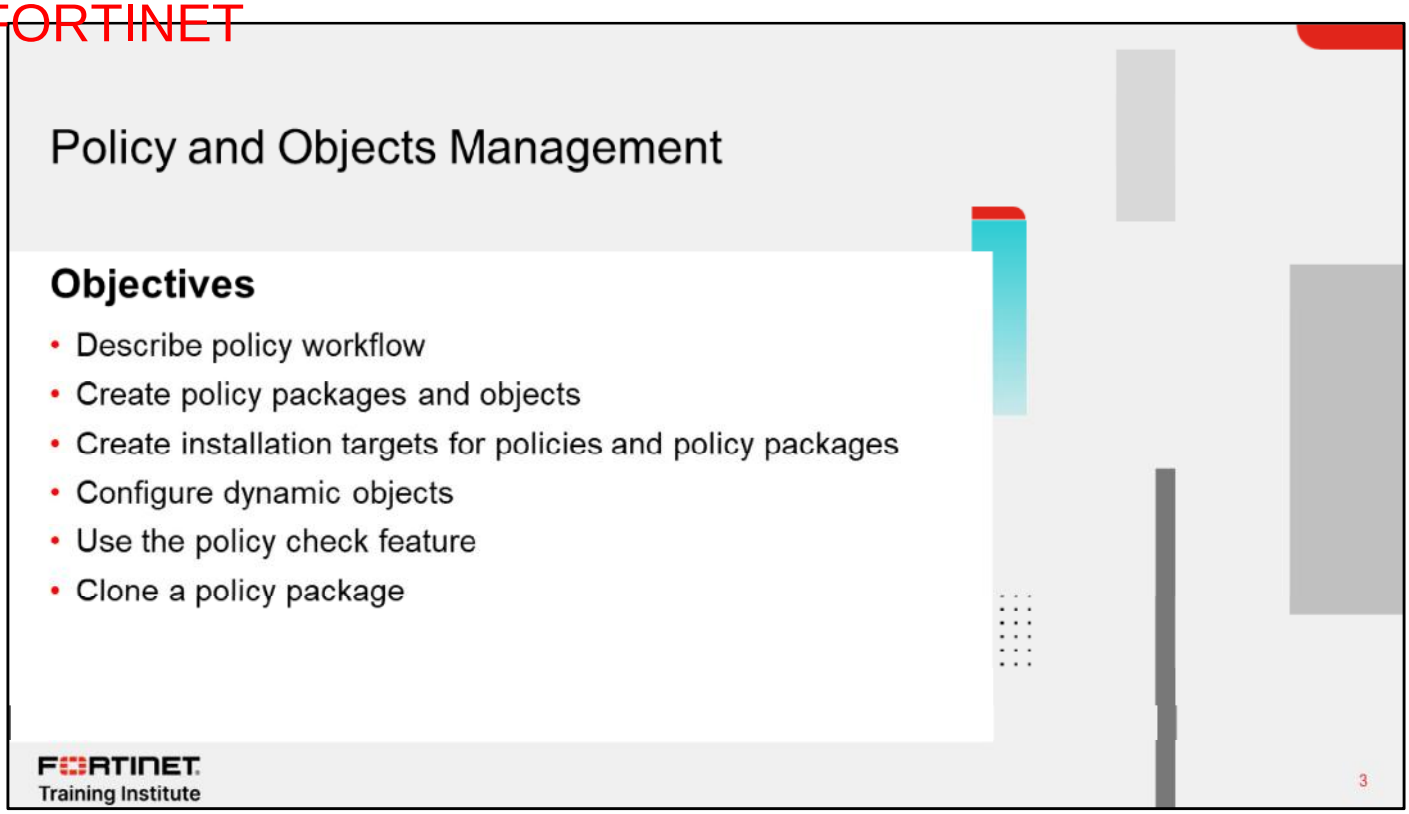
© Fortinet Inc. All Rights Reserved.

2

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 understanding, configuring, and using policies and objects, you will be able to create customized access and policies based on the needs of your organization.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Overview

- You can perform the following tasks in each ADOM:
  - Create or customize policy package or packages for each device or VDOM
  - Create policy folders
  - Point a policy package at a single device, multiple devices, all devices, a single VDOM, multiple VDOMs, or all devices in a single ADOM
  - Create objects that can be shared among policy packages in an ADOM
  - Copy or clone existing policy packages
  - Configure dynamic objects
  - Configure display options
  - Configure ADOM revisions

FORTINET Training Institute

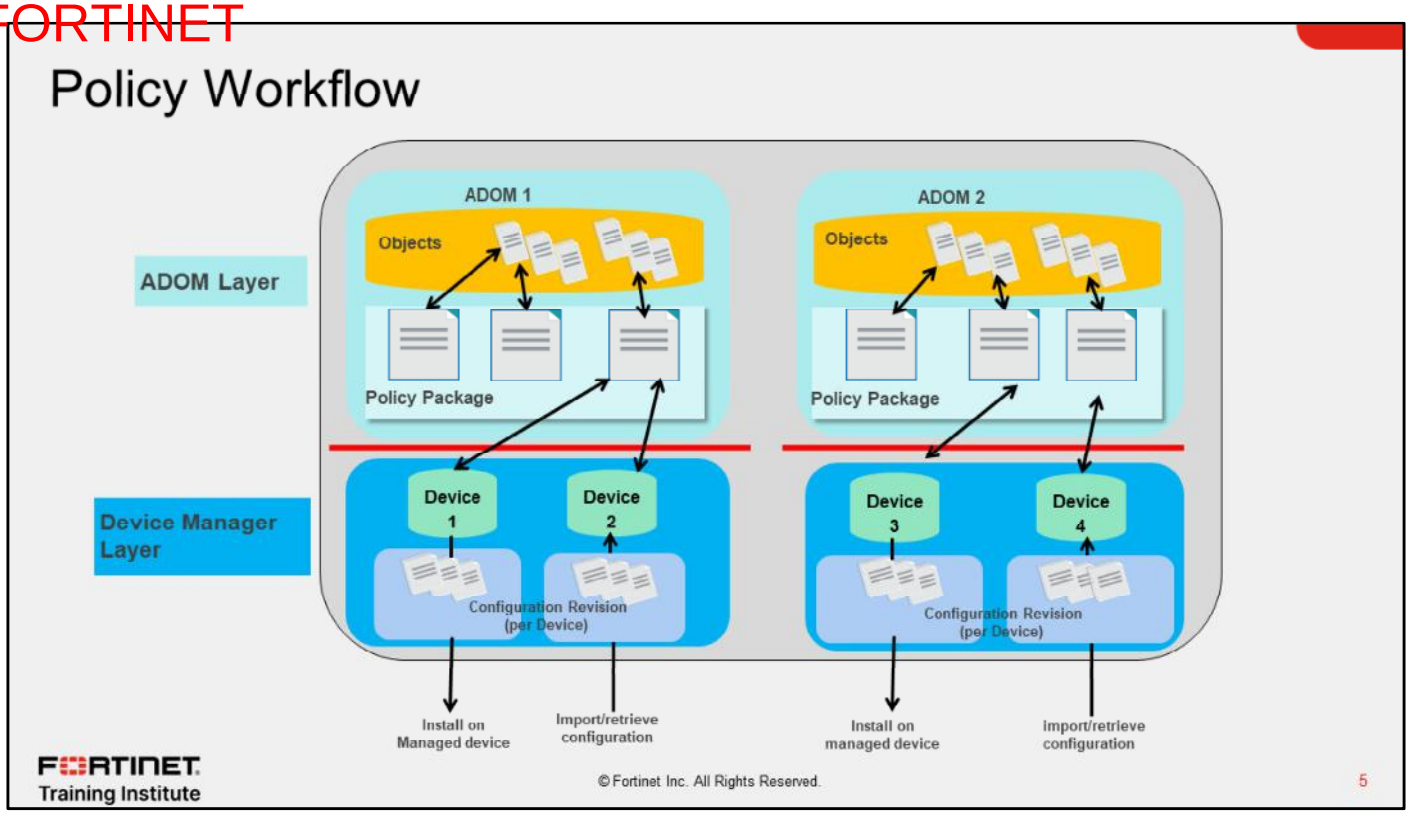
© Fortinet Inc. All Rights Reserved.

4

You can create multiple policy packages in a single ADOM. FortiManager allows you to customize policy packages for each device or VDOM in a specific ADOM. You can point these policy packages to a single device, multiple devices, all devices, a single VDOM, multiple VDOMs, or all devices in a single ADOM. FortiManager helps simplify provisioning of new devices, ADOMs, or VDOMs by allowing you to copy or clone existing policy packages. You can also create the ADOM revision, which allows you to maintain a revision of the policy packages and objects settings in an ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Policy packages simplify centralized firewall policy management by providing a useful container for your firewall rule set. Policy packages contain firewall policies which, in turn, link to the objects you define on the **Object Configuration** pane. Objects share the common object database for each ADOM. You can share objects among multiple policy packages in the ADOM.

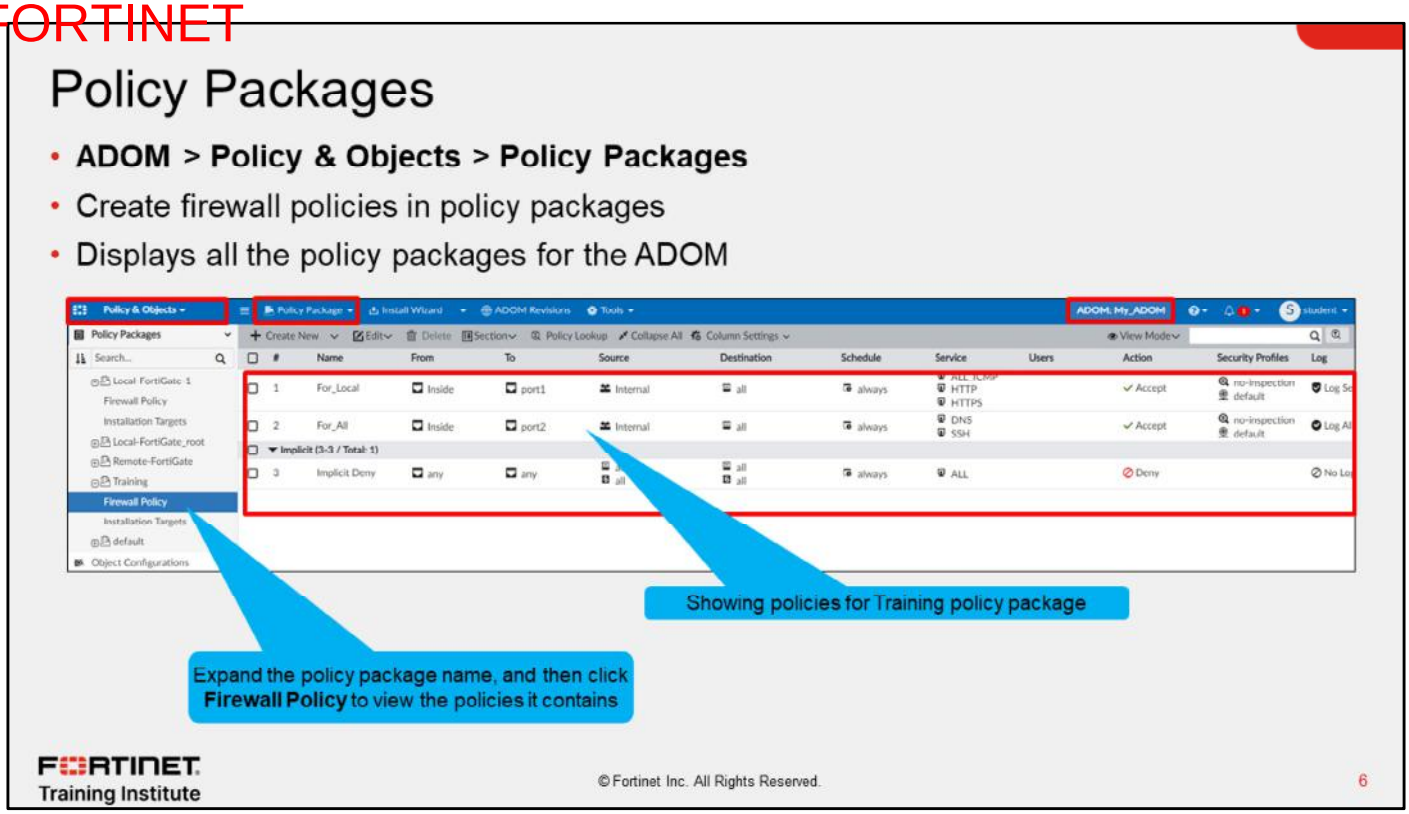
You can manage a common policy package for many devices in an ADOM, or have a separate policy package for each device. Policy packages allow you to maintain multiple versions of the rule set. For example, you can clone a policy package before you make changes, which allows you to preserve the previous rule set.

A word of caution: while policy packages allow for multiple versions of a firewall policy rule set, the objects referenced in those packages do not have multiple versions—they use only a current value.

For example, say you clone a policy package, add a new rule, and then change the value of a shared object. If you return to a previous version of the policy package, you will back out of the rule that you added, but *not* the modification to the shared object. The only way to return to a previous version of the policy package, including backing out of the rule that you added *and* the modification to the shared object, is to use ADOM revisions, which takes a snapshot of the **Policy & Objects** database for that ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

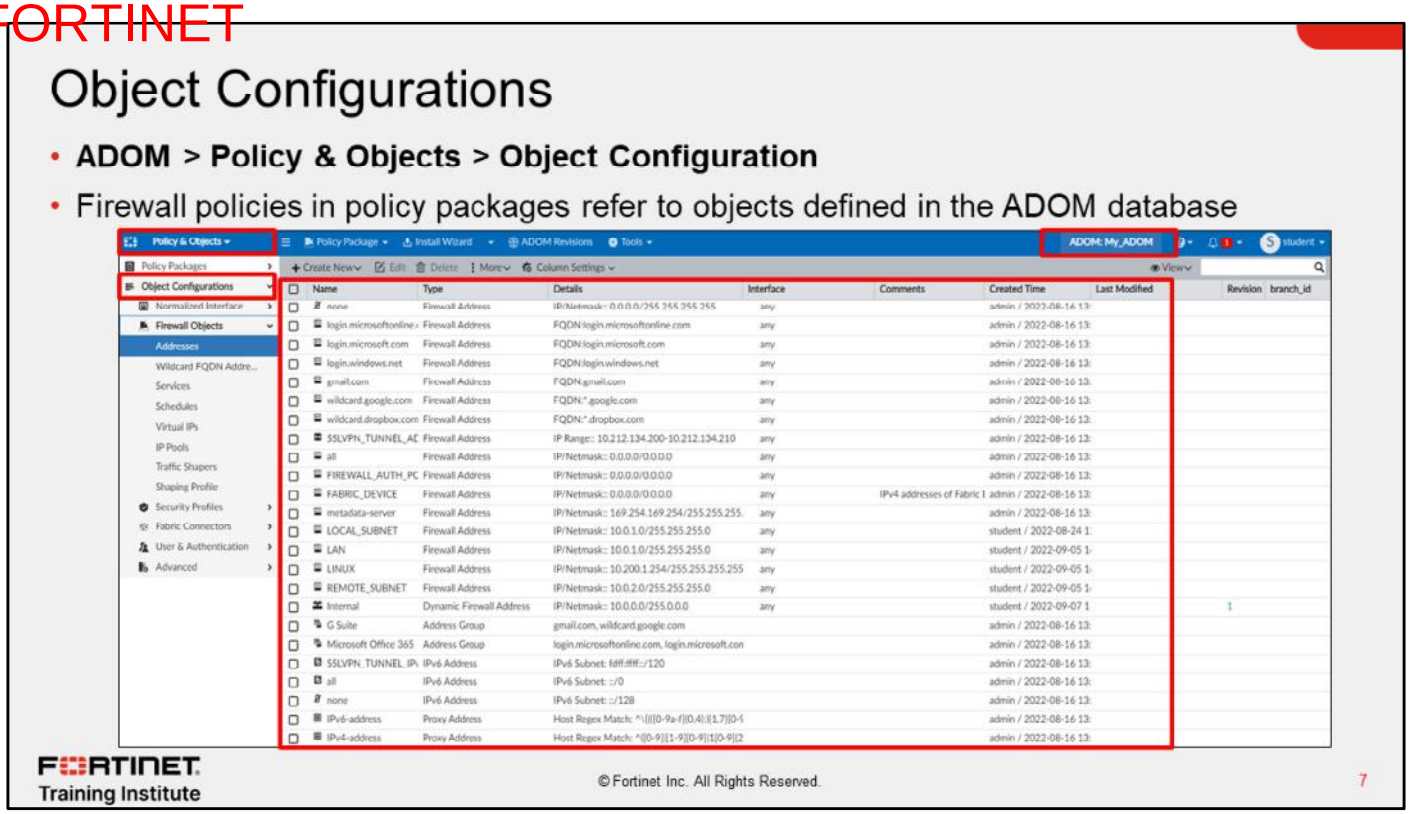
DO NOT REPRINT Brave-dumps.com
© FORTINET



In a single ADOM, administrators can create multiple policy packages. FortiManager allows you to customize the policy packages for each device or VDOM in a specific ADOM, or apply a single policy package for multiple devices in an ADOM. By defining the scope of a policy package, an administrator can modify or edit the policies in that package, without changing other policy packages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



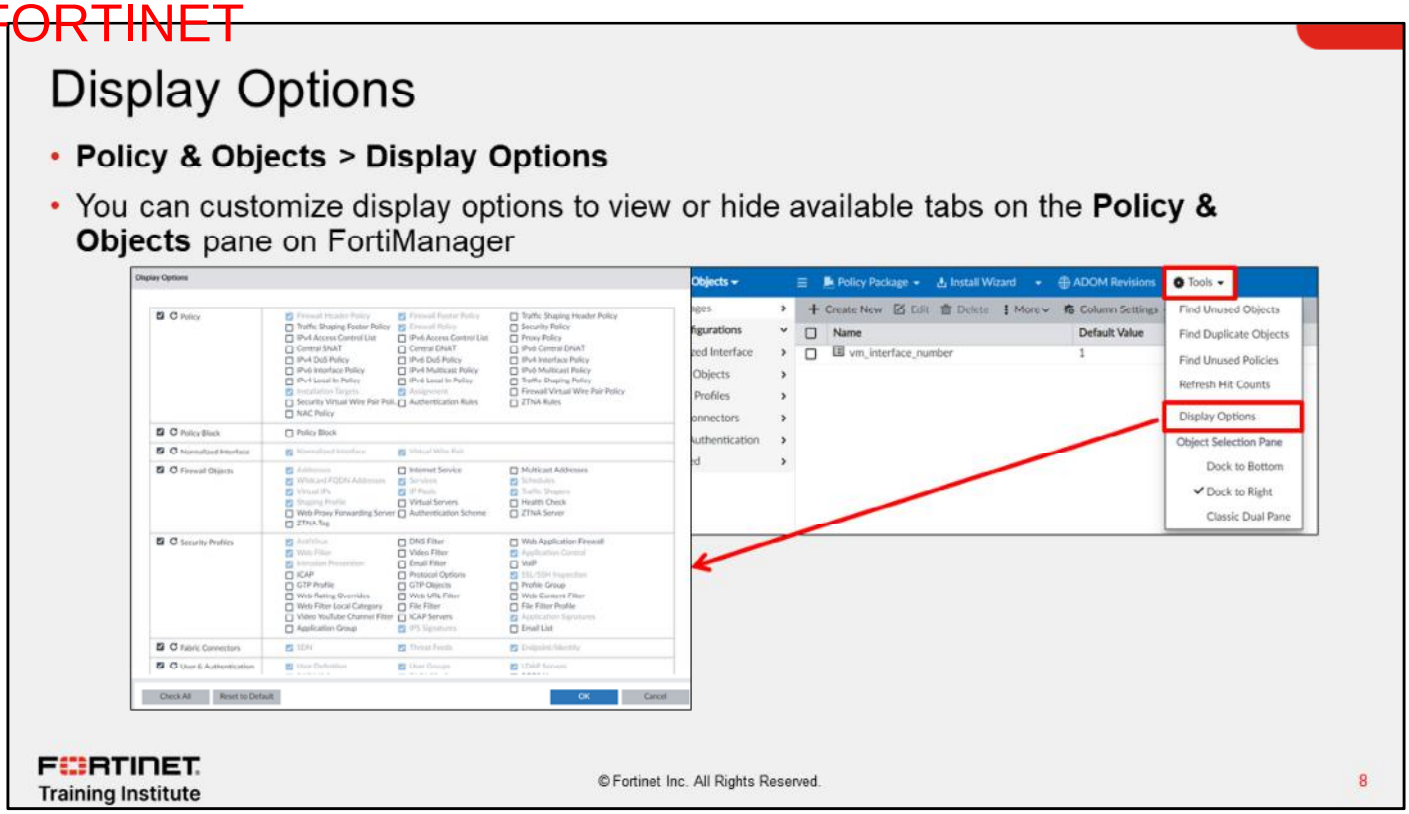
All objects in an ADOM are managed by a single database that is unique to that ADOM. Objects inside the database include firewall objects, security profiles, users, and devices.

Objects are shared in the ADOM and can be used among multiple policy packages. This simplifies the job of the administrator. For example, you can create a security profile once and attach it to multiple policy packages for installation on multiple FortiGate devices.

To create or edit the existing object, in **Object Configurations**, select the object type from the menu on the left side of the screen.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



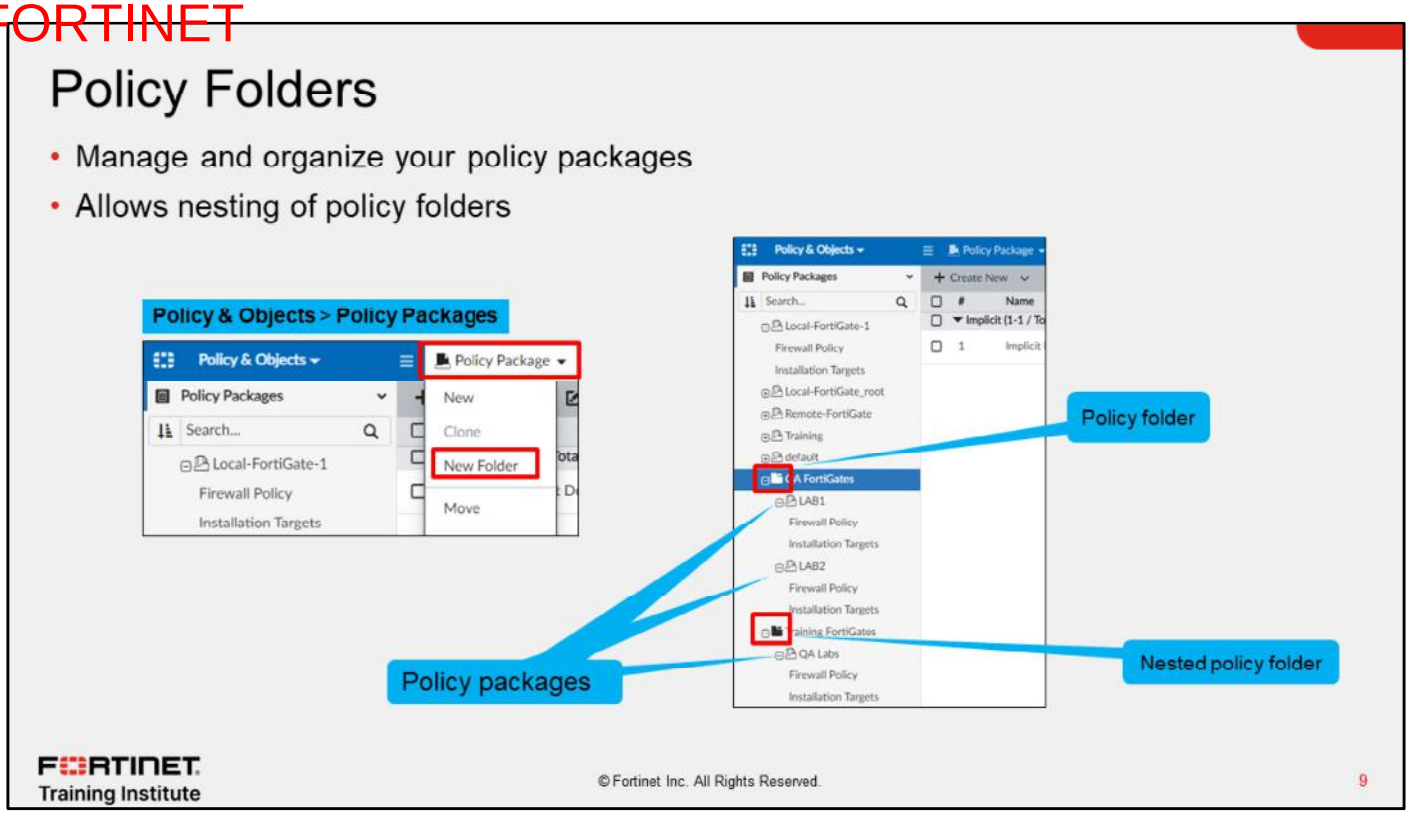
The **Display Options** feature allows you to display specific features in the GUI. The available display options depend on the ADOM version and vary from one ADOM to another.

By default, when you open **Display Options**, the checkboxes for the most common options are selected. You can show or hide a feature in **Display Options** by selecting or clearing the checkbox beside the feature. You can show all of the options in a category by selecting the checkbox beside the category name, or show all of the categories by selecting **Check All** at the bottom of the **Display Options** window.

You can also enable additional firewall policy types such as NAT64, IPv6, and interface policies in **Display Options**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

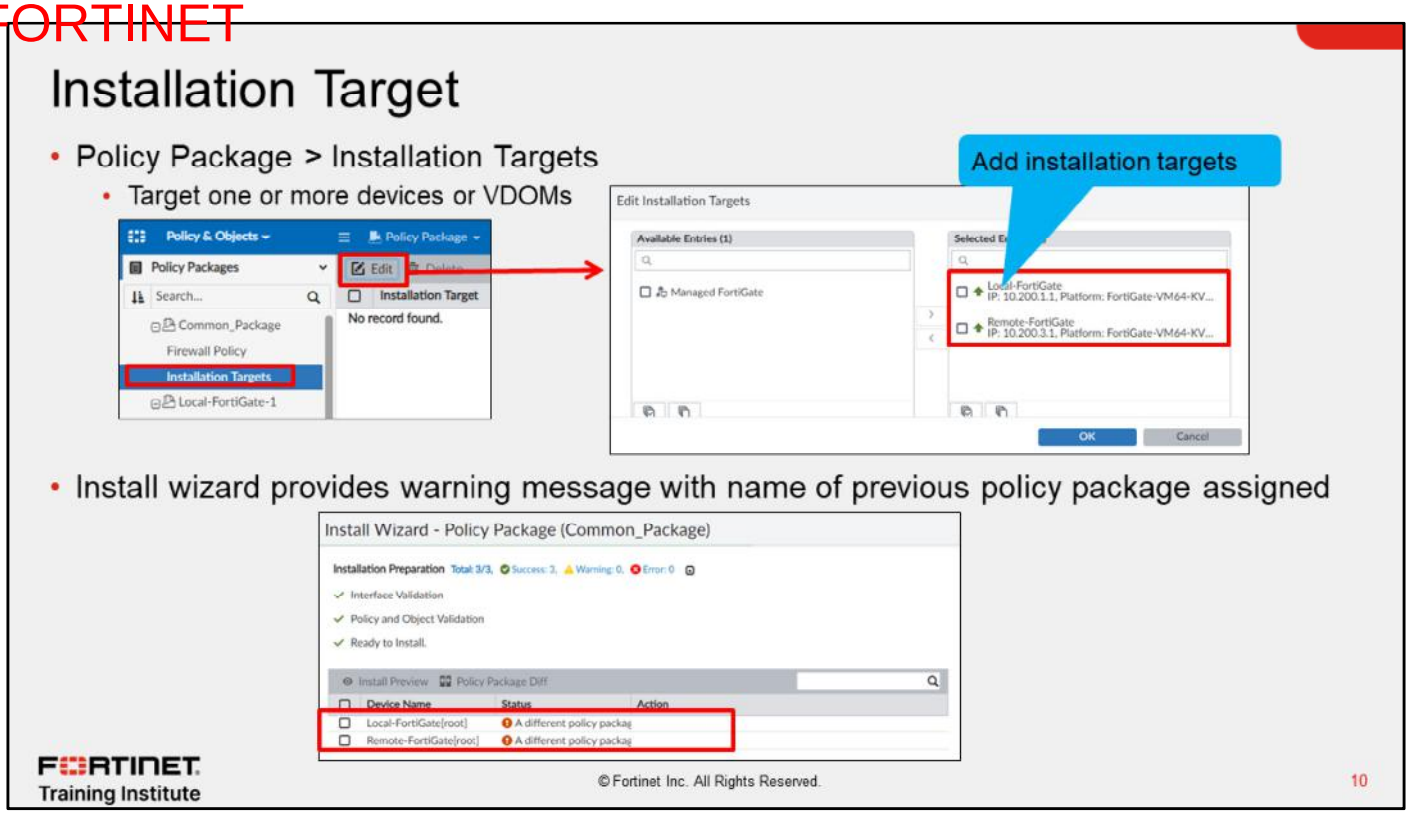


Policy folders help you manage your policy packages. You can customize policies based on organization, geography, security requirements, or legal requirements, and organize policies in specific policy folders.

You can create new policy sub-folders in policy folders to help you better organize your policy packages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



A policy package has an installation target on one or more devices or VDOMs. Policy packages can share the same installation target, however, only one policy package can be active on a device or VDOM. The active policy package is listed on the **Device Manager** pane.

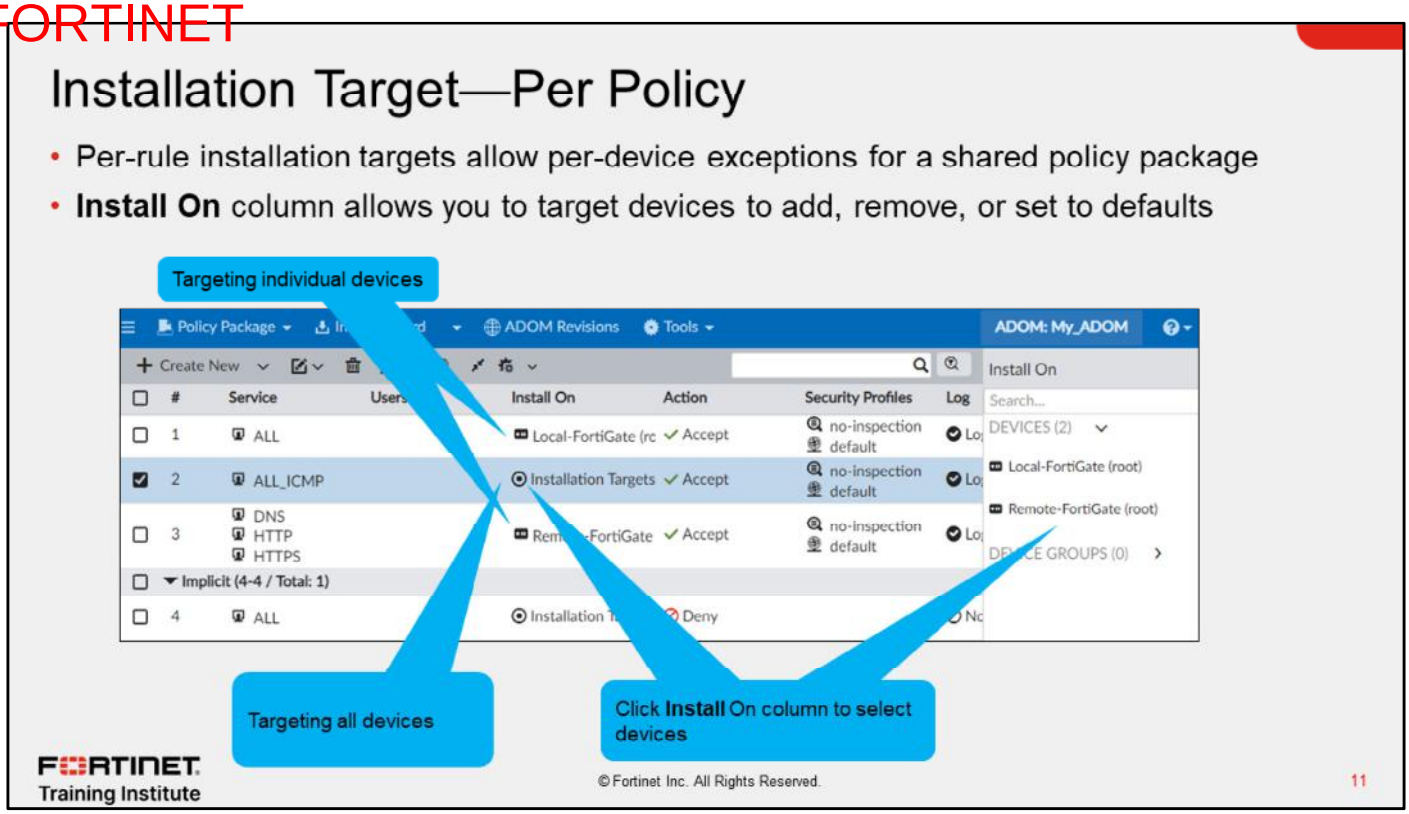
You can add, edit, or delete an installation target on the **Installation Targets** pane.

After you add an installation target, it appears in the list of **Installation Targets**. When you install a newly assigned policy package on a target, the installation wizard displays a warning message that contains the name of the previously assigned policy package.

After you install the new policy package, it appears as the active policy package for these devices or VDOMs on the **Device Manager** pane, in the **Policy Package Status** column.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



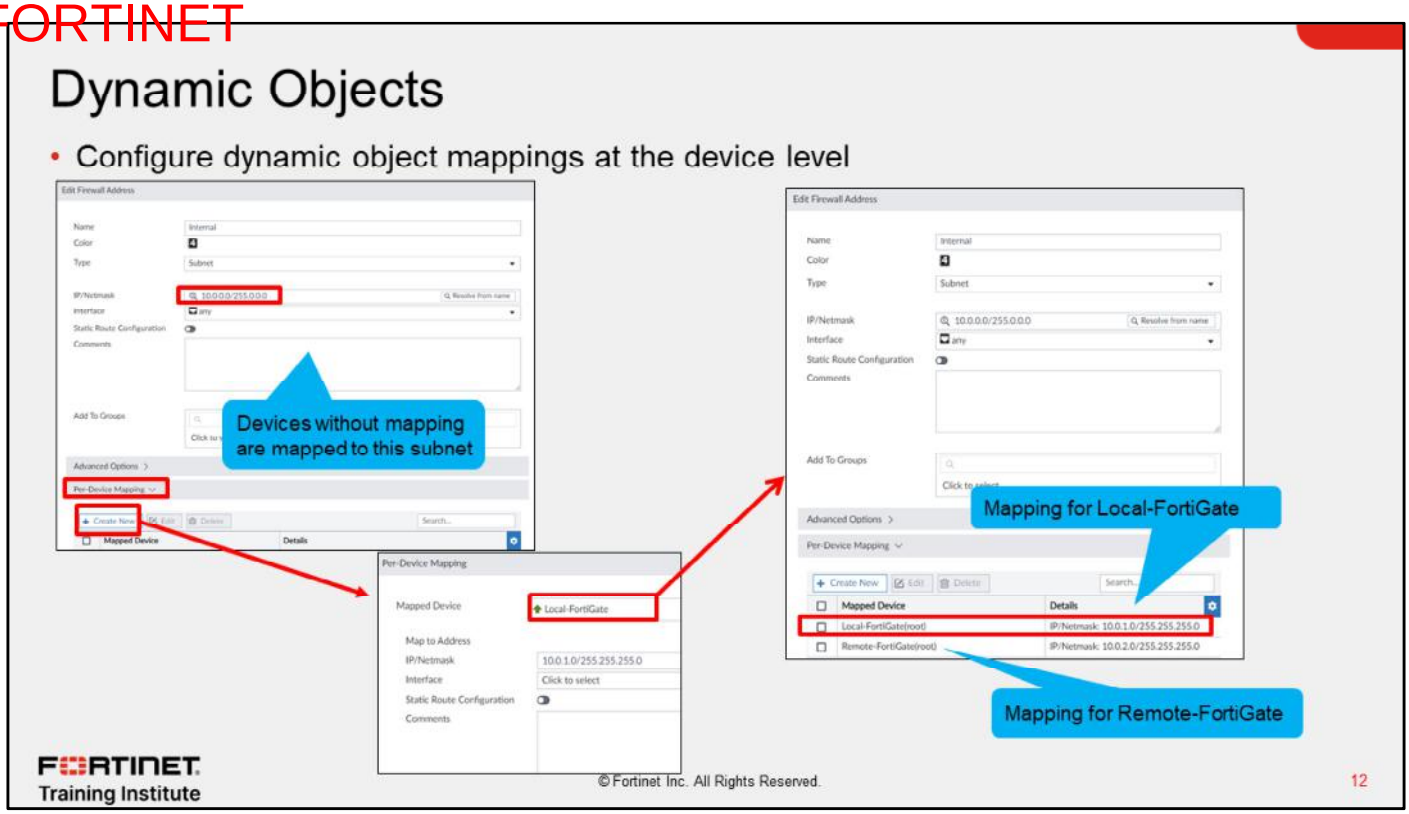
What if you need to share a policy package among many devices, with the exception of only a few policies for specific FortiGate devices?

You can perform granular installation targets per rule in the actual policy by clicking the **Install On** column. This allows you to target devices to add, remove, or set to defaults.

So, by using an installation target, you can share a policy package among multiple devices, and define rules per device in the policy. Shared policy packages are helpful in environments where many devices need to share common policies (with the exception of a few policies that you can target per device), and eliminate the need for multiple policy packages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



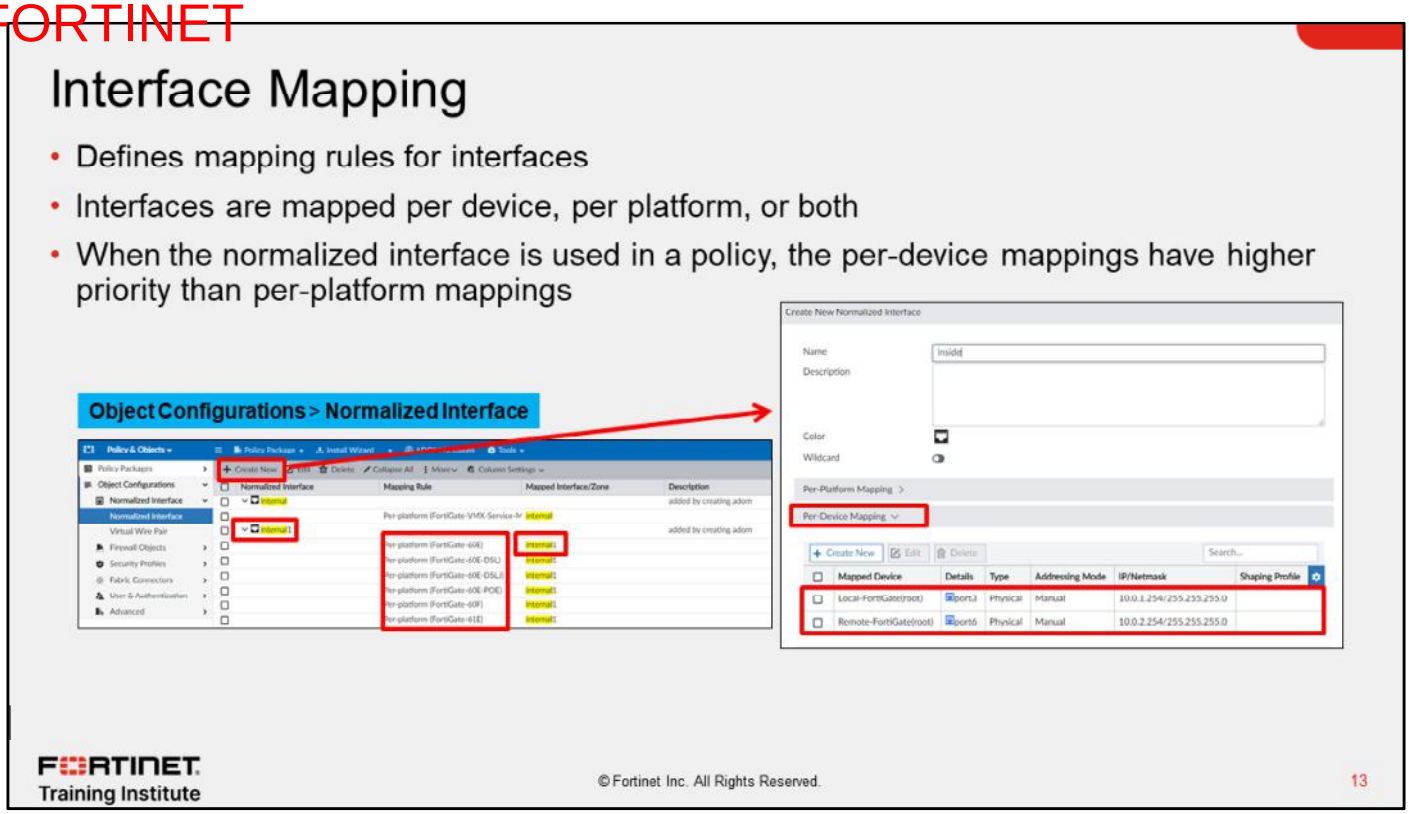
All objects in an ADOM are managed by a single database unique to the ADOM. Many objects now include the option to enable dynamic mapping. You can use dynamic objects to map a single logical object to a unique definition per device. You can dynamically map common features such as *addresses, interfaces, virtual IPs,* and *IP pools.* A common example is a firewall address. You may have a common name for an address object, but have a different value depending on the device it is installed on.

In the example shown on this slide, the dynamic address object **Internal** refers to the internal network address of the managed firewalls. The object has a default value of `10.0.0.0/8`. The mapping rules are defined per device. For Remote-FortiGate, the address object **Internal** refers to `10.0.2.0/24`, whereas for Local-FortiGate the same object refers to `10.0.1.0/24`. The devices in the ADOM that do not have dynamic mapping for **Internal** have a default value of `10.0.0.0/8`.

To add devices for dynamic mapping, select **Per-Device Mapping** arrow, and then, in the **Per-Device Mapping** section, click **Create New**. In the pop-up window that opens, select the device and set the IP range/subnet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Default normalized interfaces are created when ADOMs are created. Default normalized interfaces contain a number of per-platform mapping rules for all FortiGate models.

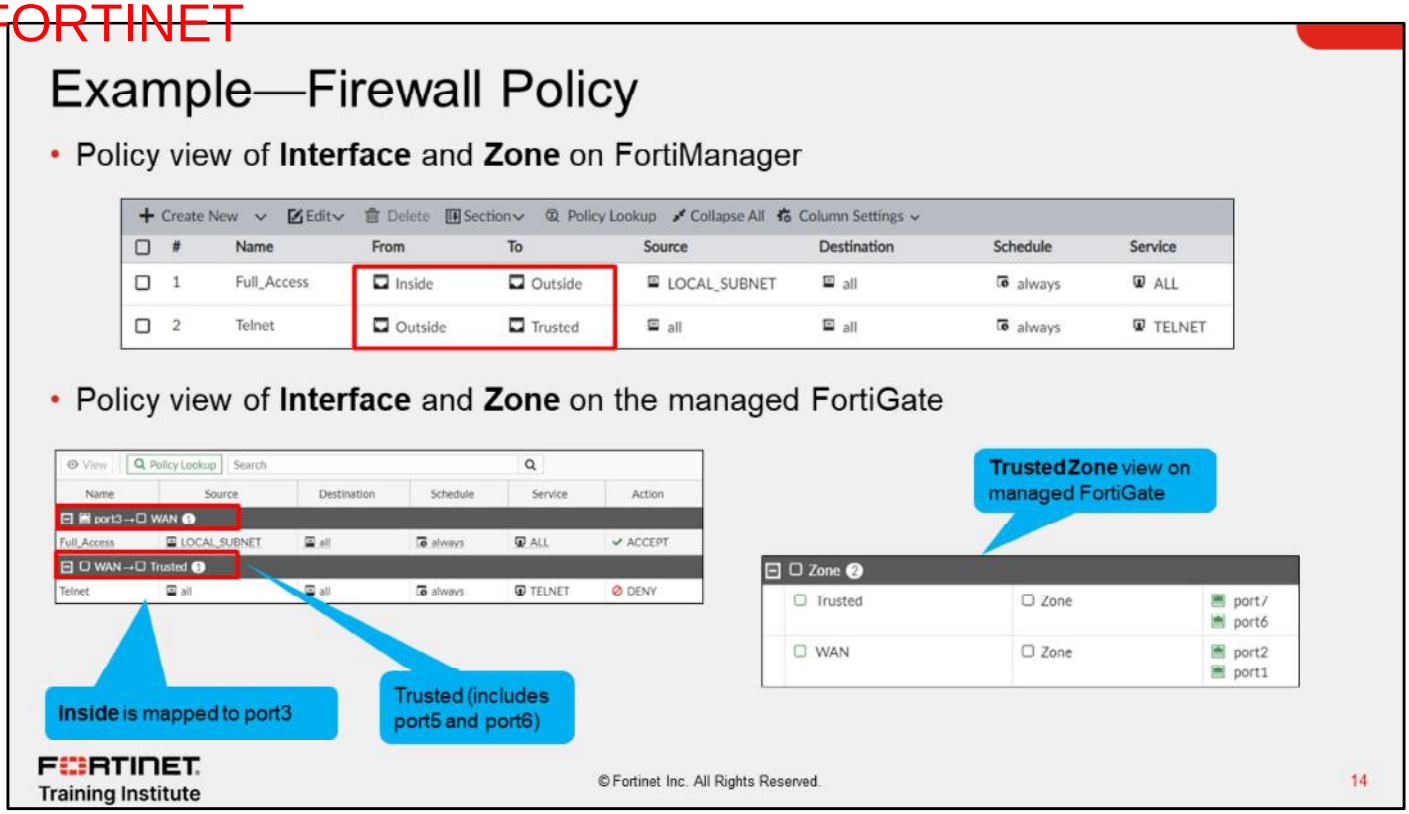
In the example shown on this slide, interface internal1 is mapped to internal1 for highlighted platforms. Default per-platform mapping rules allow you to install policies on FortiGate devices without first creating custom mapping rules.

You can map normalized interface names to different physical interface names on different FortiGate models. In the example shown on this slide, the normalized interface named Inside is mapped to port3 for Local-FortiGate and to port6 for Remote-FortiGate.

You can also select normalized interfaces when you create virtual wire pairs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Inside is mapped to port3 on Local-FortiGate. Therefore, after a firewall policy is installed on the managed FortiGate, the Inside interface will appear as port3.

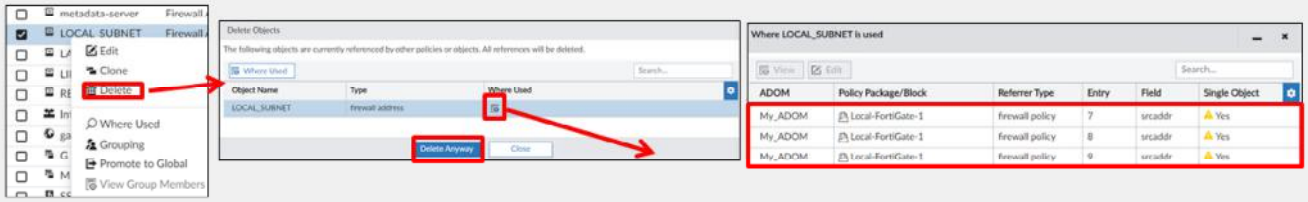
Trusted, however, remains untouched, because you installed it on the device as a zone and the port6 and port7 interfaces are part of it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Used Objects

- You can delete a used object
  - You can view where the object is used before deleting



- However, if you delete an object that is referenced in a firewall policy, FortiManager replaces it with a **none** object
  - **none** object is equal to null, which means any traffic that meets that firewall policy will be blocked

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

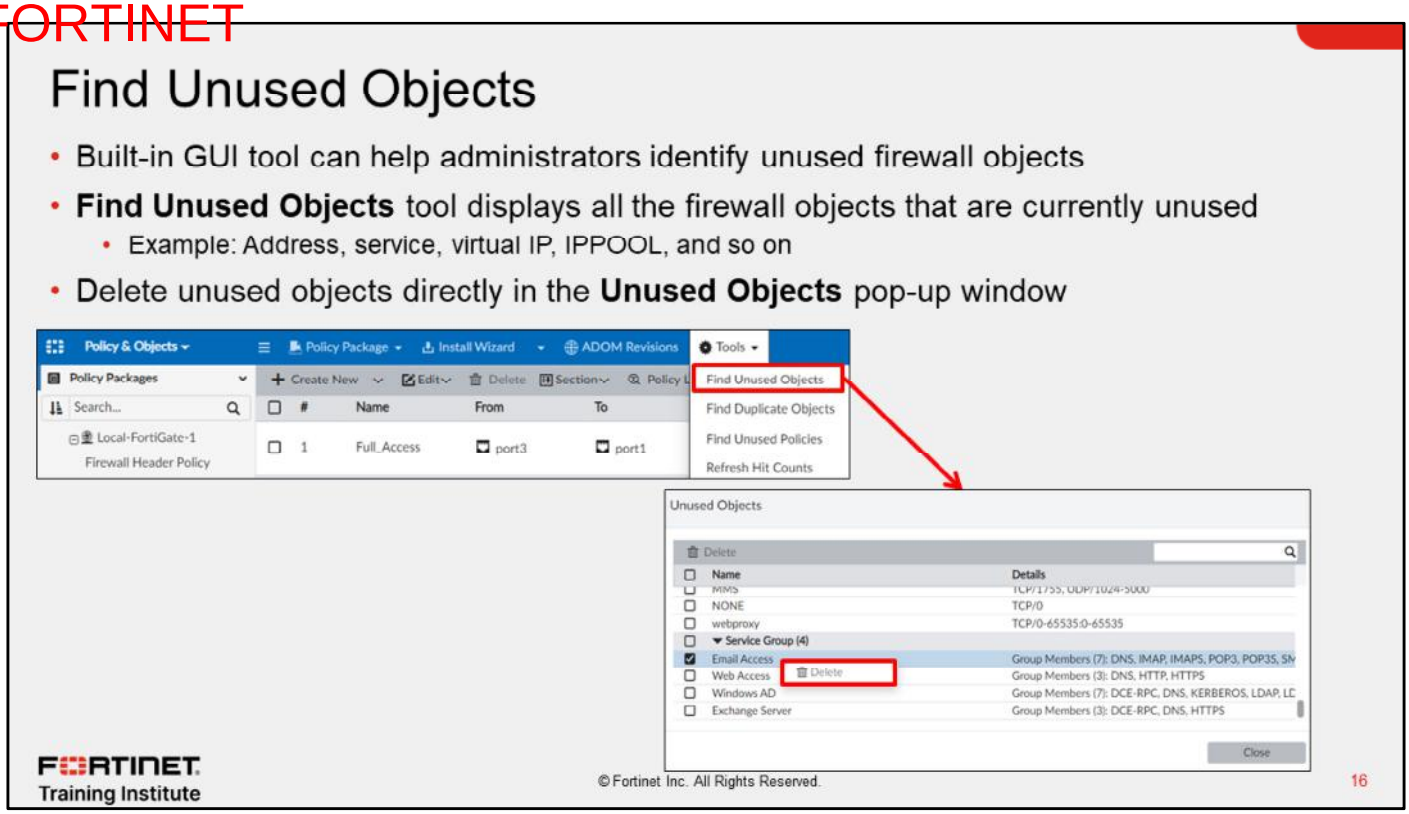
15

On FortiManager, it is possible to delete a used object. FortiManager will display a warning message stating that the object is currently used by other firewall policies or objects. To view the references of this object, click **Where Used**. However, if you delete a used object, FortiManager will replace it with a **none** object. The **none** object is equal to null, which means any traffic that meets that firewall policy will be blocked. Unless, there is a more broad policy that still meets the traffic requirement or a policy defined to allow all traffic (catch all).

You should double-check all references to objects before deleting them, to avoid unintended firewall policy behavior.

Vouchers & Dumps are Available | WhatsApp +201224560923

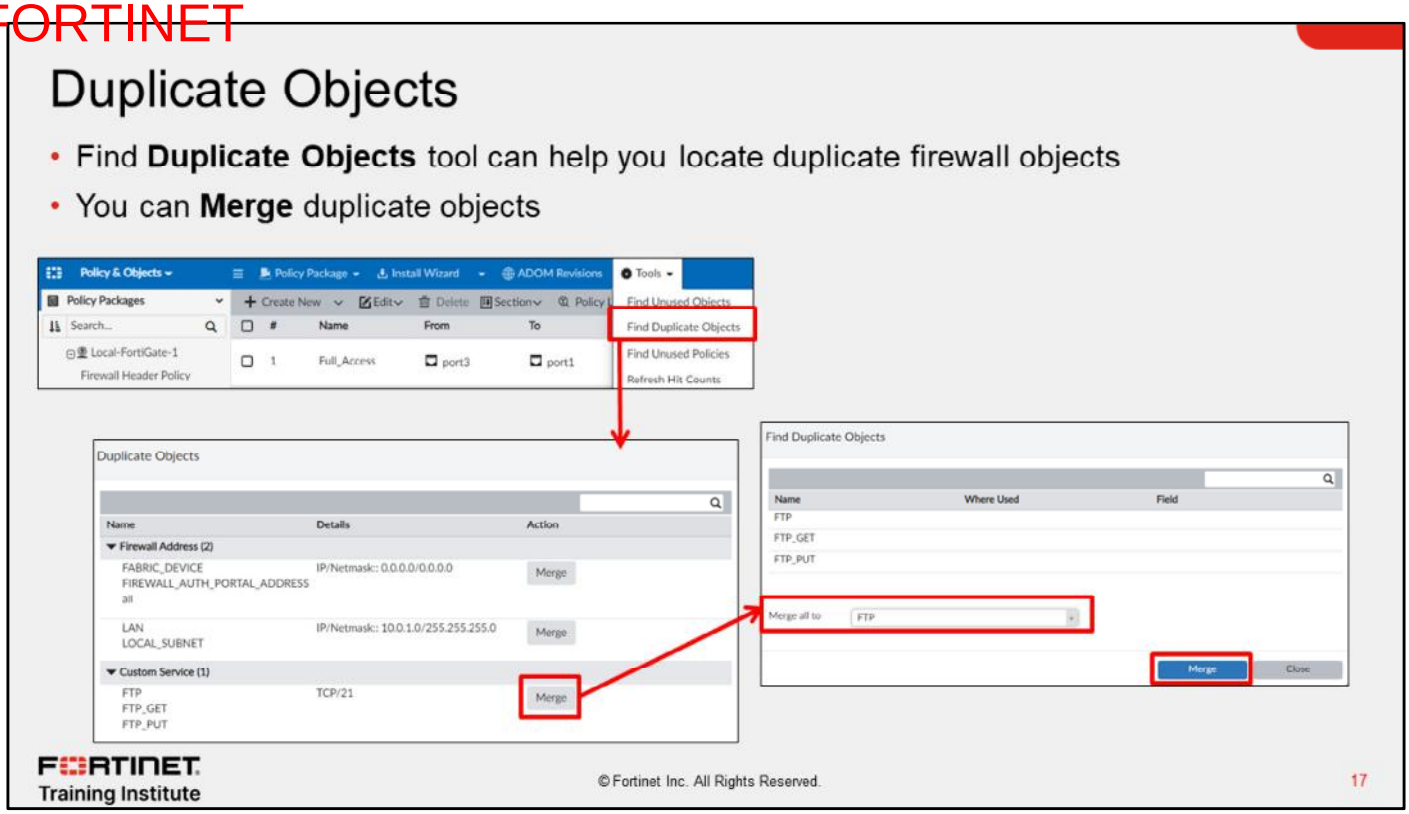
DO NOT REPRINT Brave-dumps.com
© FORTINET



Find Unused Objects is a built-in GUI tool available to administrators to help you locate all unused firewall objects in the FortiManager ADOM object database. **Find Unused Objects** searches all types of firewall objects and displays the results in a pop-up window. You can delete unused objects directly in the **Unused Objects** pop-up window. This removes the selected object from the FortiManager ADOM objects database.

