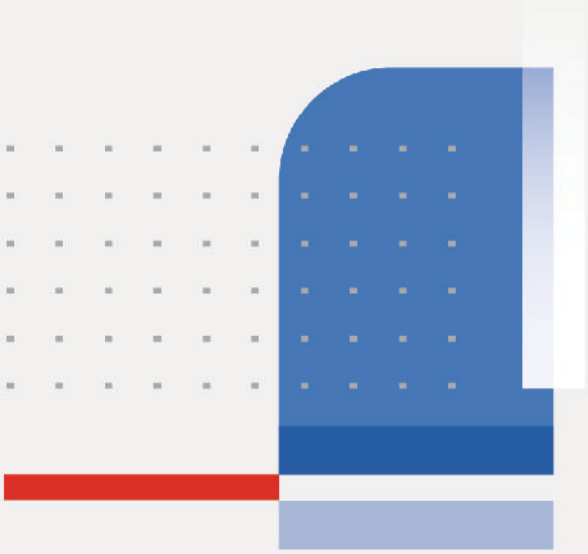
FORTINET CERTIFIED PROFESSIONAL Network Security

FortiManager Administrator Study Guide

FortiManager 7.6



FORTINET Training Institute

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

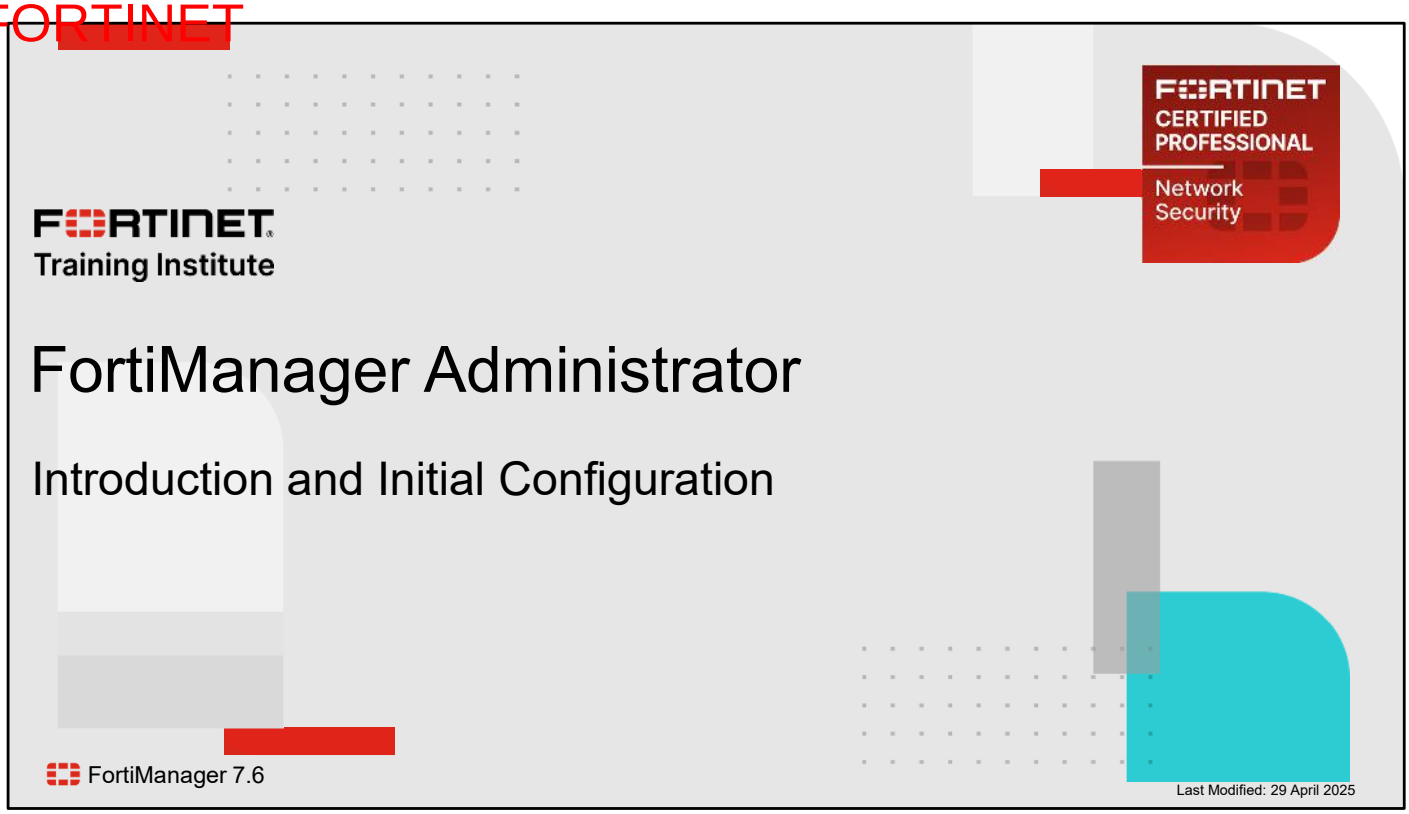
Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