Vouchers & Dumps are Available | WhatsApp +201224560923

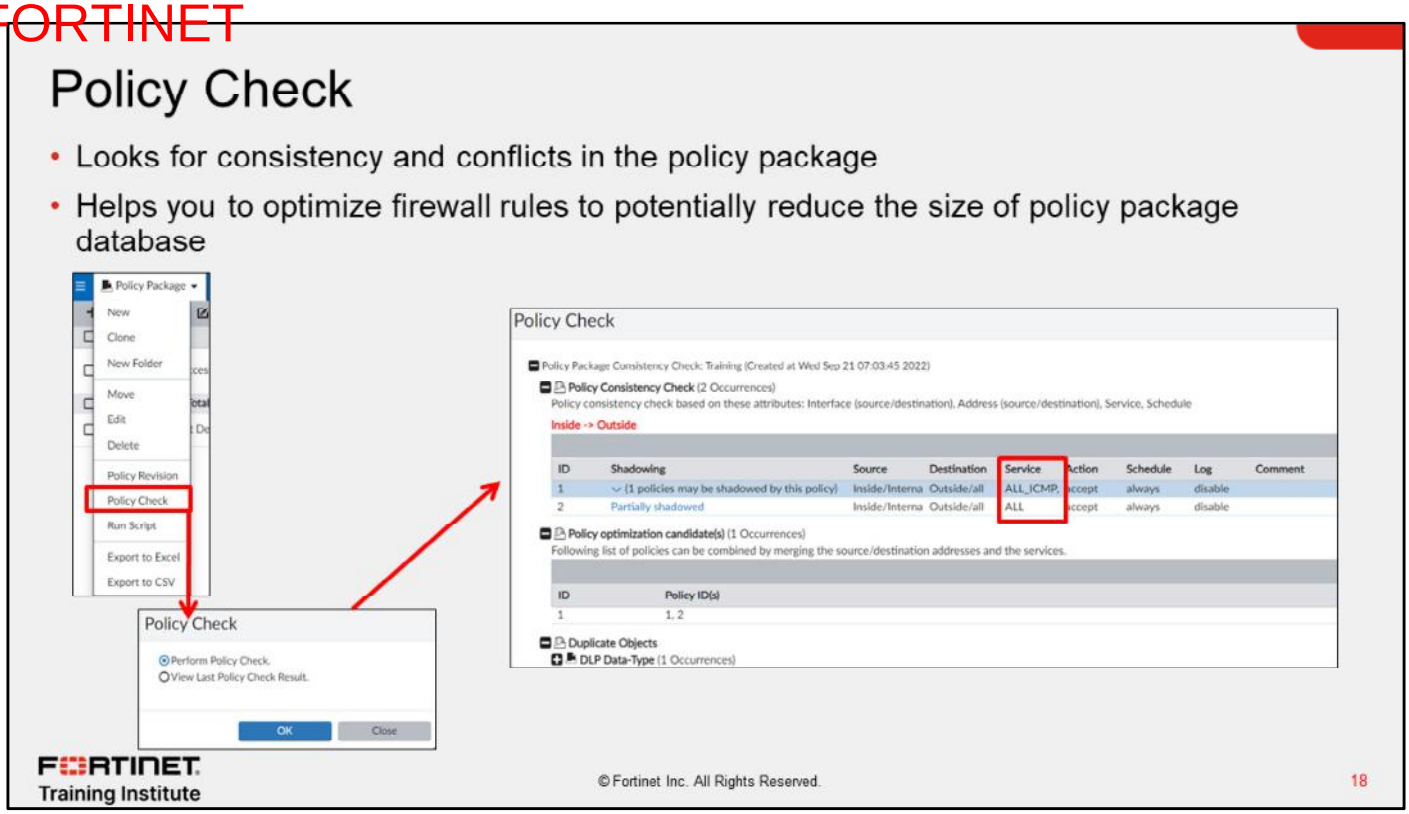
DO NOT REPRINT Brave-dumps.com
© FORTINET



Similar to **Find Unused Objects**, the **Find Duplicate Objects** tool searches the FortiManager firewall object database and displays all objects that have duplicate values assigned to them. In the example shown on this slide, the tool found that the custom service objects **FTP, FTP_GET**, and **FTP_PUT** have the same value. After duplicate objects are found, you can use the same wizard to merge objects, if needed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Policy Check provides recommendations only on what improvements can be made—it does not perform any changes. It uses an algorithm to evaluate policy objects based on:

- Source and destination interface policy objects
- Source and destination address policy objects
- Service and schedule policy objects

Policy Check checks for:

- Duplication, where two objects have identical definitions
- Shadowing, where one object completely shadows another object of the same type
- Overlap, where one object partially overlaps another object of the same type
- Orphaning, where an object has been defined, but has not been used anywhere

To perform a policy check, select a policy package, and then, in the **Policy Package** drop-down list, click **Policy Check**. In the **Policy Check** dialog box, you can select one of the following options:

- **Perform Policy Check**: This performs a policy check for consistency and provides any conflicts that may prevent your devices from passing traffic.
- **View Last Policy Check Result**: This allows you to view the results of the most recent consistency check.

In the example shown on this slide, policy ID 2 and 1 have the same source and destination in terms of interface and objects, but have different services. You can combine these two policies by adding the services to one policy.

It is important to note that the policy check only provides *recommendations* on what improvements can be made—it does not actually make any changes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What is the purpose of dynamic objects?
   A. To merge duplicate objects automatically
   ✓B. To map a single logical object to a unique definition per device

2. Which statement about a policy package is true?
   ✓A. A policy package can have multiple installation targets in an ADOM.
   B. There can be only one policy package per ADOM.

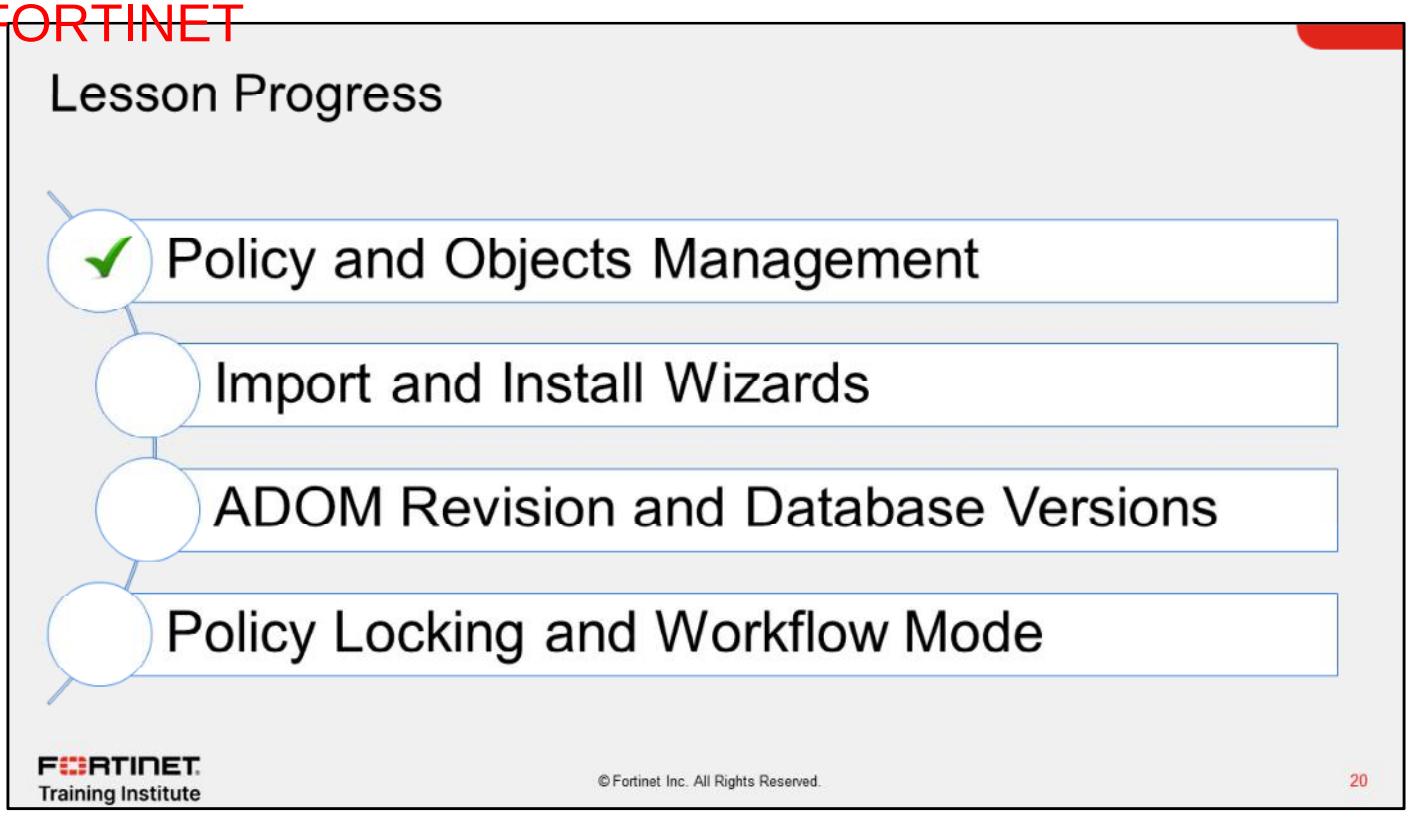
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

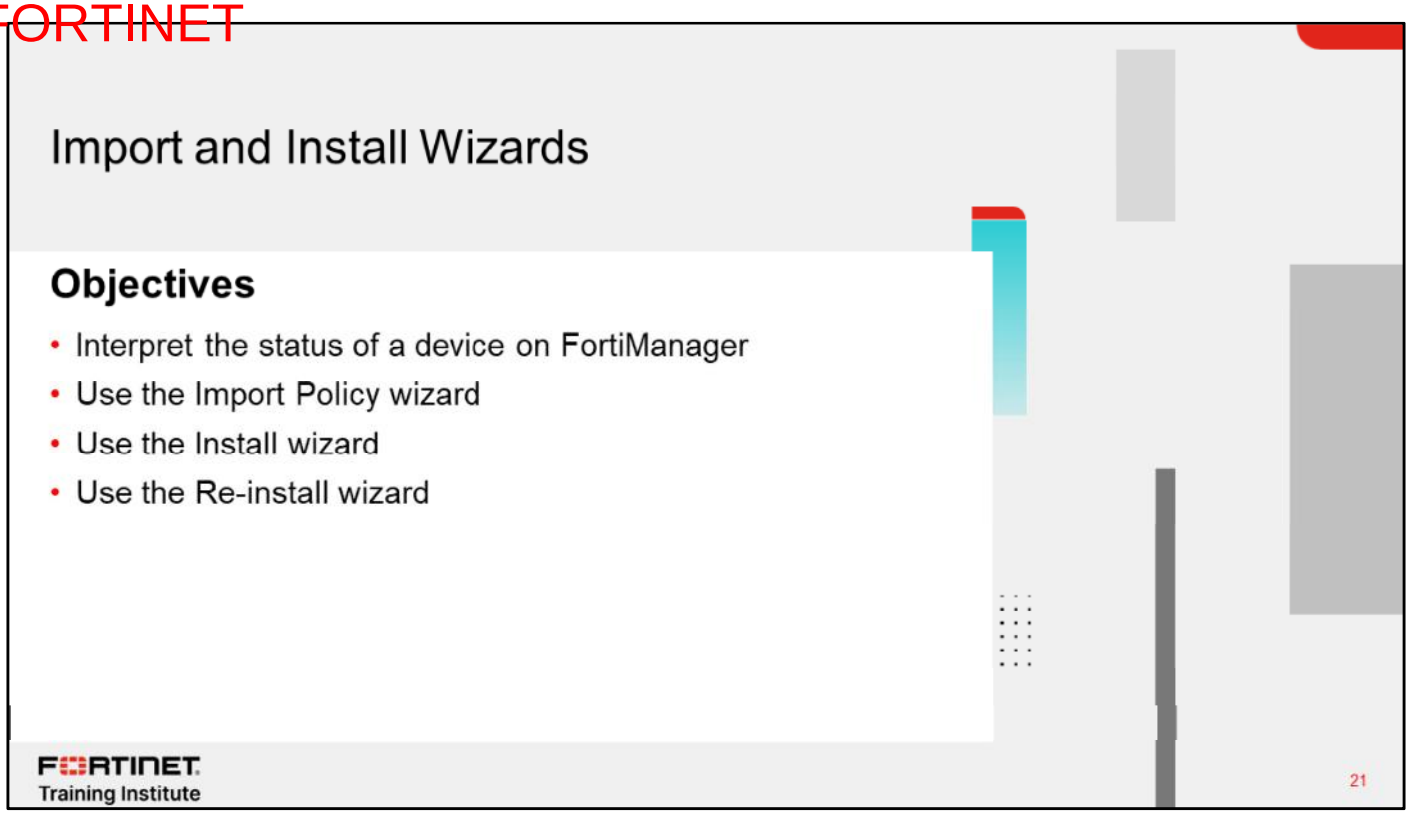


Good job! You now understand policy and objects management.

Now, you will learn about import and install wizards.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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

By demonstrating competence in understanding the options for configuring and managing firewall policies on the **Policy & Objects** pane, you will examine the **Import Policy** wizard and the **Install wizard**, which you can use to manage devices on FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Policy Package Status

```
FMG-VM64 # diagnose dvm device list
--- There are currently 3 devices/vdoms managed ---
...
TYPE              OID    SN                HA      IP              NAME                  ADOM    IPS
fmgfaz-managed    252    FGVM010000065036  -       10.200.3.1      Remote-FortiGate      root  6.00741
(regular)          |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                   |- vdom:[3]root flags:0 adom:root pkg:[modified]Remote-FortiGate
...
--- End device list ---
```

Device Manager > Managed FortiGate

Edit | Delete | Import Configuration | Install | Table View | More

Device Name	Config Status	Policy Package Status
Local-FortiGate	Auto-update	Local-FortiGate
Remote-FortiGate	Auto-update	Remote-FortiGate

FORTINET Training Institute

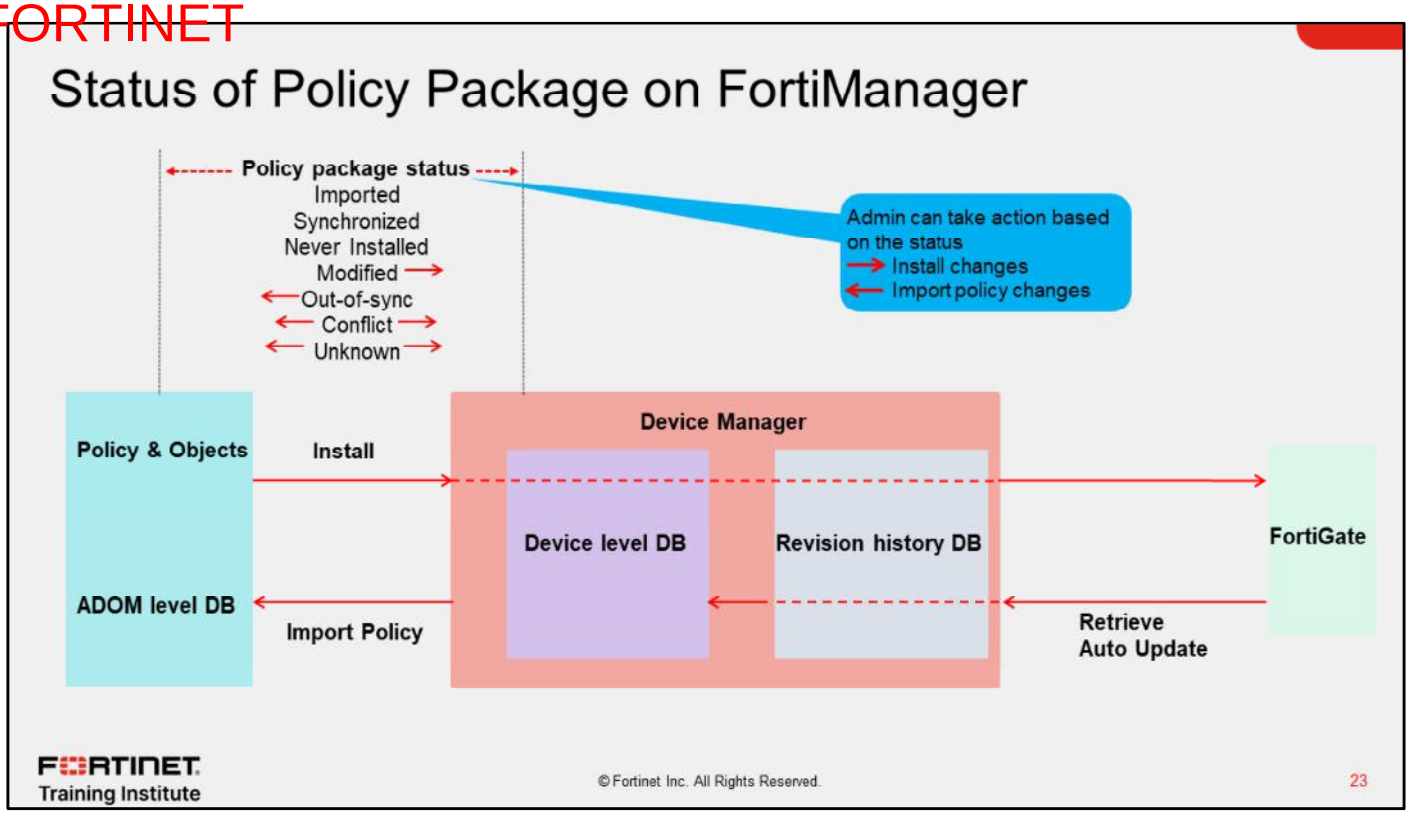
© Fortinet Inc. All Rights Reserved.

22

The screen capture at the top of the slide shows the output of the `diagnose dvm device list`, in which the policy package is `modified` while the configuration status is `in sync`. This indicates that only the policy package is modified, not the device-level settings. The same information is also available on the GUI, as shown in the screen capture on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After every retrieve, auto-update, and installation operation, FortiManager stores the FortiGate configuration in the revision history.

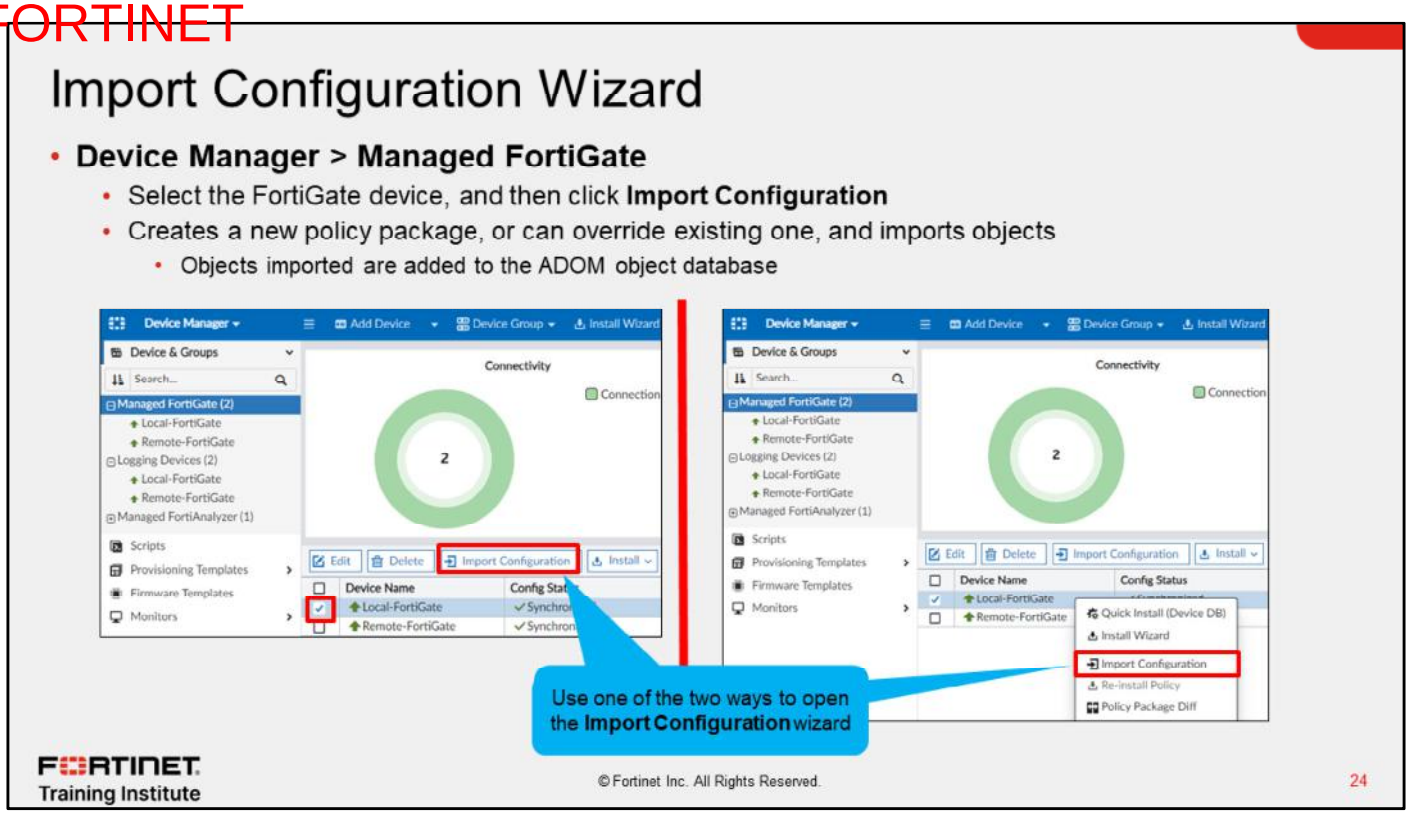
The illustration on this slide shows the status of the policy package:

- **Imported:** Indicates that a policy package was successfully imported for a managed device.
- **Synchronized:** Indicates that a policies and objects are synchronized between FortiManager and the managed device.
- **Never Installed:** Policy package was never created, hence it was never imported for a managed device.
- **Modified:** Policy package configuration is changed on FortiManager and changes have not yet pushed to the managed device.
- **Out-of-sync:** The latest policy package does not match the policies and objects configuration on the latest revision history because of configuration changes made locally on FortiGate or a previous partial installation failure. You should perform a retrieve, and then import policies from FortiManager.
- **Conflict:** If you make policy configuration changes locally on FortiGate and don't import the changes into the policy package, and you also made the changes on FortiManager, the status enters conflict state. Depending on the configuration changes, you can either import a policy package or install the changes from FortiManager.
- **Unknown:** FortiManager is unable to determine the policy package status.

You can resolve most policy status issues by importing a policy package or installing a policy package.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



It is common for FortiGate to have a running configuration already. The **Import Configuration** wizard guides you through importing policies and objects into FortiManager. When you import a device, you create a new policy package that does not interfere with other packages. However, objects you import will add to, or update, existing objects. You may want to create a new ADOM revision before performing an import.

If you add an unregistered device to FortiManager, you must run the **Import Configuration** wizard after promoting the device.

The next few slides explore the stages that the wizard guides you through.

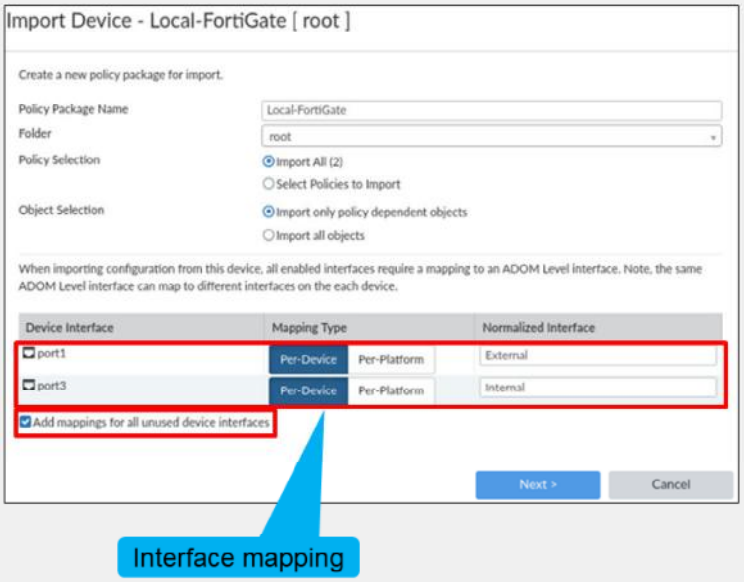
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Import Configuration Wizard—Interface Map and Policy

- Maps the device interface to the ADOM interface to create a reference of the interfaces in the FortiManager database
- Creates a policy package in **Policy & Objects > Policy Packages**

Note: By default, the **Add mappings for all unused device interfaces** checkbox is selected and creates an automatic mapping for the new interface. The FortiManager administrator doesn't need to create a manual mapping if this option is enabled. This feature is very useful in large deployments.



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

By default, interface mappings exist for interfaces configured on the firewall. This allows the device interfaces to be referenced in policy packages. You can rename the ADOM interface mapping in the wizard. In the example shown on this slide, **port1** is renamed **External** and **port3** is renamed **Internal**. Policies on the **Local-FortiGate** are on **port1** and **port3**, but on FortiManager they are referenced locally as **External** and **Internal**. Note that, by default, the **Add mappings for all unused device interfaces** checkbox is selected and creates an automatic mapping for the new interface.

The wizard performs a policy search to find all policies in preparation for import into the FortiManager database. You may choose to import all firewall policies, or select specific policies to import. If you choose to import only specific policies into the policy package and later install policy changes, the policies that were not imported will be deleted locally on FortiGate. This is because FortiManager does not have those policies in the policy package.

Also, you can choose whether to import all configured objects, or only the objects referenced by the current firewall policies. Regardless of whether you choose to import only policy-dependent objects or all objects, the system will delete orphan (unused) objects that are not tied to policies locally on FortiGate in the next installation. But if you choose to import all objects, then the system imports all used and unused objects in the FortiManager ADOM object database and can use them later by referencing the policies on FortiManager and installing them on the managed devices.

By default, **Import All** and **Import only policy dependent objects** are selected when you run the **Import Policy** wizard. As a word of caution, if you are managing many devices in an ADOM and select **Import all objects** for all devices, the object database will become too full of unused objects, which can be overwhelming for an administrator.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Import Policy Wizard—Summary

- Imports objects into ADOM database, policies into policy package

- You can save import report in .txt format

```
Start to import config from device(Local-FortiGate) vdom(root) to adom(root),
package(Local-FortiGate)
"application list",SUCCESS,"(name=wifi-default, oid=2459, update previous object)"
...
"authentication setting",SUCCESS,"(name=, oid=3393, new object)"
...
"firewall address",SKIPPED,"(name=all, oid=2264, DUPLICATE)"
"firewall address",SKIPPED,"(name=none, oid=2265, DUPLICATE)"
"firewall address",SUCCESS,"(name=REMOTE_ETH1, oid=2266, new object)"
"firewall address",SUCCESS,"(name=REMOTE_SUBNET, oid=2267, new object)"
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

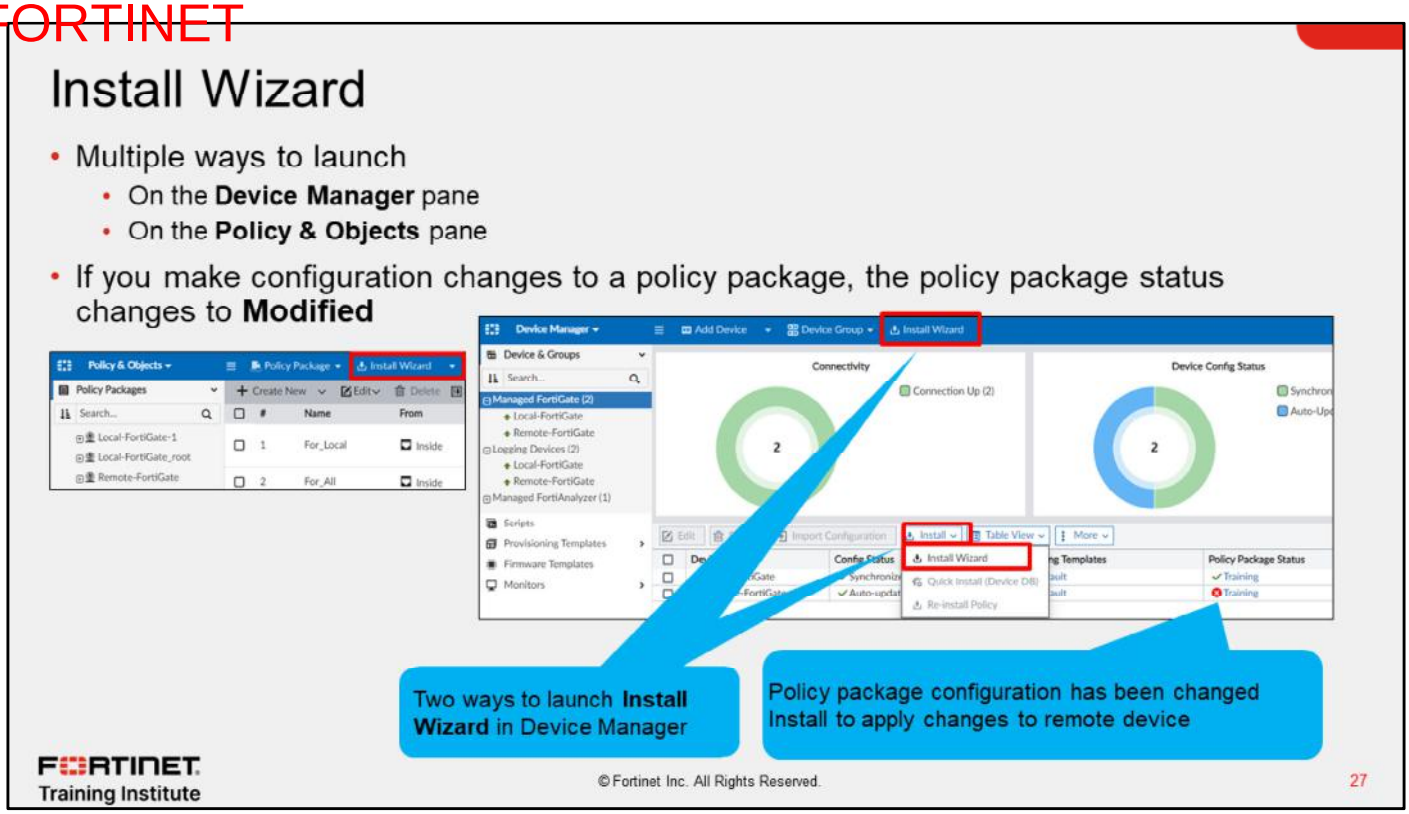
After the import is complete, the wizard provides the **Policy Import Summary** and the **Download Import Report**. You can download the import report, which is only available on the **Import Device** page. You can view the report using any text editor.

As a best practice, you should download the report.

The import report provides information about FortiGate, the ADOM name on FortiManager, and the policy package name. The report also provides additional information, such as the objects that have been added as new objects. Existing objects that have the same values locally on FortiGate and FortiManager are referred to as `DUPLICATE`. If the value of an existing object is changed, FortiManager updates that in its database and shows `update previous object` in the import report.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

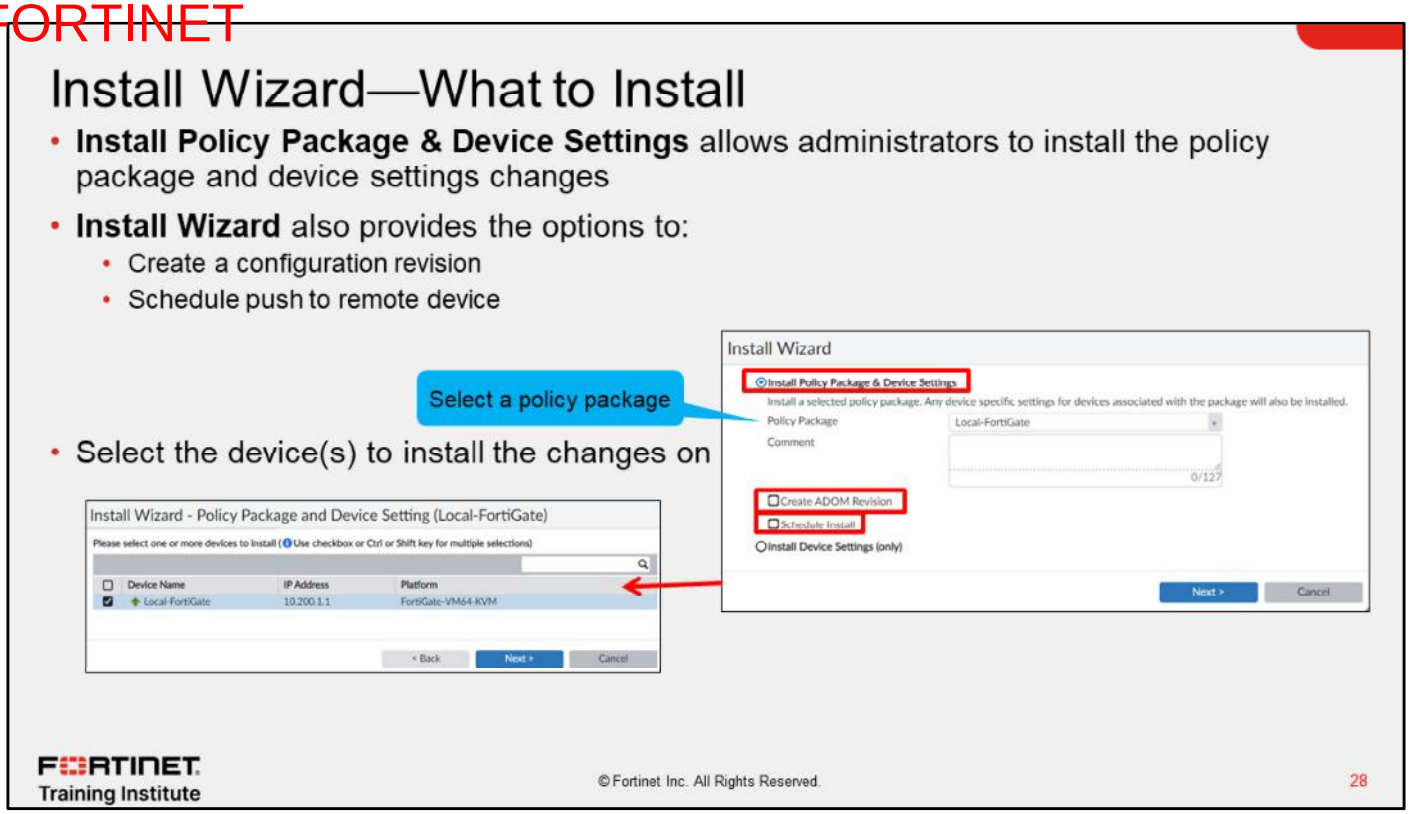


After you make configuration changes to the policy package, the **Policy Package Status** is flagged as **Modified** on the **Device Manager** pane. There are multiple ways to launch the **Install Wizard** on the **Device Manager** pane, as well as on the **Policy & Objects** pane. If you are using ADOMs, make sure you select the ADOM in the ADOM drop-down list first.

Now, you will explore the process of installing policy configuration changes using the **Install Wizard**. During this process, the policy and device configuration items are installed on the managed device. After the installation is complete, FortiManager and FortiGate are in sync and the **Policy Package Status** changes from **Modified** to **Installed** (**Synchronized**).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When you select **Install Policy Package & Device Settings**, the **Install Wizard** installs the policy package and any pending device-level changes.

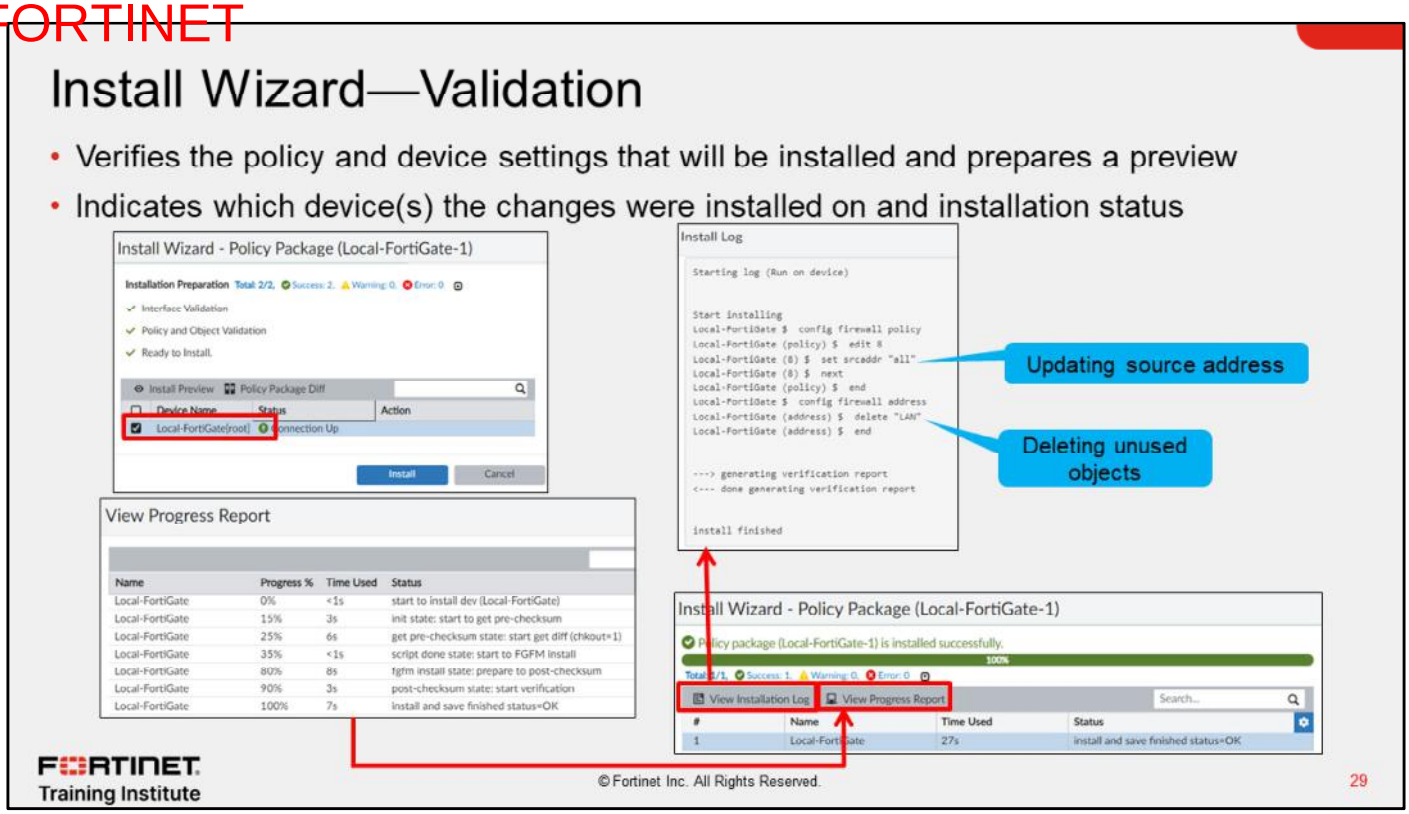
The policy package you select is displayed and you have the option to create a new ADOM revision for this installation. Note that an ADOM revision is a snapshot of the entire ADOM and not the changes specific to this policy package.

You can also enable **Schedule Install**, which allows you to specify the date and time to install the latest policy package changes.

The next step is **Device Selection**. In this step, the wizard displays the devices selected in the installation target for the specific policy package.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The next step in the wizard is validation. In this step, the wizard checks that the policy package selected is suitable for the installation targets selected, such as whether the interface mapping reference in the policy package is configured on the installation targets. If the validation fails, the installation will stop.

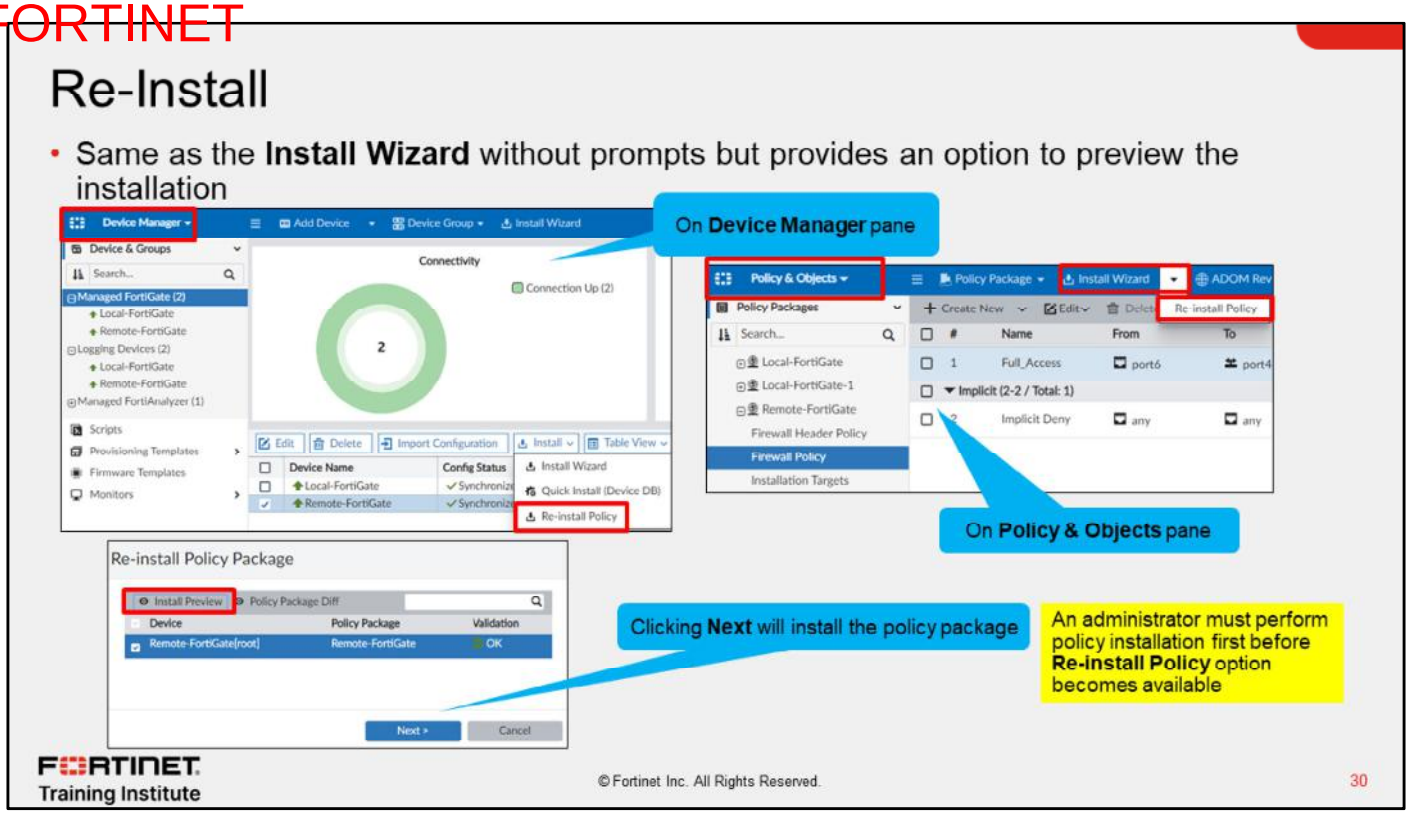
Before performing the installation, as a best practice, always preview and verify the changes that will be committed to FortiGate. If this is the first installation, you may see many changes, because objects may have been renamed during the import process and unused objects removed from the device configuration. If you don't want to proceed with the installation, you can cancel the installation at this step in the wizard.

The last step is **Install**, which is the actual installation. The wizard lists the devices on which configuration changes were installed. Any errors or warnings that occur during installation appear here as well. If the installation fails, the installation history indicates the stage at which the installation failed. You can also check the installation history for the successful installation too.

In the example shown on this slide, the wizard indicates that the configuration changes were successfully installed on FortiGate, and that FortiManager has created a new revision history for this installation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiManager also provides a **Re-install Policy** option. A re-installation is the same as an installation except there are no prompts and it provides the ability to preview the changes that will be installed on the managed device. The **Re-install Policy** will create a new revision history and apply it to all selected installation targets.

The **Re-install Policy** option works only after the first policy installation. The option is greyed out or unavailable if **Policy Package Status** on the **Device Manager** pane shows as **Never Installed** for the managed device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What does a policy package status of **Unknown** indicate?
   - ✓ A. FortiManager is unable to determine the policy package status.
   - B. The policy package was never installed from FortiManager.

2. What is the main benefit of the **Re-install Policy** option?
   - ✓ A. Can push policy with fewer steps for quick policy change
   - B. Can schedule policy push

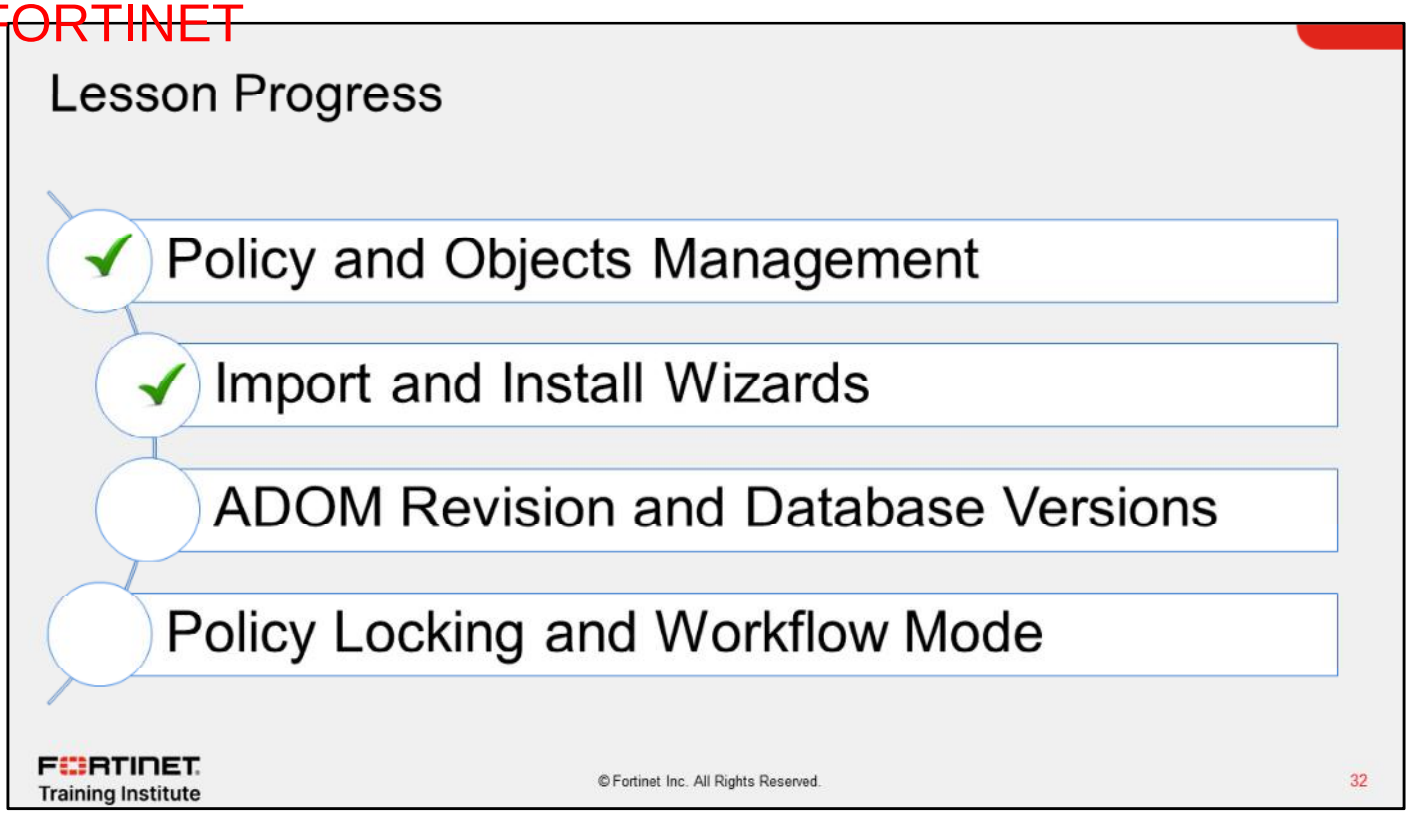
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

31

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

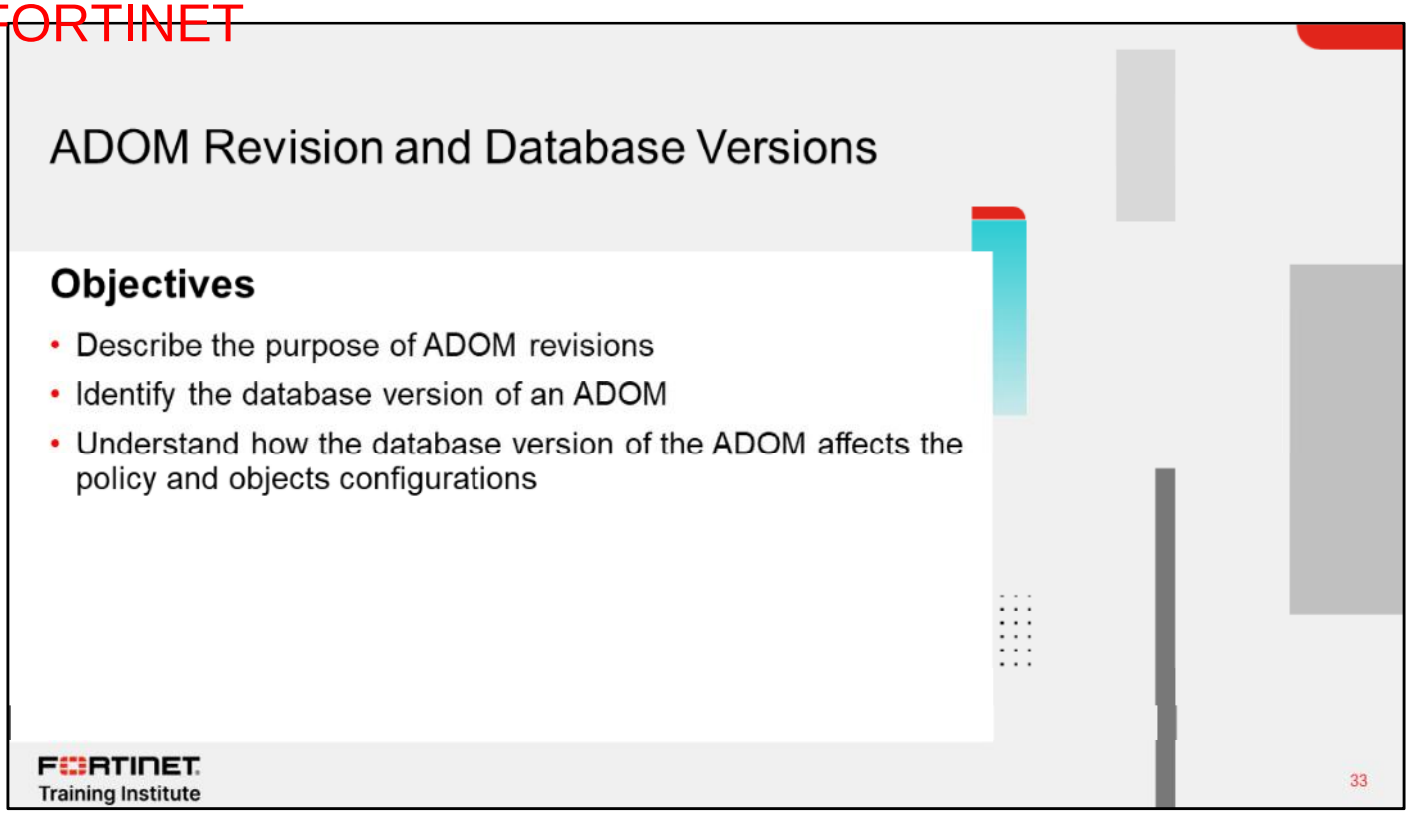


Good job! You now understand FortiManager policy and objects management, as well as the **Import** wizard and **Install** wizard.

Now, you will learn about ADOM revision and database versions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

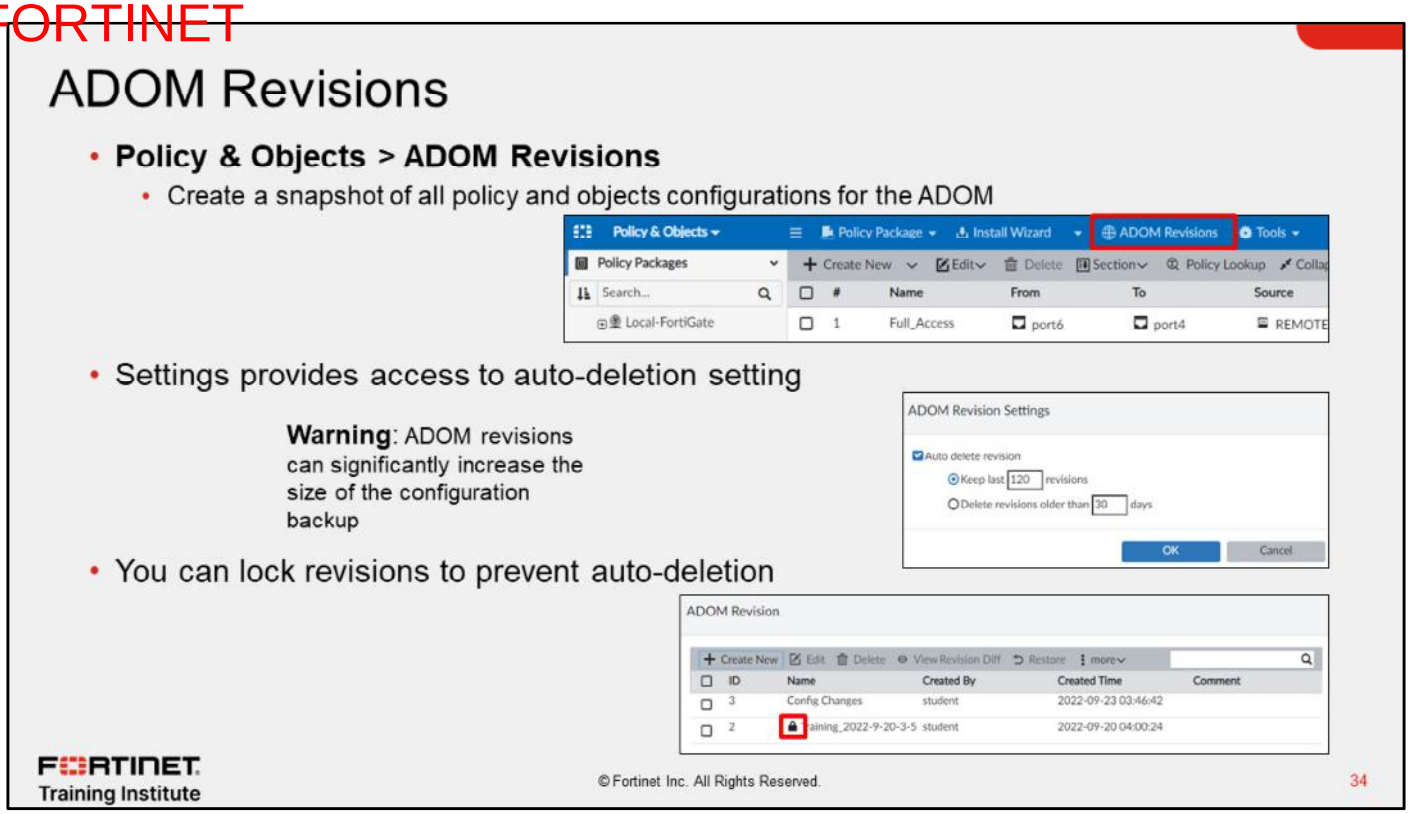


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding ADOM revisions and database versions, you will understand their effect on policy and objects configurations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



ADOM revision saves the policy package and objects locally on FortiManager.

You can create a new ADOM revision, view differences between revisions, or revert to a specific ADOM revision. As a word of caution, if you choose to revert to a specific ADOM revision, you will revert all the policy packages and objects based on that revision.

Warning: Keep in mind that ADOM revisions can significantly increase the size of the configuration backup.

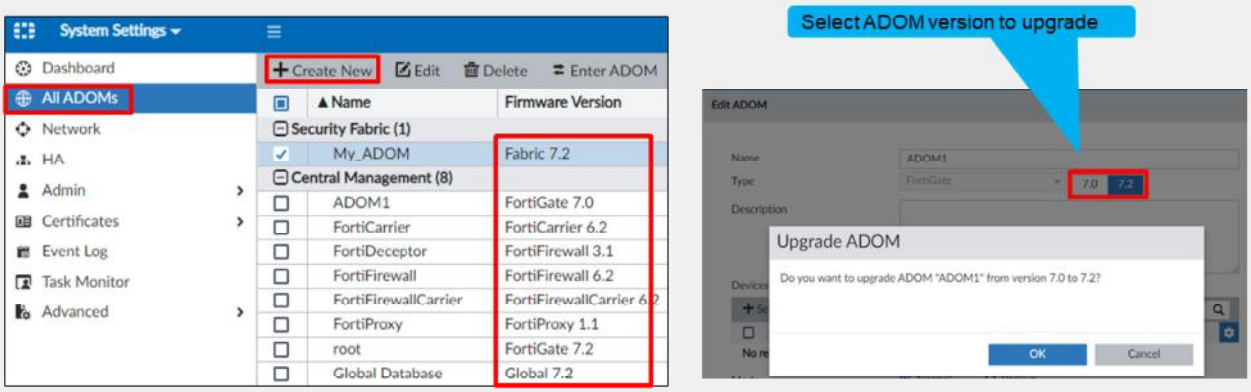
You can delete revisions automatically based on given variables, and you can lock individual revisions to prevent them from being automatically deleted. Click **Settings** for access to the auto-deletion settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Version of the ADOM Database

- Database version refers to valid syntax for that FortiOS version



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

35

Each ADOM is associated with a specific FortiOS version, based on the firmware version of the devices that are managed in that ADOM. The selected version determines the CLI syntax that is used to configure the devices. Select this version when you create a new ADOM.

It is recommended to update all of the FortiGate devices in an ADOM to the latest FortiOS firmware version before you can upgrade the ADOM version.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Moving FortiGate From One ADOM to Another

- Considerations before moving devices:
  - Policies and objects don't move to the new ADOM
    - If using a shared policy package, it is not moved to the new ADOM
  - Unused objects don't move from one ADOM to another
  - When FortiGate devices are upgraded, it is best to keep them in the same ADOM and use ADOM upgrade
- After moving the devices:
  - Import a policy package
  - Can use CLI to import unused objects if needed

```
execute fmpolicy copy-adom-object
```

- Configuration of manager panes like VPN manager does not move
  - Reconfigure all the configuration

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

36

When you move a device from one ADOM to another, policies and objects (used and unused) don't move to the new ADOM.

If you need to move a device from one ADOM to another, run the import policy wizard to import the policy package into the new ADOM.

What if you need to use unused objects from a previous ADOM in the new ADOM? You can copy objects from one ADOM to another using the FortiManager CLI.

When FortiGate devices are upgraded, it is best to keep them in the same ADOM and use the ADOM upgrade. Moving FortiGate devices to a new ADOM introduces additional work and certain complications. Also, manager panes like VPN manager does not move and FortiManager administrator must reconfigure all the VPN configuration on the managed device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the most recommended sequence of upgrading an existing ADOM?
   - ✓A. Upgrade all the devices in the ADOM first, and then upgrade the ADOM.
   - B. Upgrade the ADOM first, and then upgrade all the devices in the ADOM.

2. Why should the ADOM version match the FortiGate firmware version?
   - ✓A. To minimize CLI syntax issues between FortiGate and FortiManager
   - B. To keep the FortiGate licenses up to date

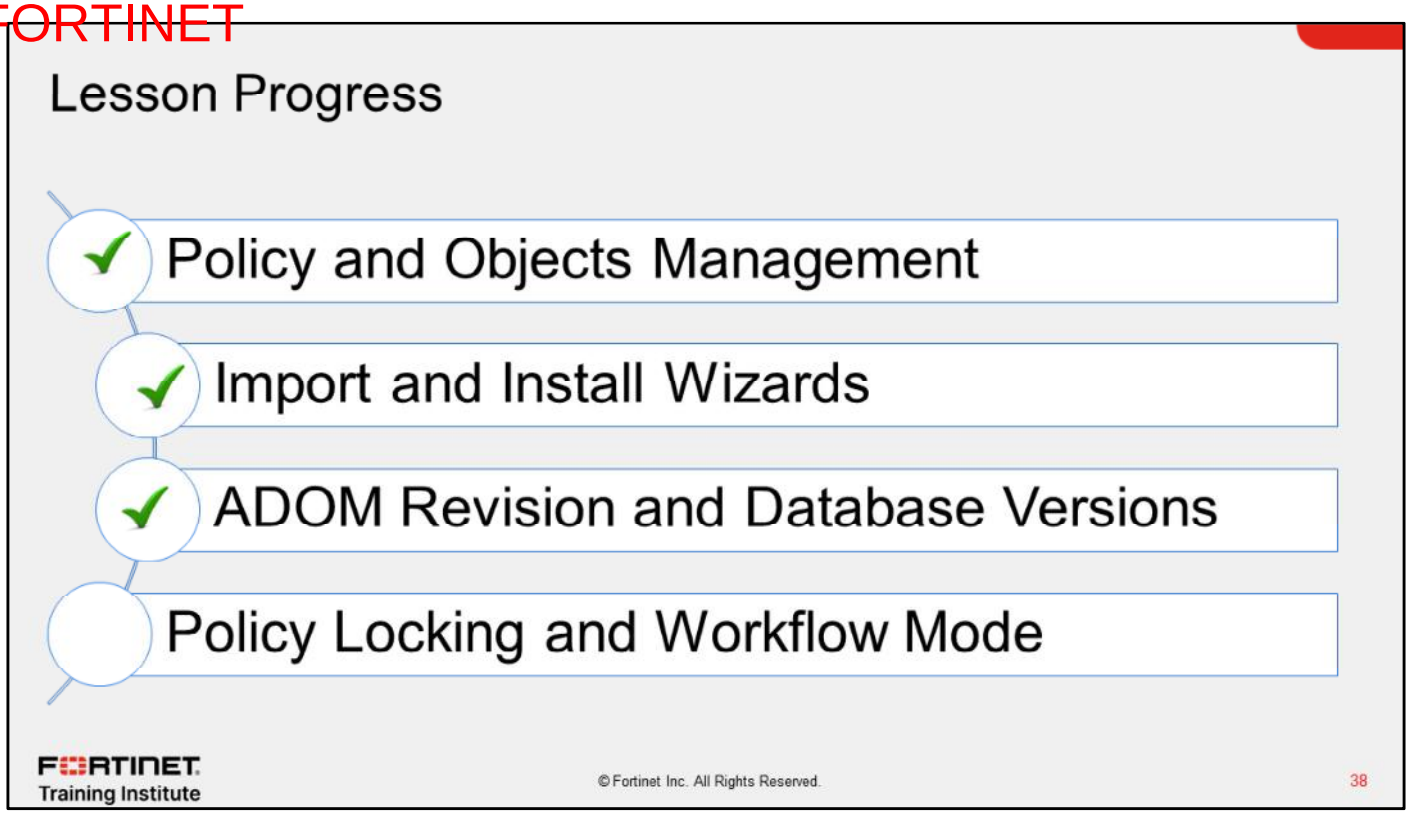
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

37

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

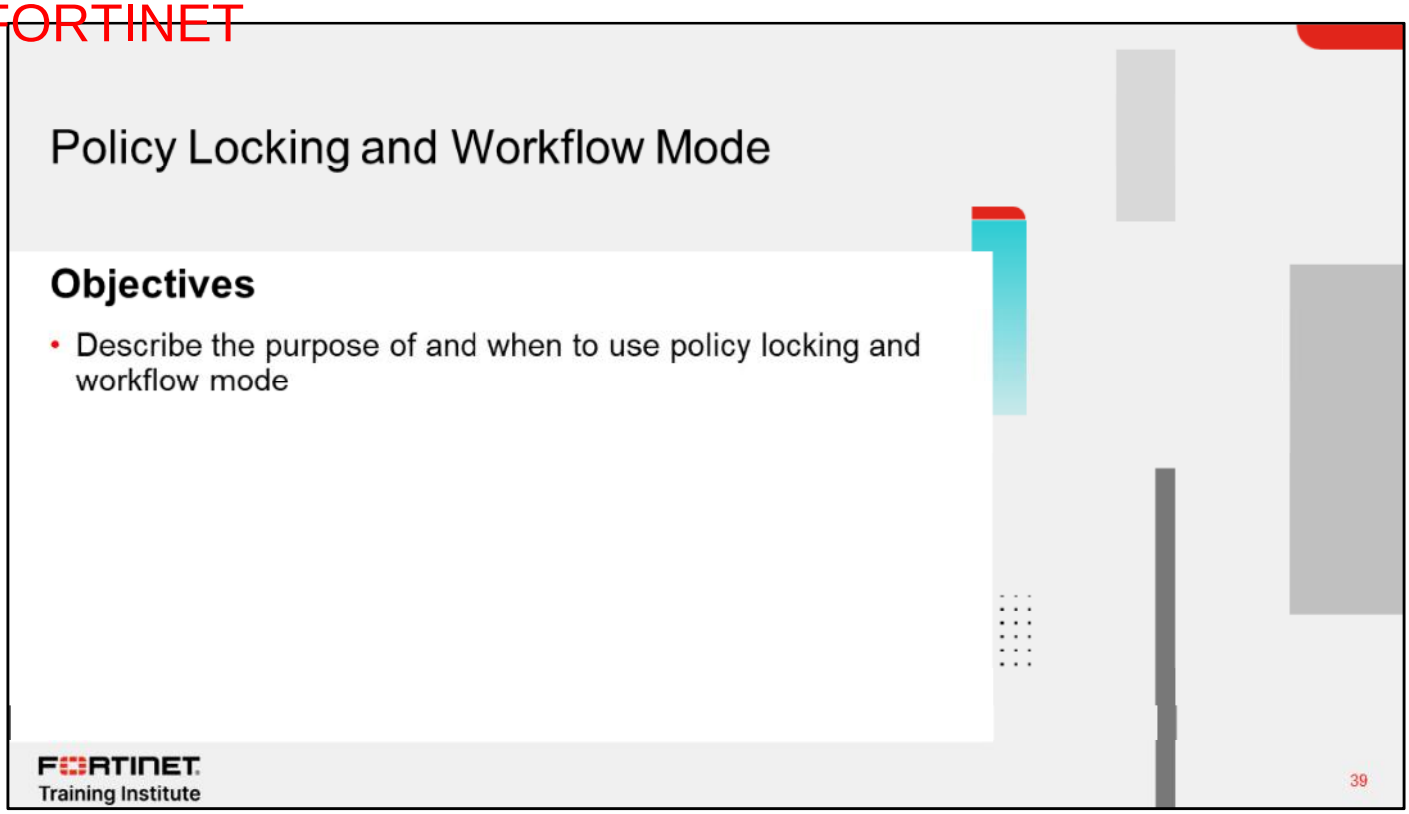


Good job! You now understand ADOM revision and database versions.

Now, you will learn about policy locking and workflow mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

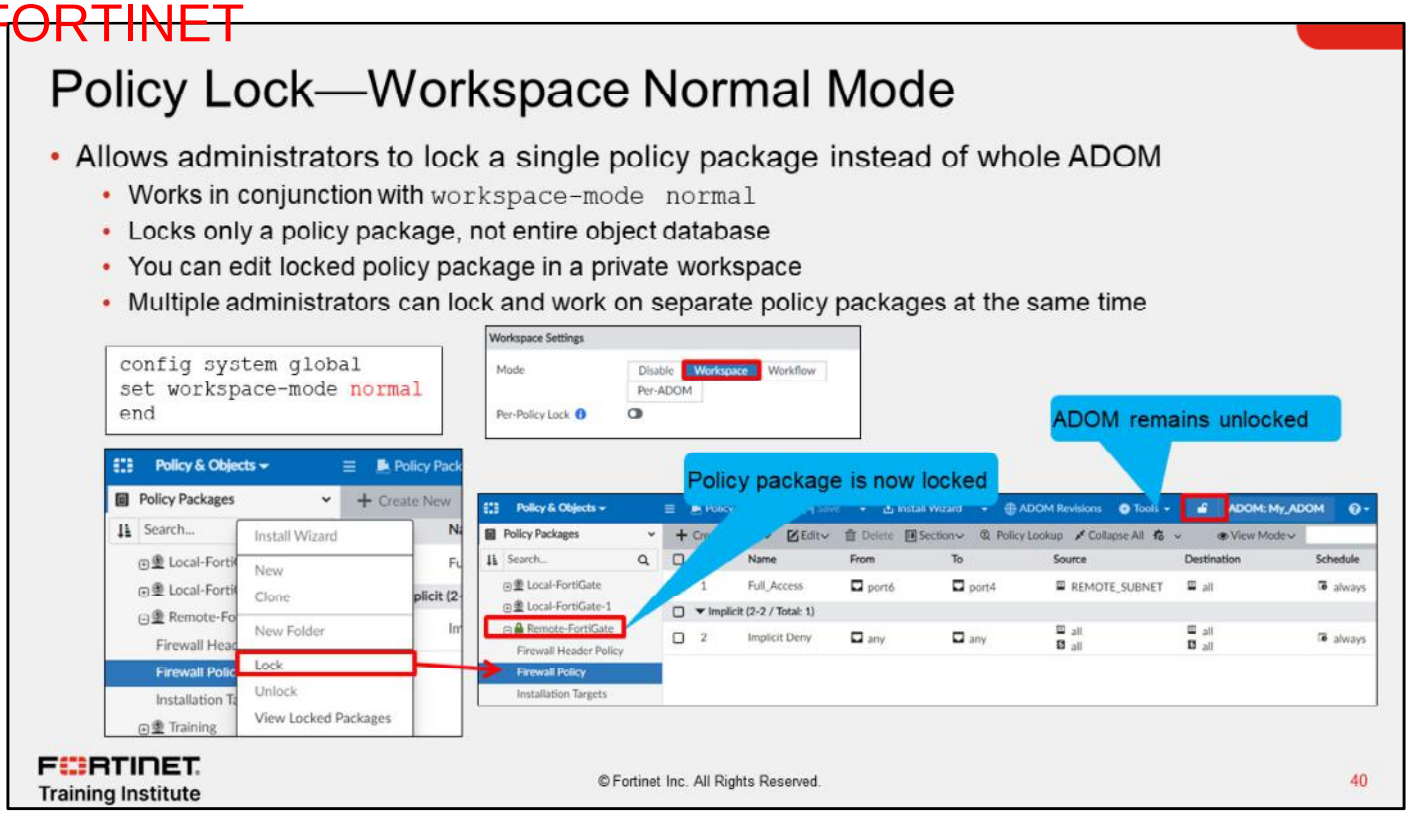


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding the purpose and use of policy locking and workflow mode on FortiManager, you will be able to understand how they impact your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



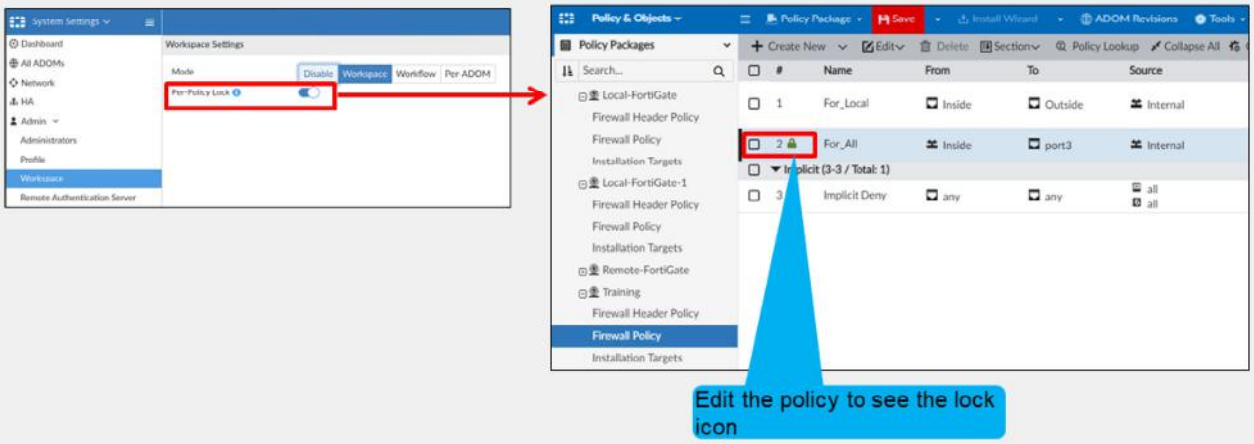
Policy locking is available in workspace normal mode only. Policy locking allows administrators to work on, and lock, a single policy package instead of locking the whole ADOM. In order to use policy locking, you must set `workspace-mode` to `normal`. You can lock either the whole ADOM or a specific policy package. Policy locking is an extension of ADOM locking, which allows multiple administrators to work on separate policy packages on the same ADOM at the same time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Per-Policy Lock—Workspace Normal Mode

- Allows administrators to lock a single policy within the same policy package
- Policy lock is released automatically at administrator timeout, or if session is closed gracefully without unlocking the policy package



Edit the policy to see the lock icon

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

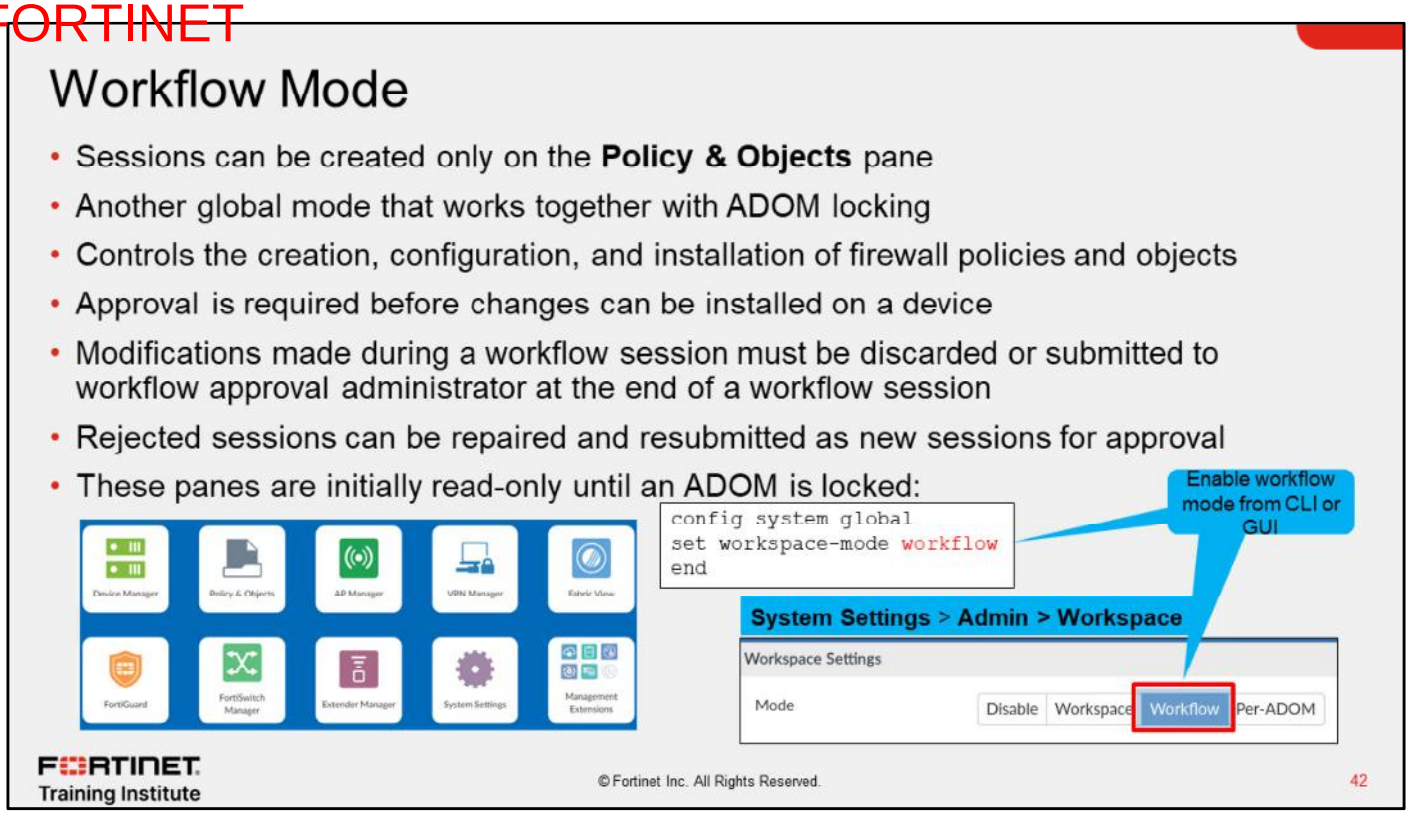
41

In workspace mode, administrators can lock individual policies, except for policies used by policy blocks. You cannot lock an individual policy when the policy is used in a policy block. If you want to modify a policy, you do not need to lock the entire policy package. Once you lock a policy, a padlock icon appears beside the policy. Other administrators are now unable to modify your policy or lock the policy package where the locked policy is in, and unable to lock the ADOM.

The policy lock is automatically released at administrator timeout, or if the administrator closes a session gracefully without unlocking the policy package or policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

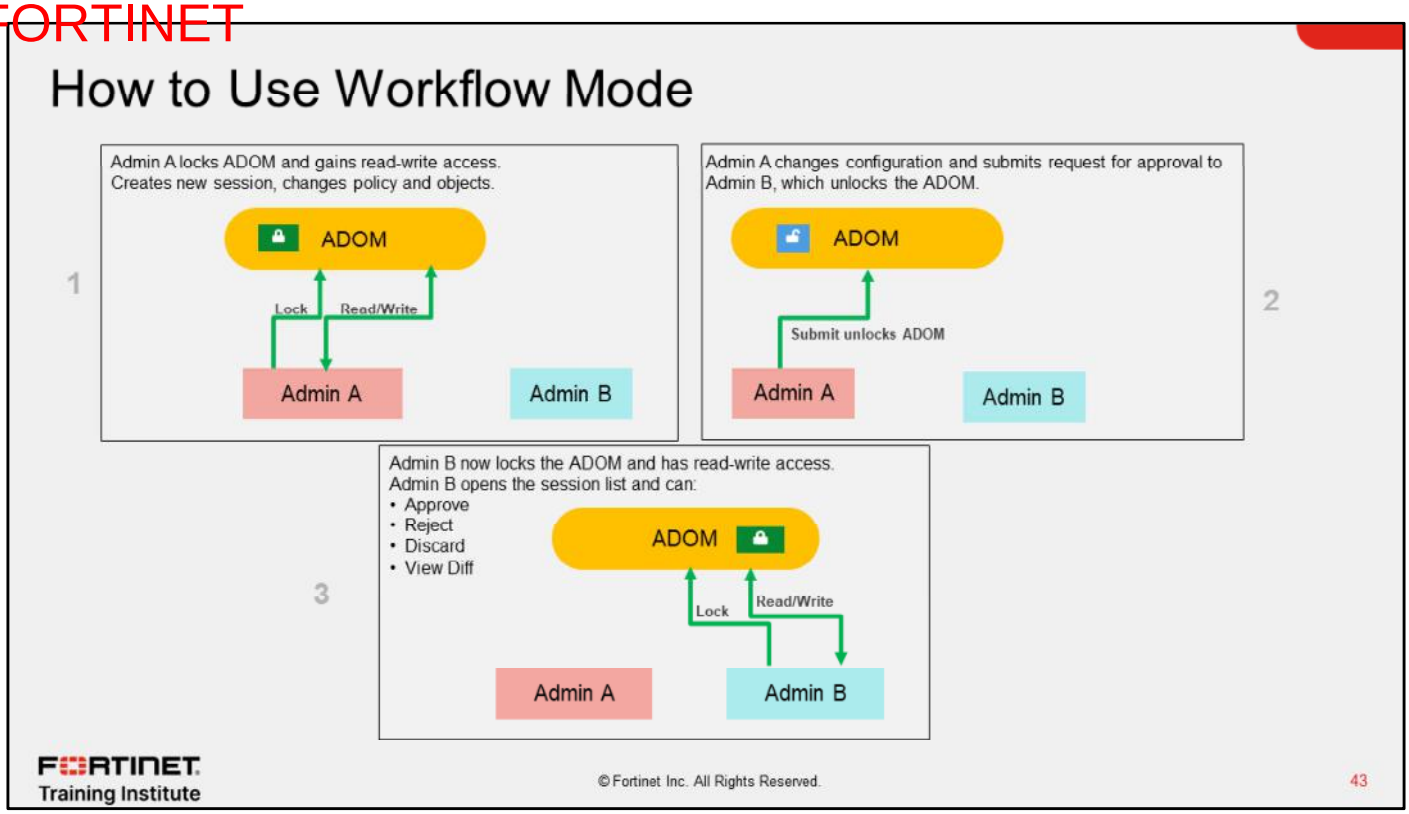


Instead of workspaces, you can use workflow mode. *Before enabling workflow mode, notify other administrators logged in to FortiManager to save their work: it will terminate all management sessions.* You can use workflow mode to control the creation, configuration, and installation of firewall policies and objects. Approval is required before changes can be installed on a device. All the modifications made in a workflow mode session must be discarded or submitted for approval at the end of the session. Sessions that are rejected can be repaired and resubmitted for approval as new sessions. All sessions must be approved in the same order in which they were created to prevent any conflicts.

In workflow mode, panes related to FortiGate configuration are read-only at first. To create a new workflow mode session, you must lock the ADOM first, similar to workspaces. You must enable workflow mode in the CLI or GUI. Enabling workflow mode will log out all administrators.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



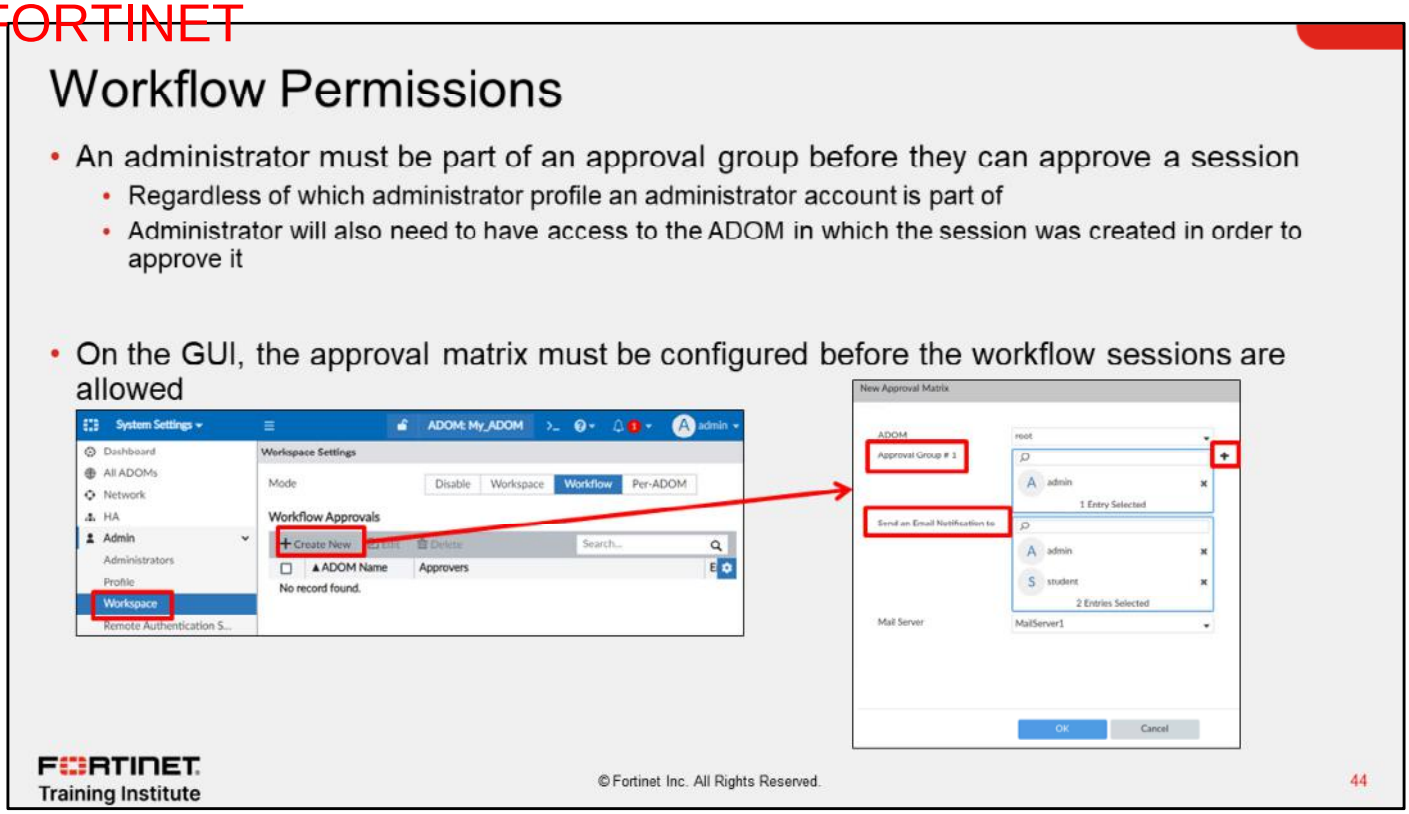
The graphic on this slide shows how to use workflow mode.

When Admin A locks the ADOM, a green lock icon appears. Admin A has read/write access and creates a new session on the **Policy & Objects** pane in the ADOM. Admin A makes configuration changes to the managed devices and submits the request for approval to Admin B. This approval submission automatically unlocks the ADOM.

Admin B must have *read/write* permission for *workflow approval*. Admin B then locks the ADOM and has read-write access. Admin B opens the session list and has the option to approve, reject, discard, or view differences in the changes submitted by Admin A.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



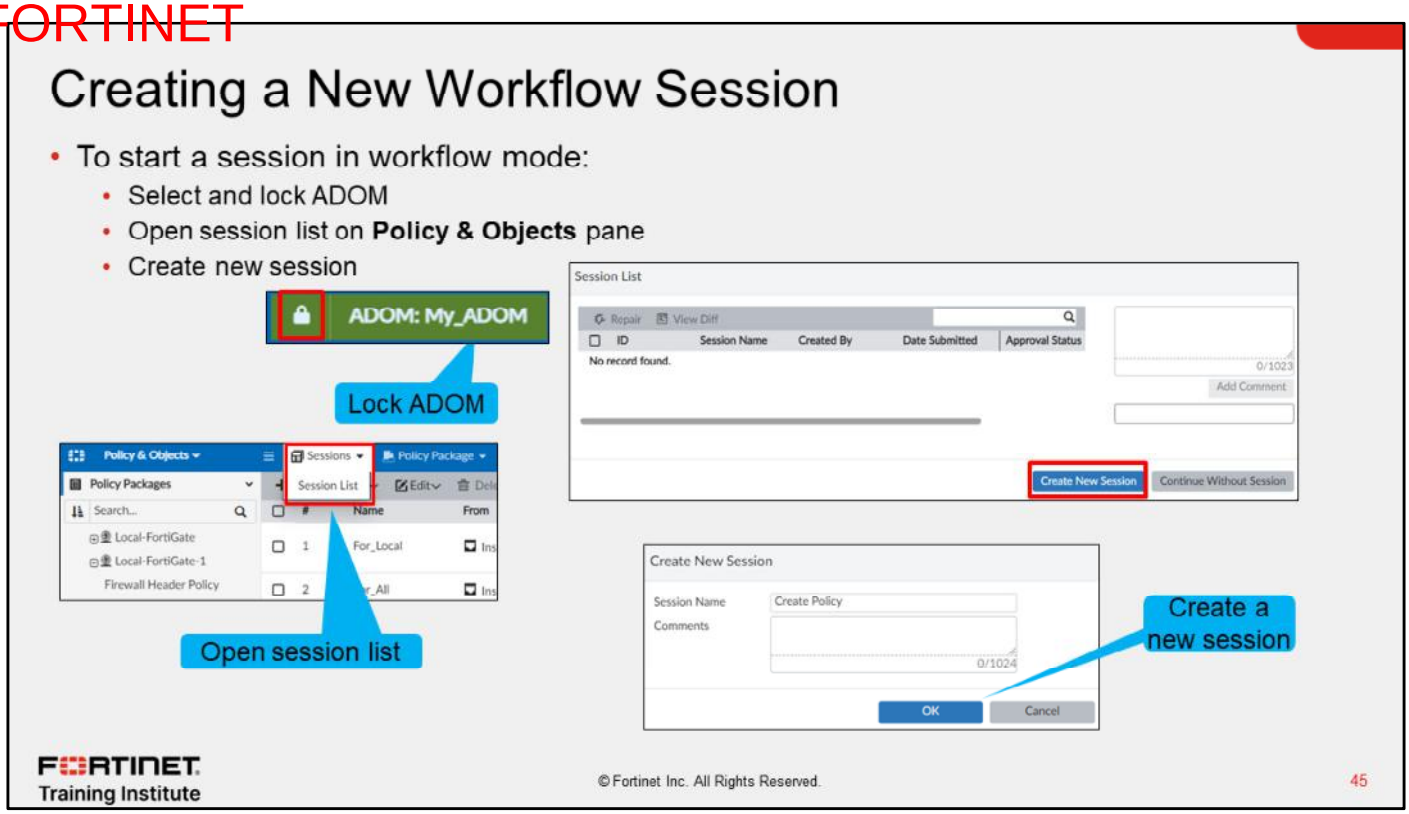
An administrator must be part of an approval group, and have rights over the ADOM in which the session was created, in order to approve a session. Being part of the `Super_Admin` profile is not enough to approve a session.

On the **Workflow Approval** pane, configure the workflow approval matrix using the following values:

- **ADOM**: Select the ADOM you want to apply workflow mode to.
- **Approval Group #1**: Add the administrators who will approve the changes in the ADOM.
- **Send email notification to**: Send administrators email notifications when another administrator makes changes and submits the changes for approval.
- **Mail server**: Select the email server that FortiManager will use to send its notifications on the **Mail Server** pane.

Vouchers & Dumps are Available | WhatsApp +201224560923

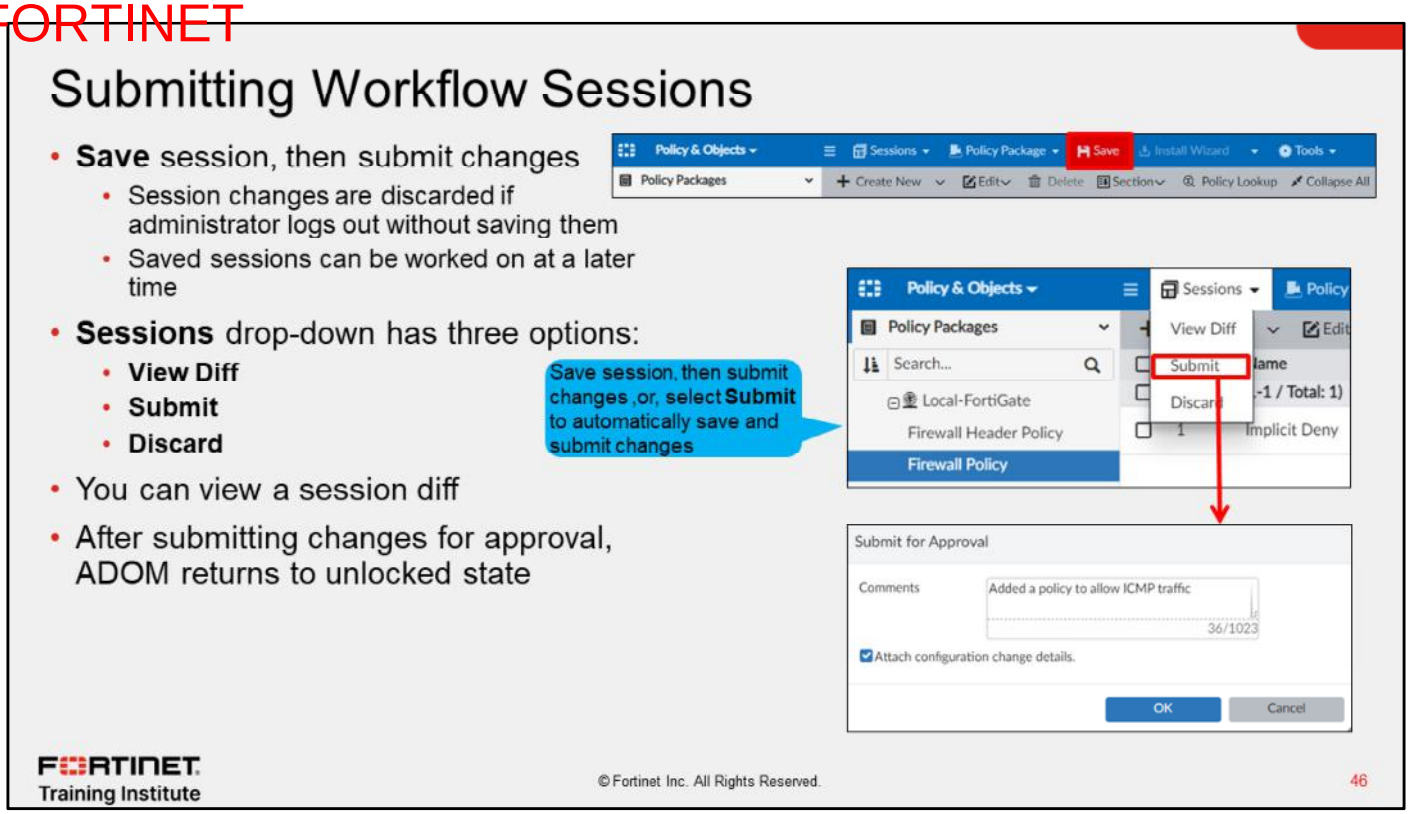
DO NOT REPRINT Brave-dumps.com
© FORTINET



The administrator must lock the ADOM before they are allowed to create a new session. After the ADOM is locked, the administrator has the option to create a new session and start making changes to the policy package. Note that the administrator cannot make any changes to policy packages until they create a new session.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After you edit firewall policies or objects, click **Save** to save your session, then submit your changes. Alternatively, you can click **Submit,** which saves and submits the changes automatically. You can view a session diff before submitting the session for approval.

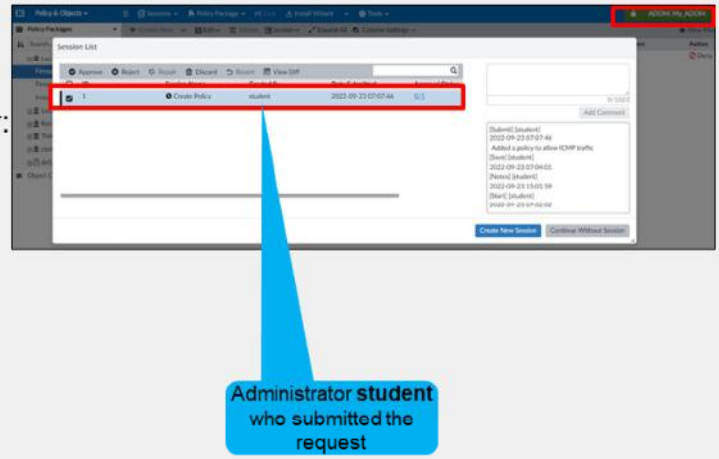
After you submit your changes for approval or have discarded them, the ADOM automatically returns to the unlocked state.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Approving, Rejecting, or Repairing Workflow Sessions

- To approve a session:
  - Administrator must have appropriate rights required to approve a session
  - Must lock the ADOM in which the changes were made
  - Open **Session List**
- Four options for approval administrator:
  - **Approve**
  - **Reject**
  - **Discard**
  - **View Diff**
- Rejected sessions can be resubmitted with proposed changes



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

47

After the workflow request is submitted, administrators with the appropriate permissions can approve or reject the pending request.

The approval administrator must lock the ADOM during the decision process. After the ADOM is locked, they can open the session list. The session list shows the administrator who submitted the request and other information, such as date of submission, total requests, and comments by the submitting administrator.

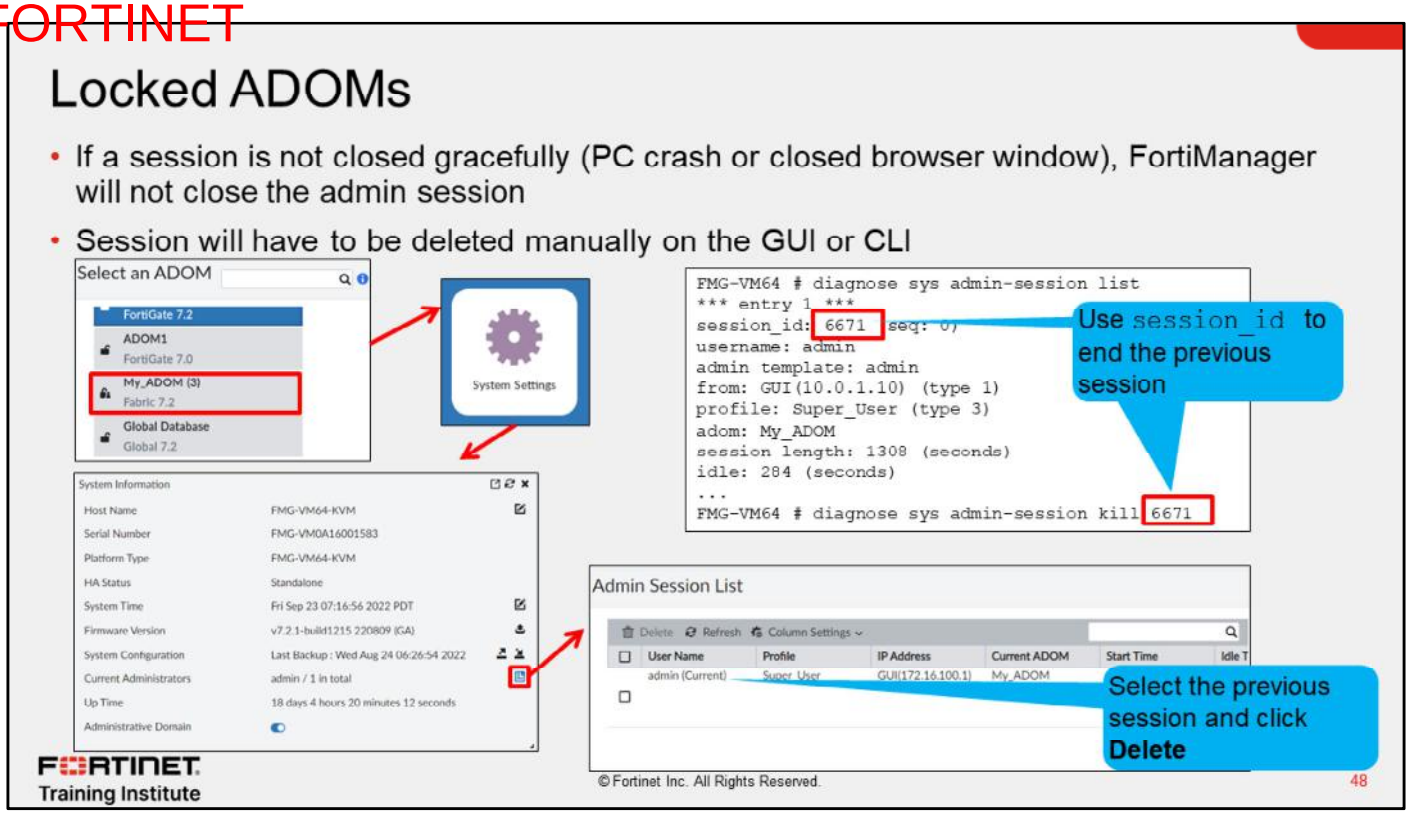
The approver administrator has four options:

- **Approve**: The session is waiting to be reviewed and approved. If the session is approved, no further action is required.
- **Reject**: If the session is rejected, the system sends a notification to the administrator who submitted the session. The approver administrator has the option to repair the changes. A session that is rejected must be fixed before the next session can be approved.
- **Discard**: The approval administrator doesn't agree with the changes and discards them. No further action is required.
- **View Diff**: The approval administrator can view the differences between the original policy package and changes made by the submitting administrator.

In the example shown on this slide, the admin user **student** submitted the request for approval to admin user **admin**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



If a connection to FortiManager unexpectedly closes (PC crashed or browser closed) while an ADOM is locked, it will remain locked until the administrator session times out or the session is deleted. You can delete administrator sessions on the GUI or CLI. After the previous session is deleted, the ADOM will be unlocked immediately.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about workflow mode is true?
   - ✓A. Workflow sessions that are rejected can be repaired and resubmitted for approval as new sessions.
   - B. Workflow sessions can be created by locking an individual policy package.

2. What is the main benefit of the policy locking feature?
   - ✓A. It allows you to lock a single policy package instead of the whole ADOM.
   - B. It allows you to lock multiple firewall policies in a policy package.

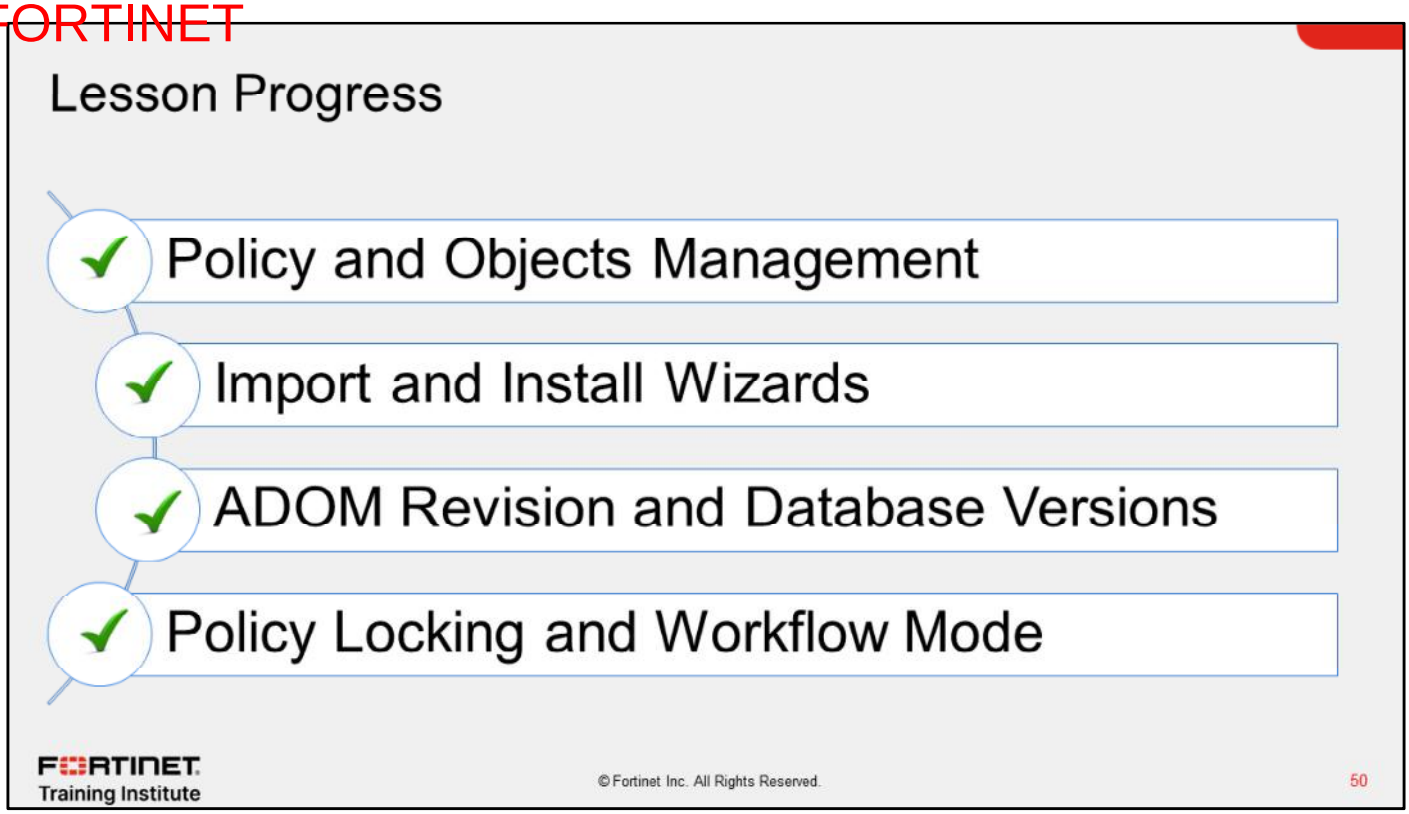
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

49

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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 Brave-dumps.com
© FORTINET

Review

- ✓ Describe policy workflow
- ✓ Create policy packages and objects
- ✓ Create installation targets for policies and policy packages
- ✓ Configure dynamic objects
- ✓ Use the policy check feature and clone a policy package
- ✓ Interpret the status of a device on FortiManager
- ✓ Use the Import Policy wizard and the Install wizard
- ✓ Use the Re-install wizard
- ✓ Describe the purpose of ADOM revisions
- ✓ Identify the database version of an ADOM
- ✓ Understand how the database version of the ADOM affects the policy and objects configurations
- ✓ Describe the purpose of and when to use policy locking and workflow mode

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

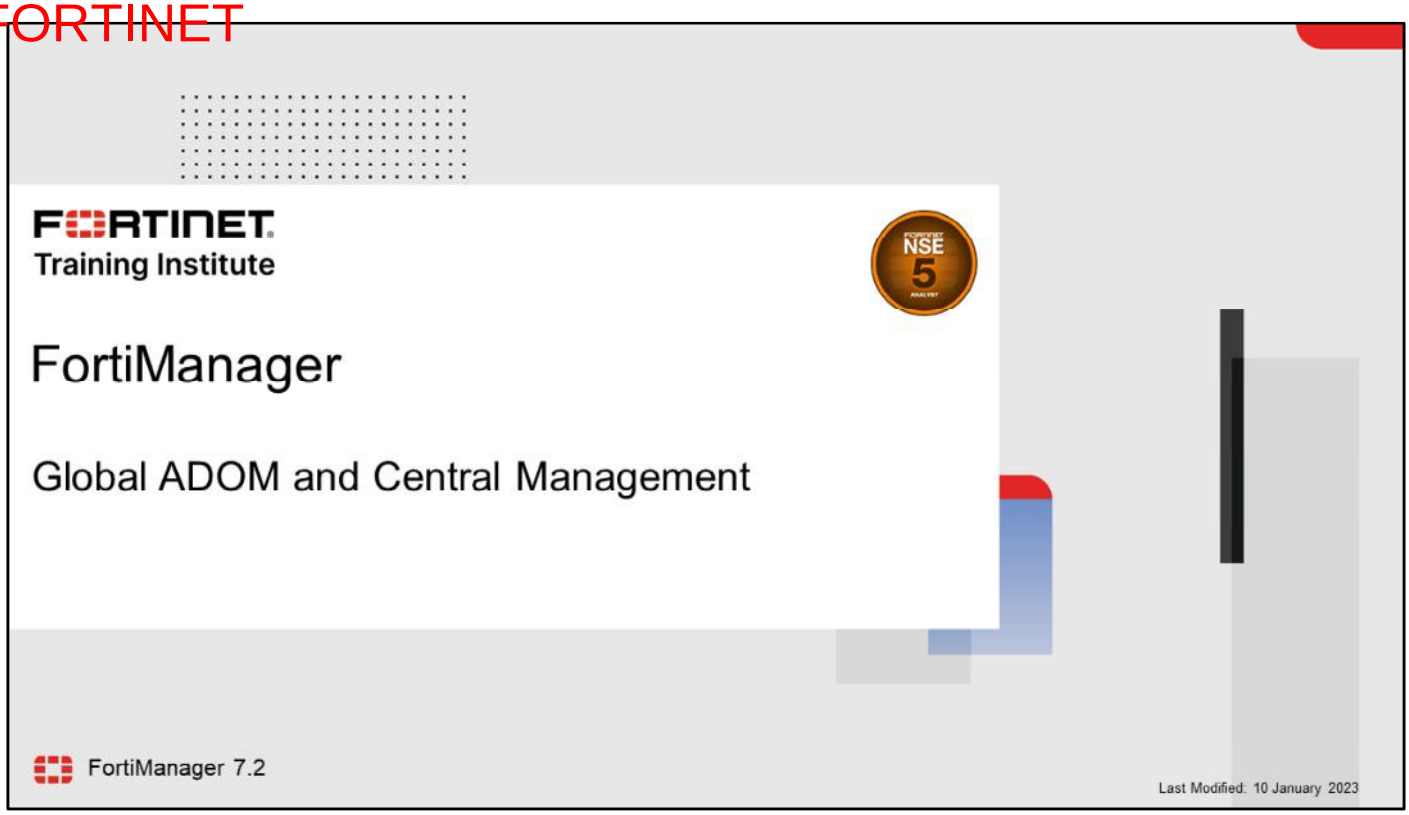
51

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

By mastering the objectives covered in this lesson, you learned how to manage policy and objects on FortiManager for FortiGate. You also learned how to configure policy and objects on FortiManager, and then install them on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

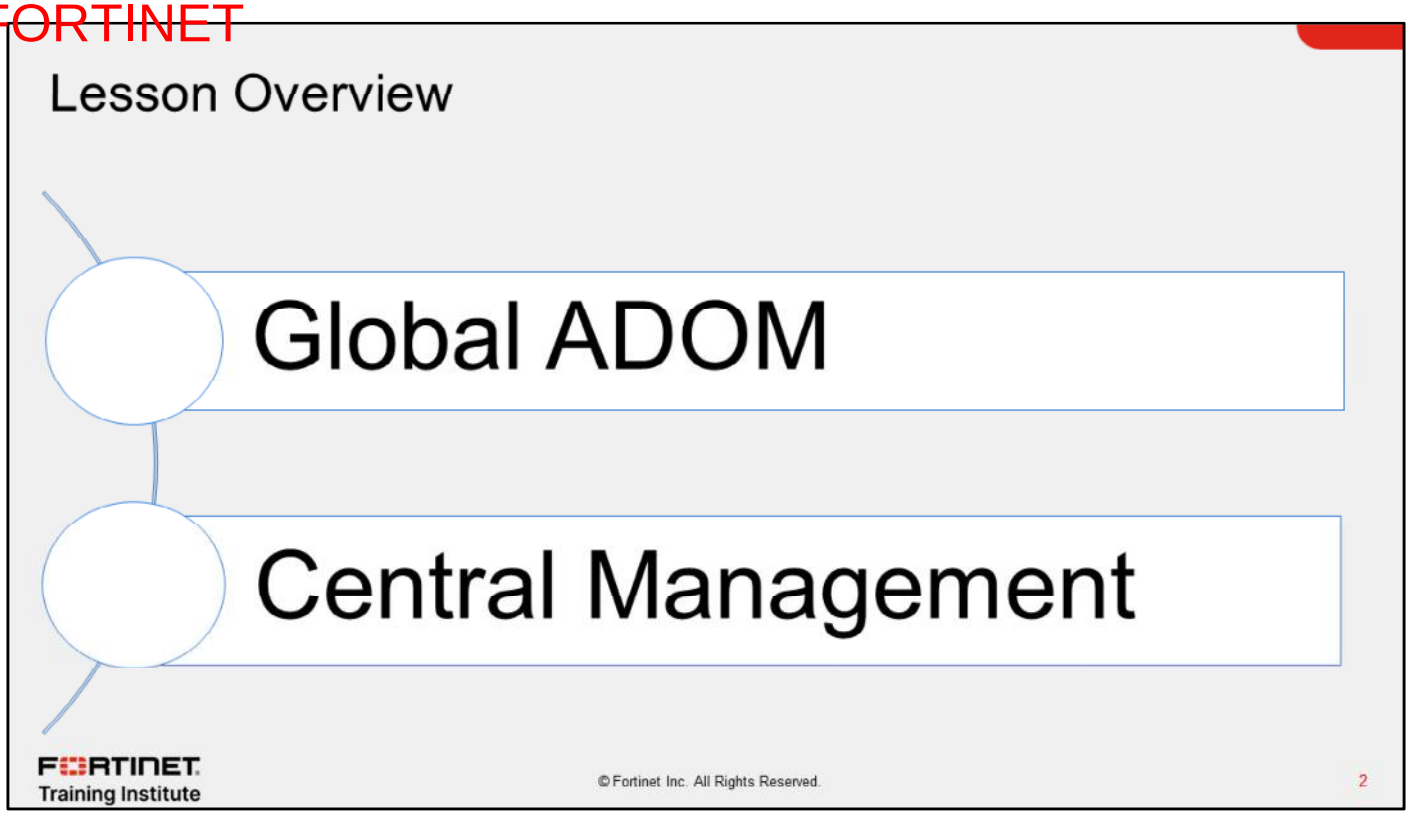
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the global administrative domain (ADOM), and central management.

Vouchers & Dumps are Available | WhatsApp +201224560923

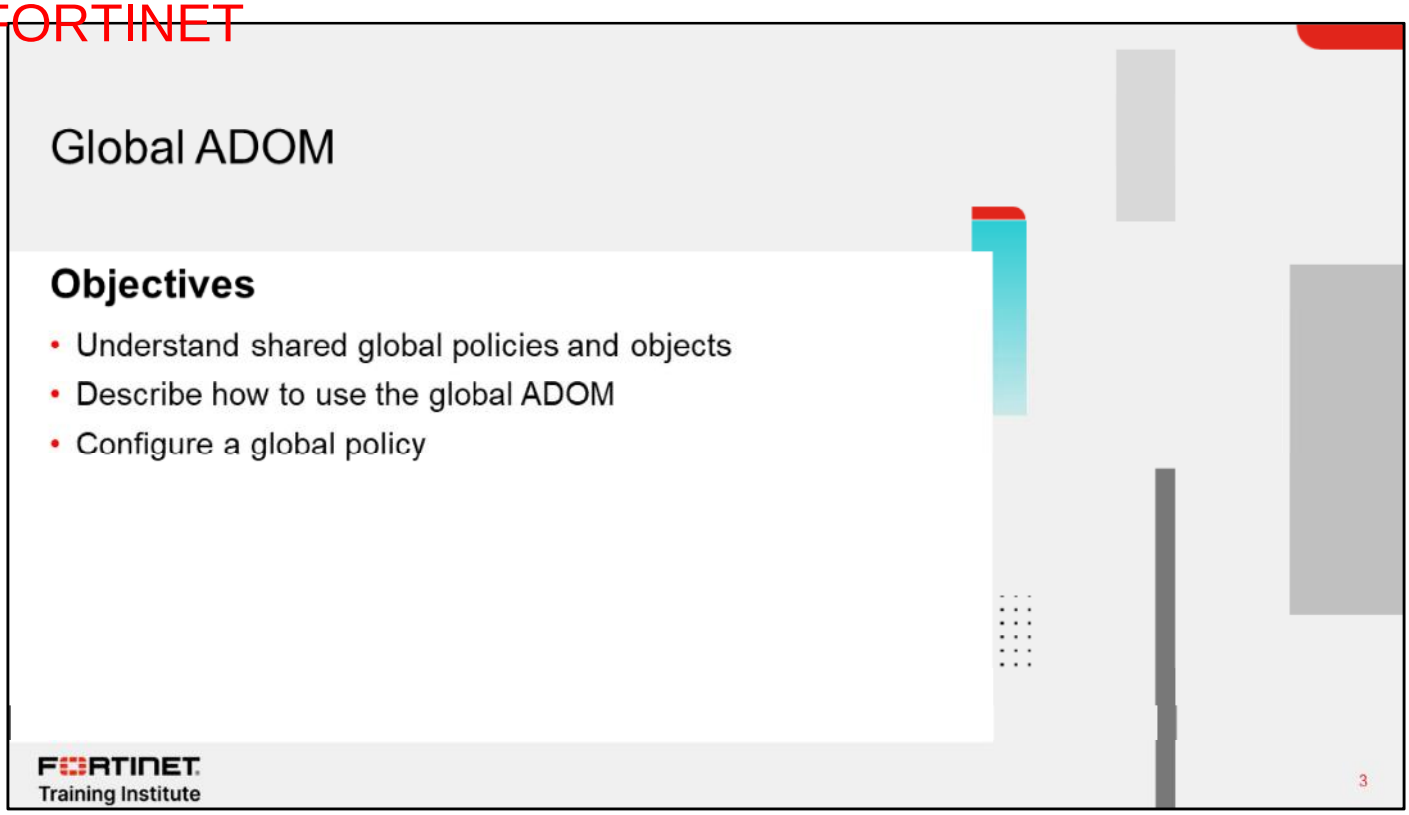
DO NOT REPRINT
© FORTINET
Brave-dumps.com



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

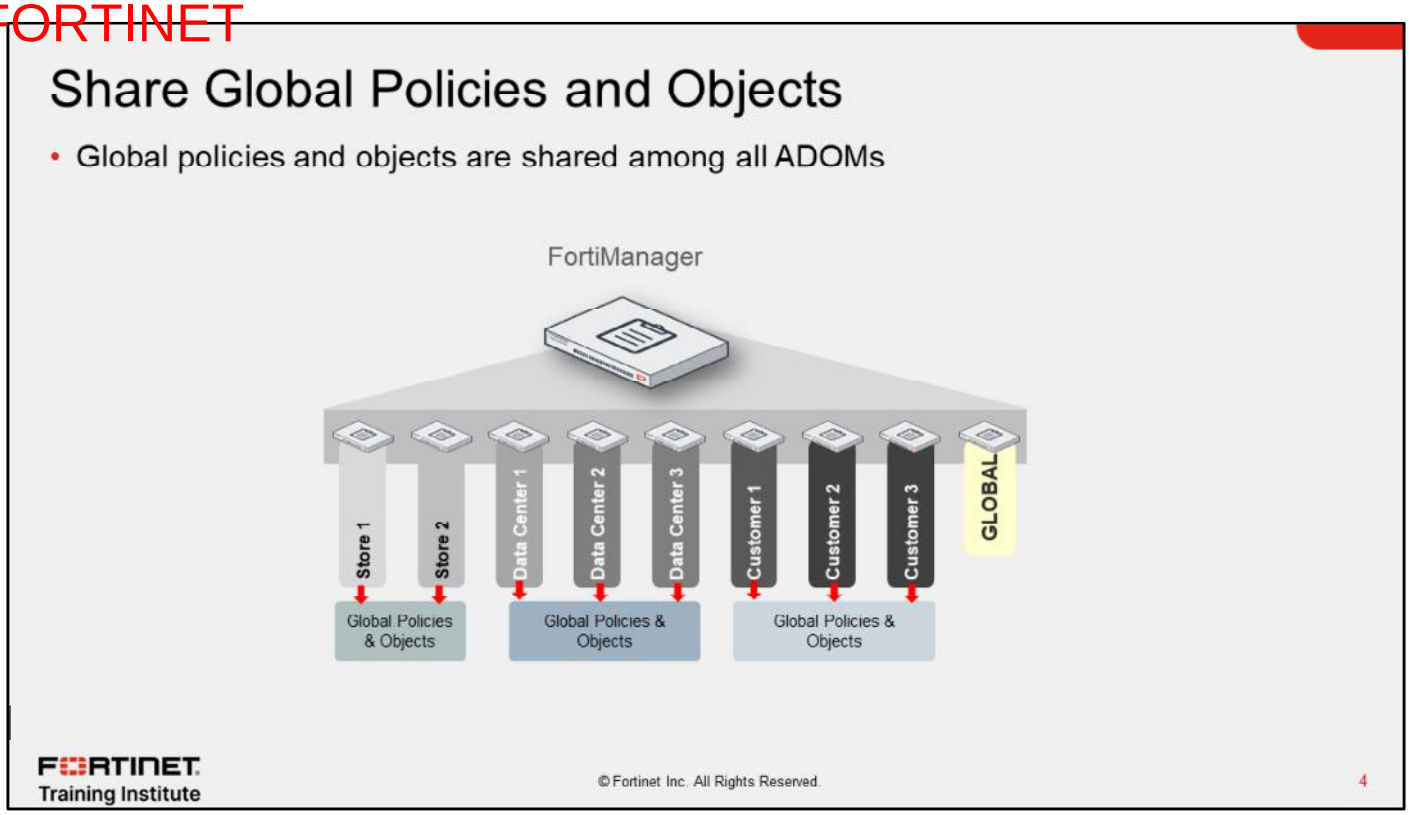


After completing this section, you should be able to achieve the objectives shown on this slide.

Now, you will learn about the global ADOM and its feature sets.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



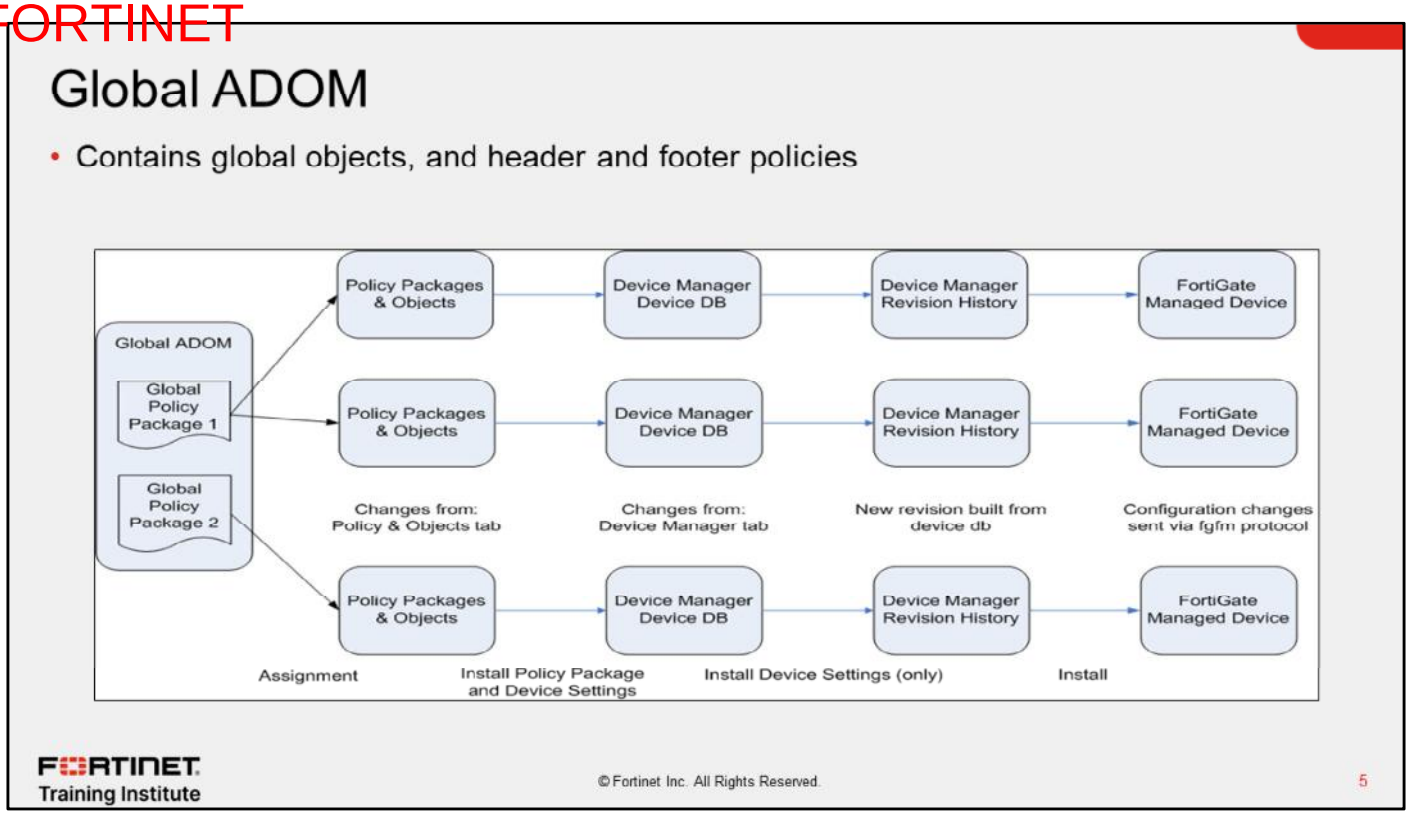
Global policies and objects allow administrators to push firewall policies universally, to all ADOMs. You must explicitly assign global policy packages to specific ADOMs on which administrators want to install similar policies.

The illustration on this slide shows that different ADOMs can use separate global policies. When you create a global policy package, you can choose ADOMs that you want to apply specific policies to. Furthermore, you can even pick specific policy packages in individual ADOMs that you want to apply the global policies to.

You can create global policy packages based on the type of network environment that you are managing, and apply header or footer policies to meet the security requirements.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can use header and footer policies to wrap policies in each individual ADOM. An example of where header and footer policies would be used is in a carrier environment, in which the carrier would allow customer traffic to pass through their network, but would not allow the customer to have access to the carrier network assets.

The illustration on this slide shows how global policies and objects are assigned to ADOM policy packages.

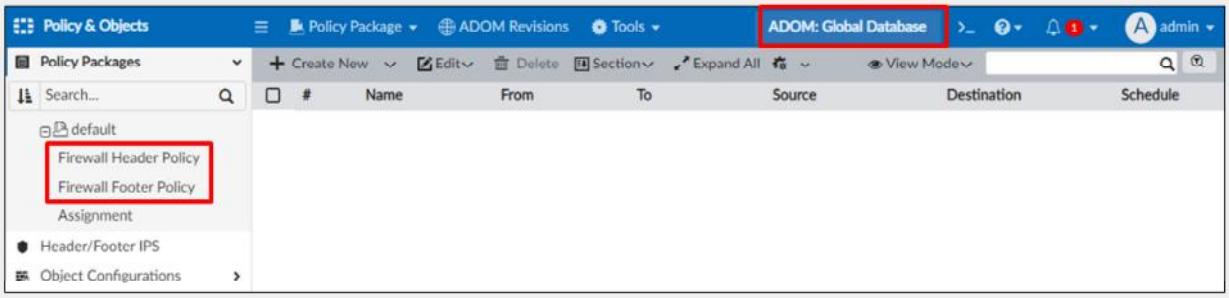
In this section, you will learn how to apply a global header policy in order to deny all Telnet traffic to a public IP address, and then assign it to an ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Global ADOM—Policy Types

- Switch to **Global Database** ADOM
- You can create two types of policies:
  - Header policy–placed at the top of the policy package in the individual ADOM
  - Footer policy–placed at the bottom of the policy package in the individual ADOM



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

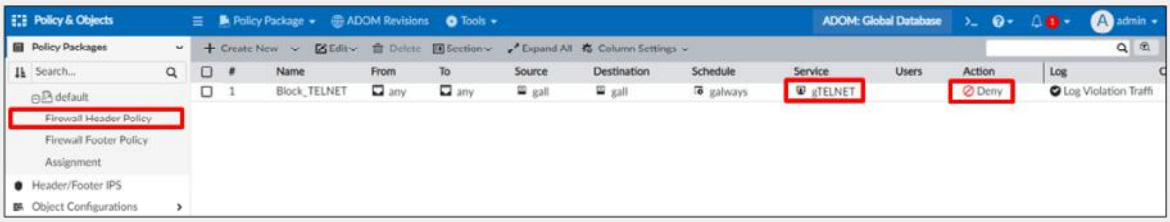
Enter the **Global Database** ADOM to access the global policy database. Header policies are the policies located at the top of the policy package in the individual ADOM. Footer policies are the policies located at the bottom of the policy package in the individual ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Example—Header Policy

- Create a firewall policy to block TELNET



- After you assign the global policy package to an ADOM and install a package in that ADOM to a managed device, Telnet traffic is blocked

FORTINET Training Institute

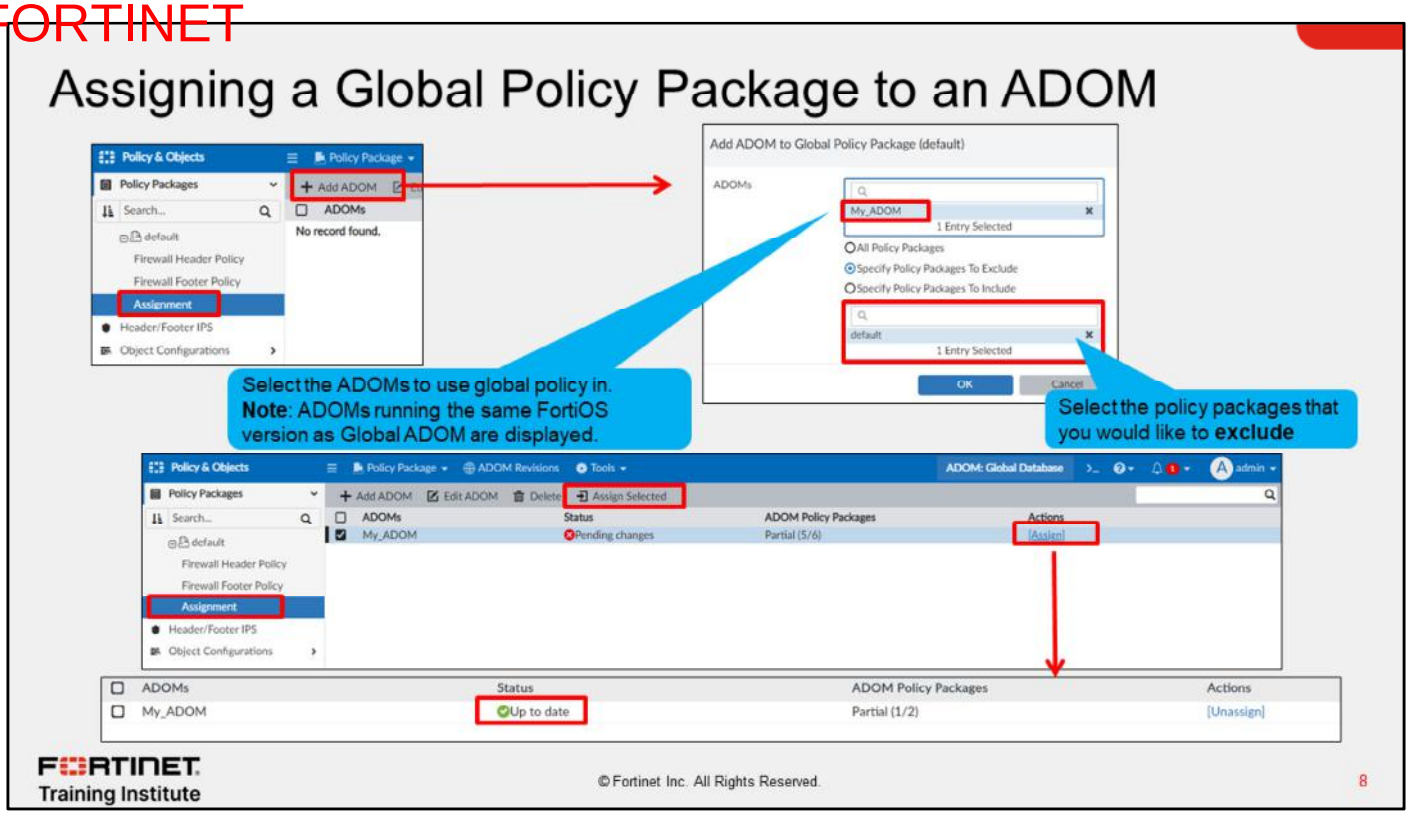
© Fortinet Inc. All Rights Reserved.

7