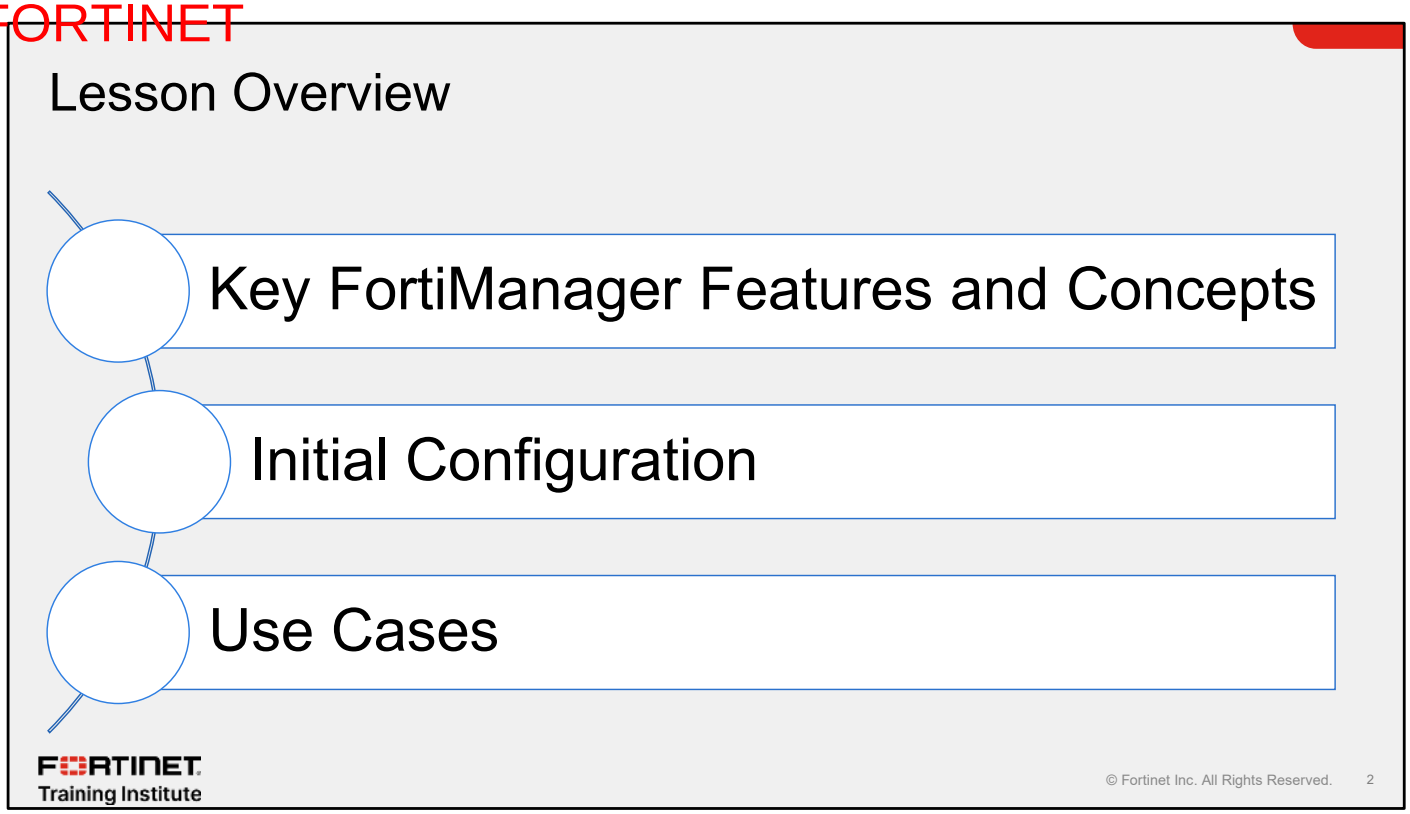
Fortinet Training Institute Helpdesk (training questions, comments, feedback)