In the example shown on this slide, a header policy blocks Telnet traffic from passing through the managed firewalls. The next step is to assign this policy to one policy package in an individual ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Select the global policy package that you would like to assign to the individual ADOM policy package, and then click **Assignment** > **Add ADOM**.

In the example shown on this slide, the **default** global policy package is added to the four policy packages except default and cloned policy packages in the **MyADOM** ADOM. After you add the global policy package, the status appears as **Pending changes**, because it is not assigned to the individual ADOM policy package. The **ADOM Policy Packages** column shows only five policy packages selected out of six packages available in the **MyADOM** ADOM. To assign the global policy package to the individual ADOM policy package, click **Assign** or **Assign Selected**.

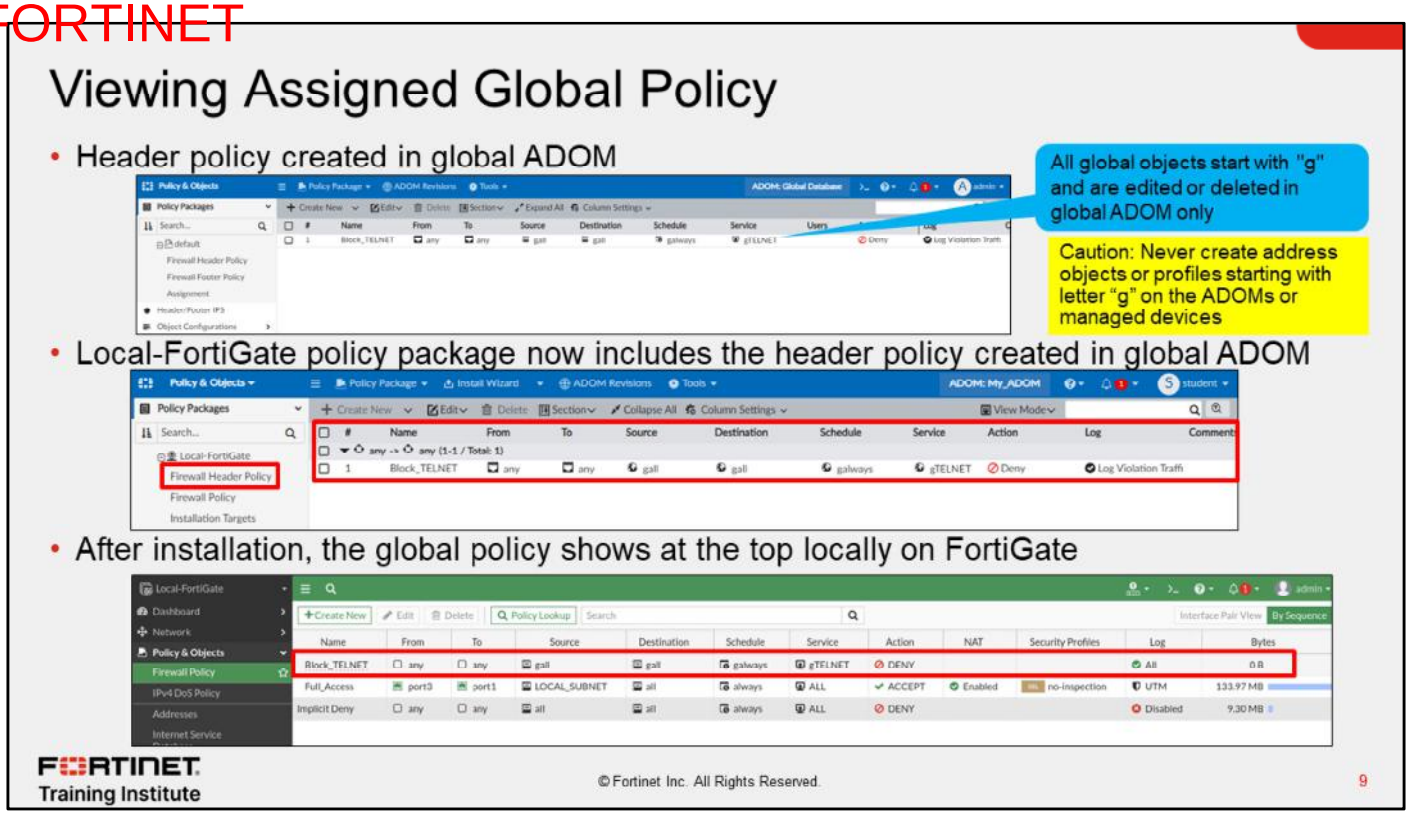
The **Assign** option commits the global policy package and used objects to the individual ADOM policy package.

Assign Selected, on the other hand, provides more advanced options, including:
- Assign used objects only
- Assign all objects
- Automatically install policies on ADOM devices

After installation, the status changes to **Up to date**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After you assign the global ADOM objects, they appear on the **Policy & Objects** pane for that ADOM. All global objects start with "g" and are edited or deleted in the global ADOM only. A word of caution, never create address objects or security profiles starting with letter “g” on ADOM database or directly on the managed devices because this conflicts with global ADOM objects and cause configuration failure issues.

In the example shown on this slide, the header policy is added to the Local-FortiGate. You can assign only one global policy package to an individual ADOM policy package. Assigning an additional global policy package to the same individual ADOM policy package removes previously assigned policies. Also, you can`t edit and move the header and footer policies between the rules in an individual ADOM policy package.

You must install policy packages on the managed devices for the new rules to work. You install a header policy at the top of the list of firewall rules on the target device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the purpose of the global ADOM on FortiManager?
   A. To push global device-level changes to devices in selected ADOMs
   ✓ B. To push similar firewall policies universally to selected ADOMs

2. How are global objects identified?
   ✓ A. Global objects start with “g”.
   B. Global objects start with “o”.

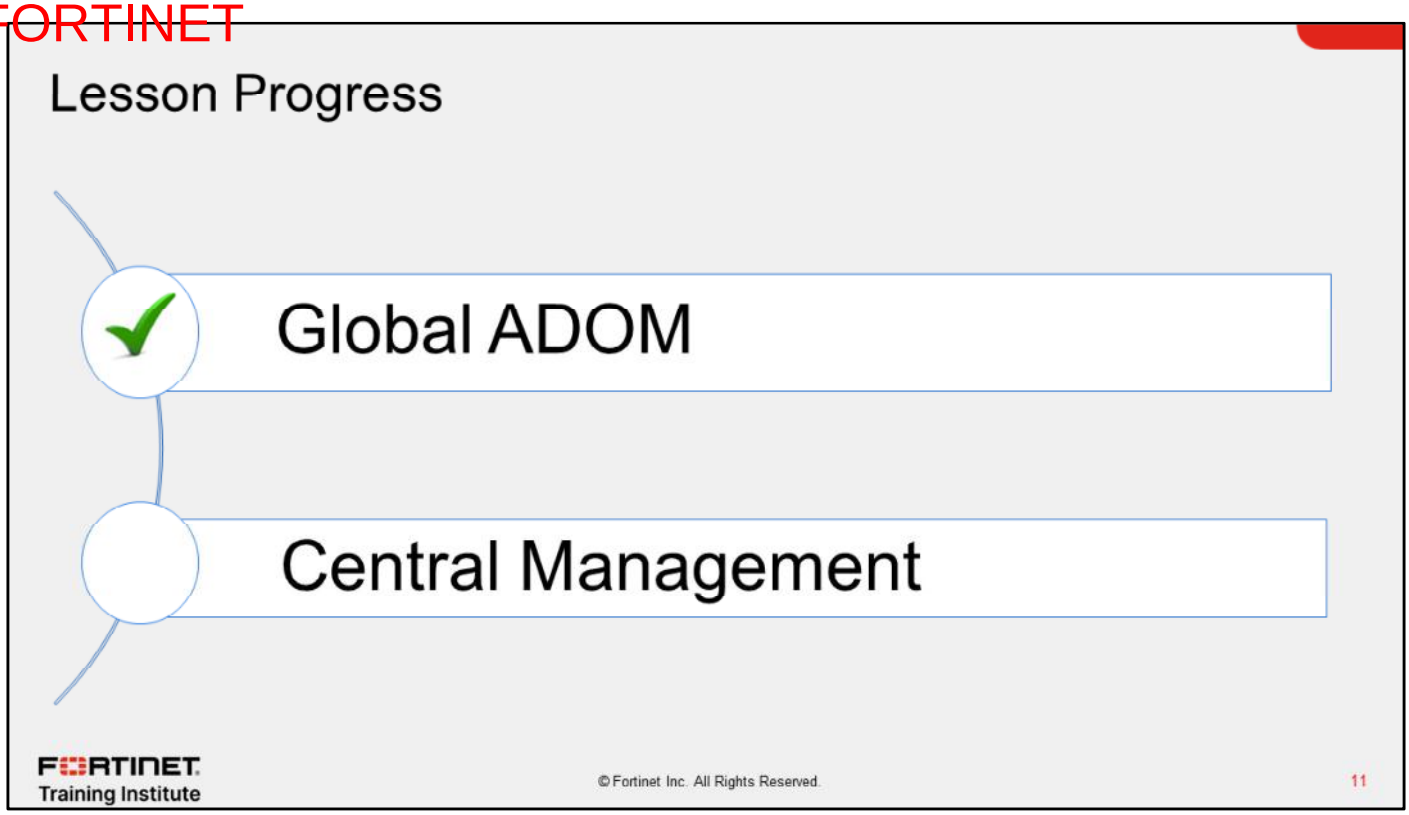
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

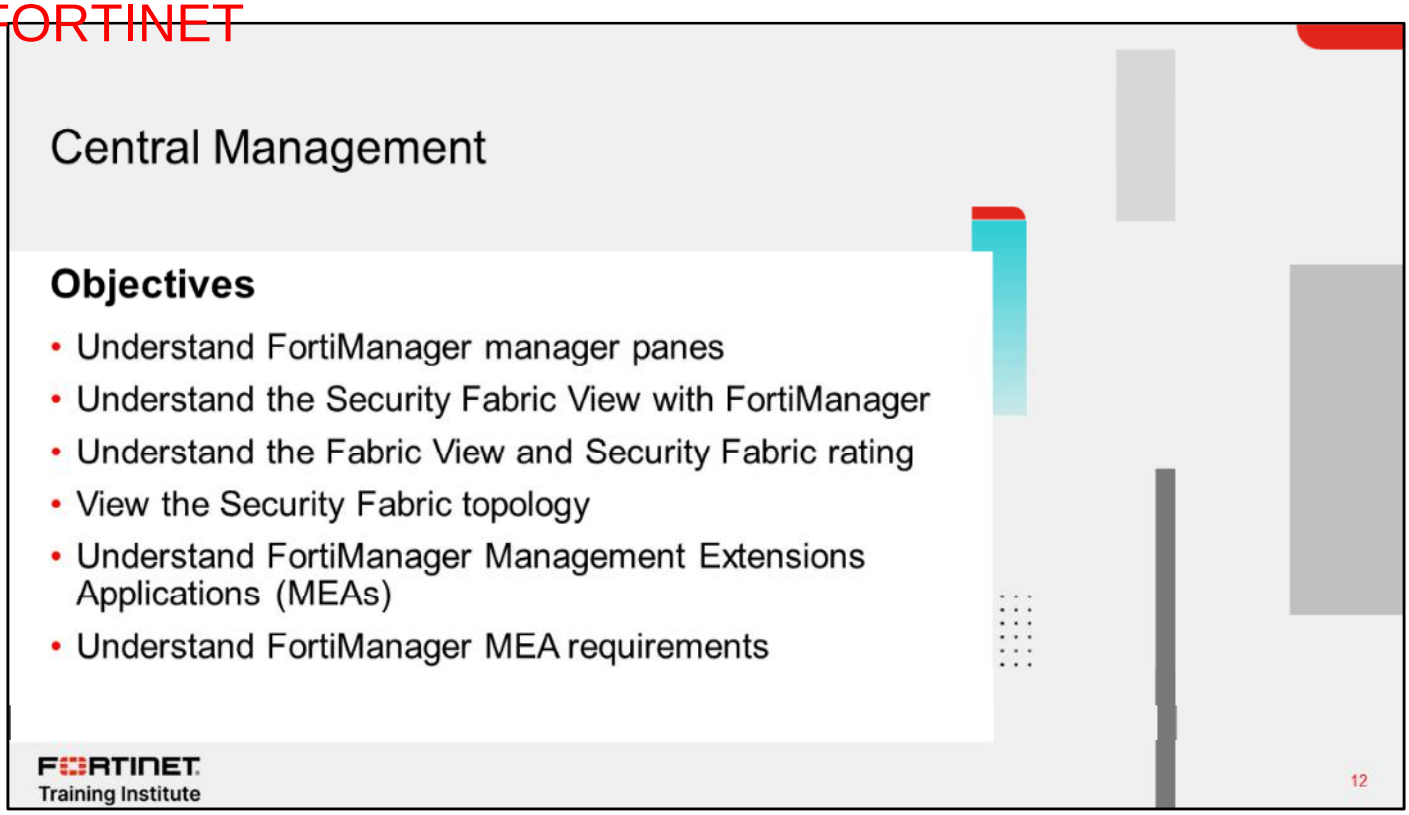


Good job! You now understand the global ADOM.

Now, you will examine the Security Fabric and its features.

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 the Security Fabric and its feature sets, you will be able to use the Security Fabric effectively in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Manager Panes

- VPN Manager
  - VPN Manager simplifies the administration of multiple IPsec VPNs
- AP Manager
  - Centrally manage managed FortiAP devices
- FortiSwitch Manager
  - Centrally manage FortiSwitch templates and VLANs, and monitor FortiSwitch devices that are connected to FortiGate devices
- Extender Manager
  - Centrally manage managed FortiExtender

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

13

FortiManager enables you to manage your Fortinet devices centrally using manager panes.

VPN Manager: On the VPN Manager pane, you can configure IPsec VPN settings that you can install on multiple devices. The settings are stored as objects in the objects database. You push the IPsec VPN settings to one or more devices by installing a policy package. Enabling VPN Manager for an ADOM overrides existing VPN configurations for managed devices in that ADOM. Mixed-mode VPN allows you to configure VPNs concurrently through VPN Manager and on the FortiGate device in Device Manager.

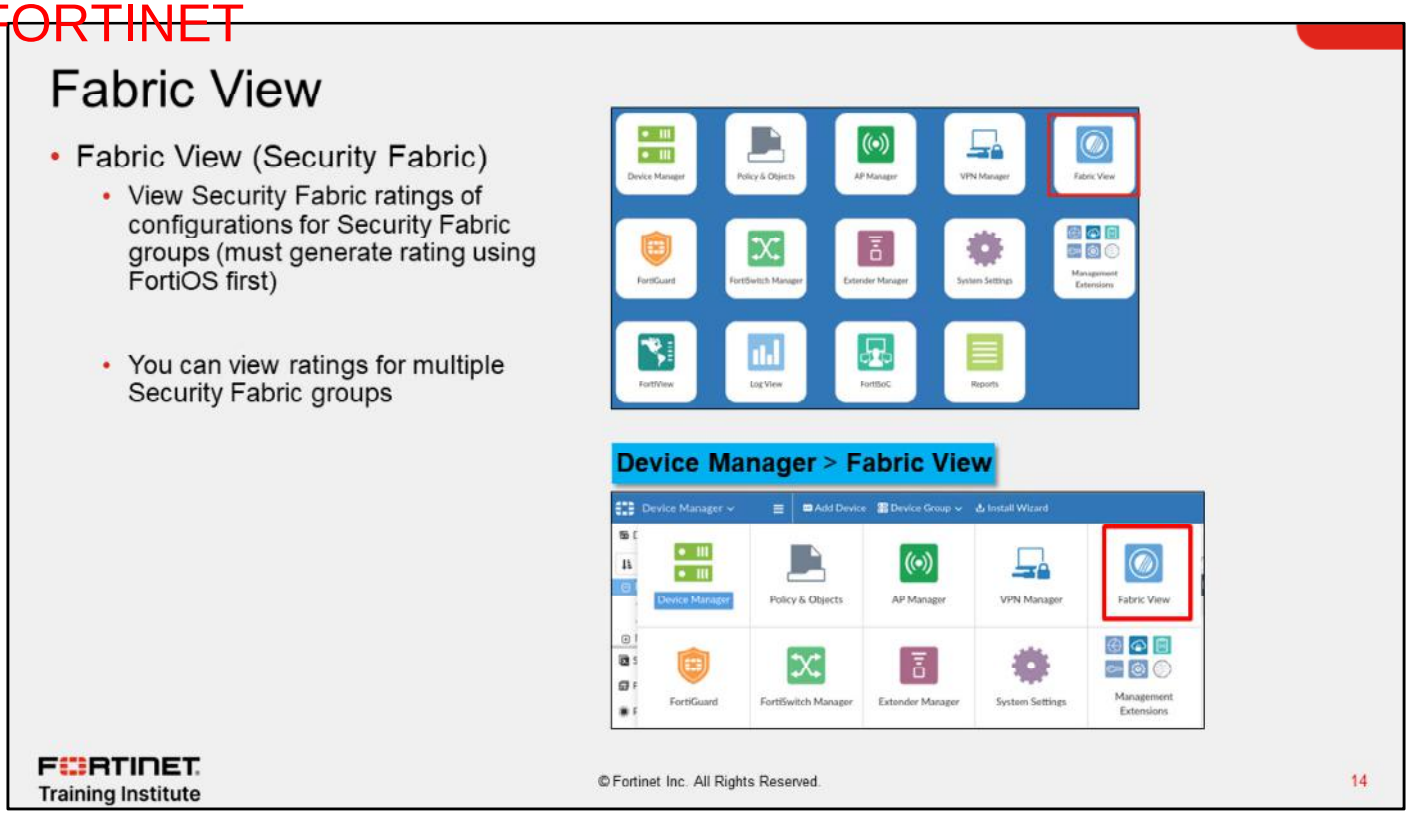
AP Manager: The AP Manager pane allows you to manage FortiAP devices that are controlled by FortiGate devices that are managed by FortiManager. The administrator can use Wi-Fi templates to easily manage and distribute AP profiles, SSIDs, and wireless intrusion detection system (WIDS) profiles. The administrator can also monitor all wireless clients and check AP health.

FortiSwtich Manager: The FortiSwitch Manager pane enables you to centrally manage FortiSwitch templates and VLANs, and monitor FortiSwitch devices that are connected to FortiGate devices. You can configure multiple templates for specific FortiSwitch platforms that can be assigned to multiple devices.

Extender Manager: The Extender Manager pane enables you to manage managed connected FortiExtender. You can use the Extender Manager to create custom templates, SIM profiles, and data plans for up to two modems.

Vouchers & Dumps are Available | WhatsApp +201224560923

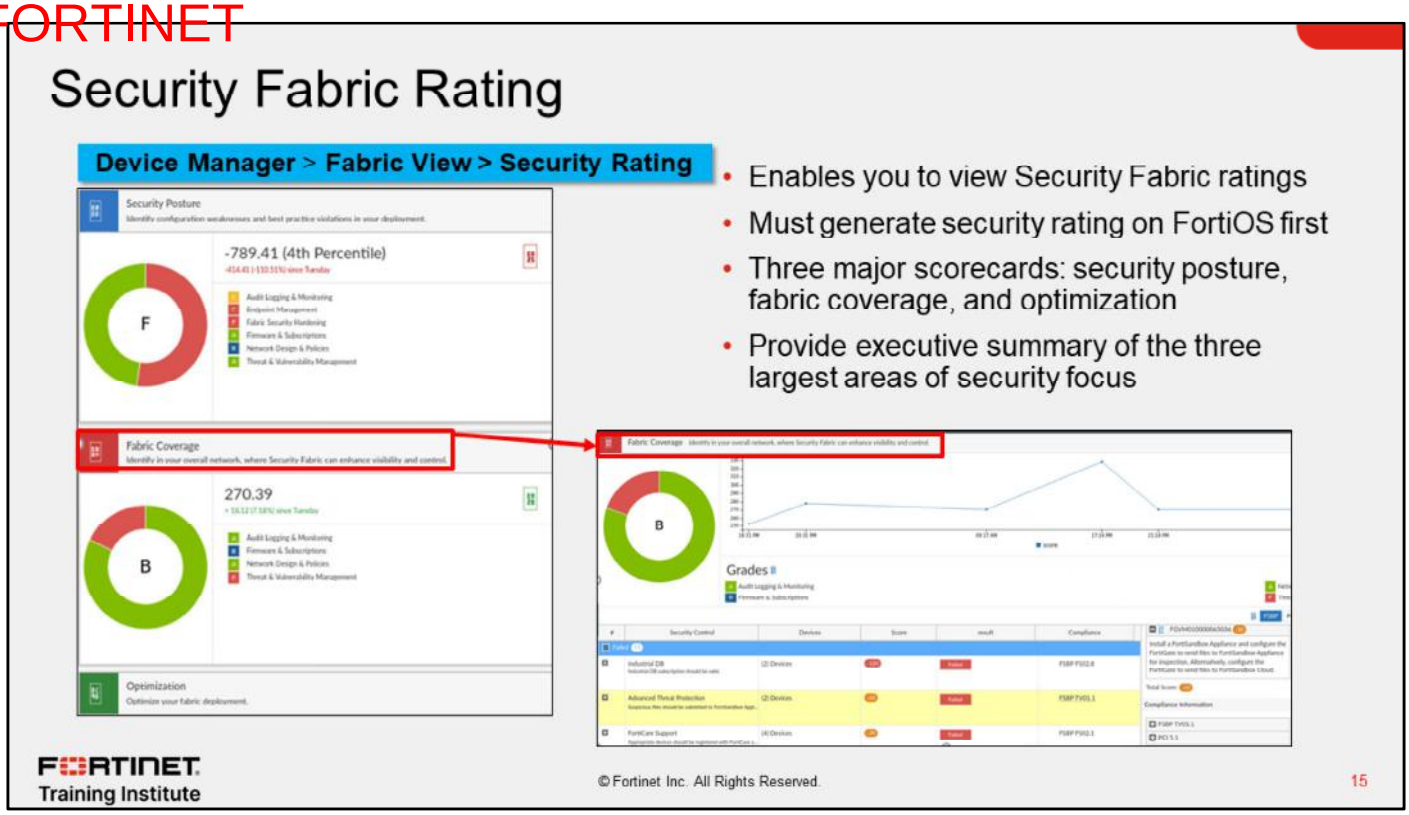
DO NOT REPRINT Brave-dumps.com
© FORTINET



Fabric View (Security Fabric): The Fabric View pane is displayed when FortiManager is managing FortiGate units that have Security Fabric enabled and are part of a Security Fabric group. You can view Security Fabric ratings of configurations for Security Fabric groups. You must generate the Security Fabric ratings by using FortiOS before you can view the information in FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Security Rating** feature includes new security checks that can help you make improvements to your organization's network, such as enforce password security, apply recommended login attempt thresholds, encourage two-factor authentication, and so on. You can view Security Fabric ratings of configurations for all FortiGate devices in a Security Fabric group, or for individual FortiGate devices in a Security Fabric group.

You cannot use FortiManager to generate Security Fabric ratings; you must use FortiOS to generate Security Fabric ratings for a FortiGate Security Fabric group, and then you can see the Security Fabric ratings in FortiManager.

The **Security Rating** page is separated into three major scorecards:

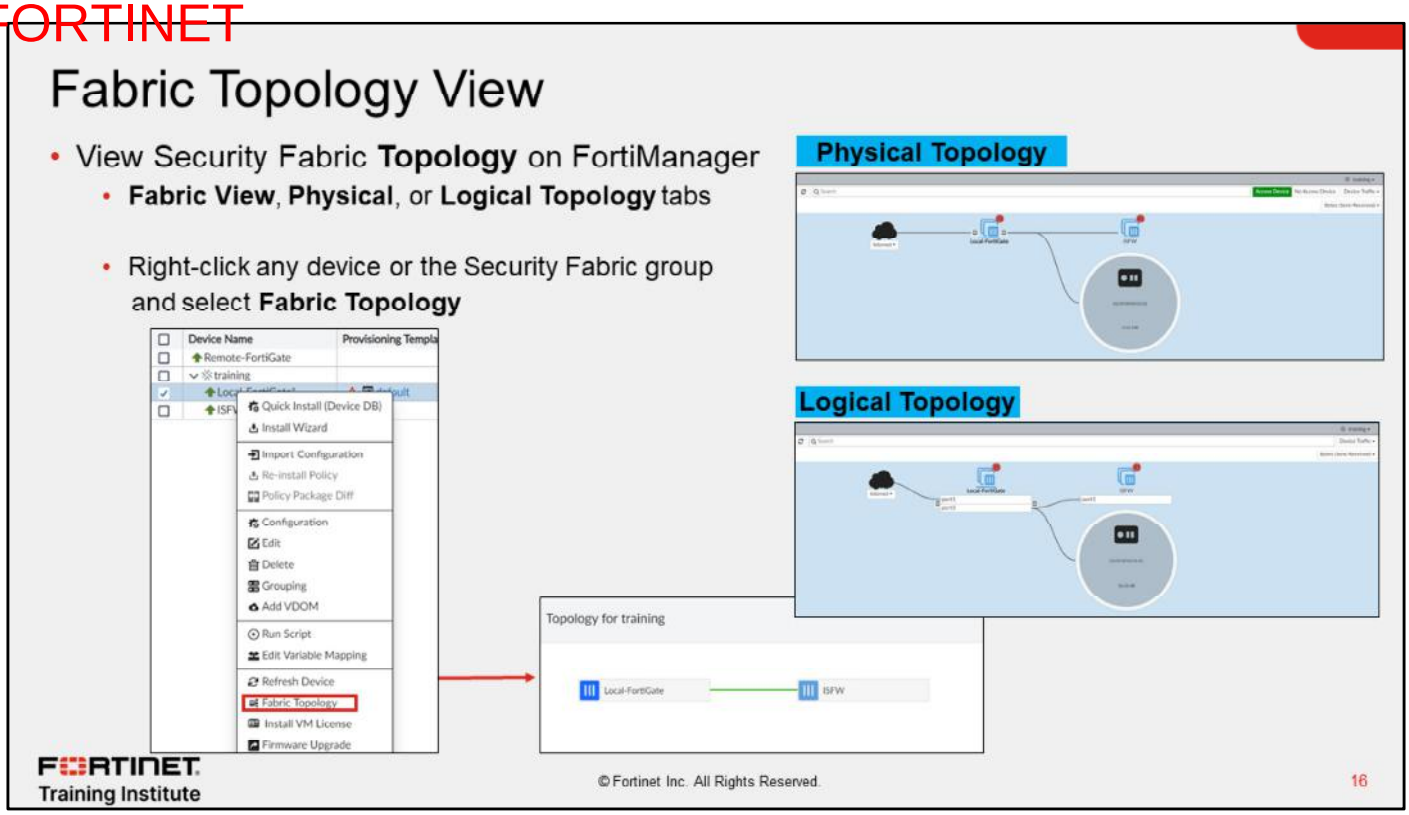
- **Security Posture**
- **Fabric Coverage**
- **Optimization**

These scorecards provide an executive summary of the three largest areas of security focus in the Security Fabric.

The scorecards show an overall letter grade and breakdown of the performance in subcategories. Clicking a scorecard drills down to a detailed report of itemized results and compliance recommendations.
The point score represents the net score for all passed and failed items in that area. The report includes the security controls that were tested against, linking to specific FSBP or PCI compliance policies. You can click the FSBP and PCI buttons to reference the corresponding standard.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

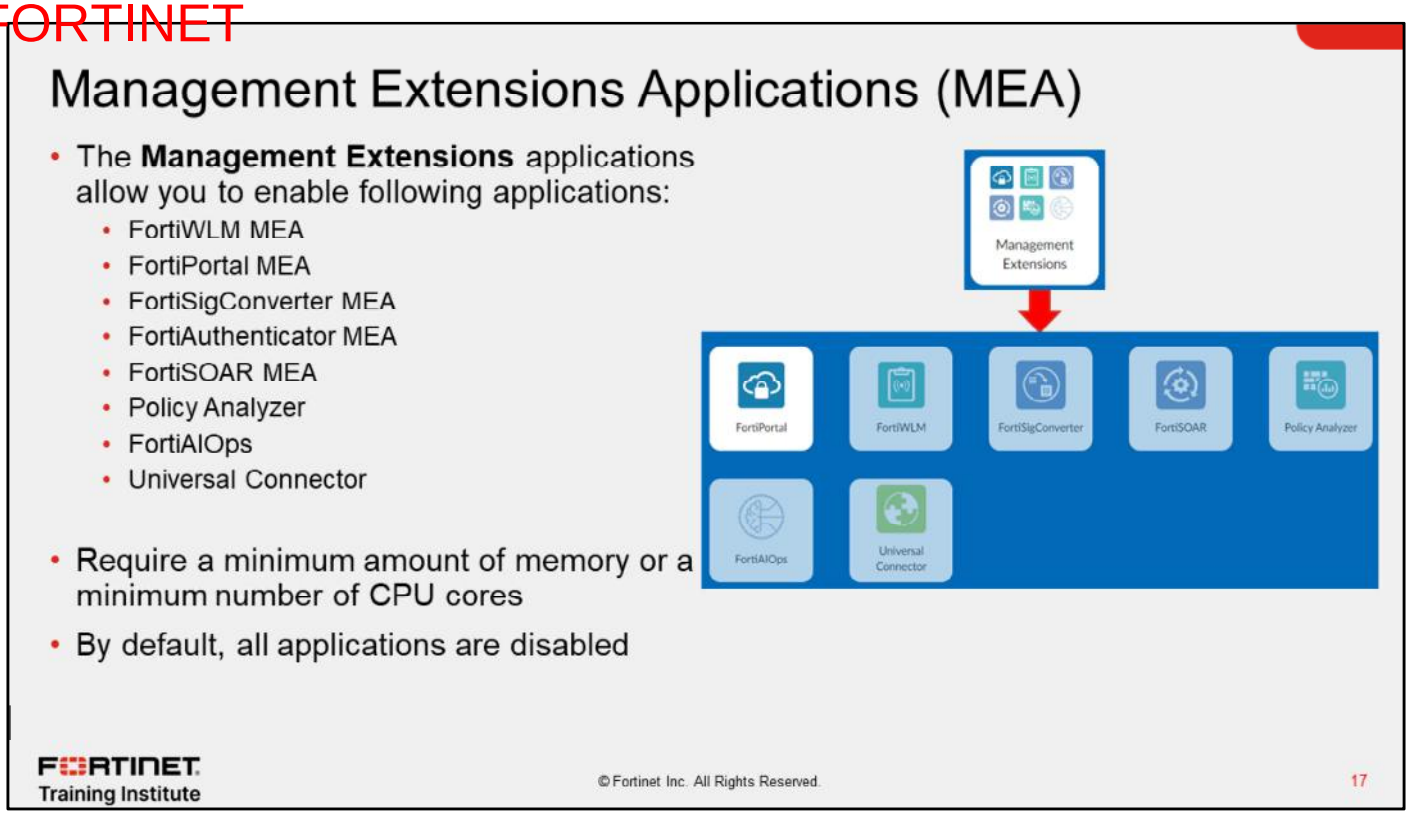


FortiManager recognizes Security Fabric groups of devices and lets you display the Security Fabric topology. You can click **Fabric View** > **Physical Topology**, **Logical Topology**, or right-click a Security Fabric device and select **Fabric Topology** to view your entire device topology in the Security Fabric group.

The Logical Topology view displays your network as a bubble chart of network connection endpoints. These devices are grouped based on the upstream device interface they are connected to. The Logical Topology view is similar to the Physical Topology view, but it shows the network interfaces, logical or physical, that are used to connect devices in the Security Fabric.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Management Extensions** applications allow you to enable licensed applications that are released and signed by Fortinet. Note that both applications are disabled in the FortiManager default configuration. It is important to understand that some MEAs require a minimum amount of memory or a minimum number of CPU cores. The following applications are available as management extensions to FortiManager:

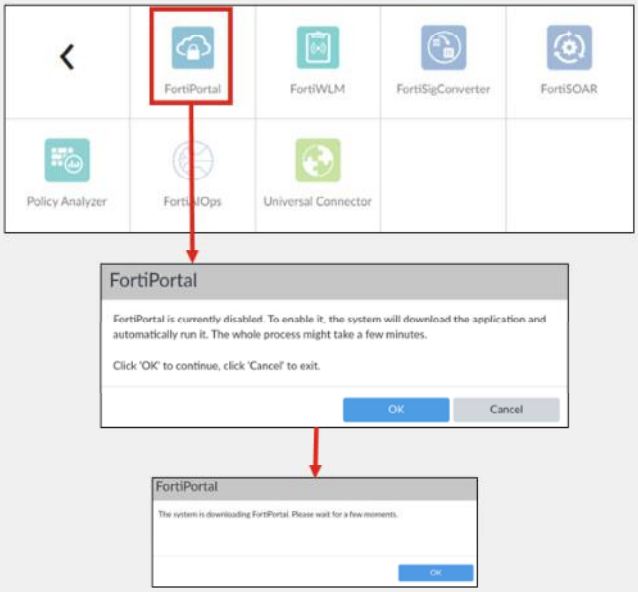
- **FortiWLM MEA**: You can use Wireless Manager (FortiWLM) to monitor, operate, and administer wireless networks on FortiGate devices that are managed by FortiManager.
- **FortiPortal MEA**: You can use FortiPortal MEA to provide a self-service management interface for customers to monitor and configure security instances without direct FortiManager access.
- **FortiSigConverter MEA**: You can use FortiSigConverter MEA to import Snort rules directly into FortiManager and convert them to Fortinet-supported IPS signatures. Snort is a popular open source network intrusion detection system (NIDS).
- **FortiAuthenticator MEA**: You can use FortiAuthenticator MEA to provide access to FortiAuthenticator user and identity management solutions through FortiManager.
- **FortiSOAR MEA**: You can use Fortinet Security Orchestration, Automation, and Response (FortiSOAR) MEA on FortiManager, and use it to manage the entire lifecycle of a threat or breach within your organization.
- **Policy Analyzer MEA**: You can use Policy Analyzer MEA to learn about FortiGate traffic from logs, and present you with several policy options, based on the needs of the analyzed traffic. You can choose a policy option, and Policy Analyzer MEA adds a policy block to the policy, and triggers installation of the updated policy package to FortiGate.
- **FortiAIOps**: You can use FortiAIOps MEA to diagnose and troubleshoot network issues by analyzing potential problems and suggesting remedial steps based on the artificial intelligence (AI) and machine learning (ML) architecture that it is built upon.
- **Universal Connector MEA**: You can use Universal Connector MEA to configure fabric connectors to external applications, such as Guardicore Centra.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

MEA (Contd)

- Unavailable tiles represent disabled applications
- Enabling FortiPortal MEA, FortiManager downloads the application



FORTINET Training Institute

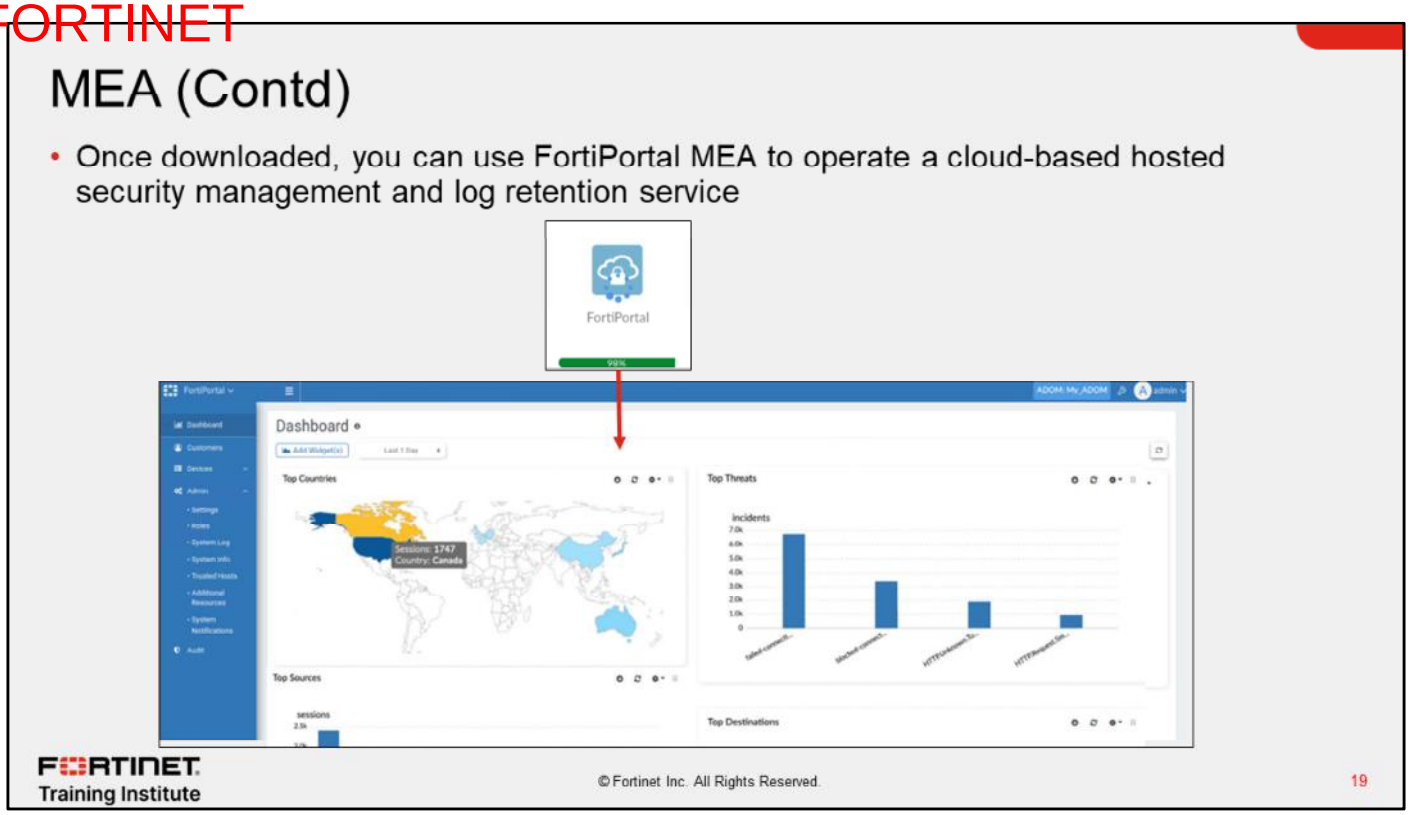
© Fortinet Inc. All Rights Reserved.

18

The unavailable tiles represent disabled applications. As shown on this slide, FortiPortal MEA starts to download.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



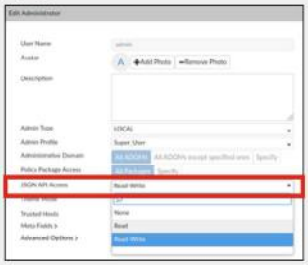
The downloading process might take some time to install the application. When FortiPortal is enabled, you can use it to provide a self-service management interface for customers to monitor and configure security instances without direct FortiManager access. FortiPortal provides a comprehensive set of security management and analytics within a multi-tenant, multi-tier management framework. FortiPortal enables Managed Security Service Providers (MSSPs) to give their customers controlled access to configuration and analytics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

MEA Requirements

- Some MEAs require a minimum amount of memory or a minimum number of CPU cores
- FortiManager uses TCP port 443 or TCP port 4443 to connect to the Fortinet registry and download MEAs
- Ensure that the port is open on any upstream device
- FortiManager administrator with a super user profile can enable MEAs
- Some MEAs require read write JSON API access
- RAM and CPU are capped at 50% for MEAs



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

It is important to understand that some MEAs require a minimum amount of memory or a minimum number of CPU cores. If FortiManager has eight CPUs and 16 GB RAM, then only four CPUs and eight GB RAM are available to MEAs by default, and the four CPUs and eight GB RAM are used for all enabled MEAs. Keep in mind that FortiManager uses lots of resources in the MEA, so, before you enable MEAs, make sure to review the requirements in the FortiManager release notes.

FortiManager uses port TCP port 443 or TCP port 4443 to connect to the Fortinet registry and download MEAs. Make sure that the port is also open on any upstream FortiGate devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What does the Fabric View pane allow you to do?
   - ✓ A. View Security Fabric ratings of configurations for Security Fabric groups.
   - B. Generate Security Fabric ratings for FortiGate devices.

2. Which criteria is a requirement for MEAs?
   - A. Open TCP Port 80
   - ✓ B. Read and write JSON API access

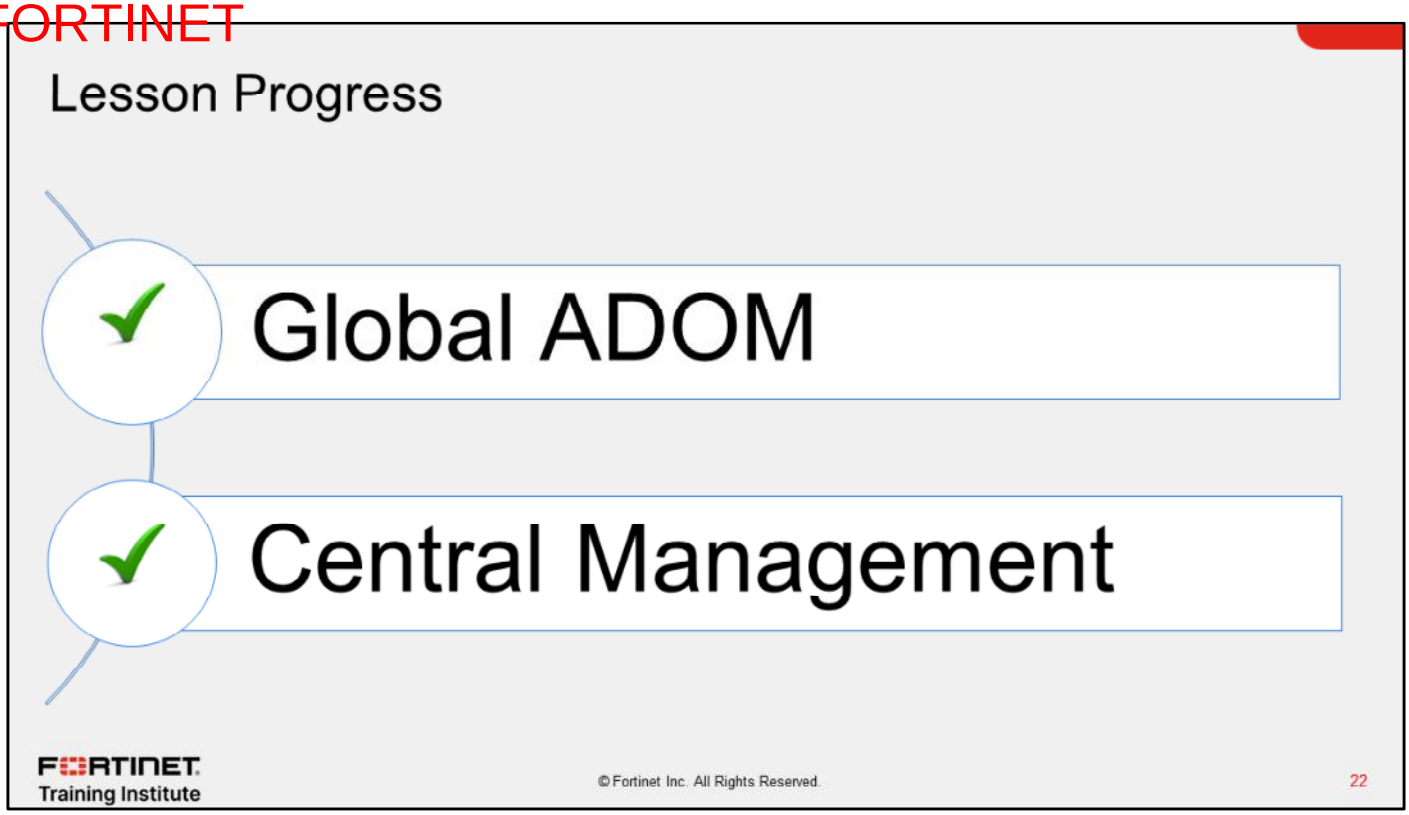
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

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

Review

- ✓ Understand the global ADOM
- ✓ Understand FortiManager manager panes
- ✓ Understand the Security Fabric View with FortiManager
- ✓ Understand the Fabric View and Security Fabric rating
- ✓ View the Security Fabric topology
- ✓ Understand FortiManager MEAs
- ✓ Understand FortiManager MEA requirements

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

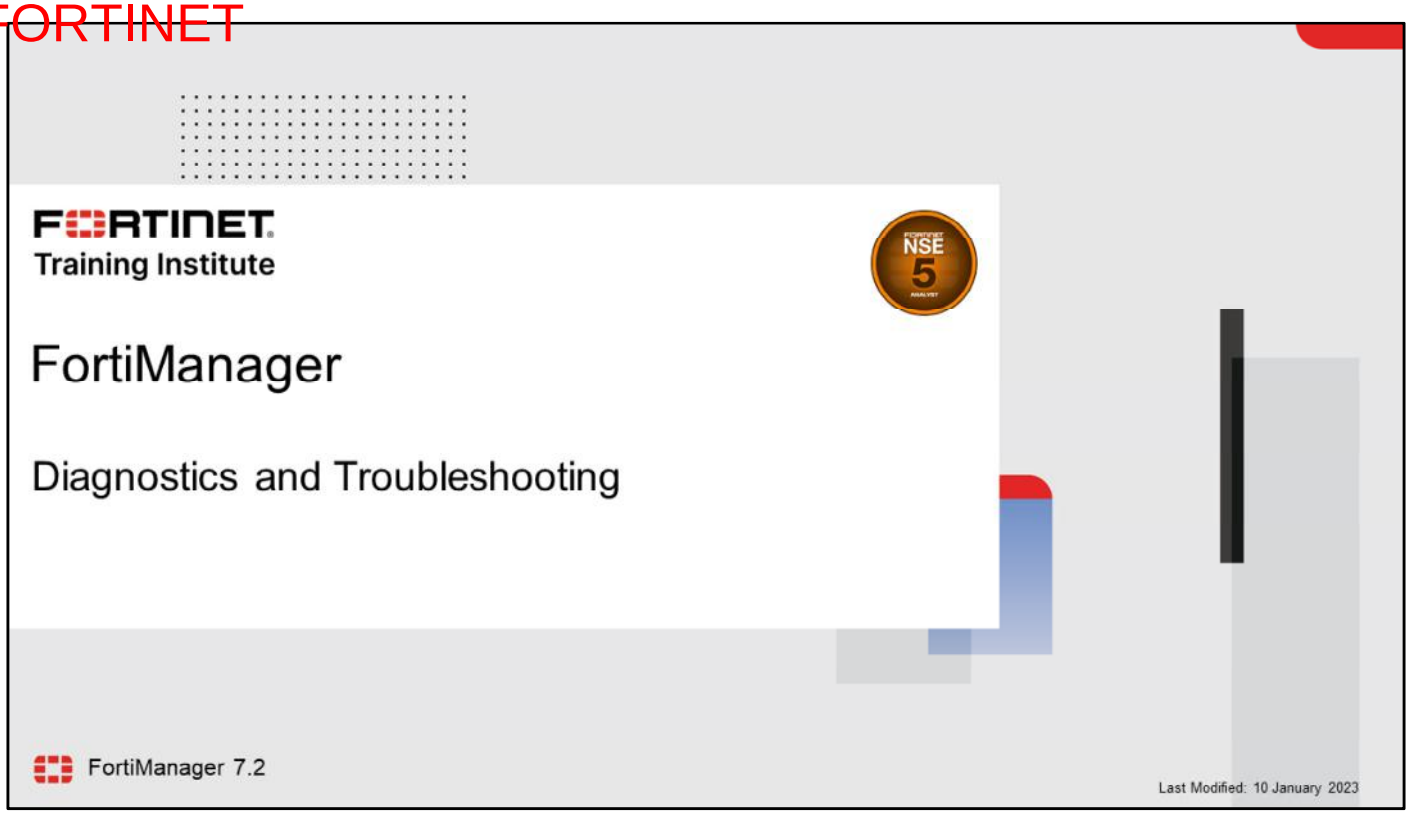
23

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

By mastering the objectives covered in this lesson, you learned about SD-WAN, global ADOM, and the Security Fabric.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to diagnose and troubleshoot issues related to FortiManager and managed devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Deployment Scenarios
- Diagnostics and Troubleshooting
- Troubleshooting Device and ADOM Databases
- Import and Installation Issues

FORTINET Training Institute

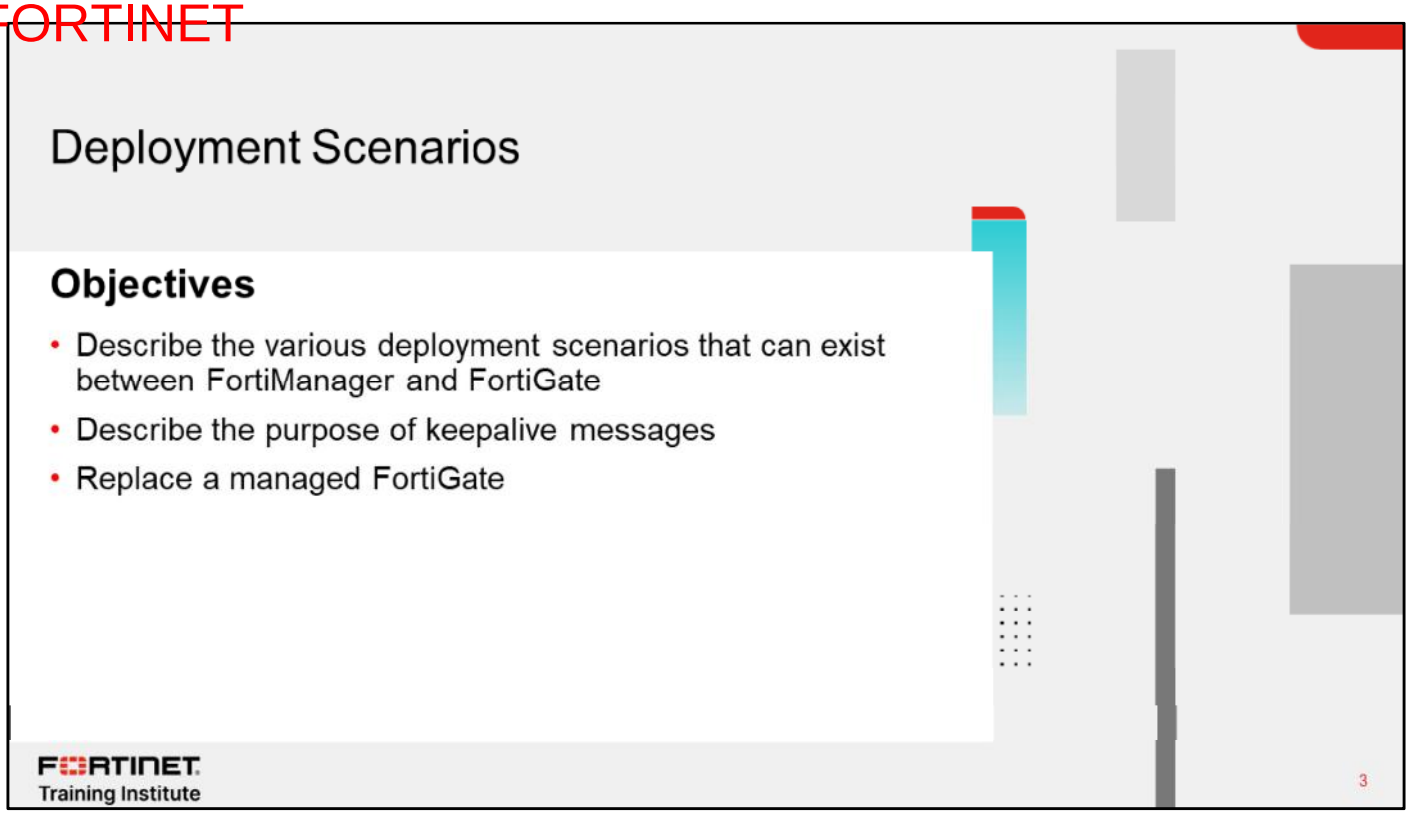
© Fortinet Inc. All Rights Reserved.

2

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 understanding various FortiManager deployment scenarios, keepalive messages, and how to replace a managed FortiGate device, you will be able to deploy FortiGate devices in various scenarios and manage FortiGate devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager Behind a NAT Device

- Only FortiManager can discover the device
- During discovery, the FortiManager NATed IP address is *not* set on FortiGate
- Only FortiManager tries to reestablish the FGFM tunnel, if it is torn down