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

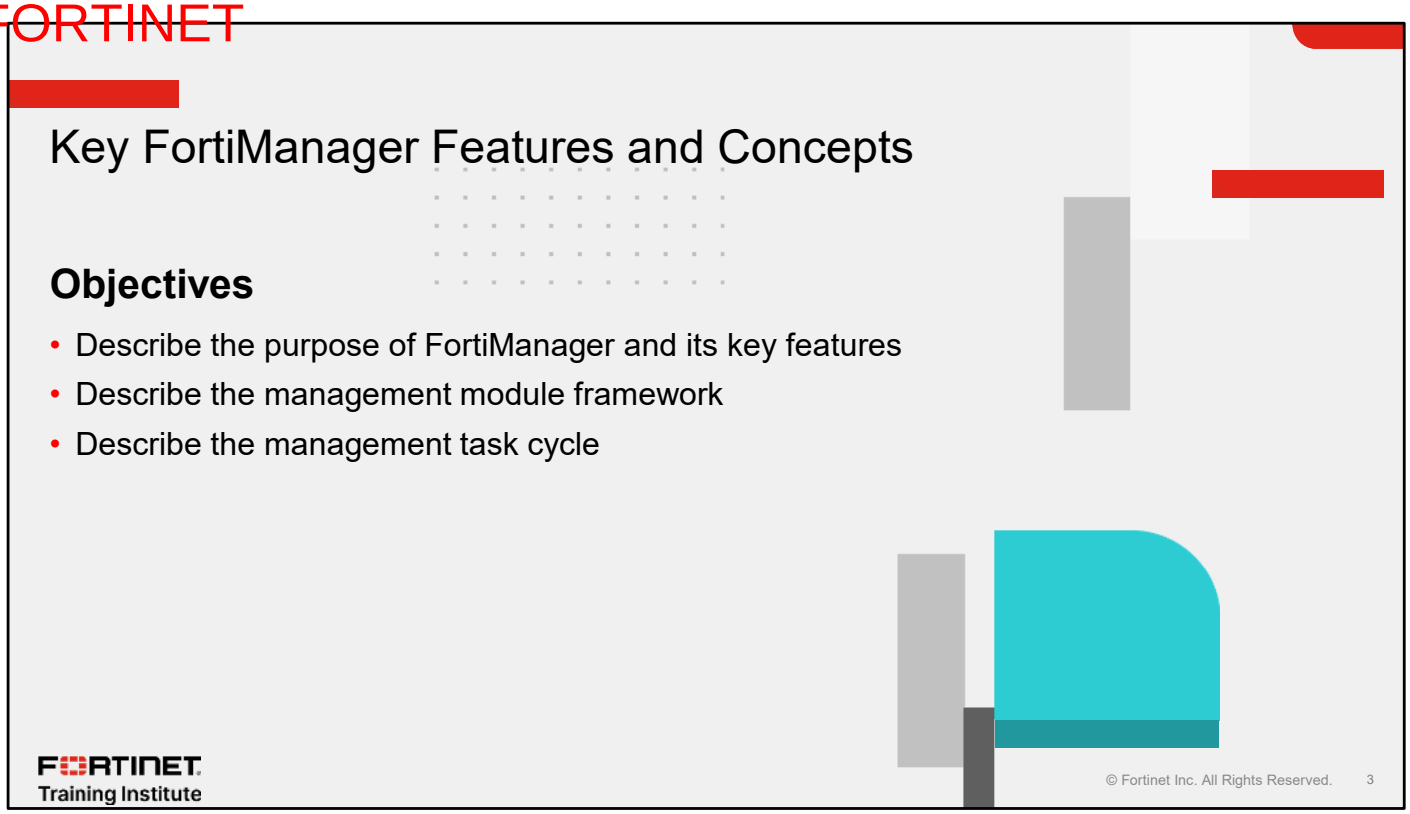
TABLE OF CONTENTS



In this lesson, you will learn about the key features of FortiManager and how FortiManager fits into your existing network infrastructure.