```
config system central-management
set fmg <FMG_NATed IP address>
```

Configuring the NATed IP address of FortiManager on FortiGate allows:

- FortiGate to announce itself to FortiManager
- Both FortiManager and FortiGate to try to re-establish the FGFM tunnel, if torn down

```
config system admin setting
set mgmt-addr <FMG_NATed IP address>
```

If FortiManager is behind a NAT device, it is recommended that you configure the FortiManager NATed IP address using `system admin settings` on FortiManager

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

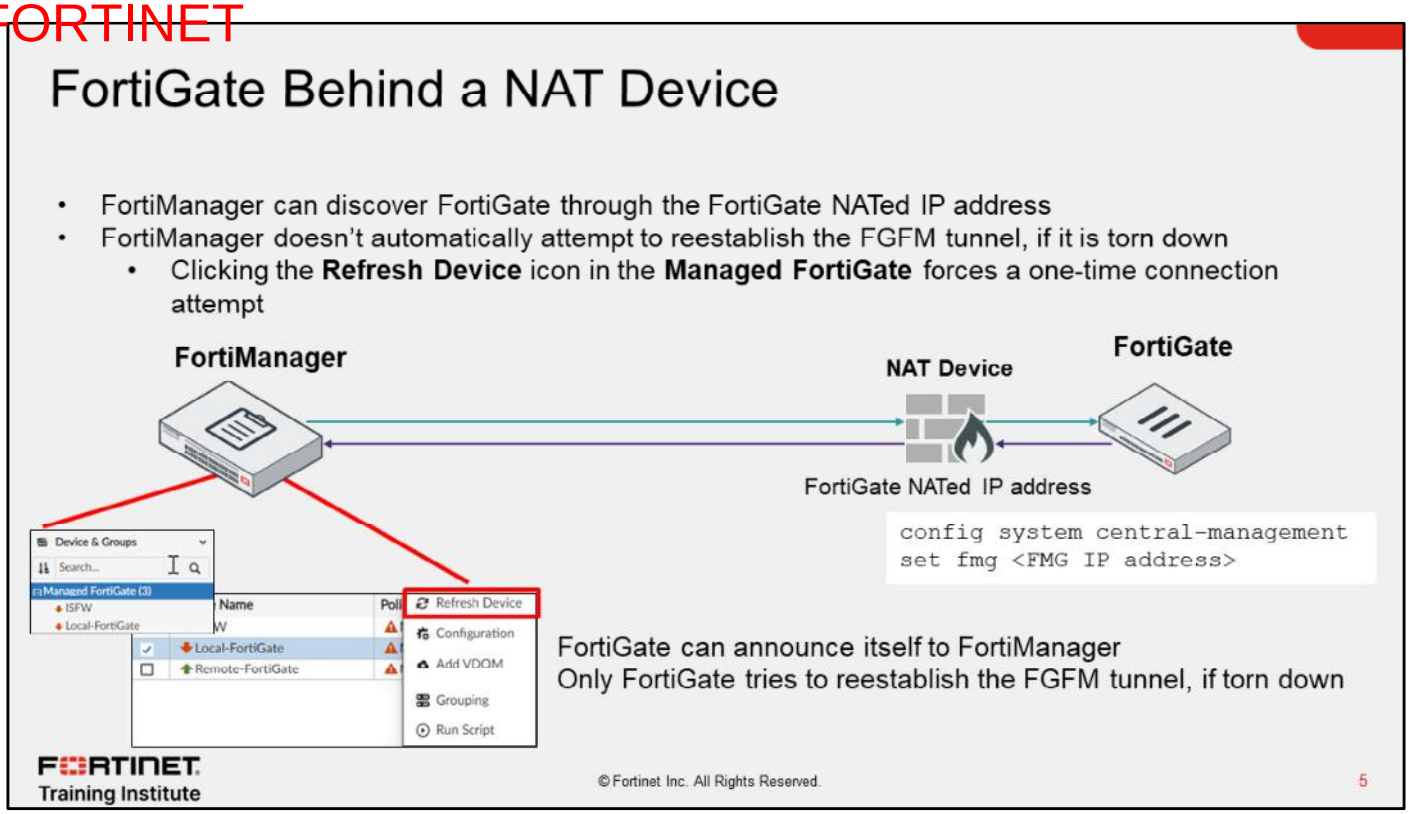
In the scenario shown on this slide, FortiManager is operating behind a NAT device. By default, *only* FortiManager can discover a new device. If the FGFM tunnel is torn down, *only* FortiManager tries to reestablish the FGFM tunnel. This is because, by default, the NATed FortiManager IP address is not configured on FortiGate central management.

How can FortiGate announce itself to the NATed FortiManager, or try to re-establish the FGFM tunnel if it is torn down?

You can configure the FortiManager NATed IP address on FortiGate under the central management configuration. This allows FortiGate to announce itself to FortiManager and try to re-establish the FGFM tunnel, if it is torn down. Configuring the FortiManager NATed IP address on FortiGate allows both FortiManager and FortiGate to re-establish the FGFM tunnel. Also, if you configure the FortiManager NATed IP address under the FortiManager system administrator settings, FortiManager sets this address on FortiGate during the discovery process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this scenario, FortiGate is operating behind a NAT device. FortiManager can discover FortiGate through the FortiGate NATed IP address. FortiGate can also announce itself to FortiManager. What if the FGFM tunnel is interrupted? If the FGFM tunnel is torn down, only FortiGate attempts to reestablish the connection. FortiManager treats the NATed FortiGate as an unreachable device and doesn't attempt to reestablish the FGFM tunnel. However, you can force a one-time connection attempt from FortiManager by clicking the **Refresh Device** icon in the **Managed FortiGate** for the managed device in Device Manager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Both Devices Behind a NAT Device

- FortiManager can discover FortiGate through a NATed FortiGate IP address
- Clicking the **Refresh** icon in the **Connection Summary** widget forces a one-time connection attempt

```
config system central-management
set fmg <FMG_NATed IP address>
```

If a FortiManager NATed IP address is configured on FortiGate, then:

- FortiGate can announce itself to FortiManager
- If the connection is torn down, only FortiGate attempts to reestablish the connection

FORTINET Training Institute

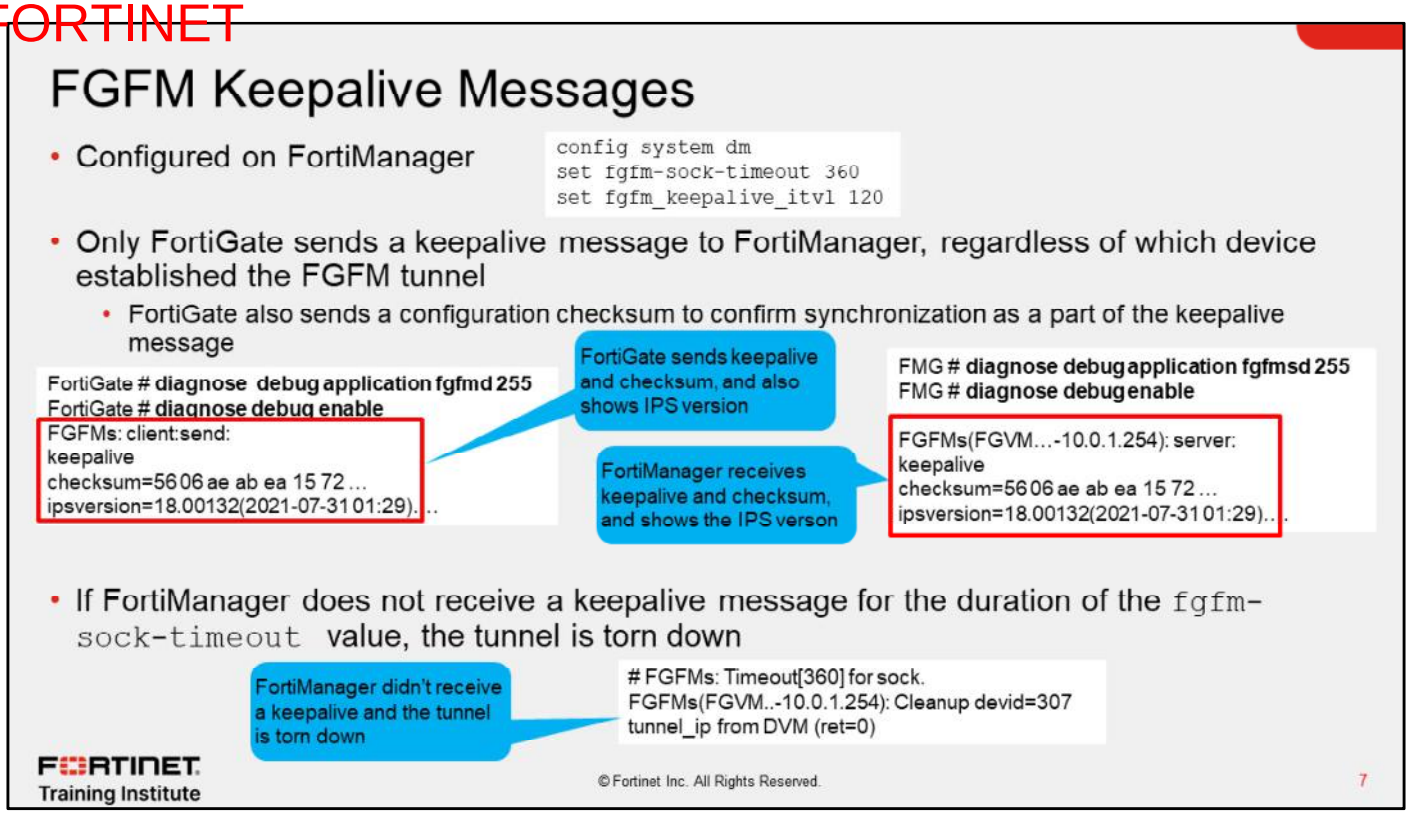
© Fortinet Inc. All Rights Reserved.

6

What if both devices—FortiManager and FortiGate—are behind a NAT device? Then, the FortiGate device is discovered by FortiManager through the FortiGate NATed IP address. Just like it was in the NATed FortiManager scenario, the FortiManager NATed IP address in this scenario is not configured under the FortiGate central management configuration. FortiManager does not attempt to reestablish the FortiGate to FortiManager (FGFM) tunnel to the FortiGate NATed IP address, if the FGFM tunnel is interrupted. If the FortiManager NATed IP address is configured on FortiGate under the central management configuration, FortiGate tries to reestablish the FGFM tunnel, if it is torn down.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Keepalive messages, including the configuration checksums, are sent from FortiGate at configured intervals. The messages also show the intrusion prevention system (IPS) version of the FortiGate device. The keepalive message includes:

- `fgfm-sock-timeout`: the maximum FortiManager or FortiGate communication socket idle time, in seconds
- `fgfm_keepalive_itvl`: the interval at which the FortiGate sends a keepalive signal to a FortiManager device to keep the FortiManager or FortiGate communication protocol active

If there are no responses to the keepalive messages for the duration of the sock timeout value, the tunnel is torn down and both ends attempt to reestablish it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Recovery Logic

- To make configuration changes to FortiGate, FortiManager sends `set` and `unset` CLI commands
- FortiGate devices:
  - Apply `set` commands
  - Test the FGFM connection to FortiManager
- If the connection fails, FortiGate applies the `unset` command after 15 minutes
- If the connection fails again, FortiGate reboots and recovers the previous configuration from its configuration file (optional)
  - Can be enabled from the FortiManager CLI

```
config system dm
set rollback-allow-reboot enable
end
```

Default disabled

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

When an installation is performed from FortiManager to FortiGate, FortiManager always tries to ensure connectivity with the managed FortiGate device. If the connection fails, FortiManager tries to recover the FGFM tunnel by unsetting the command that caused the tunnel to go down.

For each installation, FortiManager sends the following commands to the managed FortiGate device:
- Set commands, needed to apply the configuration changes
- Unset commands, to recover the configuration changes

When applying changes, FortiGate:
- Applies the set commands, using memory only, nothing written to a configuration file
- Tests the FGFM connection to FortiManager

If the connection fails to reestablish, FortiGate applies the unset command after 15 minutes (not configurable and not based on sock timeout values). If the connection remains down, and `rollback-allow-reboot` is enabled on FortiManager, FortiGate reboots to recover the previous configuration from its configuration file.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Replace a Managed Standalone Device

- When a management connection request is made, the FortiGate serial number is verified
- When replacing a standalone device, you must manually change the serial number and redeploy the configuration
- When replacing a FortiGate cluster member, FortiManager learns the new serial number through the FGFM tunnel

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

FortiManager saves the configuration revisions of a managed device. But what happens if you need to replace the standalone managed device because of hardware failure or return merchandise authorization (RMA)?

You can replace the faulty standalone device by manually changing the serial number of the faulty device to the serial number of the replacement device on FortiManager. Then, you redeploy the configuration. The serial number is verified before each management connection, because the licenses are attached to the FortiGate serial number. When replacing a FortiGate cluster member, FortiManager learns the new serial number through the FGFM tunnel.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Replace a Managed Standalone Device (Contd)

- Steps to replace a managed device are:
  1. Note original FortiGate device name

     ```
     diagnose dvm device list
     ```

  2. Update the serial number of the replaced FortiGate

     ```
     execute device replace sn <devname> <New serialnum>
     ```

  3. Verify that FortiManager updated the serial number in its database

     ```
     diagnose dvm device list
     ```

  4. Send a registration request from the replaced FortiGate
  5. If connectivity is down after updating the serial number, you might need to reclaim the management tunnel

     ```
     execute fgfm reclaim-dev-tunnel <optional device name>
     ```

devname = Original FortiGate device name
serialnumber = Serial number of replaced FortiGate

Replacement FortiGate should not contact FortiManager before `execute device replace sn <devname> <serialnum>` is run. *If it does, you must delete the unregistered device entry prior to rerunning the command!*

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

Note that the replacement FortiGate should not contact FortiManager before the `execute device replace sn <devname> <serialnum>` command is run. If it does, you will have to delete the unregistered device entry *prior* to rerunning the command.

To replace the faulty device with the new device, take the following steps:

1. Note the device name of the original FortiGate.
   If the replacement device is already listed as unregistered, then you will need to delete it from the unregistered device list in the root ADOM.
2. Add the serial number of the replacement FortiGate.
   After the replace command is executed, FortiManager updates the serial number in its database.
3. Verify that the new device serial number is associated with the faulty device in FortiManager.
   You can do this using the CLI or the **System Information** widget of FortiGate.
4. Send a request from the replacement device to register it with FortiManager.

If connectivity fails after you update the serial number, you might need to reclaim the management tunnel. The device name is optional. If you run the command without the device name, FortiManager tries to reclaim tunnels from all managed devices.

Optionally, you can change the device password that you used when you added the device by running the `execute device replace pw <device_name> <password>` command.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. If FortiManager is behind a NAT device, which step is recommended?
   - ✓A. Configure the NATed IP address of FortiManager with the `set mgmt-addr` command under the `config system admin setting`.
   - B. Configure the NAT device IP address on FortiGate.

2. What does the `fgfm-sock-timeout` command do?
   - ✓A. It sets the idle time out setting for communication between FortiManager and FortiGate.
   - B. It sets the idle time out setting for communication between FortiManager and the public FortiGuard server.

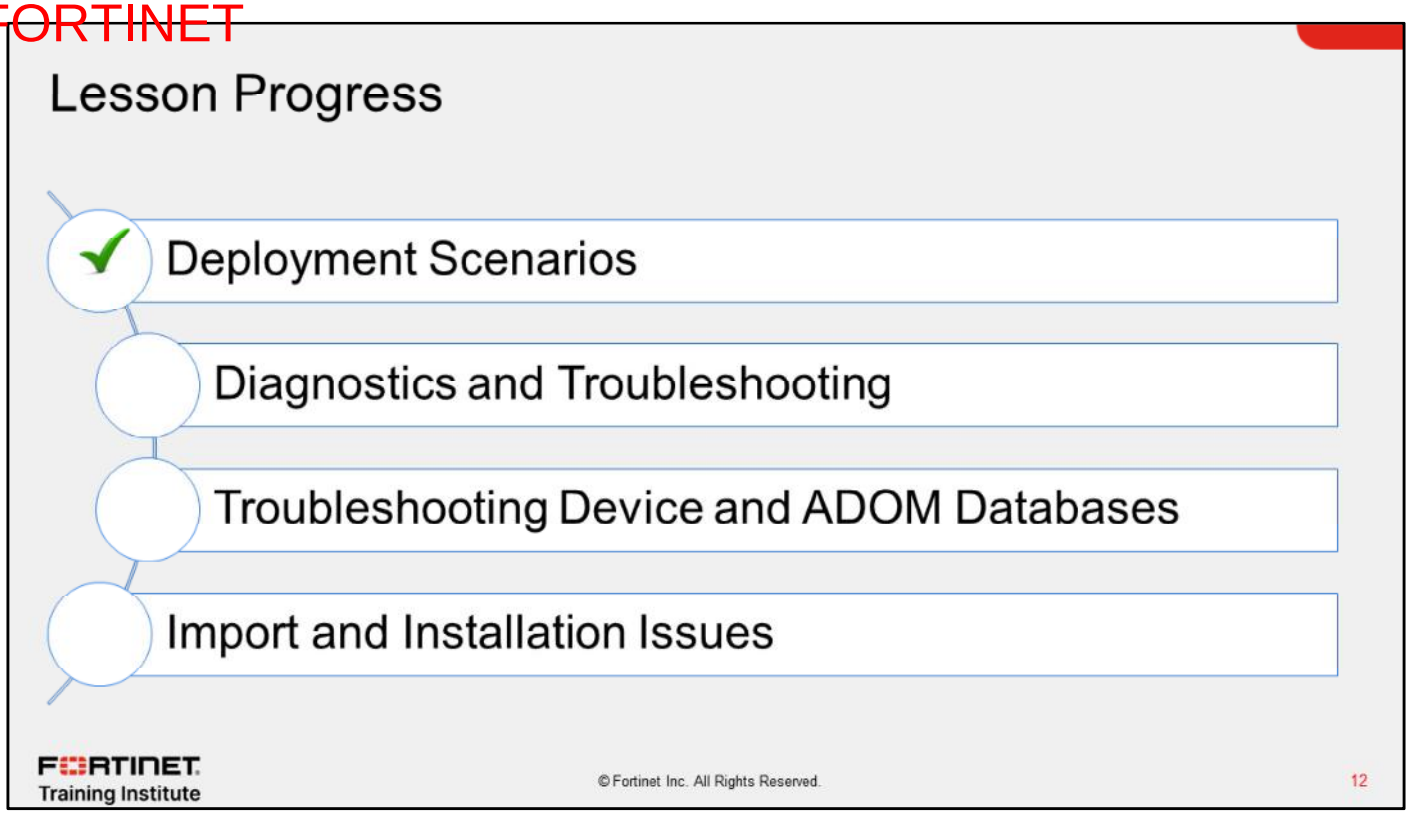
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

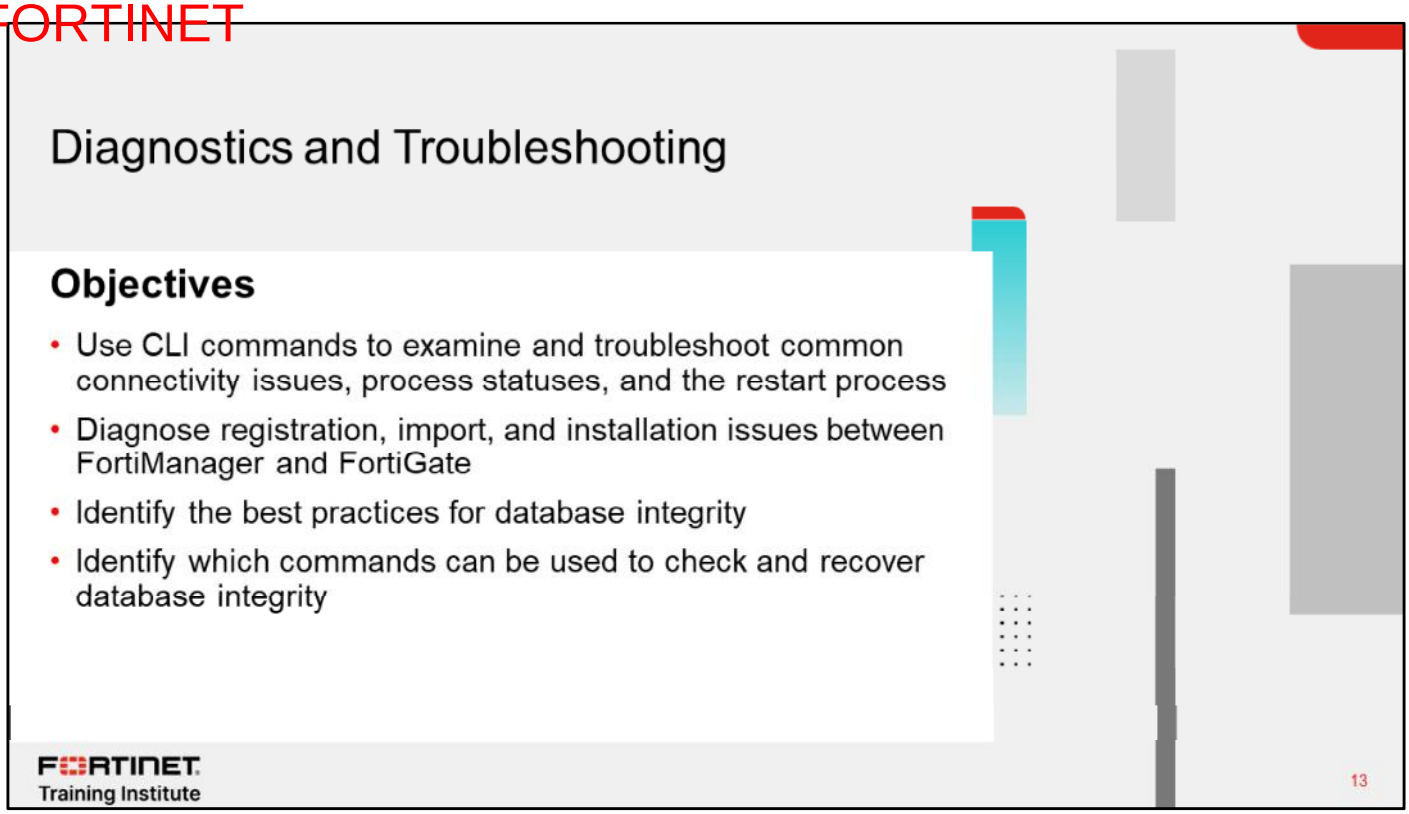


Good job! You now understand deployment scenarios.

Now, you will learn how to use some diagnostics commands to troubleshoot issues with FortiManager connectivity and performance.

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 using diagnostics and troubleshooting techniques, you will be able to manage and maintain the integrity of FortiGate devices in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Basic Commands

Command	Information
# get system status	Current status – serial number, firmware version, ADOM status, HA Status
# get system performance	Overall resource utilization – CPU, memory, disk
# execute top (lists processes with high CPU or memory usage) # execute iotop (lists processes with high i/o usage)	Top processes
# diagnose debug crashlog read	Crash logs
# diagnose sniffer packet <interface> <filter> <verbose> <count> <timestamp>	Packet sniffer
# execute ping <FortiGate IP> # execute ssh <FortiGate IP> # execute ssh <FortiGate FGFM IP> (link level IP address from session-list or dvm device list command) # diagnose fgfm session-list # diagnose dvm device list	Testing device reachability from FortiManager Confirming FGFM tunnel is up
# diagnose system print df # diagnose system print partitions	Disk partition layout and status

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

14

This slide shows some CLI commands that you can use to troubleshoot FortiManager connectivity and resource issues.

These commands are similar to the FortiGate commands that you can use to diagnose and troubleshoot common issues. For example, to view the top running processes you can run `execute top`. You can use the `execute iotop` command to identify system processes with high I/O usage (usually the disk activity). You can view the crash log entries. If FortiManager is dropping packets or not receiving packets, you can run a packet capture (sniffer) to help diagnose the reason. You can also test the device reachability and confirm the status of the FGFM tunnel.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System Resources Usage

- `get system performance` displays information about system resources, such as CPU, memory, hard disk, and flash disk usage

```
FMG-VM64 # get system performance

CPU:
        Used:                                   0.72%
        Used(Excluded NICE):    0.72%
                        %used   %user   %nice   %sys        %idle %iowait         %irq %softirq
        CPU0             0.21    0.00    0.00    0.21   99.79    0.00    0.00     0.00
        CPU1             0.62    0.00    0.00    0.41   99.38    0.00    0.00     0.21
Memory:
        Total:      6,141,820 KB
        Used:       1,804,192 KB            29.4%
        Total (Excluding Swap): 4,044,672 KB
        Used (Excluding Swap):  1,804,192 KB            44.6%
Hard Disk:
        Total:      82,041,240 KB
        Used:       9,185,896 KB            11.2%
        Inode-Total:            5,242,880
        Inode-Used: 45,528      0.9%
        IOStat:   tps     r_tps    w_tps    r_kB/s    w_kB/s    queue   wait_ms  svc_ms  %util sampling_sec
                   8.9      6.3      2.6     191.3     647.2      1.9   217.4     5.2     4.6       974.45
Flash Disk:
        Total:      1,007,512 KB
        Used:       228,900 KB  22.7%
        Inode-Total:            65,536
        Inode-Used: 38          0.1%
        IOStat:   tps     r_tps    w_tps    r_kB/s    w_kB/s    queue   wait_ms  svc_ms  %util sampling_sec
                   2.4      2.4      0.0     269.8       0.3      0.0    15.9     8.2     2.0       974.45
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

The `get system performance` command provides information about system resource usage and displays the output by resource type:

- `CPU`: provides an overview of CPU usage information on the system. It shows what type of processes are using what percentage of the CPU
- `Memory`: provides total memory available to the unit and how much memory is currently in use
- `Hard Disk`: provides hard disk usage information, including total disk space available and how much is in use
- `Flash Disk`: provides flash disk usage information

Always check the `Used` column to check resource usage. If the resources usage is high, you may experience issues managing devices from FortiManager. For example, adding devices or installing changes may take a long time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

High CPU and Memory Troubleshooting

- `execute top` displays real-time system monitoring command

```
FMG-VM64 # execute top
1 top - 13:08:23 up 1 day,  1:01,  0 users,  load average: 2.40, 3.19, 3.34

2 Tasks: 188 total,   2 running, 186 sleeping,   0 stopped,   0 zombie

3 %Cpu(s): 15.4 us,  7.7 sy,  0.0 ni, 76.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st

4 MiB Mem : 2010.164 total,   41.250 free,  974.086 used,  994.828 buff/cache

5 MiB Swap: 2027.867 total, 1361.922 free,  665.945 used.  855.359 avail Mem

  PID USER      PR  NI    VIRT    RES %CPU %MEM     TIME+ S COMMAND
6 1163 root     20   0   17.6m   2.1m  7.1  0.1   0:00.05 R top
    1 root     20   0  602.2m  14.9m  0.0  0.7   0:11.67 S /bin/initXXXXXXXXXX
    2 root     20   0    0.0m   0.0m  0.0  0.0   0:00.00 S [kthreadd]
...
```

Process ID

FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.
16

The `execute top` command displays real-time system statistics that are very useful for system monitoring. The statistics are displayed in rows, as follows:
Row 1: current time, uptime, users sessions, average system load (last minute, five minutes and 15 mins)
Row 2: total number of processes running, processes actively running, processes sleeping, stopped, in zombie state
Row 3: CPU usage for: user processes, system processes, priority processes, CPU idle, processes waiting for I/O, hardware irq, software irq, and steal time
Row 4 and Row 5: memory usage
Row 6: process ID, user, priority process, nice value of the process, virtual memory usage is a swap file, memory usage is RAM, CPU usage, memory usage percentage, total activity time, state of the process, and name of the process

When you are troubleshooting issues with high CPU or memory usage, check the overall system resources. Then check individual processes for high CPU or memory usage.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

High Disk Usage Troubleshooting

- `execute iotop` displays the processes that are responsible for high I/O usage

```
FMG-VM64 # execute iotop

Total DISK READ :       0.00 B/s | Total DISK WRITE :       0.00 B/s

Actual DISK READ:       0.00 B/s | Actual DISK WRITE:       0.00 B/s

  TID  PRIO  USER     DISK READ  DISK WRITE  SWAPIN     IO>    COMMAND
  512 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % fortilogd
[fortilogd.wrtr2]
    1 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % initXXXXXXXXXX
    2 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kthreadd]
    3 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksoftirqd/0]
  516 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % fortilogd
[fortilogd.stat]
    5 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kworker/0:0H]
...
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

17

FortiManager displays the individual processes that are responsible for high I/O wait state when you use the command `execute iotop`. You can use this command to identify the process that is causing high I/O usage when you are troubleshooting performance issues related to heavy I/O usage.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Crash Log

- Inspect crash logs for debugging purposes
- Output is sorted based on time
- The most recent crash is listed at the bottom

Displays system information

```
FMG-VM64 # diagnose debug crashlog read
Firmware FMG-VM64 v7.2.1-build1215 220809 (GA)
Application fgdsvr
Signal 11 (Segmentation fault)
Date 2022-09-13 19:04:49
Pid 978 ppid 676 backtrace:
[0x7fc30aff330a]  libsegfault.so  print_tra  +0x25/0x12c
[0x7fc30aff34e9]  libsegfault.so  catch_segfaul  0xd8/0x13d
[0x7fc309b920ef]  libpthread.so.0  +0x130ef
[0x7fc30975a506]  libc.so.6  epoll_wait+0x16/0x9d
```

Displays application name and signal used to interrupt the process

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

Another area you may want to monitor, purely for diagnostics, is the crash logs. The crash logs are available through the CLI. The most recent crash log is listed at the bottom of the output. In this example, process `fgdsvr` was restarted with signal 11, and crash information was logged in the crash log file. The crash log displays the firmware information in the first line, followed by process name, and signal information.

Most of the logs in the crash log are normal. Some logs in the crash log might indicate problems. For that reason, crash logs may be requested by Fortinet Technical Support for troubleshooting purposes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Packet Sniffer

- The packet sniffer command is useful for troubleshooting connectivity and traffic-related issues
- FortiManager supports verbose options 1, 2, and 3
- diagnose sniffer packet <interface> <filter> <verbose> <count> <timestamp>

```
FMG-VM64 # diagnose sniffer packet any "host 192.168.1.99 and port 541" 1 5 l
interfaces=[any]
filters=[host 192.168.1.99 and port 541]
2021-10-08 09:09:35.339199 192.168.1.69.541 -> 192.168.1.99.14288: psh 3363626479 ack
1008803733
2021-10-08 09:09:35.340822 192.168.1.99.14288 -> 192.168.1.69.541: psh 1008803733 ack
3363626713
2021-10-08 09:09:35.340840 192.168.1.69.541 -> 192.168.1.99.14288: ack 1008803903
2021-10-08 09:09:35.340912 192.168.1.69.541 -> 192.168.1.99.14288: psh 3363626713 ack
1008803903
2021-10-08 09:09:35.379884 192.168.1.99.14288 -> 192.168.1.69.541: ack 3363626819
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

The packet sniffer command is useful for troubleshooting connectivity and traffic-related issues. The packet sniffer command shown on this slide is set up to capture packets from host `192.168.1.99` on port `541` and to display the packet header only (verbose 1) for five packets and the local timestamp. Unlike FortiOS, FortiManager supports only verbose options 1, 2, and 3.

For example, if you are experiencing a connectivity issue between FortiManager and FortiGate, you can sniff for management traffic on TCP port `541` to see if there is any communication between the two devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager Disk Partition

- `diagnose system print df` displays disk partition information on FortiManager
- Useful for troubleshooting incorrect disk partitioning and insufficient disk size issues

```
FMG-VM64 # diagnose system print df
Filesystem           1K-blocks      Used Available Use% Mounted o
rootfs                  987780    216008    771772  22% /
none                    987792         0    987792   0% /dev
none                   1320816        16   1320800   0% /dev/shm
none                     65536        32     65504   0% /tmp
/dev/sda1                499656     84708    414948  17% /data
/dev/mdvg/mdlv         82434736  42214320  40204032  51% /var
/dev/mdvg/mdlv         82434736  42214320  40204032  51% /drive0
/dev/mdvg/mdlv         82434736  42214320  40204032  51% /Storage
/dev/loop0                 8887        97      8278   1% /var/dm/tcl-root
```

Shared memory (a temporary file storage filesystem)

Flash disk partition

FortiManager database

FortiAnalyzer archives and Postgres database

FortiAnalyzer log and report storage

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

The `diagnose system print df` command displays disk partition information on FortiManager. It shows the filesystem, size, usage, available disk space, usage in percentage, and mount point. This command can be useful when troubleshooting disk-related issues. It can be helpful to know what each of these partitions are used for on FortiManager:

- `/dev/shm` is used as shared memory.
- `/tmp` is temporary file storage file system.
- `/data` is the pointer to the flash disk partition.
- `/var` is used for FortiManager database storage.
- `/drive0` is used as the FortiAnalyzer archives and postgres database.
- `/Storage` is used for FortiAnalyzer log and report storage.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Processes Status

- Check for unexpected locked processes
  - Processes lock and unlock the database
    - On an idle system, there should not be any processes in locked state

```
# diagnose dvm lock
Global database pending read: unlocked
Global database pending write: unlocked
Global database reserved read: unlocked
Global database reserved write: unlocked
Global database shared read: unlocked
Global database shared write: unlocked
```

- Check for a stuck process or task
  - A stuck task in **Task Monitor** may prevent pending tasks from being processed
    - Can cancel or delete stuck or pending tasks from **Task Monitor**
    - Sometime GUI does not cancel or delete stuck tasks, run CLI commands:
      - `diagnose dvm task repair`
      - `diagnose dvm task reset`

```
 # diagnose dvm proc list
dvmcmd group id=428
dvmcmd process 428 is running control
        Process is healthy.
dvmcmd process 1406 is running ...
        No associated tasks found.
dvmcmd process 1407 is running ...
        Task 81 (pending) 1 lines, 0% done
                ADOM:     My_ADOM (159)
                User:     admin
                Title:    retrievedevconftitle
                Source:   device_manager (0)
                Started:  Mon October 04 14:45:12 2022
dvmcore is running normally.
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

On FortiManager, processes lock and unlock the database, but they should not remain stuck in the locked state. There should be no locks on an idle system.

What if FortiManager is taking too long to complete a task? You can use the `proc list` command to identify any process or task that is stuck. A stuck task may prevent other subsequent tasks from being processed. If a task is taking too long to process, it is listed here. You can cancel or delete the pending (stuck) task from **Task Monitor** on the **System Settings** pane.

Sometime **Task Monitor** does not cancel or delete the stuck or pending tasks from GUI, but you can run the CLI commands to cancel or delete:

- `diagnose dvm task repair` keeps the logs while repairing the task database. Where as
- `diagnose dvm task reset` completely removes the logs from the FortiManager task database.

These CLI commands reboots FortiManager after fixing the task database.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Debug Commands

Command	Information
# diagnose debug enable # diagnose debug timestamp enable	Enable debug output on SSH/Telnet session Enable timestamp in the debug output
# diagnose debug application dmapi 255 # diagnose dvm debug enable all	Debug device-level operations: registering, deleting, refresh, auto-updates, resync process
# diagnose debug application securityconsole 255	Debug ADOM to device database copy process and import policy packages
# diagnose debug application depmanager 255 # diagnose debug dpm conf-trace enable	Debug the registration process and install process, including CLI scripts run directly on devices, retrieves, and revision history

- Before running any debugs, always check which debugs are currently enabled
  - Shows output from other debugs, if debug level is not reset
  - To reset the debug level
    `diagnose debug reset`

```
FMG-VM64 # diagnose debug  info
General
        cli debug level:                3
        console debug output:           enable
        debug timestamps:               disable
        terminal session debug output:  enable
        terminal session data  masking: disable

DPM
        dpm conf trace:                 enable

Application
        ddmd debug filter:              disable
        depmanager debug level:         255
        fgfmsd debug filter:            Local-FortiGate
        fgfmsd debug level:             255
        oftpd debug filter:             disable
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

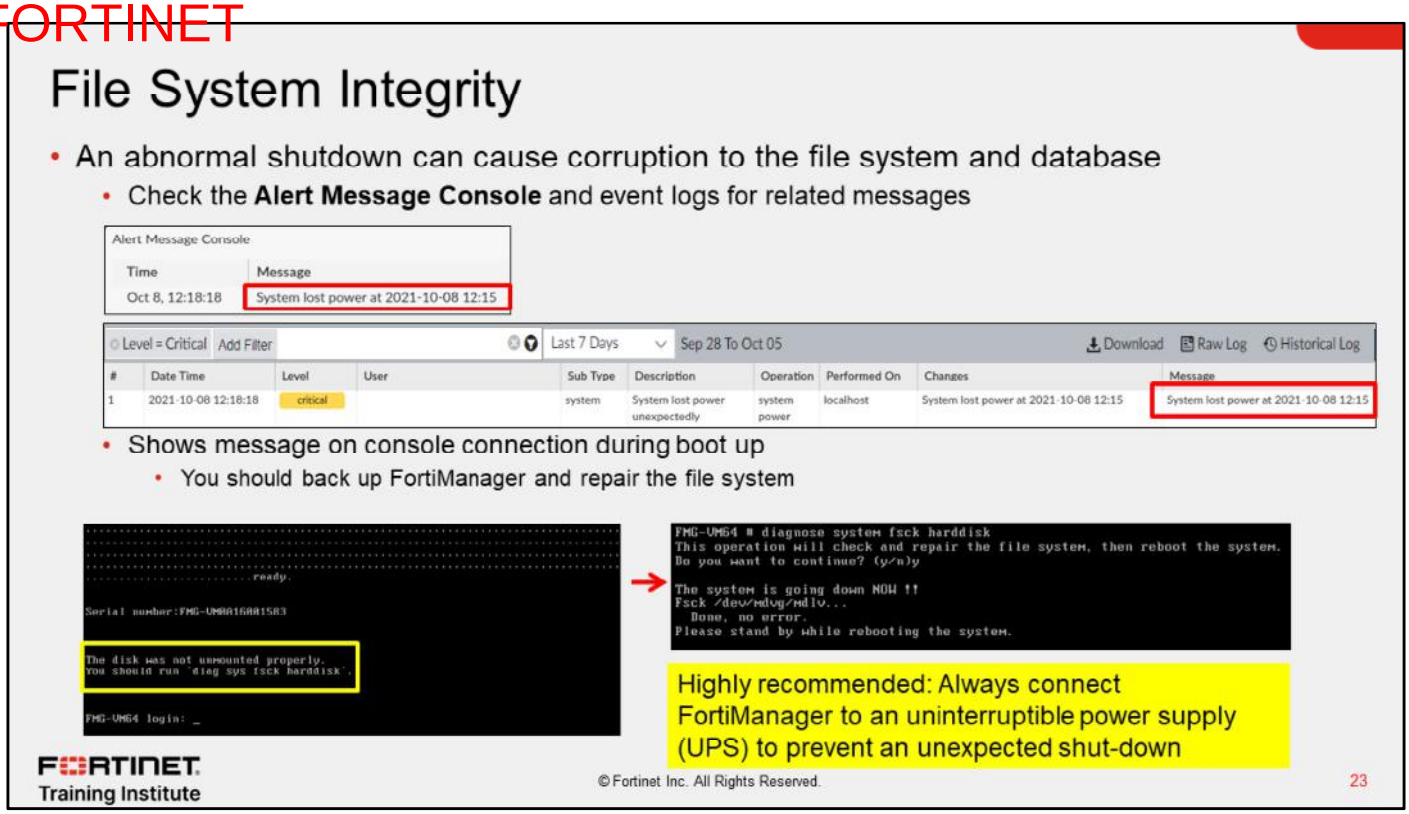
22

You can use these debug commands to troubleshoot issues between FortiManager and FortiGate. These issues could be related to actions such as adding, deleting, refreshing, auto-updating, and installing.

Before you run any debug commands, check if any other debug commands are enabled. Running a debug shows the output from all other enabled debugs, if they are not disabled or reset. Always reset the debug level before enabling any new debugs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



An ungraceful shutdown on FortiManager can cause corruption to the file system and internal database. This applies to both hardware and virtual machines. As a best practice, you should check the **Alert Message Console** and event logs for important messages.

If FortiManager loses power, a message on the console connection advises you to repair the file system. Remember, always back up FortiManager prior to repairing the file system. It is also highly recommended that you connect FortiManager to an uninterruptible power supply (UPS) to prevent an unexpected shut down.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Best Practices—Database Integrity

- Always perform a graceful shutdown before turning off FortiManager using the `execute shutdown` command
  - Ungraceful shutdown (power off) can cause damage to the internal database
- Always follow the proper upgrade path
- **Recommendation**:
  - Enable ADOM locking to avoid configuration conflicts when multiple administrators are performing actions on FortiManager
  - Before performing a firmware upgrade, make sure all administrators are logged off and perform database integrity checks and corrections
    - If you upgrade an inconsistent database, it might end up in a worse condition

If you cannot resolve a data integrity problem, you may factory reset FortiManager and restore its configuration from a good backup!

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

To ensure database integrity on FortiManager, you should follow these best practices:

- Always gracefully shut down FortiManager. Using an ungraceful shutdown can damage the internal databases.
- If multiple administrators are performing operations on FortiManager, enable ADOM locking to avoid configuration conflicts.
- Always follow the correct upgrade path. If you don't, it may cause inconsistencies in the database.
- Make sure all administrators are logged off, and perform database integrity checks before performing a firmware upgrade.

If you cannot resolve a data integrity issue, you can perform a factory reset on FortiManager, and then restore the configuration using a good backup configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Database Integrity

- **Recommendation**: Back up the FortiManager database, have all the administrators log off and have all the ADOMs unlocked before executing database integrity commands
  - Modifies FortiManager database if errors are found
- Run when there are no active operations being performed and all ADOMs are unlocked
- Configure a scheduled backup of FortiManager, which:
  - Creates a log in the event log and **Alert Message Console**
  - Automatically executes database integrity commands to check database integrity
    - Does not automatically make corrections
    - Must be run again to correct the problems

```
diagnose dvm check-integrity
diagnose cdb check adom-integrity
diagnose cdb check adom-revision
diagnose cdb check policy-packages
diagnose cdb check update-devinfo
```

Upon successful verification: "Scheduled database integrity verifications successful"

Upon unsuccessful verification: "Possible database integrity problem detected during scheduled verification. Please check manually"

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

If you are experiencing unusual behavior on FortiManager, check for issues with database integrity. Database integrity commands modify any database errors that are found. It is recommended that you perform a backup before executing database integrity commands. Also it is recommended to have all the administrators log out and all the ADOMs unlocked, if work space mode is enabled before running the integrity check commands. Having a backup is helpful when you don't want to keep changes that were made by the integrity commands and you need to restore the FortiManager configuration.