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

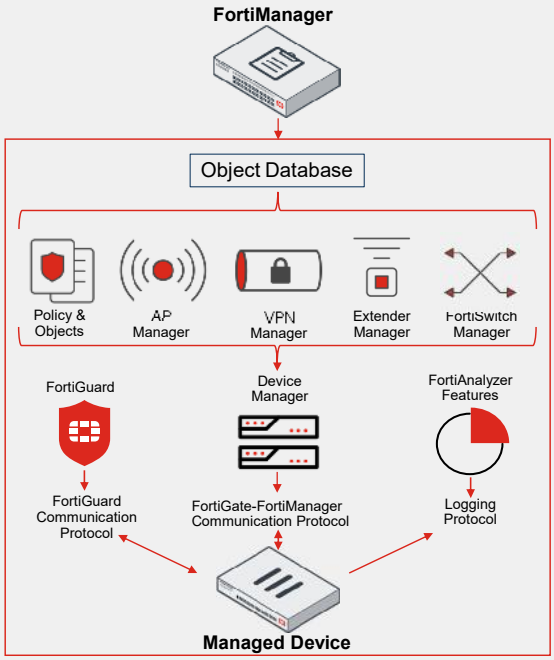


After completing this section, you should be able to achieve the objectives shown on this slide.

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

What Is FortiManager?

- Single-pane management and provisioning
- Reduces operation costs for large deployments
- Helps maintain regulatory compliance
- Local FortiGuard cache server
- Provides centralized device management for many Fortinet devices
- Automates mass device provisioning and maintains policies
  - Local distribution and control point for firmware and policy updates
  - Complex mesh-and-star IPsec VPN
- Can act as logging and reporting device



FORTINET Training Institute

 4

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

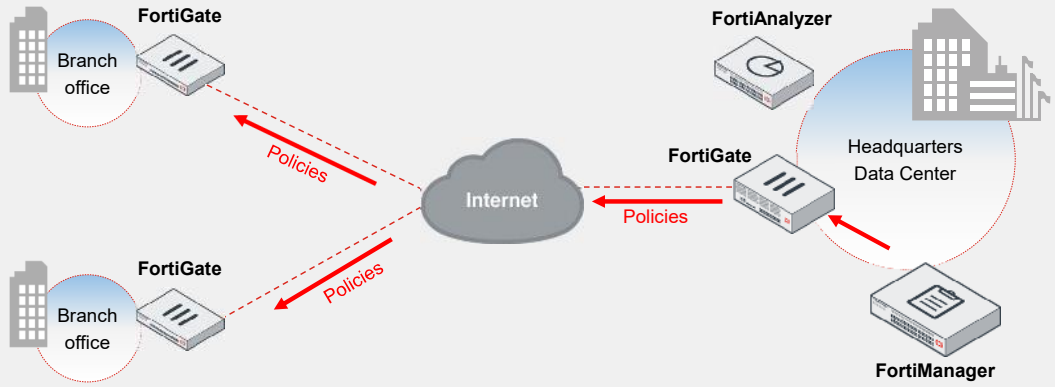
FortiManager provides automation-driven, centralized management of your Fortinet devices from a single console. Centralized management through FortiManager can help you to more easily manage many deployment types with many devices and reduce cost of operation.

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.
- Automate device provisioning and keep track of policy changes.

Key Features

- Centralized management
- Administrative domains (ADOM)
- Configuration revision control and tracking
- Local FortiGuard service
- Firmware management
- Scripting
- Pane managers – VPN, FortiAP, FortiSwitch, and Fabric View (Security Fabric)
- Logging and reporting
- Management extension applications (MEA)