As a best practice, configure a scheduled backup of FortiManager. FortiManager automatically runs database integrity commands prior to a schedule backup, and creates logs. If there are any issues with database integrity, you must rerun the commands to fix the problem.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Database Integrity Commands

Command	Information
# diagnose dvm check-integrity	Verify and correct parts of the device manager databases, including: • Inconsistent device-to-group and group-to-ADOM memberships • Unregistered, registered, and deleted device states • Device lock statuses • Duplicate VDOM entries
# diagnose cdb upgrade check objcfg-integrity	Object config database integrity—Perform a check to see if upgrade and repair is necessary
# diagnose cdb upgrade check reference-integrity	Perform a check to see if upgrade and repair is necessary for reference table.
# diagnose cdb check update-devinfo	Update device info by directly changing the database
# diagnose cdb check adom-integrity	Internally upgrades existing ADOMs to the same ADOM version in order to clean up and correct the ADOM syntax
# diagnose cdb check policy-packages	Verifies and checks dynamic mappings, and removes invalid dynamic mappings

Not all integrity problems are detected or corrected!
If corrections are performed, run the database integrity commands again to ensure corrections have been made properly.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

This slide lists commands that you can use to verify and maintain database integrity. If you execute a database integrity command that makes a change or correction to the database, it is advised that you then run the command again to verify that any changes or corrections were made properly.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Example—Database Integrity

```
FMG-VM64 # diagnose dvm check-integrity
[1/11] Checking object memberships        ... correct
[2/11] Checking adom nodes                ... correct
[3/11] Checking device nodes              ... correct
[4/11] Checking device vdoms              ... correct
[5/11] Checking duplicate device vdoms    ... correct
[6/11] Checking device ADOM memberships   ... correct
[7/11] Checking device HA Secondary       ... correct
[8/11] Checking device clusters           ... correct
[9/11] Checking groups                    ... correct
[10/11] Checking group membership          ... correct
[11/11] Checking task database             ... correct
```

No issues found

Checking My_ADOM integrity and found no errors

```
FMG-VM64 # diagnose cdb check adom-integrity My_ADOM
        General updating - adom My_ADOM                    ... ..100%    No errors

FMG-VM64 #
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

This slide shows an example of a database integrity check. FortiManager finds no issues with the device manager databases. The second example shows how to check the database integrity on an individual ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What command can you use to sniffer the FGFM protocol communication between FortiManager and FortiGate devices?
   A. `diagnose sniffer packet any "port 8113" 3`
   ✓B. `diagnose sniffer packet any "port 541" 3`

2. Which statement about FortiManager best practices is true?
   ✓A. If FortiManager needs to be turned off, always perform a graceful shutdown using the **`execute shutdown`** command.
   B. If FortiManager needs to be turned off, always unplug the power supply cable.

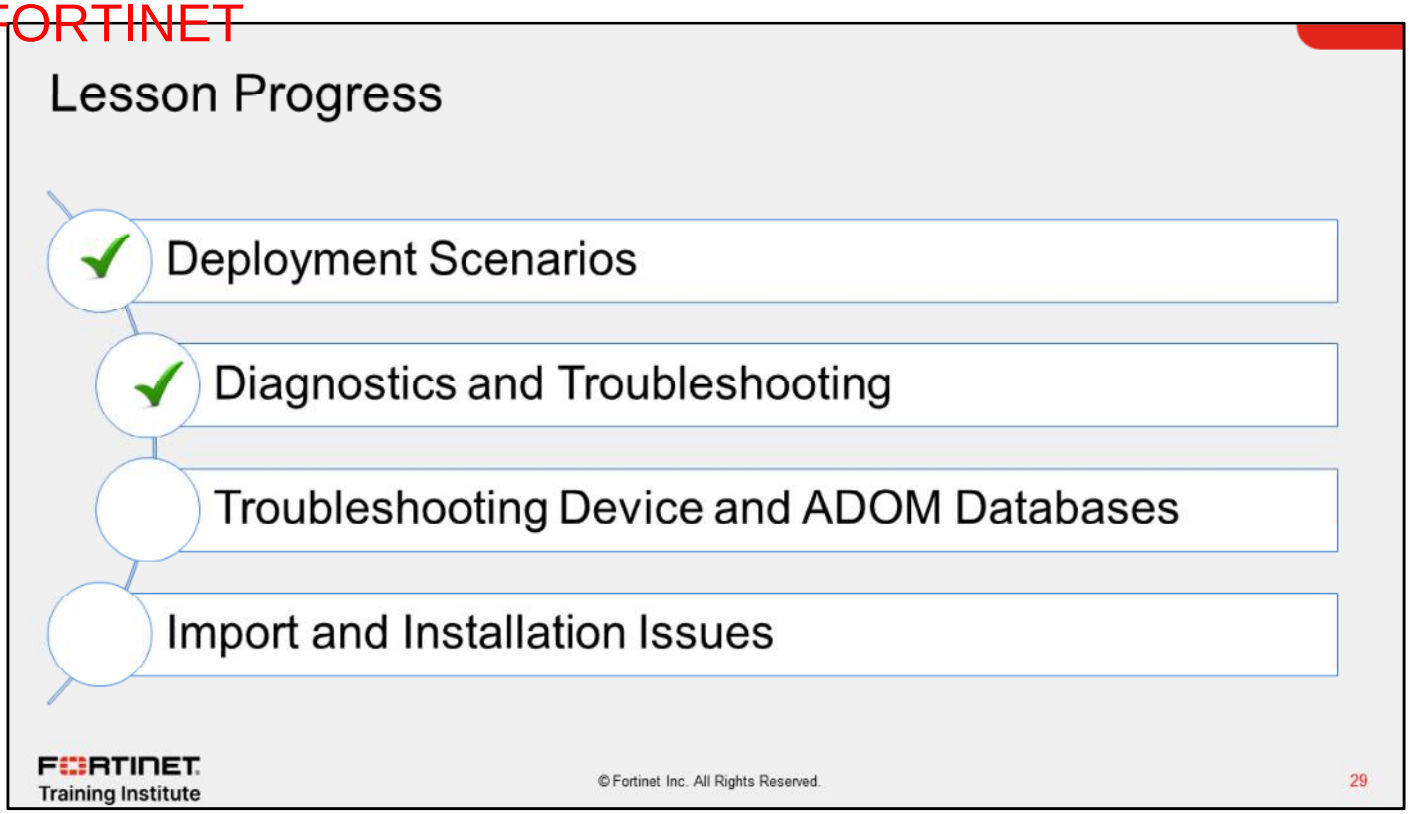
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

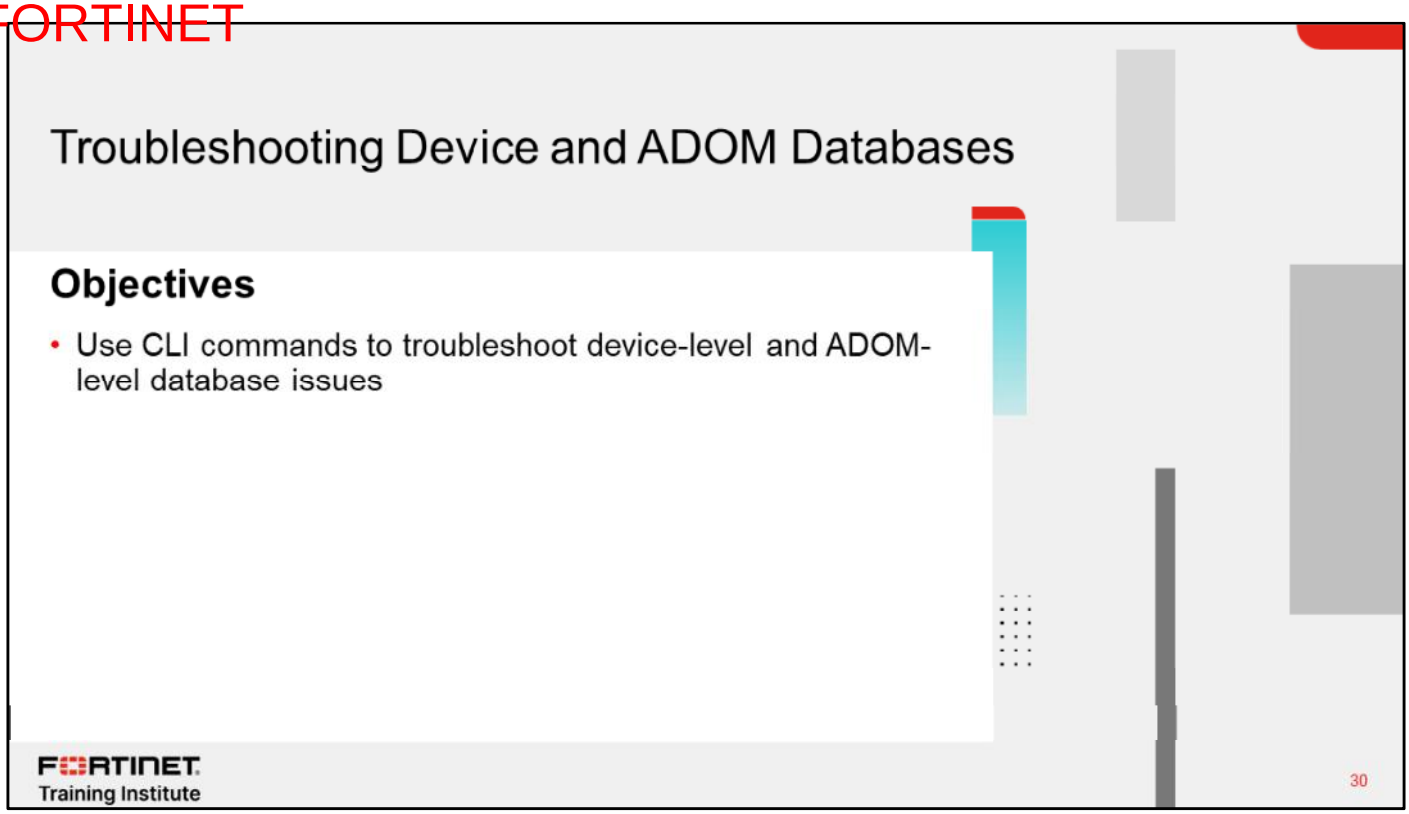


Good job! You now understand how to diagnose and troubleshoot various issues with FortiManager.

Now, you will learn about troubleshooting device and ADOM databases.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

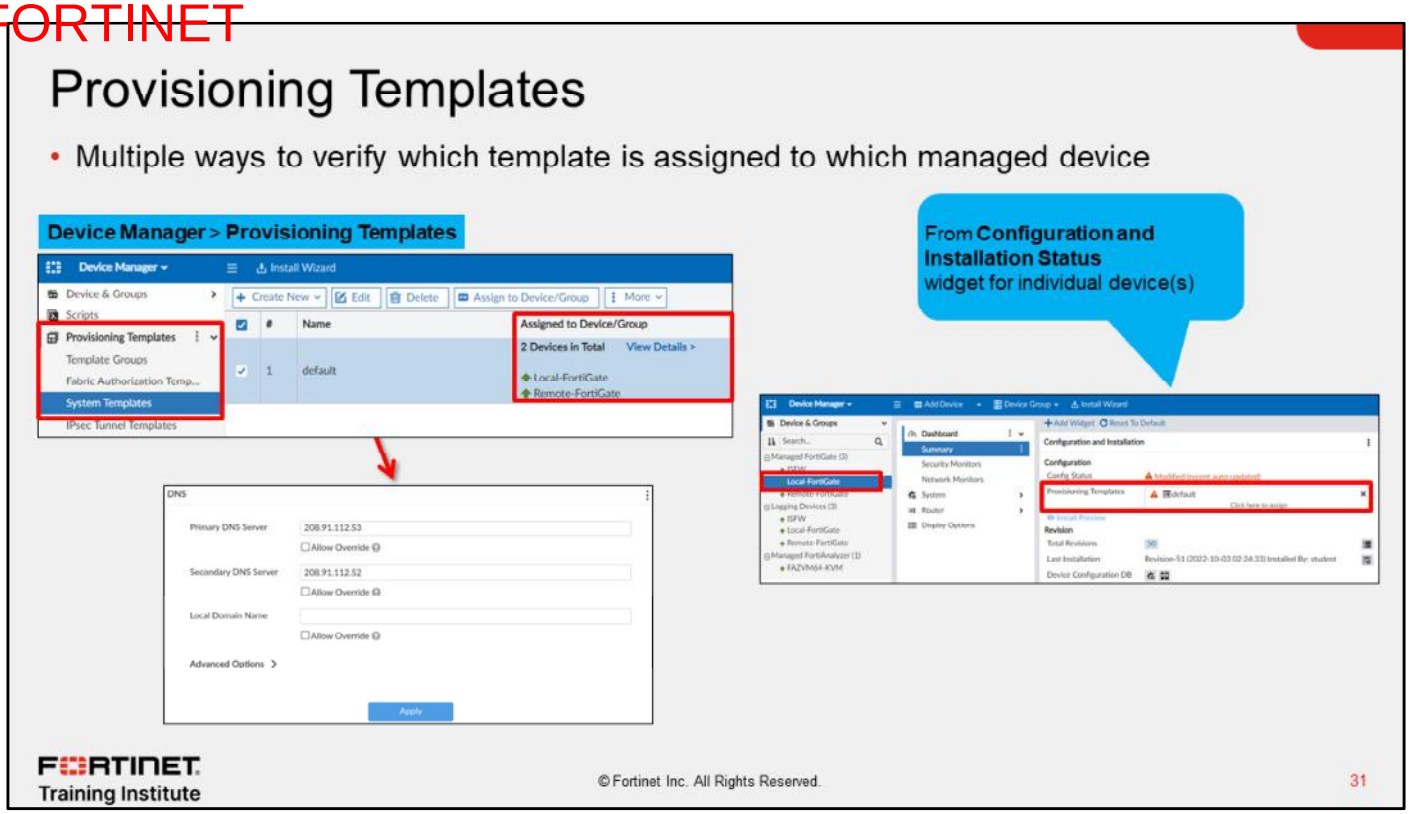


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding how to use CLI commands related to device-level and ADOM-level databases, you will learn how to troubleshoot device-level and ADOM-level issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



If you need to verify which templates are applied to which FortiGate device, you can check from the **Provisioning Templates** widget, or from the individual device **Configuration and Installation Status** widget.

In this example, the default system template is applied to Local-FortiGate and Remote-FortiGate for DNS settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Troubleshooting Provisioning Templates

- Shows CLI syntax that will be installed to the assigned managed device

```
execute fmpolicy print-adom-package <adom> <policy package/template name>
<package> <category> |all[<key>|all|list]
```

ADOM | System template type | Package name | Category name

```
FMG-VM64 # execute fmpolicy print-adom-package ADOM1 5 3547 533 dns
Dump object [dns] of category [device template widget] in adom [ADOM1] package [3547]:
---------------
config device template widget
edit "dns"
config action-list
edit 1
set action "conf-sys-dns"
set model "all"
set value "{\"server-hostname\":[],\"primary\":\"208.91.112.53\",\"secondary\":\"208.91.112.52\"}"
config var-list
edit "system dns/cache-notfound-responses"
```

Example viewing DNS widget configuration in default System Templates

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

32

You can use this command to view to the CLI configuration of templates. You can see which CLI commands will be pushed to FortiGate.

Tip: Use ? for help. In this example, the default system template is configured with primary and secondary DNS entries. Remember that the default system template is applied to Local-FortiGate and Remote-FortiGate, as shown on the previous slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Troubleshooting the Device Database

- Display the whole device configuration or individual object configuration
  - `execute fmpolicy print-device-database`: Displays device-level changes made from FortiManager
    - Does *not* display changes from applied system templates
  - `execute fmpolicy print-device-object`: Does *not* display any ADOM-level (firewall policy and related objects) changes made from FortiManager

Displays whole device configuration

```
execute fmpolicy print-device-database <adom_name> <devname>

execute fmpolicy print-device-object <adom> <devname> <vdom>
<category name>
```

Displays individual object configuration

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

33

You can use CLI commands to view the whole configuration of the managed device, or view individual object configuration.

The `execute fmpolicy print-device-database` command displays the device configuration, including device-level changes made from FortiManager. It does *not* display the changes caused by applying the system template. Also, ADOM-level configuration changes made from FortiManager, such as firewall policies and objects, are not displayed. These changes are applied (copied) to the device-level database at the installation.

If you perform an installation preview from the **Configuration and Installation Status** widget for a managed device, it displays the device-level configuration changes with the following exceptions:

- System templates
- ADOM-level configuration changes

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Troubleshooting the Device Database (Contd)

```
execute fmpolicy print-device-object <adom_name>
<device_name> <vdom_name> <category_name>
```

- Displays individual object configuration

```
FMG-VM64 # execute fmpolicy print-device-object root Local-FortiGate root 15
Dump all objects for category [system dns] in device [Local-FortiGate]
vdom[root]:
---------------
config system dns
set primary 208.91.112.53
set secondary 4.2.2.2
end
```

DNS entries based on device configuration; not based on applied default system template

Configuration of applied default system template

```
config system dns
set primary 208.91.112.53
set secondary 208.91.112.52
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

34

This slide shows an example of DNS settings for Local-FortiGate. Local-FortiGate is configured locally, using the DNS configuration shown here. The DNS entries used in this example are not the same as those used in the default system template. When installing the device-level configuration to Local-FortiGate, the installation skips the primary DNS entry and installs only the secondary DNS entry. This is because the primary DNS entry is the same, based on the applied default system template and Local-FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Troubleshooting ADOM Databases

- Displays
  - Entire ADOM database with all policy packages and objects
  - Firewall policies contained in a specific policy package in the ADOM
  - Individual objects in an ADOM

Displays entire ADOM database

Displays firewall policies in policy package

```
execute fmpolicy print-adom-database <adom> <output>

execute fmpolicy print-adom-package <adom> <policy package/template name>
<package name> <category name> <object name>

execute fmpolicy print-adom-object <adom> <category name>
```

Displays individual ADOM object

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

35

On the previous slides, you learned how to view configurations related to a specific managed device. You can also view the policies and objects at the ADOM level, using the commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Comparing the Device Database With the ADOM Database

- Display firewall policies for a managed FortiGate from:
  - ADOM database

```
execute fmpolicy print-adom-package <adom> <policy package/template name> <policy package ID> <category> <all/list>
```

```
execute fmpolicy print-adom-package root 1 3083 181 all
Dump all objects for category [firewall policy] in adom [root] package [3083]:
---------------
edit "1"
set name "Ping_Access"
set uuid 730e5790-ad0b-51e6-897c-1b314610267f
...
next
edit "2"
set name "Full_Access"
set uuid ef14d2dc-c30f-51e6-d5f7-9b14d15c7c10
...
end
```

A new policy was configured in the Local-FortiGate policy package

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

36

This slide shows an example of viewing a policy or policies in a particular policy package. In this example, the Local-FortiGate policy package initially has only one policy named `Ping_Access`. The FortiManager administrator has configured a new policy named `Full_Access` in the Local-FortiGate policy package. When viewing the policy from the ADOM level, it shows both policies—the existing policy and new policy, which needs to be installed.

If you view the policies for the Local-FortiGate at the device level, is the newly configured firewall policy shown? At the device level, ADOM-level (firewall policy and related objects) configuration changes that have been made from FortiManager are not displayed until *after* the **Policy & Objects** installation is performed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Comparing the Device Database With the ADOM Database (Contd)

- Display firewall policies for a managed FortiGate from:
  - Device database

```
execute fmpolicy print-device-object <adom> <devname> <vdom> <category name>
```

```
execute fmpolicy print-device-object root Local-FortiGate root 'firewall policy' all
Dump all objects for category [firewall policy] in device [Local-FortiGate]
vdom[root]:
---------------
edit "1"
set name "Ping_Access"
set uuid 730e5790-ad0b-51e6-097c-1b314610267f
...
...
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

37

This slide shows an example of a policy or policies being viewed for a particular device at the device level. In this example, the Local-FortiGate policies are viewed at the device level. ADOM-level configuration changes are not displayed until the **Policies & Object** installation is performed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which command is useful when troubleshooting ADOM-level issues?
   A. `execute fmpolicy print-device-object`
   ✓B. `execute fmpolicy print-adom-database`
2. Which FortiGate configuration setting is part of a device-level database on FortiManager?
   ✓A. Routing
   B. Firewall Policies

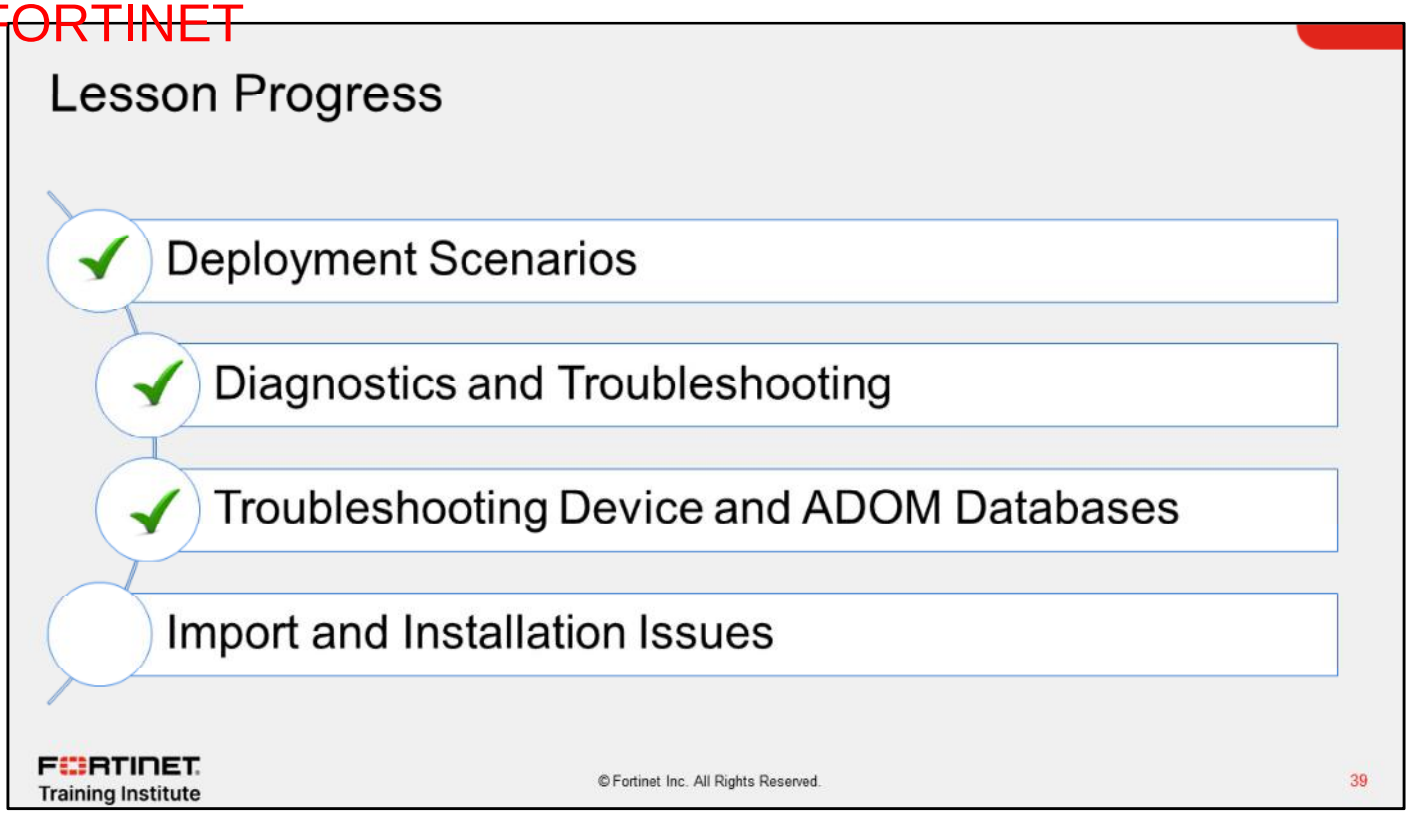
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

38

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

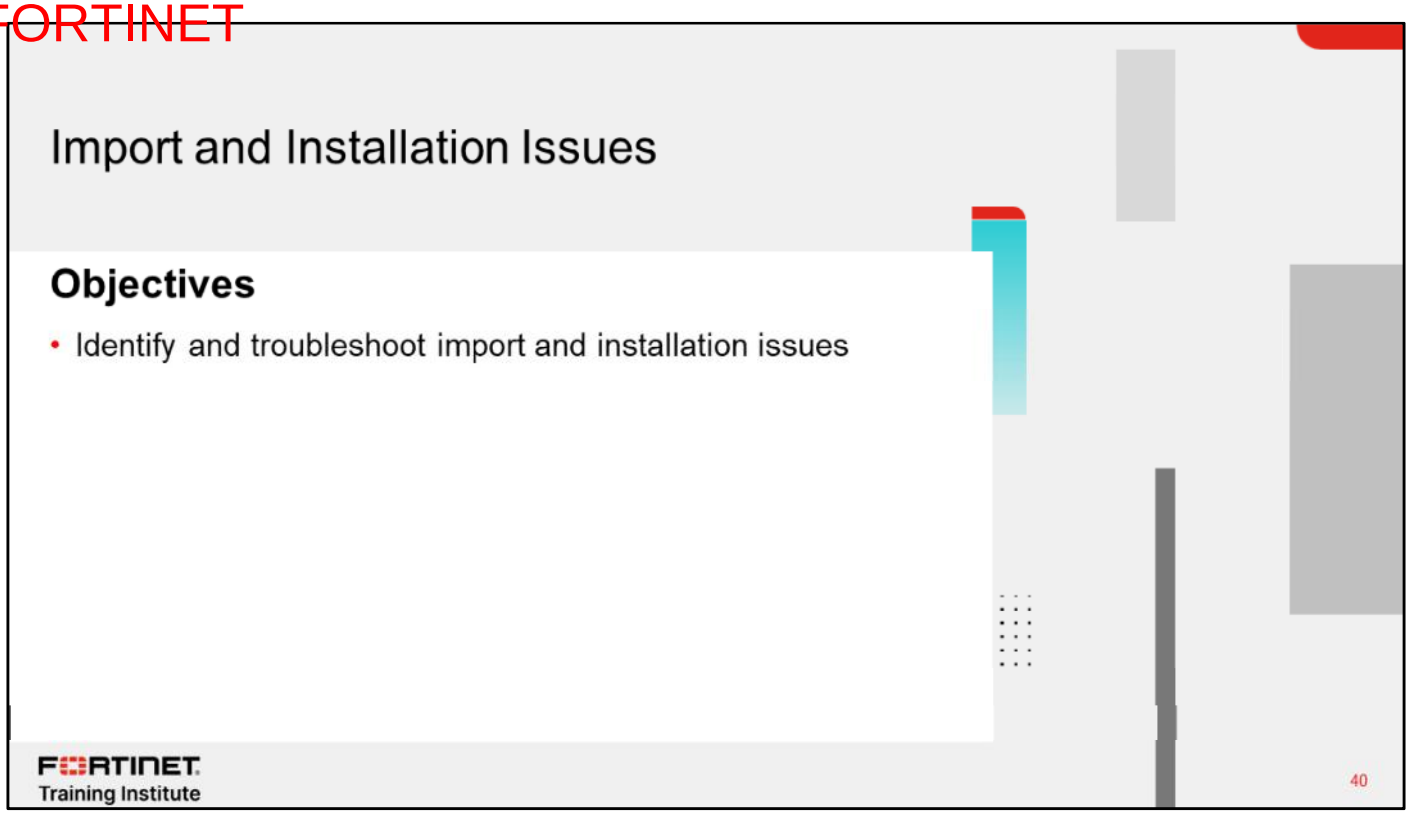


Good job! You now understand how to diagnose and troubleshoot device and ADOM database issues on FortiManager.

Now, you will learn how to troubleshoot import and installation issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

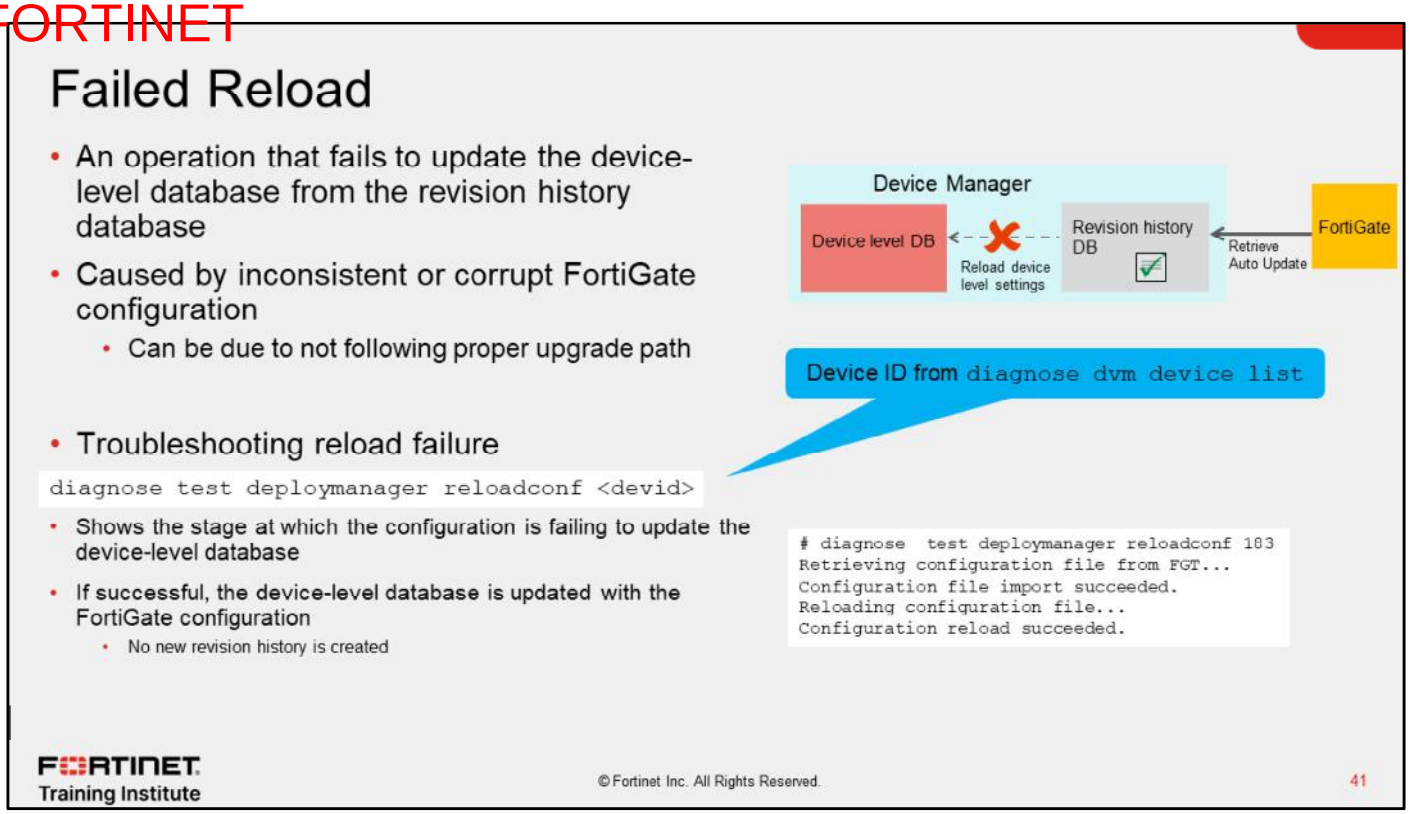


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding import and installation issues, you will be able to troubleshoot them if they occur in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this example, the configuration is correctly retrieved and saved in the revision history; however, the problem occurs when updating the device database. Usually, issues like this are caused by inconsistent or corrupt FortiGate configurations.

You can troubleshoot reload failures to see at which stage the configuration is failing to load into the device-level database.

When you execute the reload failure command, FortiManager connects to FortiGate and downloads its configuration file. Then, FortiManager performs a reload operation on the device database.

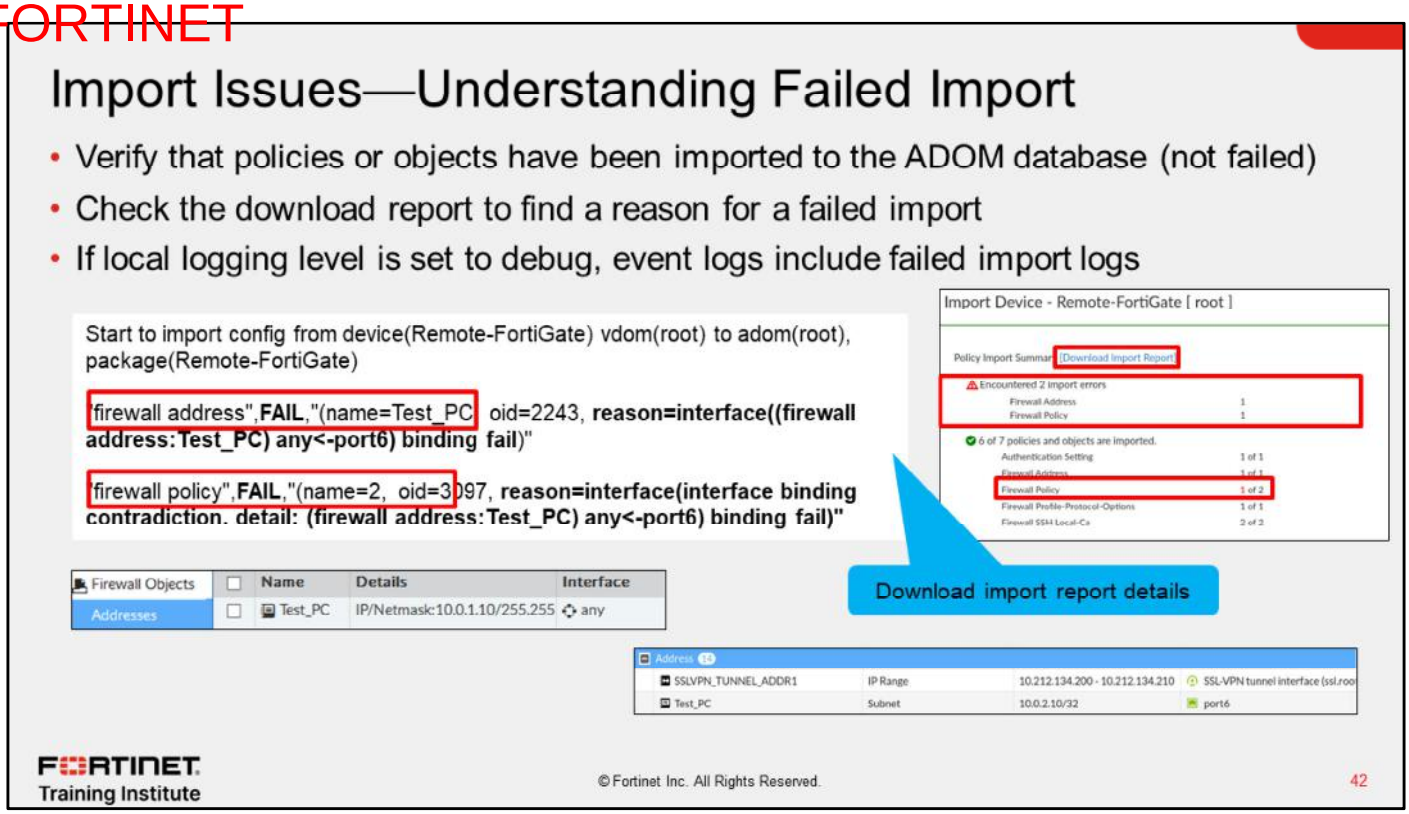
There are two possible outcomes:

- If there are *no* errors in the FortiGate configuration, the reload is successful, and the device-level database is updated with the FortiGate configuration. However, note that a new revision history entry is not created.
- If there *are* errors in the FortiGate configuration, the output of the reload command indicates the point in the configuration at which the device-level database failed to update.

You can also check the event logs to see if they contain details about the cause of the failure.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When you add a FortiGate device using the **Add Device** wizard, or import policies using the **Import Policy** wizard, always make sure that the policies and objects have successfully imported.

In this example, the FortiManager ADOM database has a firewall address object named **Test_PC** which is associated with the interface **any**.

The second FortiGate also has a firewall address object named **Test_PC** and it's associated with the interface **port6**. This firewall address object is referenced in the firewall policy on the second FortiGate.

When a policy package was added or imported to the second FortiGate, it failed to import the firewall address object **Test_PC**, as well as associated firewall policies. The FortiManager **Download Import Report** provides the reason for failed object or policy imports.

FortiManager can create a dynamic mapping for an address object, if the address object name is the same, but contains a different value locally. However, there is one restriction—the associated interface *cannot* be different. This is because, at the ADOM level, this address object might be used by other policy packages, which might not have the same interfaces.

What will the impact of the partial policy package import be?

The failed import logs on the event log provide more details and pin points the objects that cause import failure issue.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Failed Import—Impact and Resolution

- Impact
  - On subsequent policy package installations from FortiManager, the failed objects and policies are deleted
- Two ways to fix the issue
  - Remove interface binding
    - Run a script from FortiManager using the option **Remote FortiGate Directly (Via CLI)**
    - Remove the interface binding by locally logging in to FortiGate
  - Rename address object
    - Run a script from FortiManager using the option **Remote FortiGate Directly (Via CLI)**
    - Rename the address object by locally logging in to FortiGate
- *Must* reimport the policy package after fixing the address object

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

43

After you make configuration changes from FortiManager to the partial imported policy package, and attempt to install it using the installation wizard for **Policy & Objects**, FortiManager deletes the failed objects and policies. This is because the policy package is not aware of missing or failed policies and objects.

There are two ways to fix the problem:

- You can remove the interface binding to make it the same as the FortiManager ADOM object.
- If there is a need to keep the interface binding for FortiGate that is having issues with a partial policy import, you can rename the address object to a unique name that is not part of the ADOM database.

To use either of these methods, you can run a script from FortiManager using the **Remote FortiGate Directly (Via CLI)** option, or you can locally log in to FortiGate to make the configuration change.

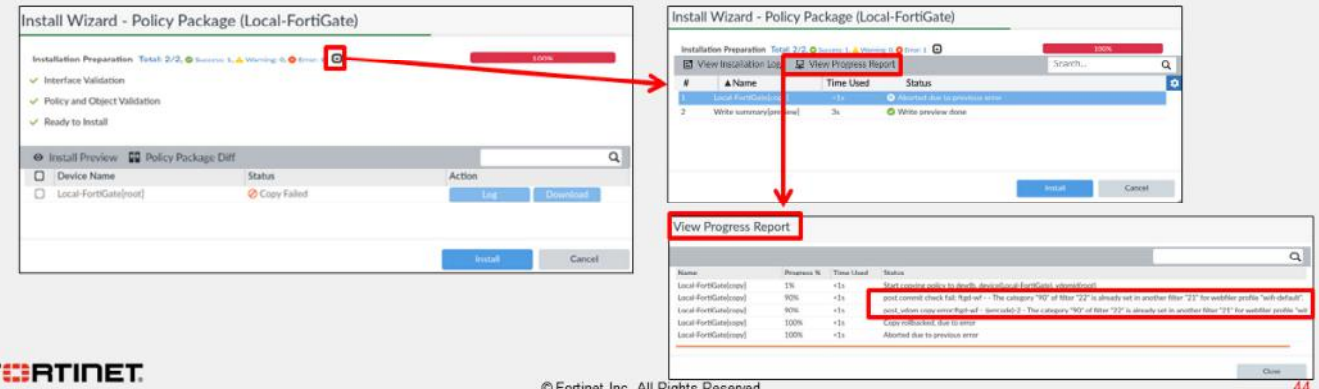
Note that FortiManger allows you to choose the object either from FortiManage or FortiGate if both has the same object name with out **Per-device Mapping**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Copy Failed Issues

- Internal operation part of policy package installation
  - First thing that is performed before the installation
- An operation that fails between the ADOM database and device database
- Usually due to missing or incorrect object dependency when copied from ADOM database to device database
- When performing the installation, **View Progress Report** shows the failing message



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

44

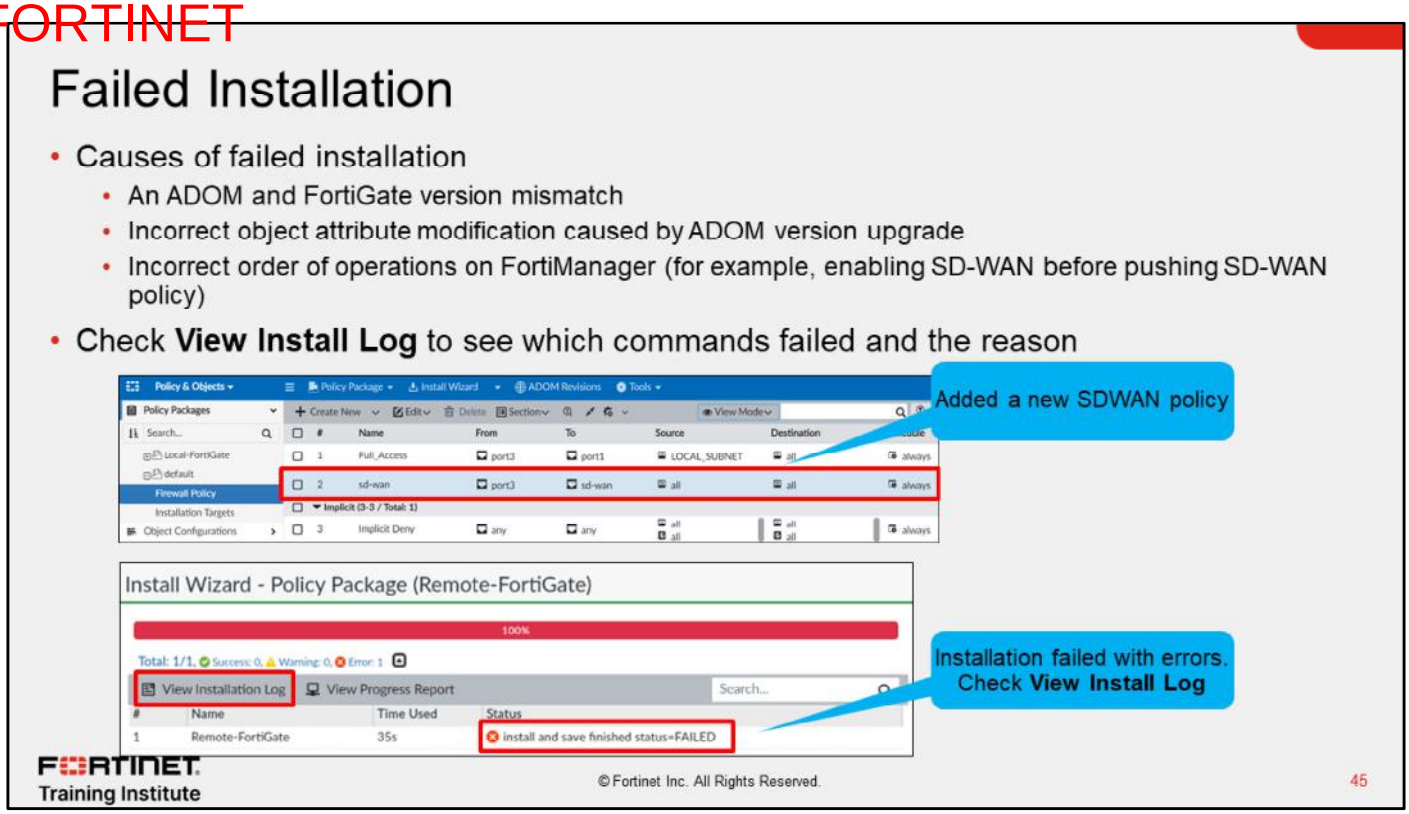
When you perform a policy package installation, the copy operation is the first operation that FortiManager performs, before you perform the actual installation. It is the operation in which FortiManager tries to copy the ADOM-level object or policy to the device database. It is the opposite of the import operation.
Copy failure issues are usually caused by having incorrect or missing object dependencies when copying from the ADOM database to the device database. The incorrect or missing object dependencies are caused by corruption or inconsistencies in the FortiManager database.

The **View Progress Report** section helps you to identify the failing issue.

When a copy failure happens, the device database is restored to its original state, prior to the copy attempt.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Always check **View Install Log** to see which CLI commands were not executed or accepted by FortiGate. It is usually caused by:

- An ADOM and FortiGate mismatch version, which created an object using incorrect CLI syntax
- An ADOM upgrade, which modifies existing objects incorrectly, because of database corruption
- Not following the correct order of operation on FortiManager, for example, pushing a SD-WAN policy without enabling SD-WAN on FortiManager

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Understanding the Failed Installation Log

- CLI commands were sent to FortiGate, however FortiGate rejected specific commands because of missing `virtual-wan-link` interface

```
Starting log (Run on device)Start installing
Local-FortiGate $ config firewall policy
Local-FortiGate (policy) $ edit 4
Local-FortiGate (4) $ set name "sd-wan"
Local-FortiGate (4) $ set uuid 9f4cf75a-1de9-51eb-dcdc-48868fd5ca82
Local-FortiGate (4) $ set srcintf "port3"
Local-FortiGate (4) $ set dstintf "virtual-wan-link"
node_check_object fail! for name virtual-wan-link

value parse error before 'virtual-wan-link'
Command fail. Return code -651
Local-FortiGate (4) $ set srcaddr "all"
Local-FortiGate (4) $ set dstaddr "all"
Local-FortiGate (4) $ set action accept
Local-FortiGate (4) $ set schedule "always"
Local-FortiGate (4) $ set service "ALL"
Local-FortiGate (4) $ set nat enable
Local-FortiGate (4) $ next
Attribute 'dstintf' MUST be set.
Command fail. Return code 1
Local-FortiGate (policy) $ end
```

New firewall policy named SD-WAN failed to add

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

46

This is the installation log for the failed installation. In the example shown on the slide, a new firewall policy named `SD-WAN` was not added (failed) because of unavailable `virtual-wan-link` interface on FortiGate. In this scenario, the administrator did not follow the correct steps to enable the SD-WAN interface before pushing the SD-WAN policy, and FortiGate rejected the addition of the SD-WAN firewall policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

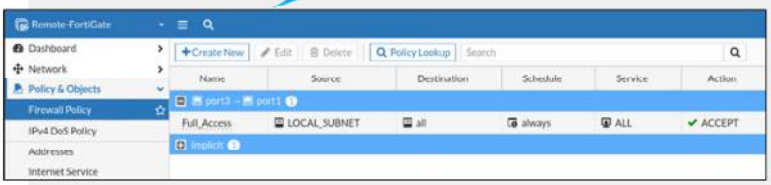
Understanding the Failed Installation Log (Contd)

- Verification report shows the differences between the FortiGate configuration collected by FortiManager, and the local database
  - remote original: The value configured on FortiGate after an installation attempt
  - to be installed: The value that was expected to be installed based on changes from FortiManager

```
--> generating verification report
( firewall policy )
add entry 3
(vdom root: firewall policy 3:name)
            remote original:
            to be installed:   "SD-WAN"
.
.
(vdom root: firewall policy 3:nat)
            remote original:
            to be installed:   enable
<--- done generating verification report

install failed
```

No SD-WAN policy got created on FortiGate



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

47

The verification report shows the differences between the configuration that was *expected* to be installed and what *was* installed on the FortiGate device.

Because the virtual-wan-link is not available, a firewall policy was not created on the FortiGate device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Failed Installation Resolution

- Verify ADOM and FortiGate version
- If the FortiGate version is not supported by the ADOM version, or FortiManager doesn't support some FortiGate CLI features, then:
  1. Move the FortiGate device to a supported ADOM or use a script to resolve the issue
  2. Perform the installation again
- If the ADOM version is correct or the ADOM upgrade was performed, then:
  1. Retrieve the FortiGate configuration and the import policy package
  2. Make and install a small device-level change to confirm or rule out a device-level database issue:
     - If the installation is unsuccessful, check the device-level settings
     - If the installation is successful, check and, if required, recreate the object or policy
  3. Perform the installation again
- As a last resort to solve the installation failure issues, take these steps:
  1. Create a new ADOM with matching firmware on FortiGate
  2. Move FortiGate to the new ADOM
  3. Retrieve the configuration and the import policy package
  4. Recreate the object or policy and install again

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

48

There are multiple ways to fix installation failure issues.
First, verify that the FortiGate version is the same as, or supported by, the ADOM version.
If the FortiGate version is not supported by the ADOM version, or if FortiManager doesn't support some FortiGate CLI features, then:
1. Move the FortiGate device to the supported ADOM, or use the script to resolve the issue.
2. Perform the installation again.

If the ADOM version is correct or the ADOM upgrade was performed, then:
1. Retrieve the FortiGate configuration so that FortiManager updates the device database with the correct syntax.
2. Make a small device-level change and install it to ensure that there is not a device-database issue.
   - If the installation is unsuccessful, check and fix the device-level settings.
   - If the installation is successful, check and, if needed, recreate the object or policy.
3. Perform the installation again.

Make sure to follow the correct order of operations on FortiManager. For example, enable SD-WAN before creating or pushing the SD-WAN firewall policy. As a last resort, to isolate and fix the installation failure issues, you can:
1. Create a new ADOM with matching firmware on FortiGate.
2. Move FortiGate to the new ADOM.
3. Retrieve the configuration and import policy packages.
4. Recreate the object or policy from the FortiManager GUI (if supported), or using a script, and perform the installation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What does a status of **Copy Failed** indicate?
   A. An operation that failed to copy the device database from the revision history
   ✓B. An operation that failed to copy the ADOM-level policy or object to a device database

2. An administrator configured a new firewall policy on FortiManager and has not yet pushed the changes to the managed FortiGate. In which database will the configuration be saved?
   ✓A. ADOM-level database
   B. Device-level database

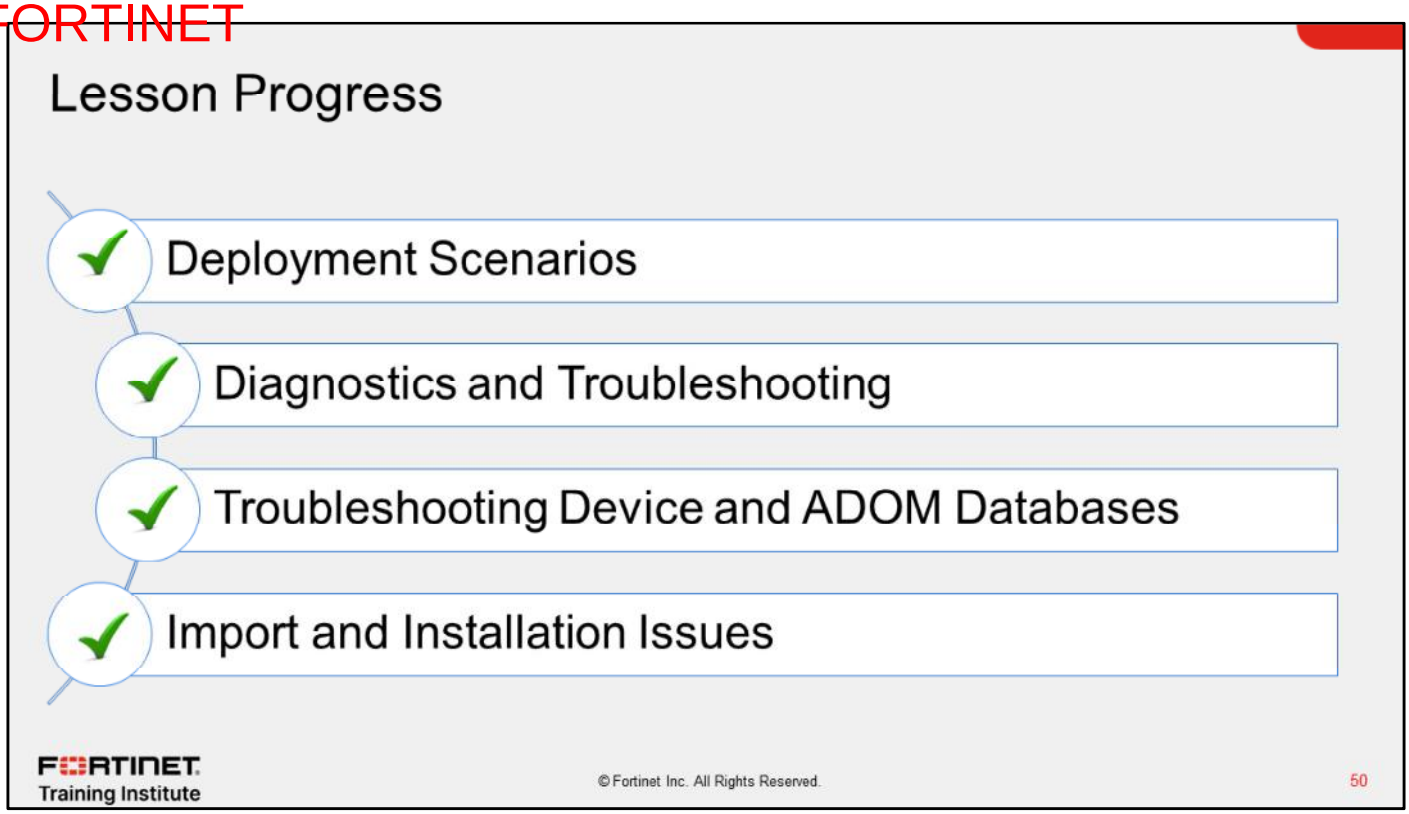
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

49

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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

Review

- ✓ Describe various deployment scenarios
- ✓ Understand FMFM keepalive messages
- ✓ Replace a standalone managed device
- ✓ Use CLI commands to troubleshoot general connectivity and resource issues
- ✓ Verify FortiManager database integrity
- ✓ Diagnose and troubleshoot device and ADOM database issues
- ✓ Troubleshoot issues related to import and installation

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

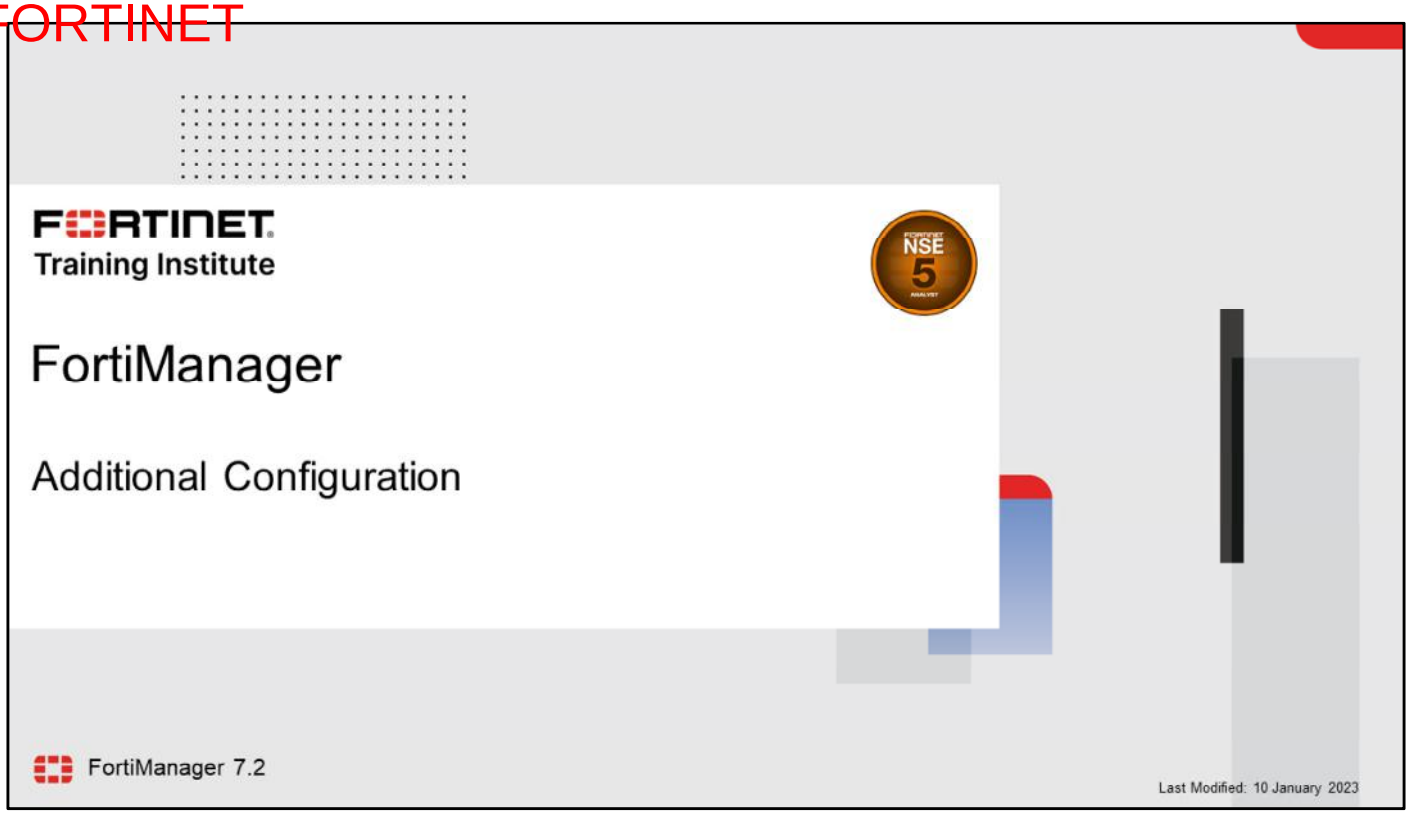
51

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

By mastering the objectives covered in this lesson, you learned how to diagnose and troubleshoot issues related to FortiManager and managed devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

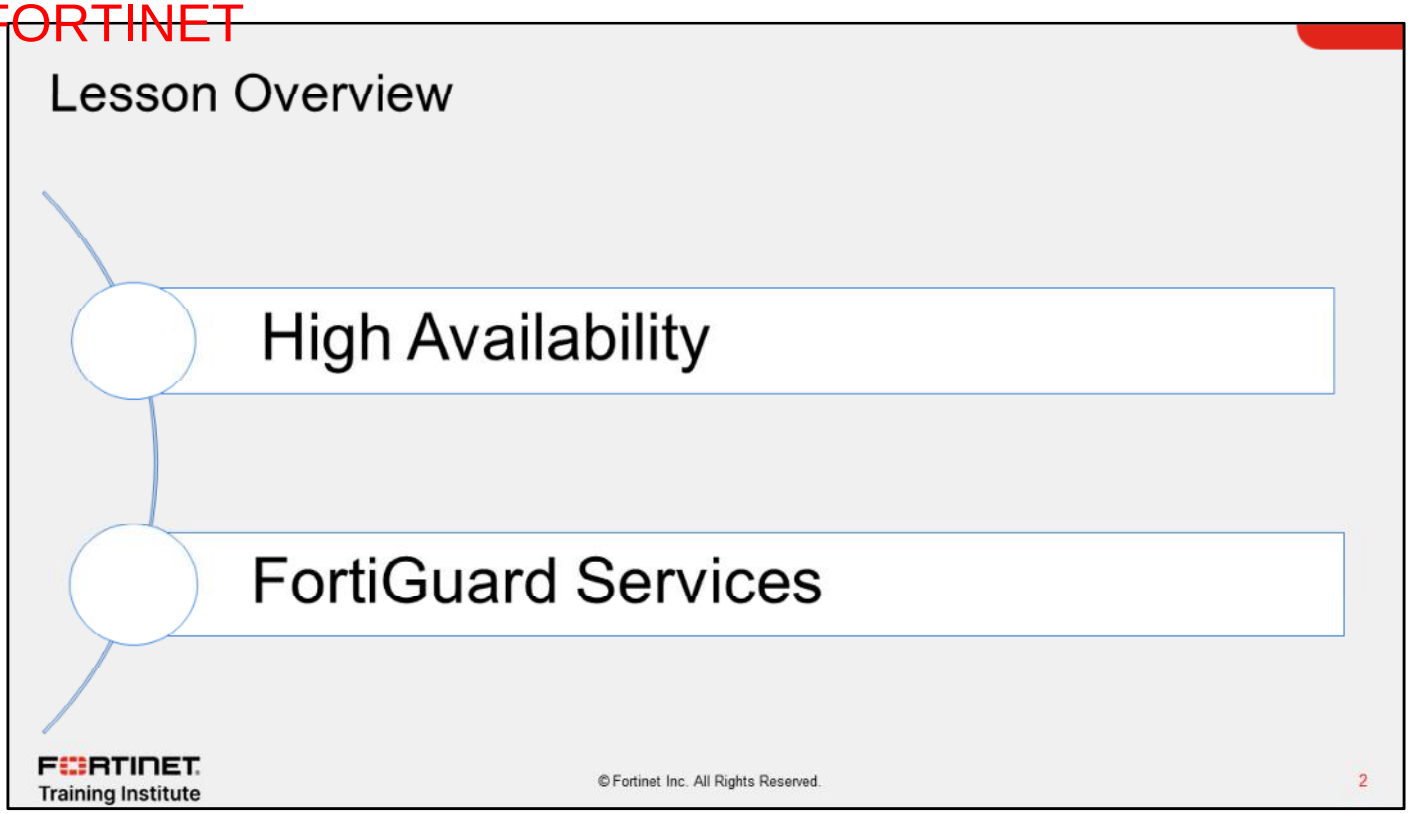
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn how to set up a FortiManager high availability (HA) cluster, and how to use FortiManager as a local FortiGuard server for your devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

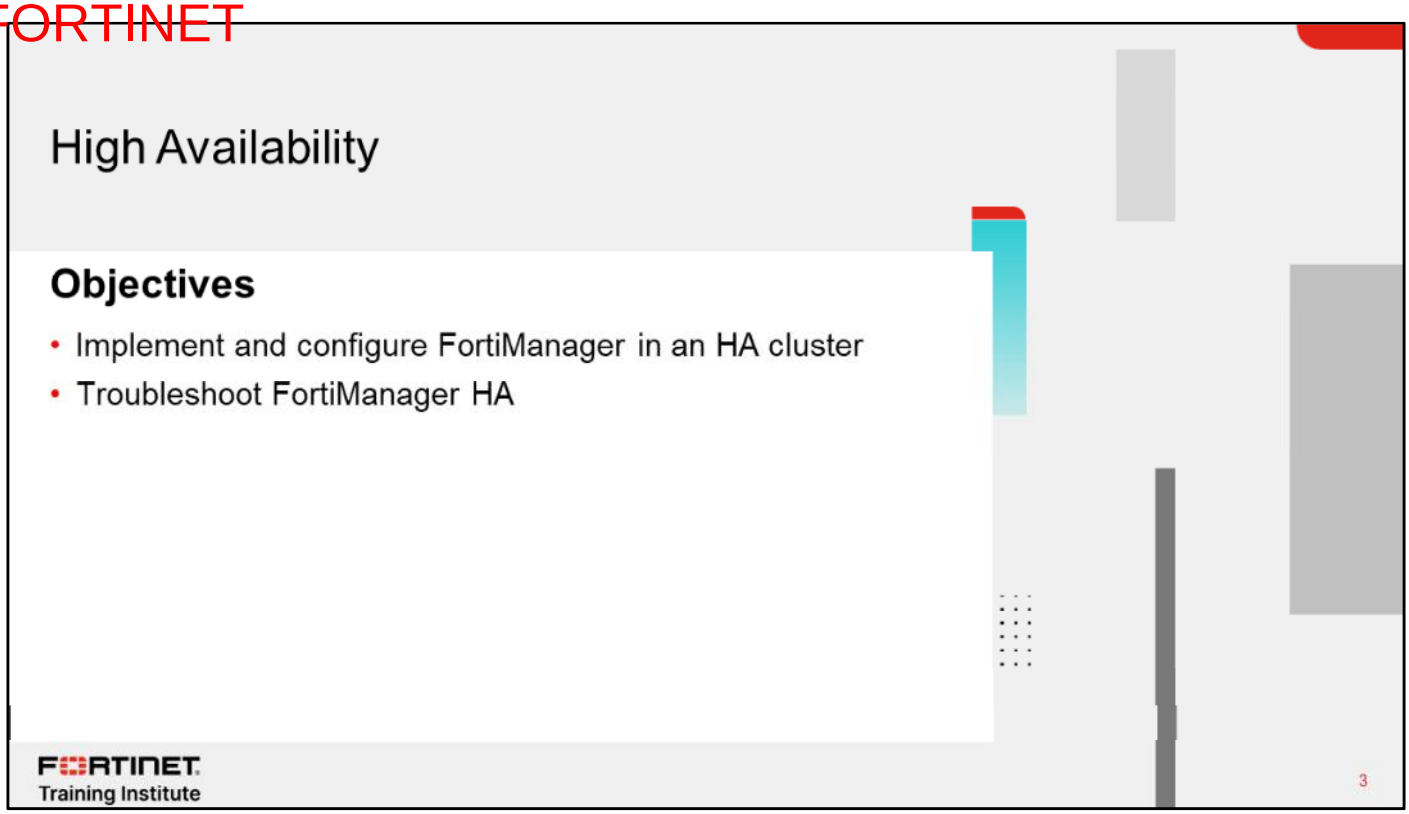
DO NOT REPRINT
© FORTINET
Brave-dumps.com



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 implementing and configuring FortiManager in an HA cluster, you will be able to use this FortiManager solution to enhance fault tolerance and reliability in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

High Availability (HA)

- All FortiManager devices in cluster must be same model and firmware
- Designed for one primary device and multiple secondary devices
  - Up to four secondary devices (five devices in total)
- Supports geographical redundancy
  - HA sync is TLSv1.0 over TCP port 5199
- Each HA member operates independently
  - Unique IP for each FortiManager
- Upgrading the primary FortiManager also upgrades all secondary devices at the same time
  - Upgrade process is similar to FortiManager standalone upgrade
  - FortiManager operations are temporarily interrupted during the upgrade
  - Reboots devices

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

4

A FortiManager HA cluster consists of up to five FortiManager devices of the same FortiManager model and firmware. One of the devices in the cluster operates as the primary device and the other devices—up to four—operate as secondary devices. The HA heartbeat packets use TCP port 5199. FortiManager HA provides geographic redundancy and each FortiManager has its own IP address.

When performing a firmware upgrade on the cluster, always schedule a maintenance window because upgrading the firmware on the primary FortiManager also upgrades the firmware on all the secondary devices, and reboots all the devices in the cluster. During the firmware upgrade procedure, you connect to the primary device GUI or CLI to upgrade the firmware.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

HA Synchronization

- Make all changes to the FortiManager database on the primary device, then synchronize with one or more secondary devices
  - Purpose
    - To replicate the primary device database
    - To promote secondary device(s) in case of primary device failure
- What is synchronized?
  - All device configurations (including global databases)
  - All configuration revisions
- What is not synchronized?
  - Configuration settings for:
    - Interface, routes, HA, SNMP, log, FortiAnalyzer feature configuration
  - FortiGuard
    - Antivirus/IPS packages, web filter, antispam databases
  - Local logs and Alert Message Console logs (data)
  - FortiGate logs sent to FortiManager

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

5

All changes to the FortiManager database are saved on the primary FortiManager, and then these changes are synchronized with the secondary FortiManager devices. The configuration and device and policy databases of the primary device are also synchronized with the secondary devices.

There are a few configuration settings, FortiGuard databases, and logs that are not synchronized between the primary and secondary devices. The FortiGuard databases and packages are downloaded separately, and each device can provide FortiGuard services to managed devices.

The cluster functions as an active-passive cluster; however, you can configure the cluster members to act as independent active local FortiGuard server(s).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

HA Failure Behavior

- If the primary FortiManager fails, there are two failover modes:
- Manual
  - Must manually reconfigure one of the secondary devices to become the primary device
  - Must reconfigure all other secondary devices to point to the new primary device
  - Don't need to reboot devices when promoting from secondary to primary
- If the secondary FortiManager fails, you can:
  - Reconfigure the primary device to remove the peer IP of the failed secondary device
  - Leave the configuration so that when the secondary device comes online, it can resynchronize with the primary
- VRRP (Automatic)
  - Must configure VIP, VRRP interface, priority, and monitored IP, but unicast is optional
  - When the monitored interface for the primary is down, HA failover will occur automatically
  - The secondary FortiManager with the highest priority automatically becomes the primary

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

There are two HA failover modes:
1. Manual
2. VRRP (Automatic)

In manual mode, FortiManager HA does not support IP takeover where an HA state transition is transparent to administrators. If a failure of the primary occurs, the administrator must take corrective action to resolve the problem. These correction may include invoking a state transition. If the primary device fails, the administrator must do the following in order to return the FortiManager HA to a working state:

1. Manually reconfigure one of the secondary devices to become the primary device.
2. Reconfigure all other secondary devices to point to the new primary device.

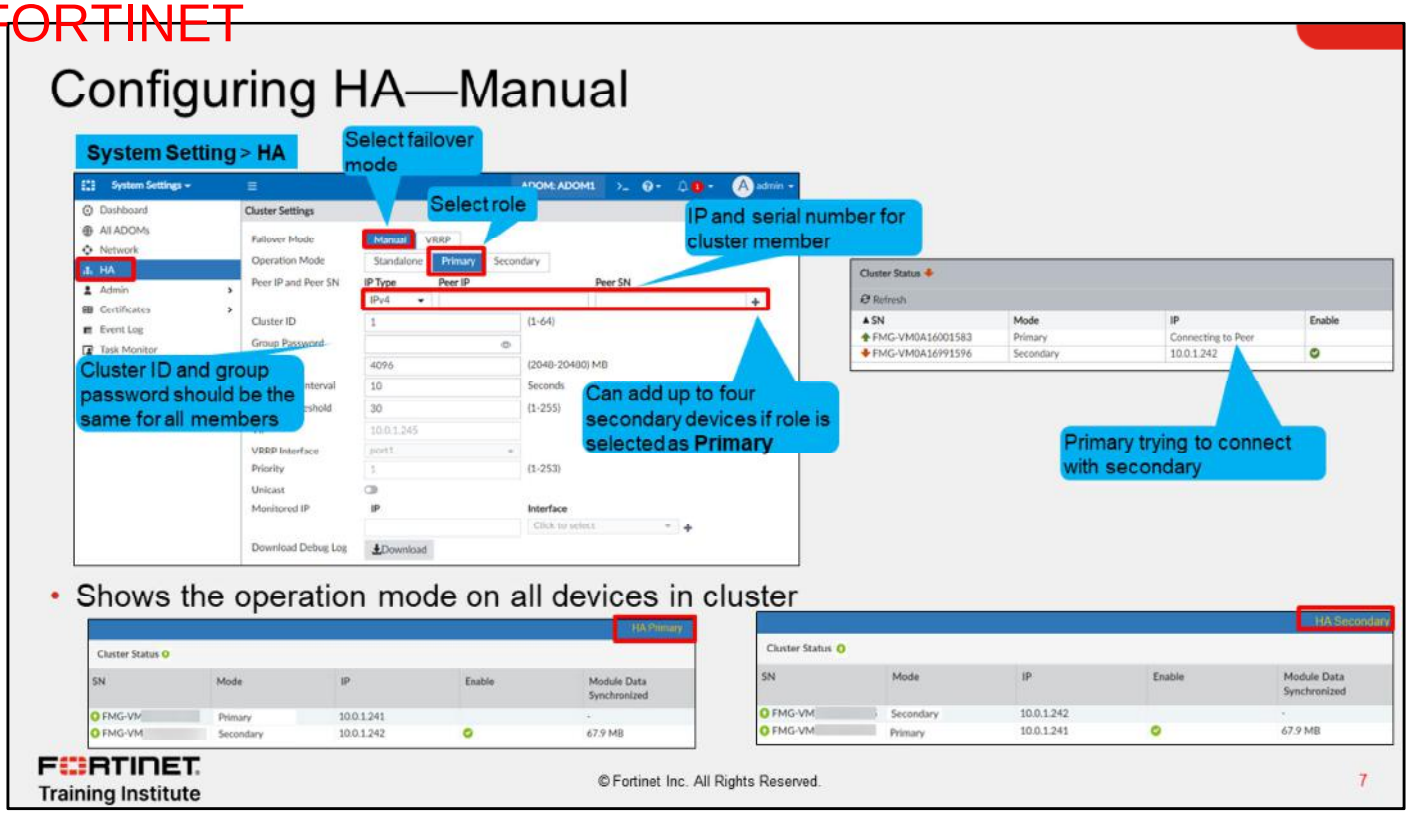
You don't need to reboot devices that you promote from secondary to primary.

If the secondary FortiManager fails, the administrator can reconfigure the primary device to remove the secondary configuration. Alternatively, the administrator can keep the secondary configuration in the HA settings and, after the secondary device comes online, it resynchronizes with the primary device.

You can select **VRRP** to configure automatic failover. When the monitored interface for the primary FortiManager is unreachable or down, HA automatic failover occurs, and the secondary FortiManager automatically becomes the primary. You must also configure virtual IP (VIP), VRRP interface, priority, and monitored IP. Unicast is optional.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After you select **Manual** in the **Failover Mode** field, you can select **Primary** as the role for one cluster member, and then add up to four secondary devices to the cluster.

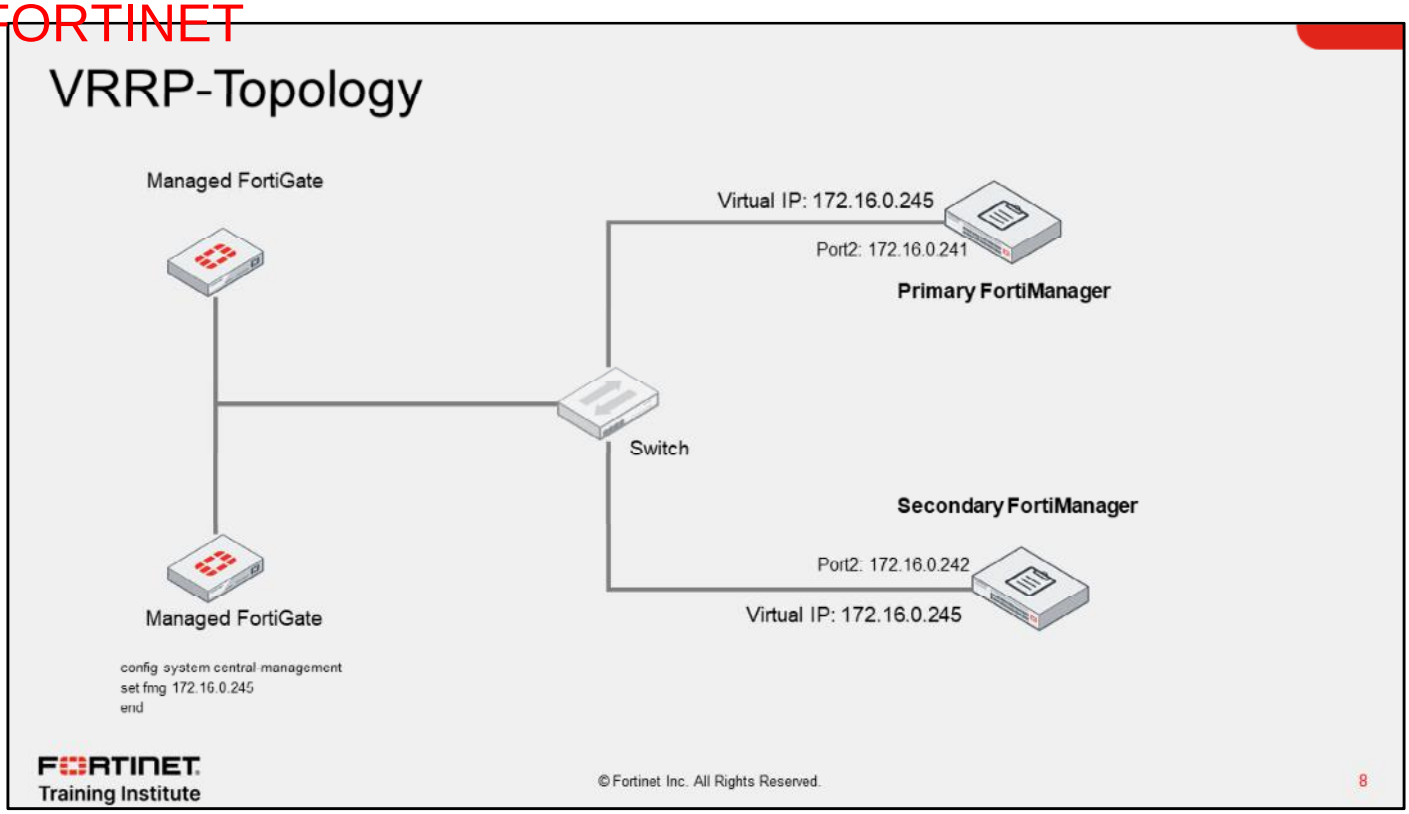
There are a few other settings that are worth mentioning that you can configure only on the primary FortiManager, including:

- **Heart Beat Interval**: The time in seconds that a cluster member waits between sending heartbeat packets and expecting to receive a heartbeat packet from the other cluster member.
- **Failover Threshold**: The maximum number of heartbeat intervals that can occur without response before FortiManager assumes that the other cluster members have failed.

After you configure the HA cluster, it shows the roles of cluster members.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

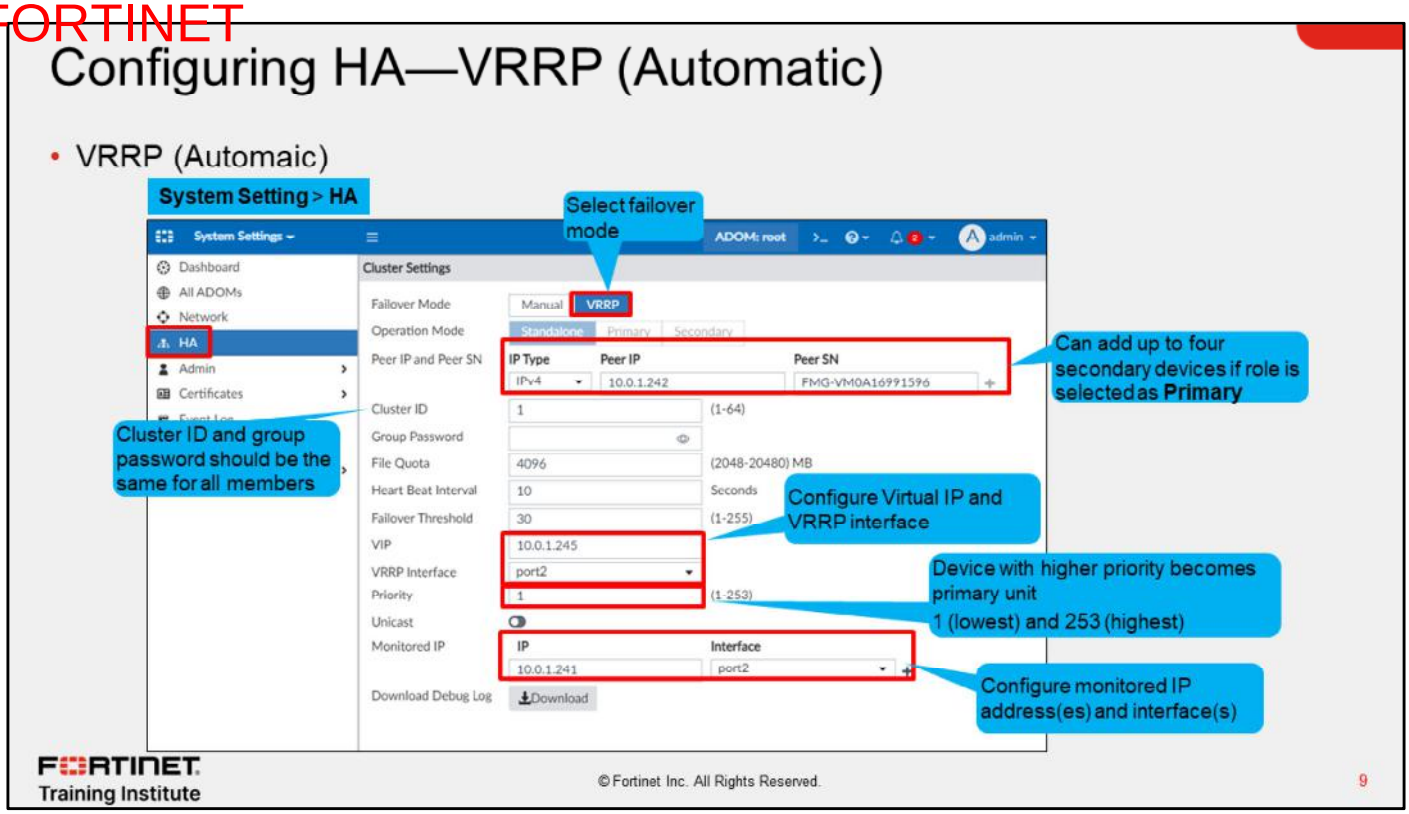


A Virtual Router Redundancy Protocol (VRRP) configuration can be used as a high availability solution to ensure connectivity. When the monitored interface for the primary FortiManager is down, HA automatic failover will occur, and the secondary FortiManager will automatically become the new primary.
The *Priority* setting determines which device will be primary and secondary in an HA configuration.

This slide shows the basic VRRP topology. Both the FortiGate devices connect to Virtual IP of the FortiManager instead of actual port 2 IP address. When primary device fails, MAC address updates in the arp table on devices for Virtual IP address 172.16.0.245 to the new primary port 2 MAC address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

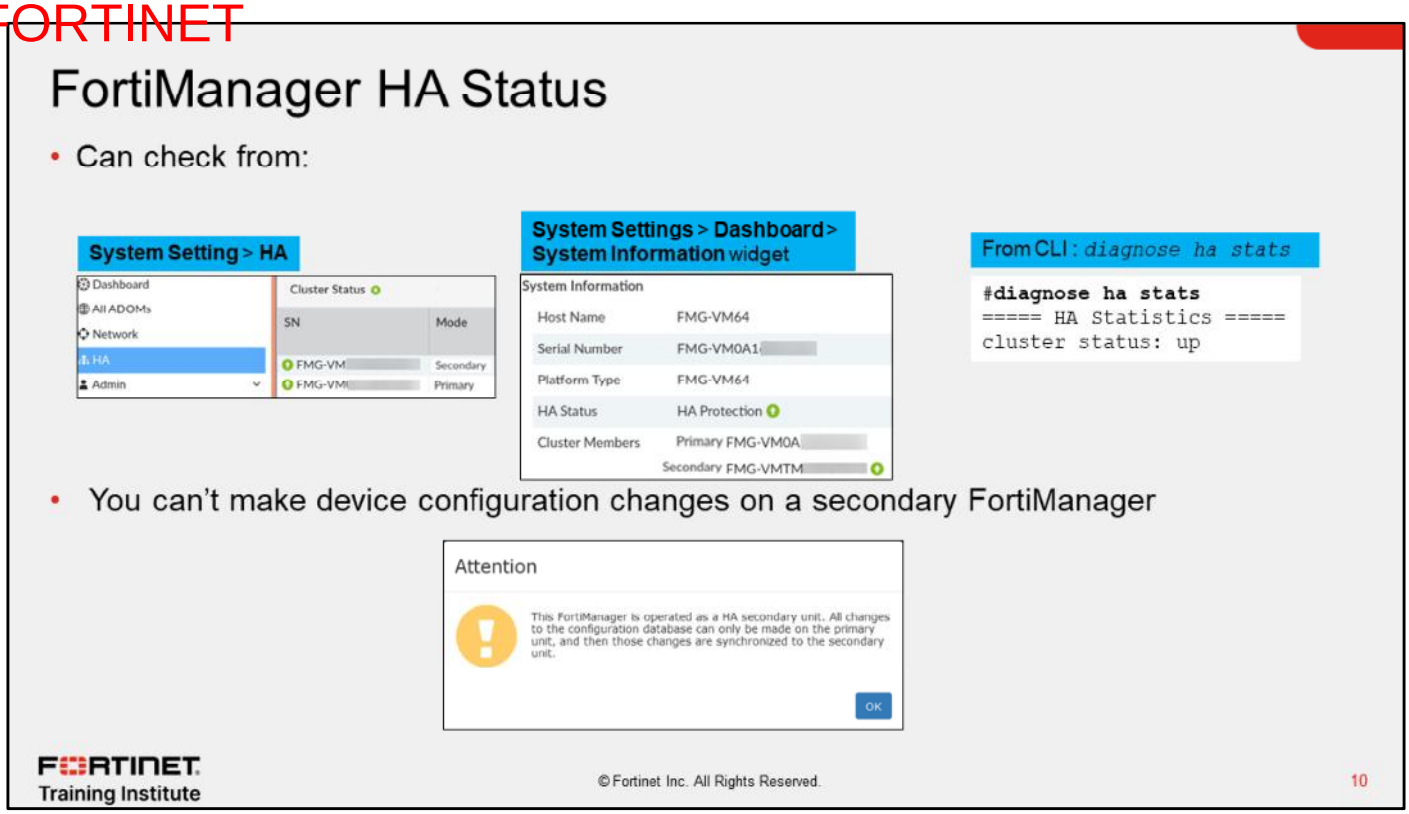


You can select **VRRP** in the **Failover Mode** field, and then add up to four secondary devices to the cluster. The following settings are required in this failover mode:

- **Virtual IP (VIP)**: is required for FortiManager HA. Generally, it is one of the IP addresses in the subnet that FortiGate devices use to communicate with FortiManager.
- **VRRP Interface**: is the interface that is bound to the VIP.
- **Priority**: determines the role of the FortiManager device in HA. The device with a higher priority operates as the primary device when possible. 1 is the lowest value and 253 is the highest.
- **Unicast**: is an optional setting. You can enable it if required (for layer 3). By default, FortiManager HA VRRP uses multicast to advertise packets.
- **Monitored IP**: allows you to configure the IP address and interface to monitor for HA failover. You can add additional monitored IP addresses by clicking **+**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After you configure the FortiManager cluster, you can view the **System Information** widget on the dashboard, **HA settings**, or CLI for the current status of the HA cluster.

You can also check the logs in the **Event Log** or **Alert Message Console** widget on the dashboard.

After you configure a FortiManager cluster, a message opens on the secondary FortiManager. It states that you can't make any device configuration changes on the secondary device. It also states that you can make changes to the configuration database only on the primary FortiManager, which will synchronize its changes with all secondary devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Update on Managed FortiGate Configuration

- Primary FortiManager updates FortiGate central management configuration with serial numbers of all cluster members

```
Local-FortiGate # get sys central-management
mode                : normal
type                : fortimanager
…
…
serial-number       : "FMG-VM0A16001583" "FMG-VMTM20010075"
fmg                 : 10.0.1.241
```

Primary and secondary serial number

- If you remove a secondary member from cluster, the primary FortiManager removes the secondary serial number from the central management configuration of FortiGate, and updates the managed FortiGate devices immediately

FORTINET Training Institute

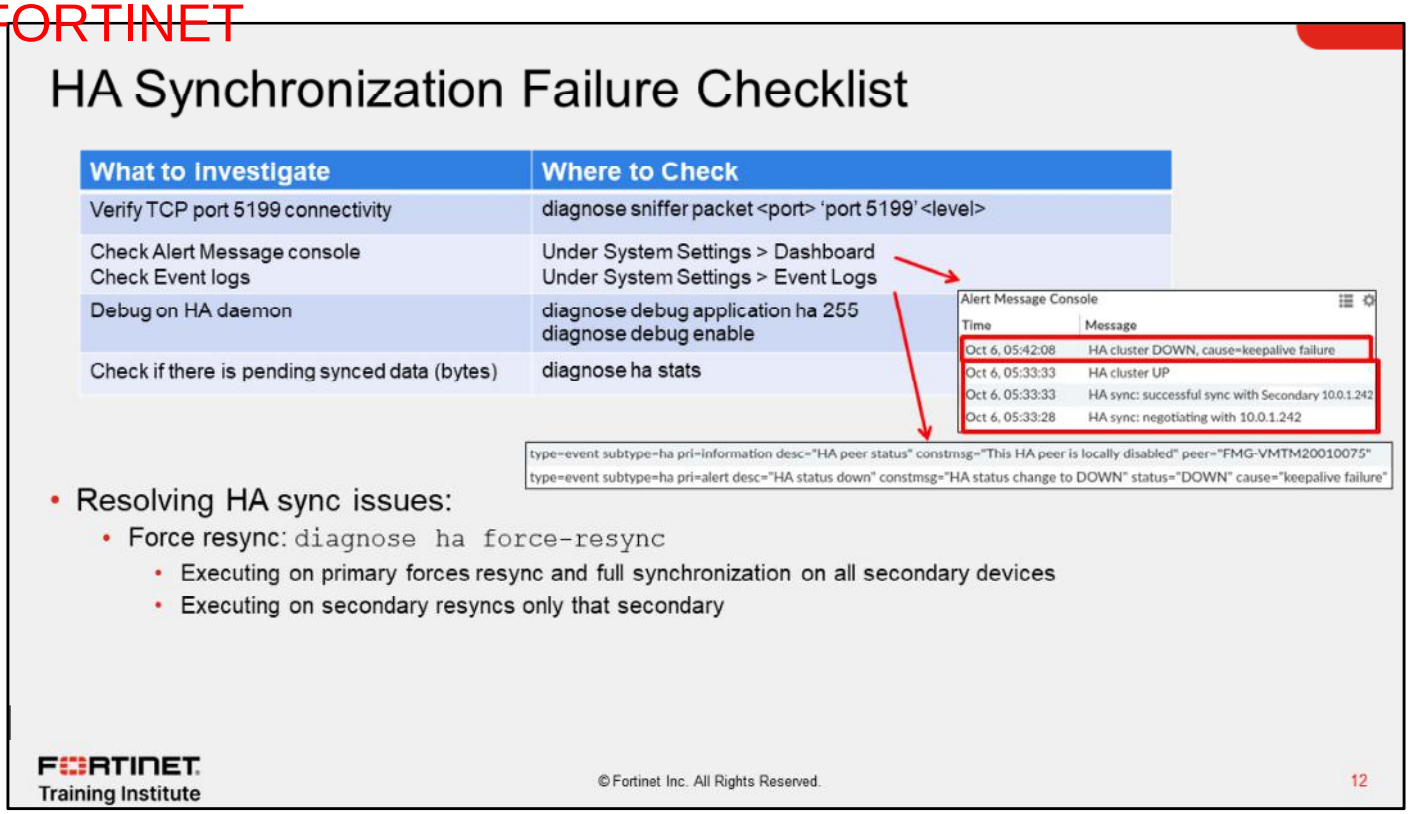
© Fortinet Inc. All Rights Reserved.

11

The managed FortiGate devices are updated by the primary FortiManager with the serial numbers of all cluster members. Similarly, if you remove a secondary member from the HA configuration, the primary FortiManager removes the secondary serial number from the central management configuration of FortiGate, and updates the managed FortiGate devices immediately.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



If you experience issues with the FortiManager HA, you can check the following:

- The HA heartbeat packets use TCP port 5199. Run sniffers on TCP port 5199 to ensure clusters members are able to send and receive HA heartbeat packets.
- Check event and alert message console for messages related to HA.
- Run real-time debugs to verify HA synchronization.
- Check HA status to confirm HA is fully synchronized.

To resolve HA issues, you can force a resync from the primary FortiManager, which resyncs its database with all secondary devices. If you run the command to resync on a secondary FortiManager, only that secondary FortiManager resyncs with the primary FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Troubleshooting HA

- **Pending Module Data** value
  - If 0, cluster is in full sync
  - If there is a value, it shouldn't remain there for more than a few seconds

Cluster Status

SN	Mode	IP	Enable	Module Data Synchronized	Pending Module Data
FMG-VM	Primary	10.0.1.241		-	-
FMG-VM	Secondary	10.0.1.242	✓	102.0 MB	0.0 KB

Should be 0, if fully in sync

Primary

```
#diagnose ha stats
===== HA Statistics =====
cluster status: up
--- cluster member information ---
ip                                : 10.0.1.241
serial number                     : FMG-VM0A16001583
hostname                          : FMG-VM64
role                              : primary
status                            : up
total sync'ed data(bytes)         : 164244678
pending sync'ed data(bytes)       : 0
secondary down alert              : off
secondary re-join alert           : off
last error                        : n/a
```

Role and status

Secondary

```
#diagnose ha stats
===== HA Statistics =====
cluster status: up
--- cluster member information ---
ip                                : 10.0.1.152
serial number                     : FMG-VMTM20010075
hostname                          : FMG-VM64
role                              : secondary
status                            : up
total sync'ed data(bytes)         : 164244678
pending sync'ed data(bytes)       : 0
secondary down alert              : off
secondary re-join alert           : off
last error                        : n/a
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

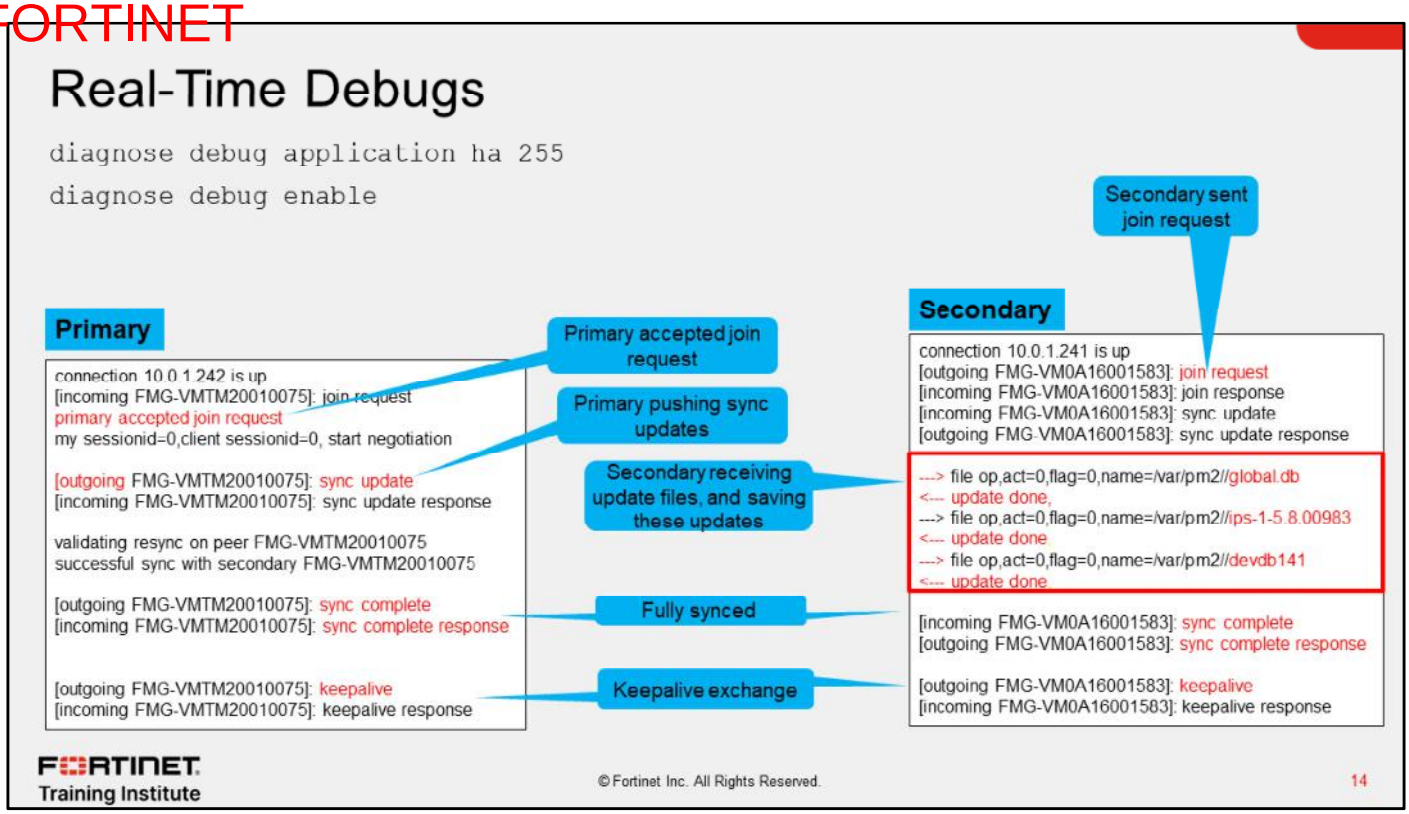
13

The first thing you should look at in the HA cluster is whether there is any pending data that needs to be synced between the cluster members. A value in the **Pending Module Data** field means there are updates that must be synced on secondary devices. The value should be 0, which indicates synchronization is working fine.

To troubleshoot, you can run real-time debugs on HA daemons on all cluster members.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can use the real-time debug commands to check sync issues and for keepalive messages.

In the example shown on this slide, a new secondary FortiManager is configured and sending a request to the primary FortiManager to join the cluster. The primary FortiManager accepts the request and sends the databases to the secondary FortiManager. Then, the secondary FortiManager saves these databases and updates the primary FortiManager. After the primary and secondary devices are fully synced, cluster members exchange keepalive messages, which confirms the cluster is up and running.

The failure is detected after you configure the heartbeat interval multiplied by the failover threshold in the HA settings on the primary FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which configuration is not synchronized between FortiManager HA cluster members?
   - ✓A. FortiGuard database
   - B. Global database

2. Which statement about a FortiManager HA cluster is true?
   - ✓A. Each HA cluster member must have a unique IP address.
   - B. A FortiManager HA cluster supports active-active configuration.

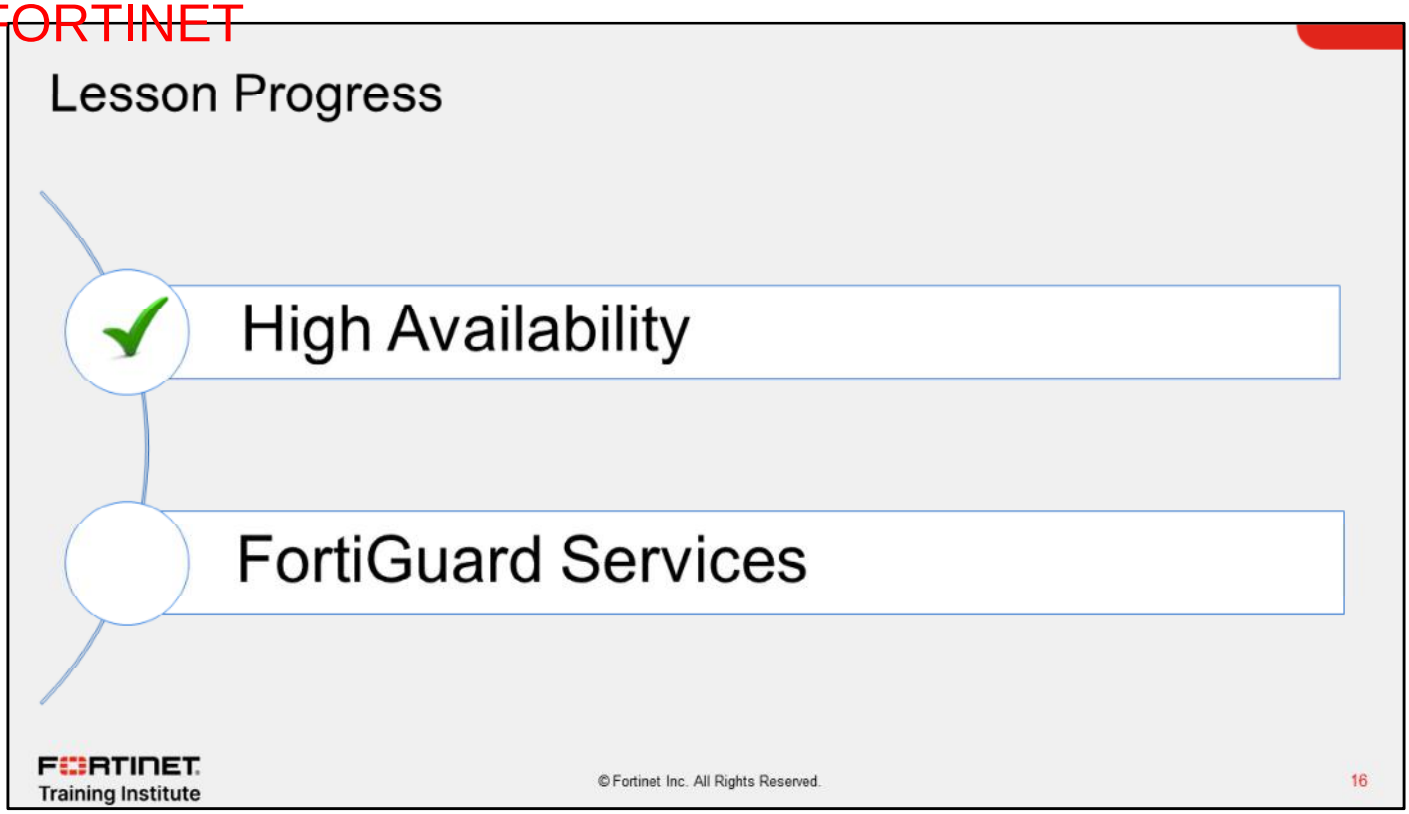
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

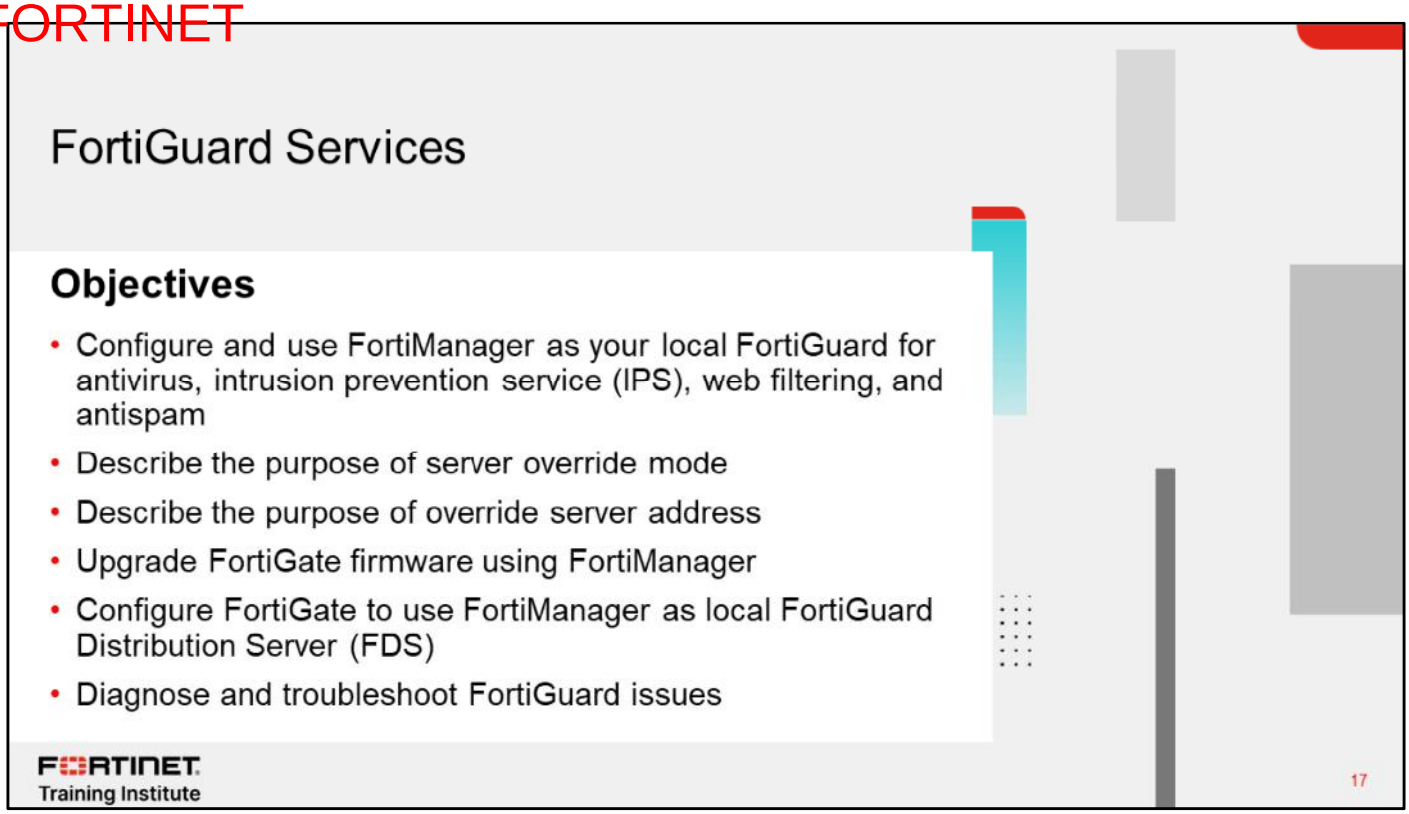


Good job! You now understand how to implement, configure, and troubleshoot an HA cluster.

Now, you will learn about FortiGuard services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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

By demonstrating competence in using FortiGuard services on FortiManager, you will be able to use your FortiManager effectively as a local FDS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiManager as a Local FortiGuard

Why do you want to configure FortiManager as a local FortiGuard server?

- Downloads all antivirus, IPS packages, web filter, email filter databases on FortiManager
- Reduces internet connection load
  - Local FortiGuard provides a faster connection
  - Can redistribute the packages to many devices
    - In some high-security environments, internet access for internal FortiGate is restricted

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

18

A FortiManager device that is acting as a local FortiGuard synchronizes the FortiGuard updates and packages with the public FortiGuard Distribution Network (FDN), then provides the updates to your private network's supported Fortinet devices. The local FortiGuard provides a faster connection, which reduces the internet connection load and the time required to apply updates, such as IPS signatures, to many devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager—Your Local FortiGuard Cache

- Periodically connects to FortiGuard servers
  - Downloads license statuses for managed devices
  - Syncs FortiGuard packages
  - *Unless configured for closed network operation*
- Can cache available firmware updates for managed devices
- Can act as a downstream FortiGuard, providing updates for:
  - Antivirus and IPS engines and signatures
  - Web filtering and antispam rating databases and lookups
- In HA, each FortiManager acts as an individual FortiGuard server
  - Each HA member independently downloads and provides these services to FortiGate devices

FortiGate devices *must* have valid and active service contracts to obtain updates!

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

FortiManager can function as a local FortiGuard Distribution Server (FDS). It continuously connects to the public FDN servers to obtain managed device license information and check firmware availability updates (unless configured for closed-network operations).

FortiManager can provide antivirus, IPS signature updates, web filtering, and antispam services to supported devices.

FortiGuard information is not synchronized across a FortiManager cluster. In a cluster, each device individually downloads and can provide these services independently.

FortiManager supports requests from registered (managed) and unregistered (unmanaged) devices.

Use of FortiGuard services on FortiManager may be resource intensive and, moreover, you may dedicate a FortiManager to this task.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Terminology Used

- The term *FortiGuard* covers
  - Intrusion prevention services (IPS)
  - Antivirus
  - Web filter and email filter

Terminology Used		Service Type
FDS	FortiGate	Antivirus and IPS
FGD		Web filter and email filter
FCT	FortiClient	Antivirus and IPS
FGC		Web filter and email filter
FDN		Public FortiGuard Distribution Network

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

FortiGuard services represent the antivirus, IPS, web-filtering, and antispam update services.

Historically, the antivirus and IPS service has been referred to as the FDS service, and the web filter and email filter service as the FortiGuard service.

Currently, the term FortiGuard covers all services; however, specific FortiManager GUI or CLI configuration sections still continue to refer to them using the terminology shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager Port and Protocol Usage

- Uses TCP port 443 to obtain updates from public FDN
- Four main FortiGuard services on FortiManager to create a replica of public FDN for FortiGate and FortiClient

FortiGuard Service		Process	Initial Connectivity to Public FDN (TCP 443)
FortiGate	FDS	fdslinkd	fds1.fortinet.com usfds1.fortinet.com - For US servers only
	FGD	fgdlinkd	guard.fortinet.net and qsvr.fortinet.net
FortiClient	FCT	fctlinkd	forticlient.fortinet.net
	FGC	fgclinkd	fgd1.fortigate.com

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

FortiManager requires internet access using TCP port 443 in order to download packages and databases, and validate FortiGate service licenses, from public FDN servers.

FortiManager uses four main FortiGuard services to create a replica of public FDN servers for FortiGate and FortiClient.

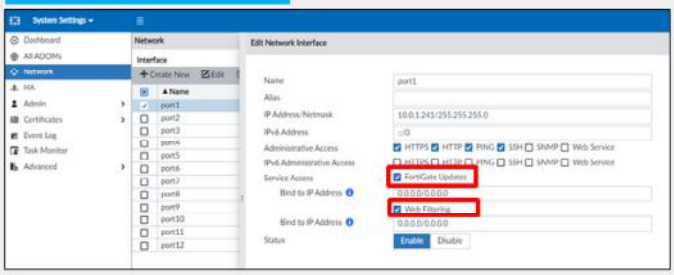
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

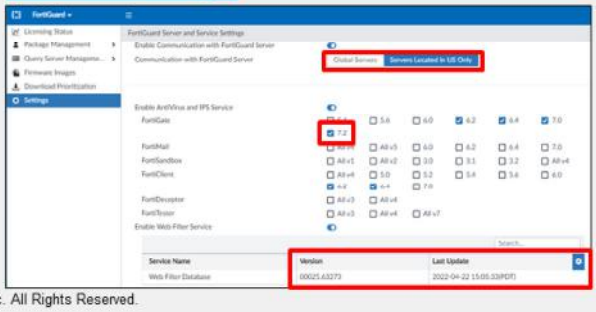
Enabling Built-In FDS (FortiGuard)

- Two steps
  1. Enable service access settings on interface
  2. Enable FortiGuard services
- Enable service access settings for each interface
  - Used by FortiManager to communicate with FortiGate devices
- Can enable the following services
  - Antivirus and IPS
  - Web filter
  - Email filter
- By default, communication with public FDN is enabled on FortiManager
- Can change FortiGuard communication between **Global Servers** or **Servers Located in US Only**

System Settings > Network



FortiGuard > Settings



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

In order to enable the built-in FDS, you must enable the service access setting on the FortiManager interface and the FortiGuard services.

You must configure the **Service Access** settings on FortiManager per interface. This is useful when different FortiGate devices are communicating with FortiManager on different interfaces. FortiGate devices use FortiGuard services to query and obtain updates from FortiManager. The **FortiGate Updates** service is for antivirus, IPS, and license validation. The **Web Filtering** service is for web filter and antispam.

The second configuration step is to enable services on FortiManager. By default, communication to the public FDN is enabled, which allows FortiManager to continuously connect to FDN servers to obtain managed device information and sync packages. However, you must enable services such as antivirus and IPS, web filter, and email filter so that FortiManager can download updates for these services from the public FDN.

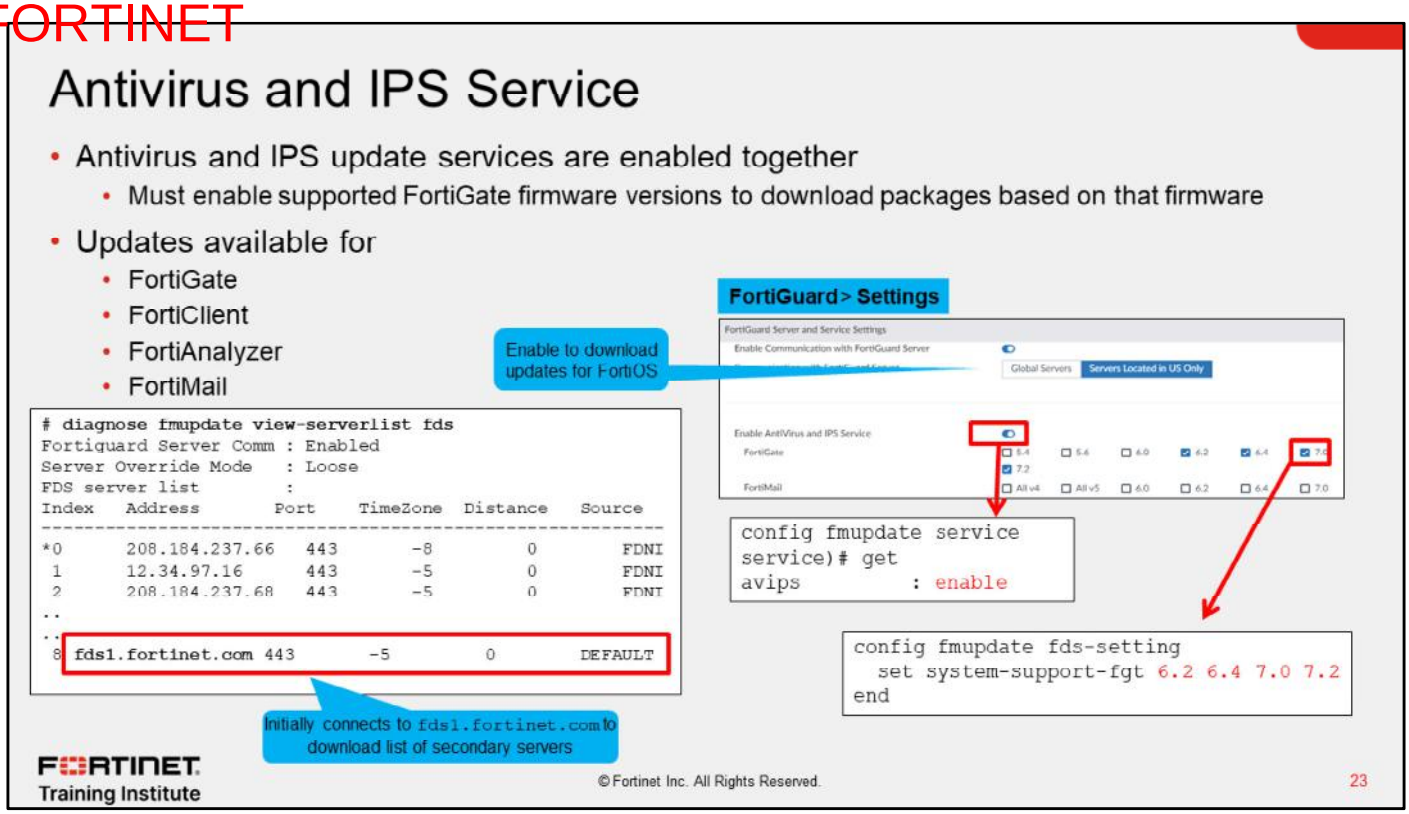
You can select **Servers Located in the US Only** to limit communication to FortiGuard servers located in the USA. Select **Global Servers** to communicate with servers anywhere.

When you use FortiManager in a closed network, disable communication with FortiGuard. When communication is disabled, you must upload antivirus, IPS, license packages, web filter, and email filter databases manually because they are no longer automatically retrieved from the public FDN server(s).

During the first-time setup, FortiManager is still receiving updates from the public FDN and you should disable service access at the interface level. This is because FortiManager is still downloading updates and may not be able to provide accurate ratings or updates to FortiGate. You can enable service access after FortiManager has downloaded the packages and databases.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The antivirus and IPS services are enabled together and use TCP port 443 to obtain the updates from public FDN. You can enable updates for the supported products by enabling the firmware version that you want to download the updates for.

By default, FortiManager first attempts to connect to the public FDS server `fds1.fortinet.com` through TCP port 443, to download the list of secondary FDS servers that it will download AV/IPS packages from.

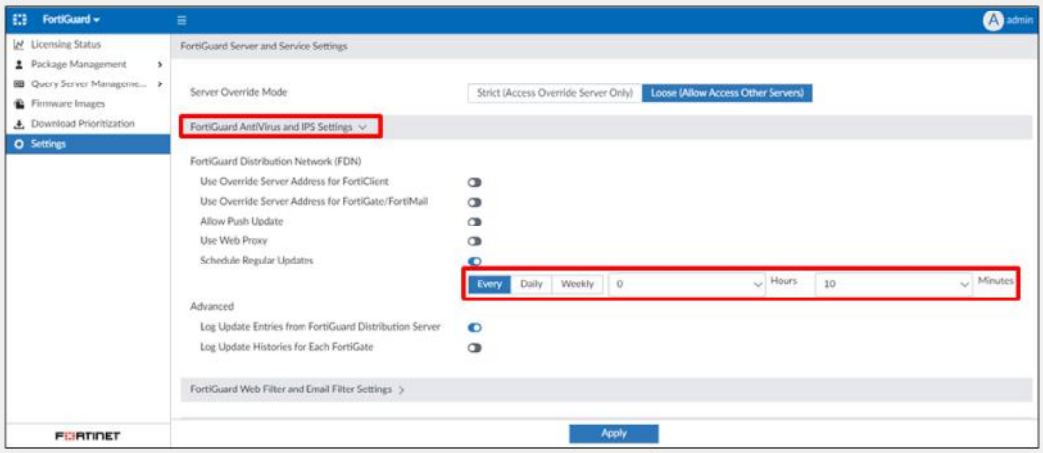
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Schedule Updates for Antivirus and IPS

How frequently does FortiManager communicate with public FDN servers for AV/IPS updates?

- By default, FortiManager schedules updates every ten minutes
  - But, you can select a different interval



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

Keeping the built-in FDS up-to-date is important to provide current FDS update packages. By enabling **Schedule Regular Updates**, you are guaranteed to have a relatively recent version of signature and package updates. A FortiManager system acting as an FDS synchronizes its local copies of FortiGuard update packages with the FDN when:

- FortiManager is scheduled to poll or update its local copies of update packages
- Push updates are enabled (it receives an update notification from the FDN)

If the network is interrupted when FortiManager is downloading a large file, FortiManager downloads all files again when the network resumes. You can configure scheduled updates on an hourly, daily, or weekly schedule.

By default, FortiManager schedules updates every ten minutes because antivirus updates occur frequently.

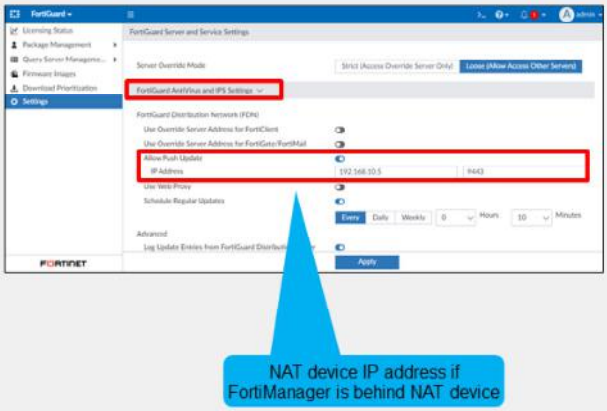
What if there are important IPS updates available on the public FortiGuard? How can you ensure that FortiManager always receives new updates?

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Push Updates

- By default, FortiManager contacts public FDS on a configured schedule
- Push updates allow urgent or critical updates to be pushed directly to FortiManager when they become available on the FDN
  - FortiManager immediately downloads these updates
- To use push updates, you must enable both:
  - Built-in FDS on FortiManager (AV/IPS settings)
  - Push updates
- By default, FortiManager sends its IP address to FDN for push updates
- Push updates fail if FortiManager is behind NAT device
  - NAT device IP address in push updates
  - Allow traffic from NAT device to FortiManager to receive updates



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

If you enable **Allow Push Update**, the FDN can push update notifications to the FortiManager built-in FDS, as soon as new signature updates are released publicly by FortiGuard. FortiManager then downloads the updates immediately.

Usually, when you enable push updates, FortiManager sends its IP address to the FDN. FDN uses this IP address as the destination for push messages.

What if FortiManager is behind a NAT device?

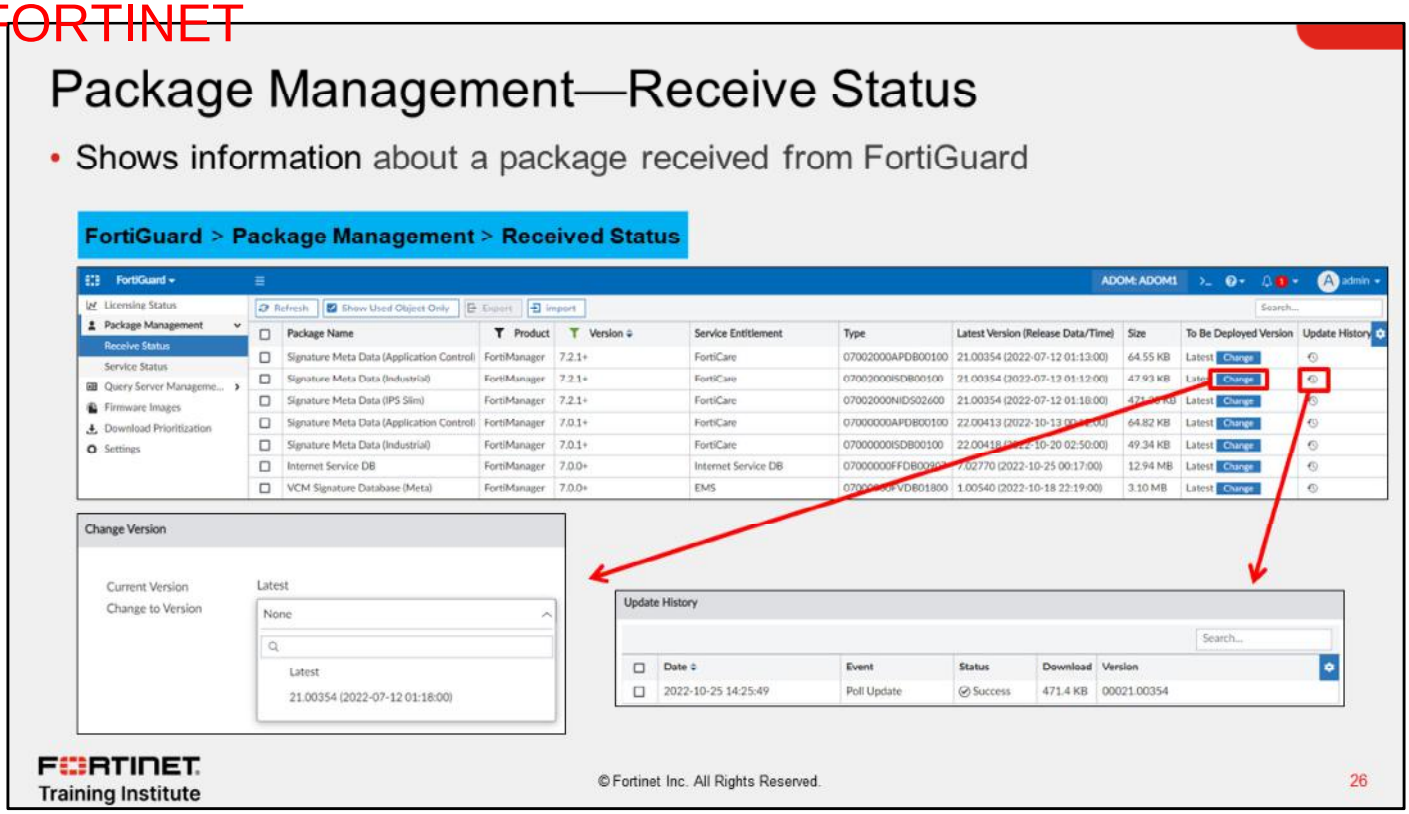
If FortiManager is behind a NAT device, sending its IP address for push updates causes push updates to fail because this is a non-routable IP address from the FDN. You must configure the following:

- On FortiManager, configure the NAT device IP address and port used for push updates. By default, the port for push updates is UDP 9443, but you can configure a different port number.
- On the NAT device, configure the virtual IP and port that forwards to FortiManager. FortiManager may not receive push updates if the external IP address of the NAT device changes.

The built-in FDS may not receive push updates if the external IP address of any intermediary NAT device is dynamic (such as an IP address from PPPoE or DHCP). When the external IP address of the NAT device changes, the FortiManager push IP address configuration becomes out of date.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Receive Status** displays the package received, latest version, size, to be deployed version, and update history for the antivirus and IPS signature packages received from FortiGuard.

The **Update History** shows the update times, the events that occurred, the status of the updates, and the versions downloaded.

You can also change the version you want to deploy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Package Management—Service Status

- Shows list of managed FortiGate devices, their last update, and status
- Main statuses:
  - **Up to Date**
  - **Never Updated**
  - **Pending**
  - **Problem**
  - **Unknown**

FortiGuard > Package Management > Service Status

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

There are five main statuses for FortiGate devices configured to receive updates from the FortiManager:

- **Up to Date**: The latest package has been received by the FortiGate device.
- **Never Updated**: The device never requested or received the package.
- **Pending**: The FortiGate device has an older version of the package because of an acceptable reason (such as the scheduled update time is pending).
- **Problem**: The FortiGate device missed the scheduled query, or did not correctly receive the latest package.
- **Unknown**: The FortiGate device status is not currently known.

You can also push pending updates to the devices, either individually or all at the same time.

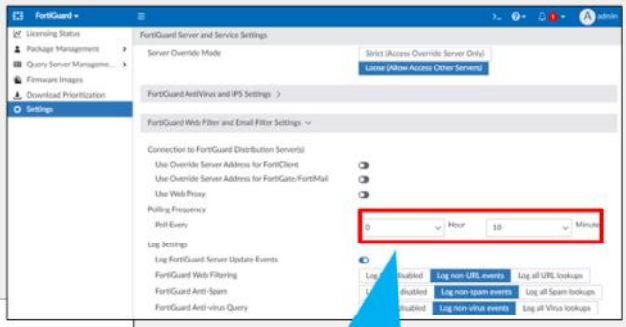
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuring Web Filter and Email Filter

- Through FortiGuard settings

```
# diagnose fmupdate view-serverlist fgd
Response=202|Current fds server list :grpindex:0
Index   Address                Port          TimeZone        Distance
-----------------------------------------------------------------------
 0      208.184.237.64           443           -8               0
 1      208.184.237.63           443           -8               0
..
*11     usguard.fortinet.net    443           0                0
Current fds server list :grpindex:1
Index   Address                Port          TimeZone        Distance
-----------------------------------------------------------------------
 0      208.91.113.75           443           -5               3
*1      usfqsvr.fortinet.net    443           0                0
```



Default polling frequency

Initially connects to guard.fortinet.net to download a list of secondary servers

Used by file query service updates

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

You must enable the web filter and email filter services individually. By default, FortiManager first attempts to connect to the public FortiGuard server over TCP port 443 to download the list of secondary FortiGuard servers from which it then downloads web and antispam packages. By default, FortiManager is scheduled to check for updates every ten minutes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Web Filter and Email Filter

- First time may take multiple hours to download databases
  - Expect some high CPU and I/O wait times

```
# execute top
%Cpu(s):  0.0 us,  6.2 sy,  0.0 ni,  0.0 id, 93.8 wa, ...
PID USER      PR  NI    VIRT   RES  %CPU   %MEM    TIME+   S  COMMAND
28993 root    20   0  676.8m  27.8m  87.0  1.4  686:18.68 S  ../fgdlinkd..
20510 root    20   0  239.0m  92.7m  11.6  4.6   48:02.83 S  fgdupd
```

- Three main processes
  - fgdlinkd
    - Responsible for downloading web filter and email filter databases
  - fgdups
    - Responsible for database merging and consolidating smaller delta files into larger files
  - fgdsrv
    - Serves FortiGate and FortiClient for web filter and email filter requests

FORTINET Training Institute

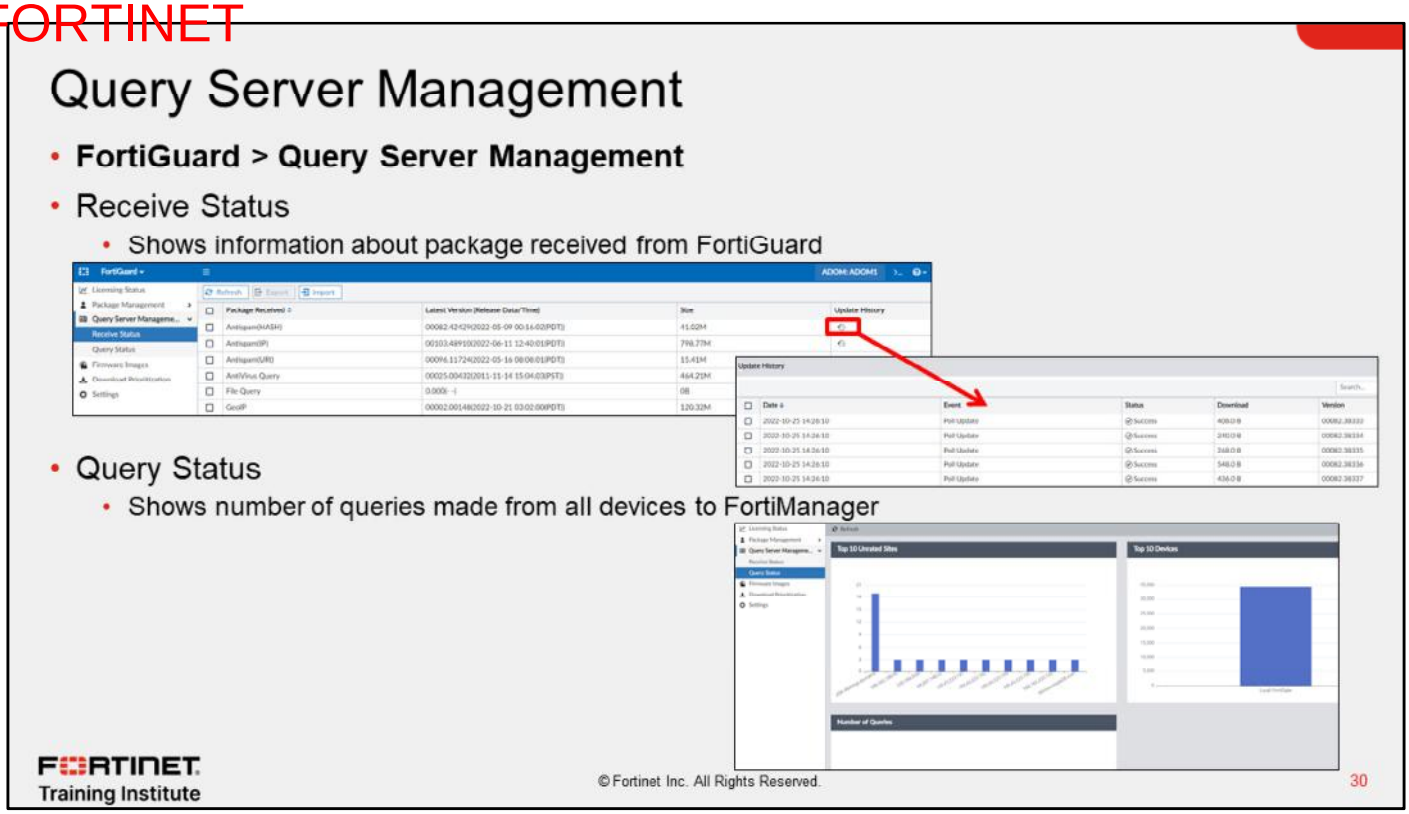
© Fortinet Inc. All Rights Reserved.

29

When you enable web and anti spam services for the first time, it may take several hours to download and merge the databases. During this time, you will notice higher I/O wait times and a spike in CPU usage related to web and email processes on FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The web and antispam databases received from FortiGuard are listed under **Receive Status**. The date and time updates are received from the server, the update version, the size of the update, and the update history are also shown. You can click **Update History** to see more information about individual packages downloaded.

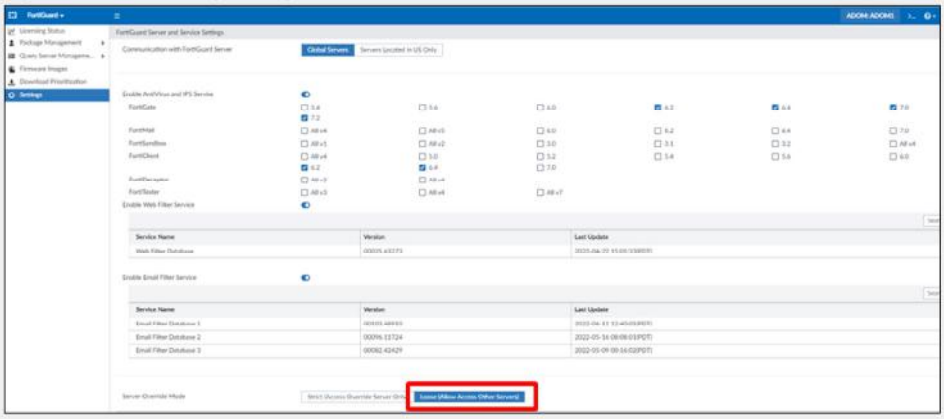
The **Query Status** shows the number of queries made from all managed devices to the FortiManager device that is acting as a local FDS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Server Override Mode

- Two modes
  - Loose
    - Default mode
    - Allows fallback to the other FDN server
  - Strict
    - FortiManager can access only configured override servers



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

31

By default, **Server Override Mode** is set to **Loose**, which is the recommended mode. This setting allows FortiManager to fall back to the other FDN servers if FortiManager is not able to communicate with one of the configured servers in the override server address list.

You can change the **Server Override Mode** to **Strict**, which prevents the fallback from occurring. This setting allows FortiManager to communicate only with the servers configured in the override server address list.

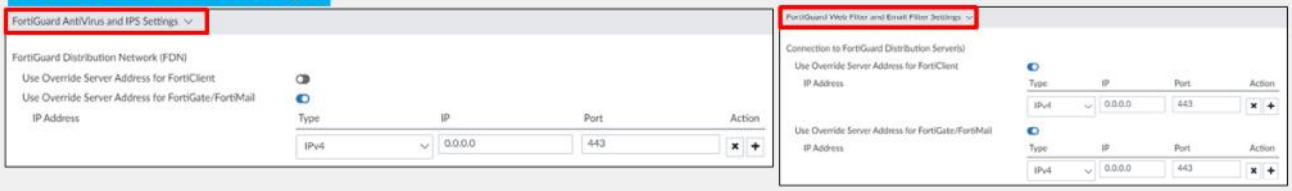
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Override Server Address

- Addresses of FDS servers for FortiManager to connect to and get updates
- Option used:
  - When necessary to connect FortiManager to a specific FDN server on the internet
  - To connect a downstream FortiManager to another upstream FortiManager to download updates
- Can configure override server address for
  - Antivirus, IPS
  - Web filter and email filter

FortiGuard > Settings



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

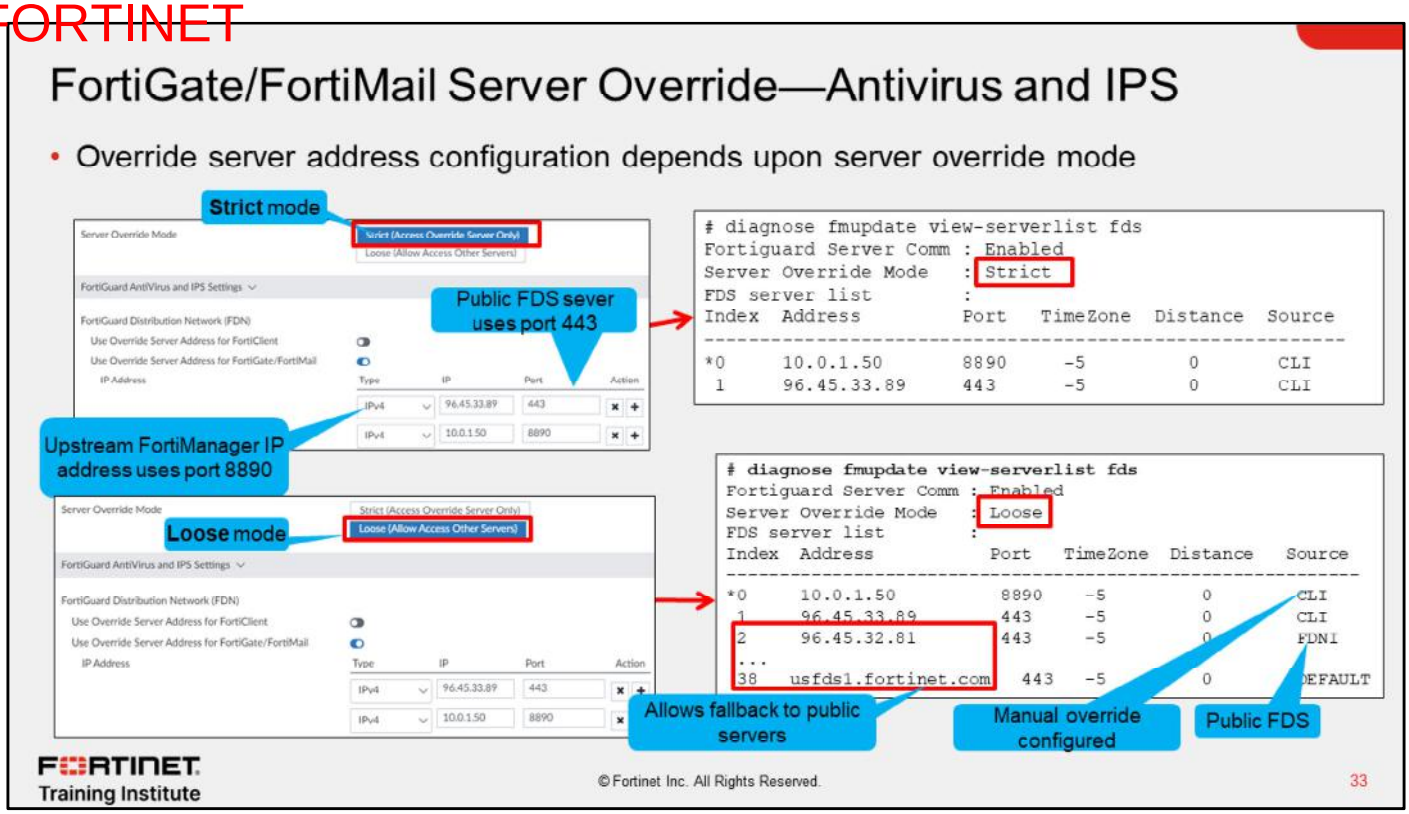
32

You can configure an override server address, which allows FortiManager to communicate to the servers listed in the override servers. You can configure the override server addresses for antivirus, IPS, web filter, and email filter for FortiGate, FortiMail, and FortiClient.

An example of a good situation in which to configure an override server address is if you have a dedicated upstream FortiManager that you use to download antivirus and IPS updates. In this case, you can configure your downstream FortiManager to get the updates from the dedicated upstream FortiManager by configuring the IP address and port used by the upstream FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



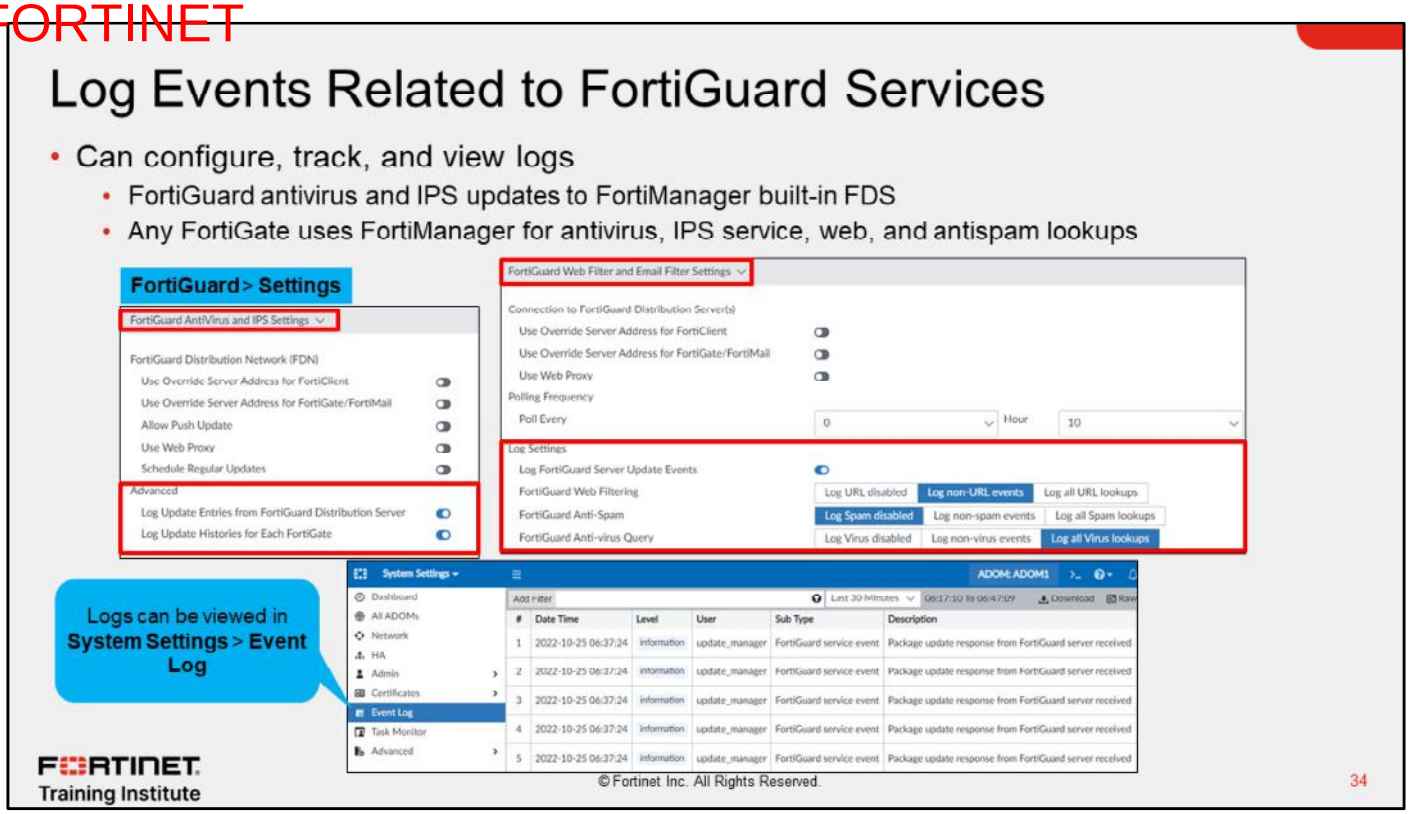
FortiManager tries to obtain updates from the servers configured in the **Use Override Server Address for FortiGate/FortiMail** section. Depending on the **Server Override Mode** configuration, you can restrict FortiManager to receiving updates from the configured override servers list, or allowing fallback to other public FDS servers, if FortiManager is not able to communicate and receive updates from the configured server list.

In the example shown on this slide, two override server addresses are configured. When **Server Override Mode** is set to **Strict**, FortiManager gets updates *only* from these two servers. There is no fallback to other public servers, if these two configured servers are not available.

If you set **Server Override Mode** to **Loose**, FortiManager first tries to get updates from the configured server list; if they are unavailable, FortiManager falls back to other public FDS servers to get updates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

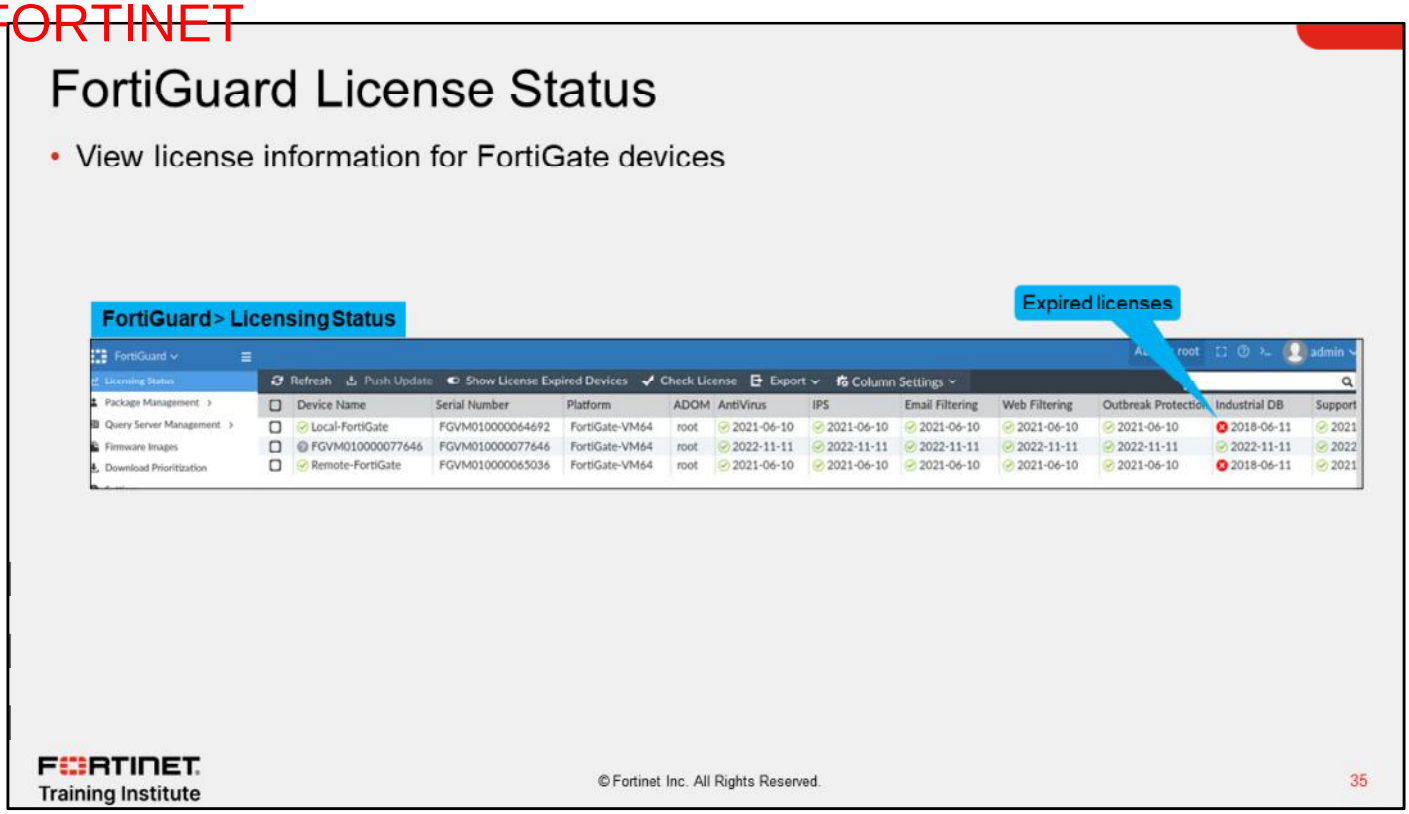


You can configure logging of FortiGuard events, such as FortiManager built-in FDS updates, and FortiGate devices using FortiManager as an FDS.

You can view the logs in **Event Logs**, which can be helpful in diagnosing or troubleshooting issues related to FortiGuard updates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

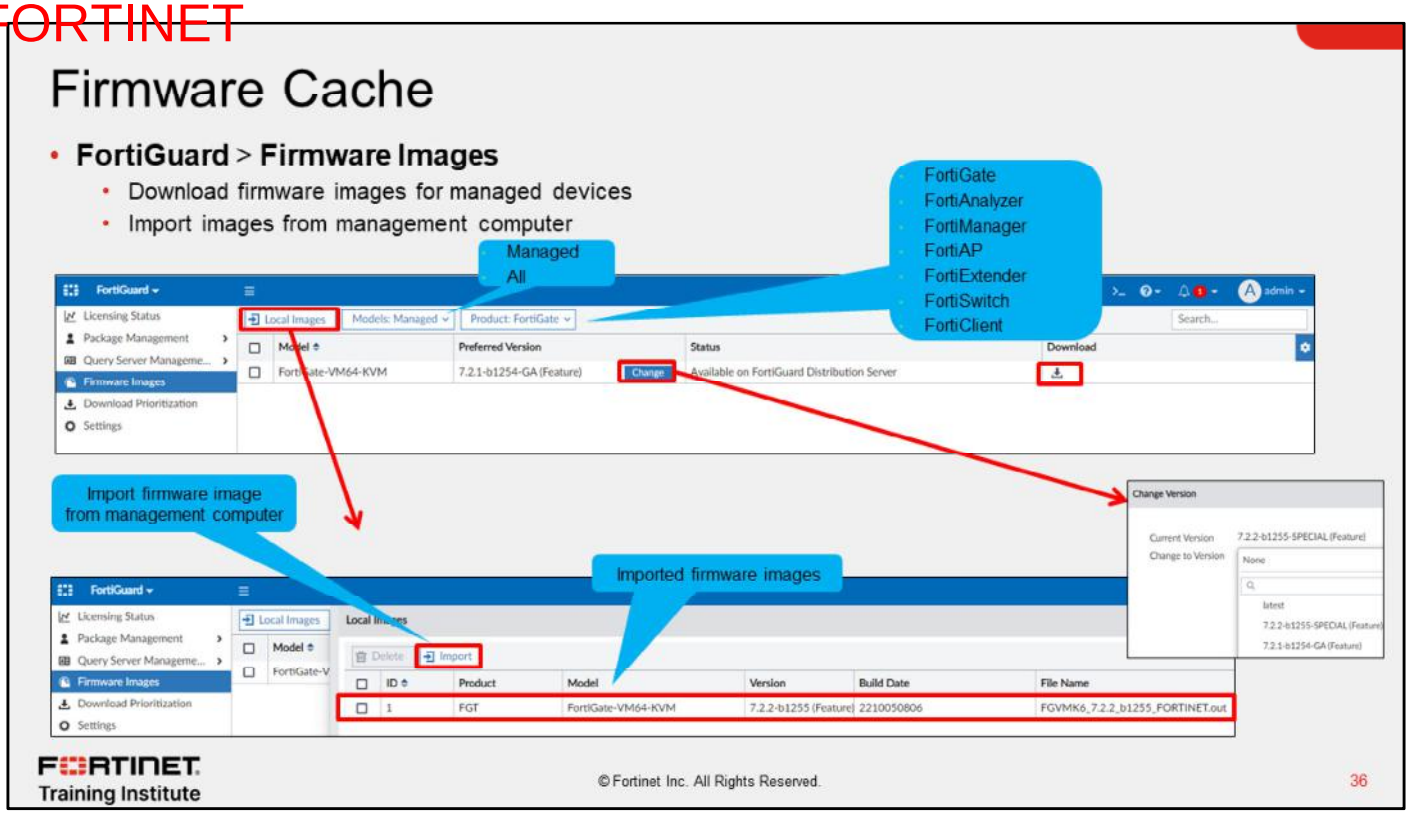


FortiManager includes a licensing overview page that allows you to view license information for all managed FortiGate devices. You can quickly verify if the FortiGate license has expired or not.

If you are managing many FortiGate devices in an ADOM, you can use filters to check the statuses. For example, you can check service licenses for the FortiGate devices expiring in the next 30 days. This helps you to take proactive steps to renew the licenses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiManager can download images from the FDN, or you can upload firmware images from your management computer. If the latest firmware doesn't suit your needs, you can change the latest firmware or you can import firmware images from your management computer. This allows you to change the device firmware using your FortiManager device.

You can view the available firmware based on the supported product type, and filter for all devices or only managed devices.

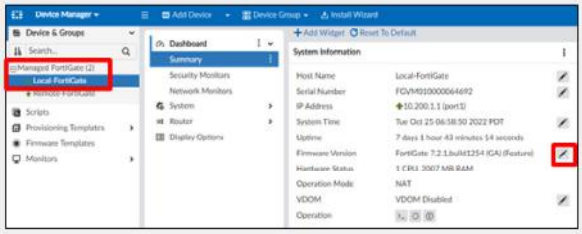
Vouchers & Dumps are Available | WhatsApp +201224560923

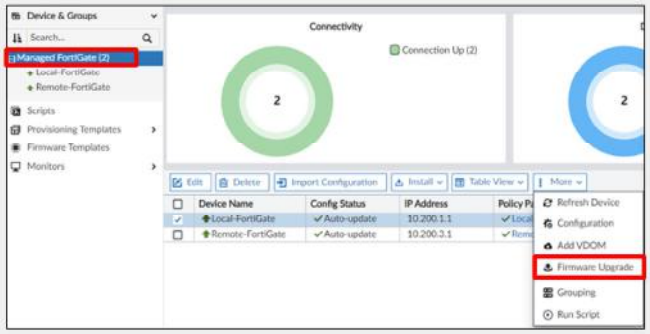
DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate Firmware Update From FortiManager

Firmware can be upgraded in following ways:

- For individual devices
  - From the **System Information** widget
- For multiple devices in an ADOM
  - From the **Device Manager** pane
  - Can upgrade firmware on group





Can schedule firmware upgrades using **Firmware Templates**

- **Device Manager** > **Firmware Templates**

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

37

You can upgrade the FortiGate firmware in a few ways:

- For each device, using the **System Information** widget
- For multiple devices, on the **Firmware** tab in the ADOM**.** You can upgrade the firmware version of all the FortiGate devices, selected FortiGate devices, or FortiGate devices in a group.

FortiManager allows you to upgrade the firmware now, or schedule the upgrade using the **Firmware Templates**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Unmanaged FortiGate to Use FortiManager as FDS

- Devices are not required to be registered with the FortiManager **Device Manager** to use the built-in FDS
- Unmanaged FortiGate can be configured to use FortiManager for FDS updates

```
config system central-management
        config server-list
            edit 1
                set server-type update rating
                set server-address 10.0.1.241
            next
        end
    set include-default-servers {enable/disable}
end
```

Configure server-list to override default FDS servers

- update – antivirus, IPS, license verification
- rating – web filter, email filter

FortiManager IP address

enable – use public FDS, if FortiManager is unavailable
disable – use only FortiManager for FDS updates

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

38

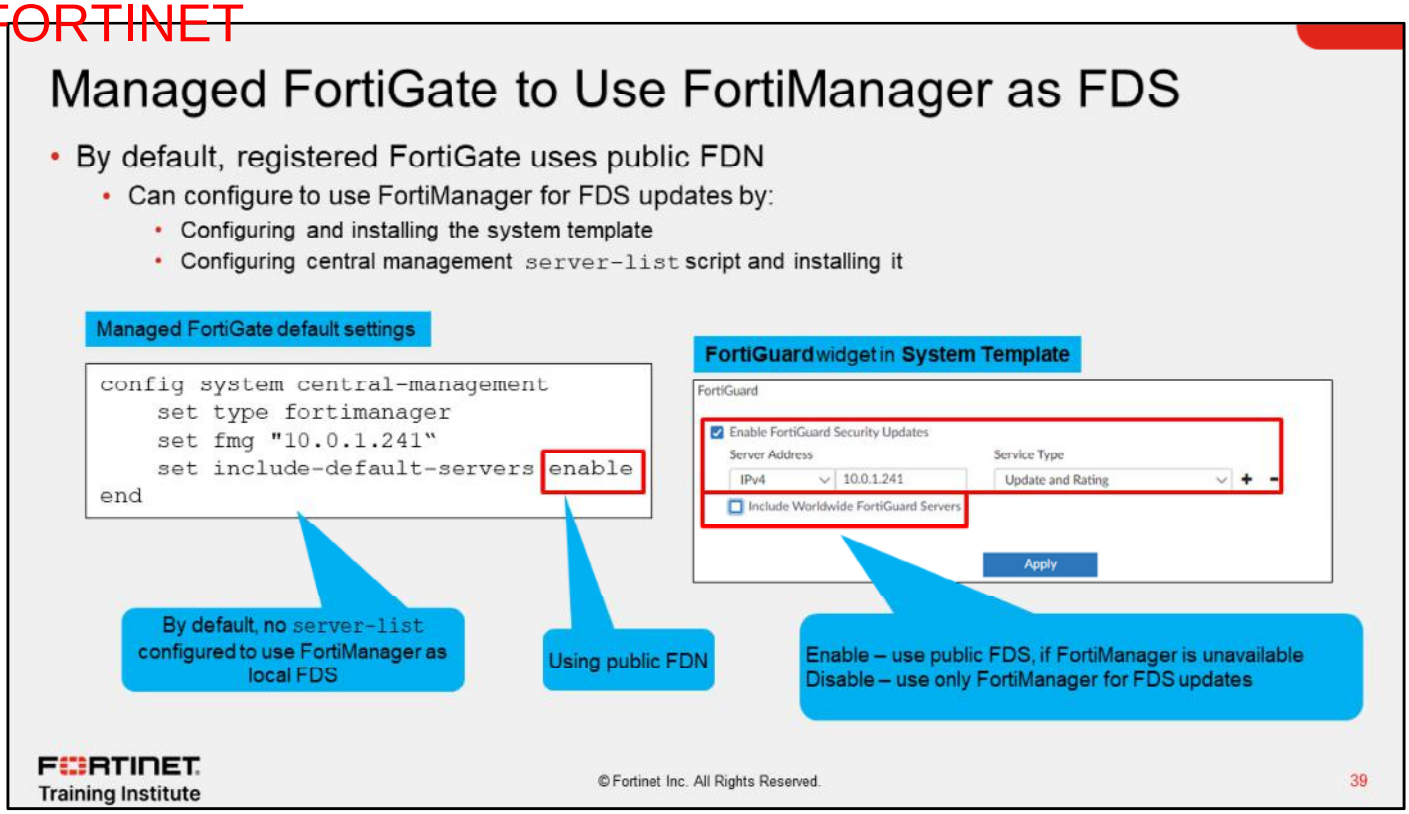
You can also configure unmanaged FortiGate devices to use FortiManager as a local FDS. You must configure the `server-list` in the `central-management` settings of FortiGate, which include:

- The IP address of FortiManager used as the local FDS for FortiGate devices
- The server type, which include:
    - `update` — used for antivirus, IPS updates, and FortiGate license verification
    - `rating` — used for web filter or anti-spam rating

By default, `include-default-servers` is enabled, which allows a FortiGate device to communicate with the public FortiGuard servers if a private server (configured in the `server-list)` is unavailable. You can enable or disable inclusion of public FortiGuard servers in the override server list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



By default, when FortiGate is managed by FortiManager, it uses public FortiGuard servers. This is because not every organization uses FortiManager for local FDS.

There are multiple ways to configure FortiGate to use FortiManager as a local FDS. You can:

- Configure FortiGuard settings in the **FortiGuard** widget, which you can assign to and install on managed devices. The decision to override the default FDS server and use FortiManager is a device-level setting. Remember to enable service access settings on the FortiManager interface.
- Configure and install a script for the central management `server-list`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Verifying Configuration to Troubleshoot FortiGuard Issues

- Verify the following:
  - FortiGuard server on FortiManager is resolved

```
execute ping <FortiGuard domain address>
```

  - Communication to public network is enabled

```
# get fmupdate publicnetwork
status              : enable
```

  - Service is enabled

```
#config fmupdate service
get
avips               : enable
query-antispam      : enable
query-webfilter     : enable
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

40

The first step you should perform when troubleshooting FortiGuard issues is to verify the configuration on FortiManager. You should confirm that:

- You are able to resolve the public FDN servers by domain name. For example, check if you are able to ping `fds1.fortinet.com` for antivirus and IPS for FortiGate or FortiMail.
- Communication to public network and services are enabled on FortiManager
- Services are enabled on FortiManager

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Troubleshooting FortiGuard Connectivity

- `diagnose fmupdate view-serverlist [fds|fct|fgd|fgc|fmtr]`
  - Lists all upstream FDN servers FortiManager is communicating with for updates
- FortiManager is unable to connect to the FDN servers

Antivirus and IPS

```
# diagnose fmupdate view-serverlist fds
Fortiguard Server Comm : Enabled
Server Override Mode   : Loose
FDS server list        :
Index   Address          Port   TimeZone   Distance   Source
-----------------------------------------------------------
*0   fds1.fortinet.com   443     -5          0         DEFAULT
```

Web filter and antispam

```
# diagnose fmupdate view-serverlist fgd
Response=202|Current fds server list :
0 ip = guard.fortinet.net port = 443 timezone=0
distance=0
```

Only one primary FDN server on list. FortiManager is unable to connect the public FDN servers yet because of unreachability or disabled service

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

41

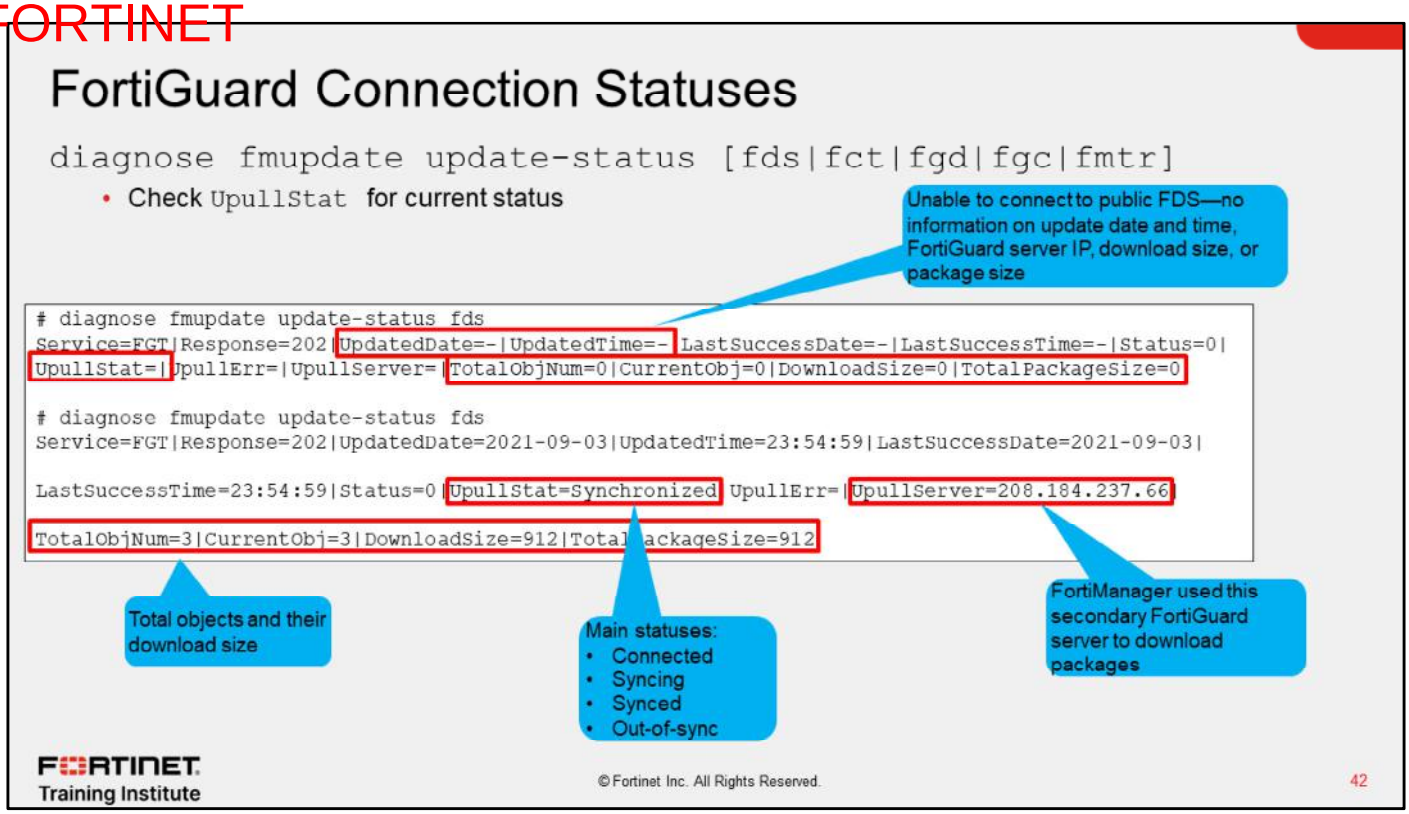
After you verify the configuration, check if FortiManager is communicating with the upstream FortiGuard server(s).

If FortiManager is unable to connect to the public FDN servers, only the primary FDN servers appear in the server list. This can be caused by FortiManager being unreachable or disabled services on FortiManager.

After FortiManager connects to the public FDN servers, it downloads the list of secondary FDN servers from which it downloads the updates and packages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can also check the status of the connection to the public FDN. If FortiManager is not able to connect to the public FDN, or the service is disabled, the `UpullStat` for the current status is empty, and there is no information about the date, time, download size, and package.

After FortiManager is able to communicate with the public FDN, FortiManager displays the download size, package, and IP address of the FDN server that FortiManager is communicating with to download the updates.

The `UpullStat` has four main statuses:

- `Connected`: The FortiManager connection to FDN initially succeeds, but a synchronization connection has not yet occurred.
- `Syncing`: The built-in FDS is enabled, and FortiManager is downloading and syncing packages available on the FDN.
- `Synced`: The built-in FDS is enabled and the FDN packages download successfully.
- `Out-of-sync`: The initial FDN connection succeeds, but the built-in FDS is disabled.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Verifying FortiGate Contract Information on FortiManager

```
diagnose fmupdate dbcontract [<optional fds |fgd> <optional device serial number>]
```

- Lists contract information for all the devices

```
FMG-VM64 # diagnose fmupdate dbcontract
FGVM010000077646 [SERIAL_NO]
  AccountID:yyyy@Fortinet.com
  Industry: Technology
  Company:  Fortinet
  Contract: 13
        AVDB-1-06-20221111
        AVEN-1-99-20180531
        NIDS-1-99-20190611
  Contract Raw Data:
    Contract=AVDB-1-06-20220531:0:1:1:0*AVEN-1-99-20180531:0:..

FGVM010000064692 [SERIAL_NO]
  AccountID: yyyyy@fortinet.com
  Industry: Technology
  Company:  Fortinet
  Contract: 13
        AVDB-1-06-20260121
        AVEN-1-06-20260121        ..

  Contract Raw Data:
    Contract=AVDB-1-06-20260121:0:1:1:0*AVEN-1-06-20260121:0:1..
```

FortiGate devices *must* have valid and active service contracts to obtain updates!

99 are trial or expired licenses

FortiGate serial number

AV service contract

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

43

FortiGate devices must have valid and active service contracts to receive updates from FortiManager.

You can check the contract information of all FortiGate devices on the FortiManager CLI. An expired or trial FortiGate license shows as 99, which means FortiGate is unable to receive the updates from FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate Troubleshooting

- Shows version, last update, contract expiration date

```
 # get system fortiguard-service status
NAME                VERSION LAST UPDATE          METHOD    EXPIRE
AV Engine            6.276  2022-05-18 01:46:00  manual    2026-01-19 23:59:59
Virus Definitions    90.1635  2022-04-25 20:04:46  scheduled 2026-01-19 23:59:59
Extended set         90.1635  2022-04-25 20:04:46  scheduled 2026-01-19 23:59:59
```

- Real-time update

```
# diagnose debug application update -1
# diagnose debug enable
# execute update-now

Local-FortiGate # upd_daemon[1796]-Received update now request
upd_daemon[1613]-Found cached action=00000002
do_update[608]-Starting now UPDATE (final try)
upd_comm_connect_fds[455]-Trying FMG 10.0.1.241:8890
[782] ssl_new: SSL object is created pack_obj[183]-Packing pack_obj[196]-Packing
obj=Protocol=3.2|Command=Update|Firmware=FGVM64-FW-7.20-
1254|SerialNumber=FGVM010000064692|UpdateMethod=0|AcceptDelta=1|Uid=42384969a5690d78bcc75b3c921fda4
e|DataItem=07000000AVDB00201-00090.01635-211011826* ……
] ssl_disconnect: Shutdown
do_update[636]-UPDATE successful
```

FortiGate trying to get updates from configured FortiManager

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

44

On the FortiGate CLI, you can check the version, when it was last updated, and contract information for FortiGate.

You can also run a real-time debug along with the update command, which tries to download the latest definitions and packages from the FDS server (or configured local FDS server in the central management configuration).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. On FortiManager, what is the `fgdlinkd` process responsible for?
   A. Serving FortiGate and FortiClient URL-lookup requests
   ✓B. Downloading web-filter and email-filter databases from public FortiGuard servers

2. Which statement about FortiManager used as a local FDS is true?
   A. It uses a lot of bandwidth because FortiManager needs to get updates from the internet.
   ✓B. It provides updates for antivirus and IPS signatures only.

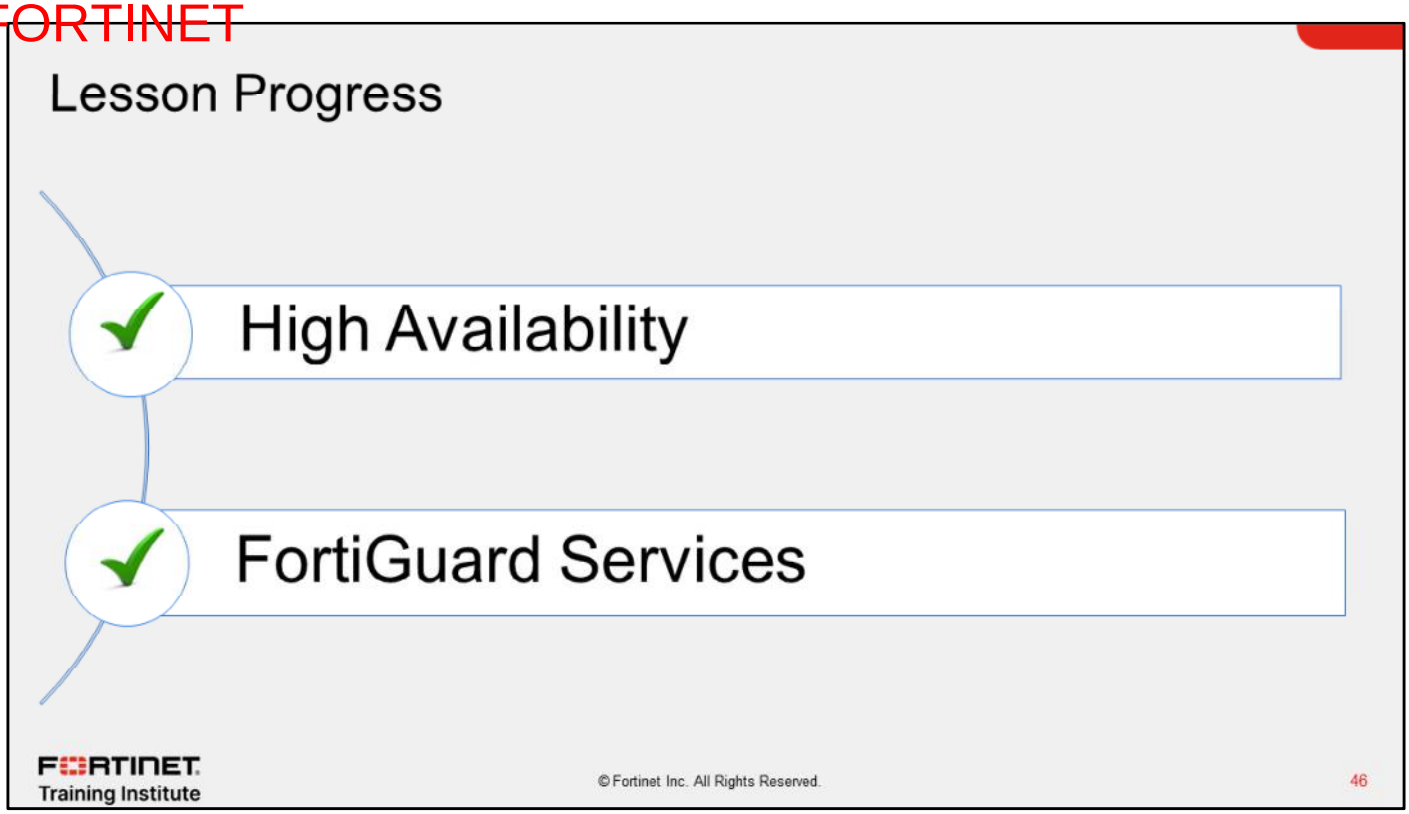
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

45

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



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

Review

- ✓ Deploy FortiManager in an HA cluster
- ✓ Understand what is synchronized between HA cluster members
- ✓ Recover a failed device
- ✓ Configure FortiGuard settings on FortiManager
- ✓ Understand the purpose and use of server override mode and override server address
- ✓ Configure FortiGate devices to use FortiManager as a local FortiGuard server
- ✓ Troubleshoot FortiGuard issues

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

47

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

By mastering the objectives covered in this lesson, you learned how to set up a FortiManager HA cluster and how to use FortiManager as a local FortiGuard server for your devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

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