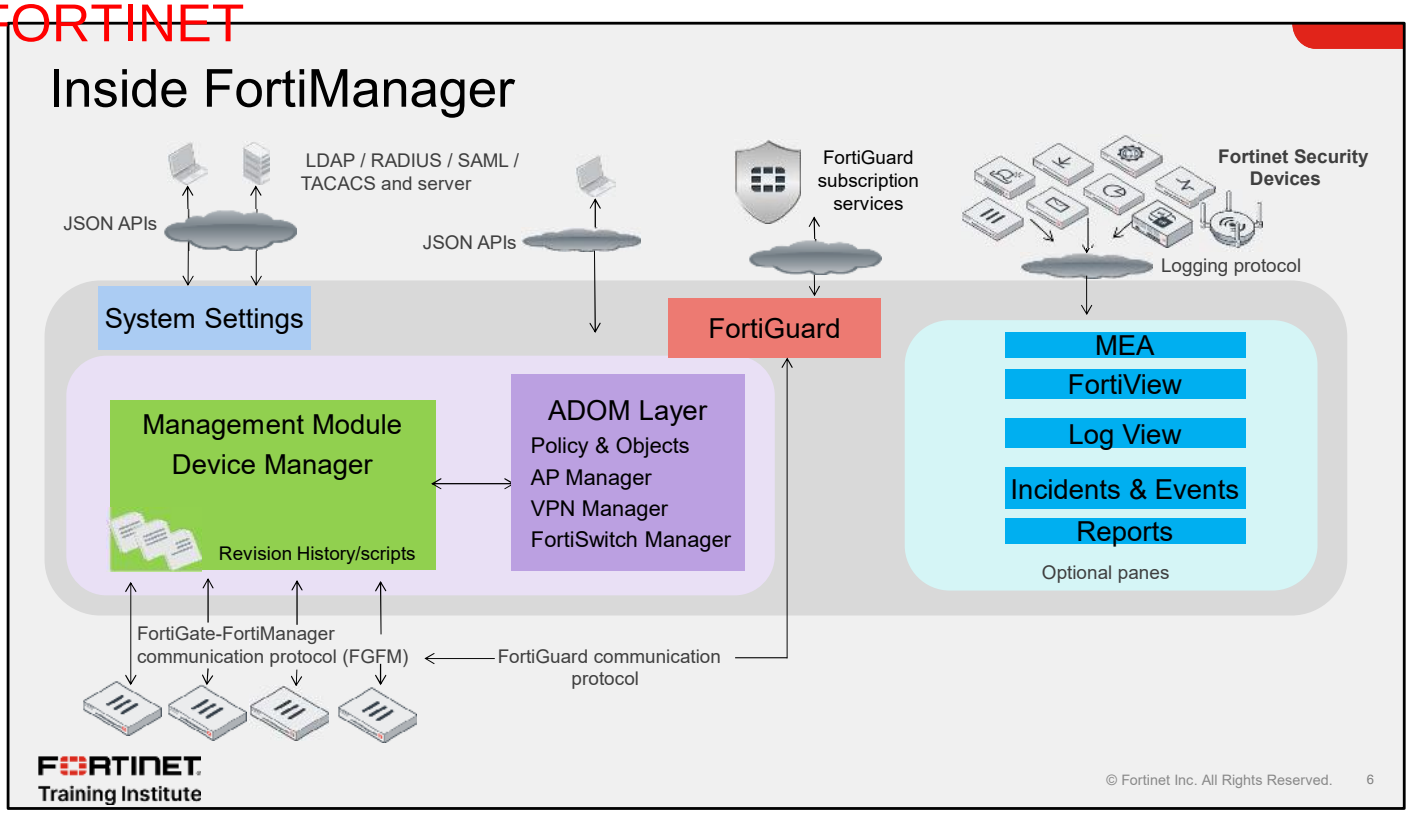


FORTINET Training Institute

 5

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 use, your managed devices can use FortiManager as a private FortiGuard server.
- Firmware management: FortiManager can schedule firmware upgrades for managed devices.
- Scripting: FortiManager supports CLI and Tool Command Language (Tcl)-based scripts to simplify configuration deployments.
- Manager panes (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.
- MEAs: allow you to enable licensed applications that are released and signed by Fortinet. The applications are installed and run on FortiManager as docker containers. Refer to the *Fortimanager Administrator Guide* for more details.



Inside FortiManager, there are several management layers that are represented as panes on the GUI.

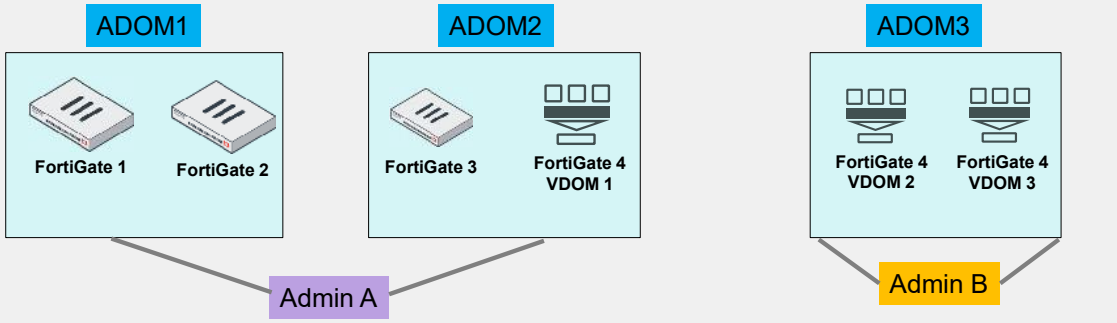
The default panes include:

- Device Manager: Add and authorize devices, create device configuration changes, and install device and policy packages.
- Policy & Objects: Centralize the management of firewall policies, objects, and security profiles, among others.
- VPN Manager: View and configure IPsec VPN and SSL VPN settings that you can install on one or more devices.
- AP Manager: Manage FortiAP access points (AP) that are controlled by FortiGate devices.
- FortiSwitch Manager: Manage FortiSwitch devices that are controlled by FortiGate devices.
- Extender Manager: Manage connected FortiExtenders.
- Fabric View: View Security Fabric ratings of configurations for FortiGate Security Fabric groups, as well as create Fabric connectors.
- FortiGuard: Provide FortiGuard services for FortiManager system and its managed devices and FortiClient agents.
- System Settings: Manage system options for FortiManager.

You can add other menus, depending on the requirements of your network, for example, when you add FortiAnalyzer features.

ADOMs

- ADOMs allow you to group devices logically for administrators to manage
  - A device is assigned to an ADOM and administrators are assigned to one or more ADOMs
- ADOMs can work in two device modes: normal or advanced.
  - In advanced mode, each FortiGate virtual domain (VDOM) can be assigned to a different ADOM
- Accounts with the **Super_User** profile can manage devices in all ADOMs



Admin A have access to ADOM1 and ADOM2

Admin B have access to ADOM3 which includes some VDOMs from FortiGate4

FORTINET Training Institute

 7

FortiManager administrators can use ADOMs to group devices logically, and then specify which administrators can manage them. For example, you can create an ADOM for each branch office, and then restrict administrators to manage devices only on their assigned branches.

ADOMs can be used in two device modes: normal or advanced. When advanced mode is enabled, you can assign different FortiGate VDOMs to different ADOMs.

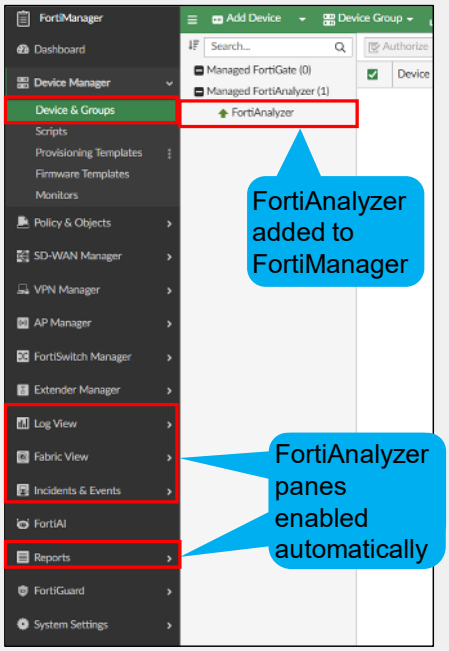
Administrator accounts can be tied to one or more ADOMs and can only manage those devices or VDOMs that belong to the ADOMs to which they are assigned.

Administrator accounts with the Super_User profile, such as the admin account, can manage all ADOMs and the devices within them.

Managing FortiAnalyzer

- You can add and then manage most FortiAnalyzer features from FortiManager
- Tasks that can be done from FortiManager include:
  - View logs and run reports on FortiAnalyzer
  - Manage incidents and events
- Recommended solution for dealing with a high volume of logs
  - Logs are stored on FortiAnalyzer, not FortiManager

You cannot enable advanced ADOM mode when FortiManager is managing FortiAnalyzer



FORTINET Training Institute

 8

You can add and then manage most FortiAnalyzer features from FortiManager. This is the recommended solution for environments with a high volume of logs.

After you add a FortiAnalyzer device, the following panes are enabled automatically on FortiManager:

- **FortiView** and **LogView**: provide visibility of FortiAnalyzer logs.
- **Incidents & Events**: allows you to manage FortiAnalyzer incidents, events, handlers, and work with the threat hunting tool and outbreak alerts,, when available.
- **Reports**: allow you to manage FortiAnalyzer reports.

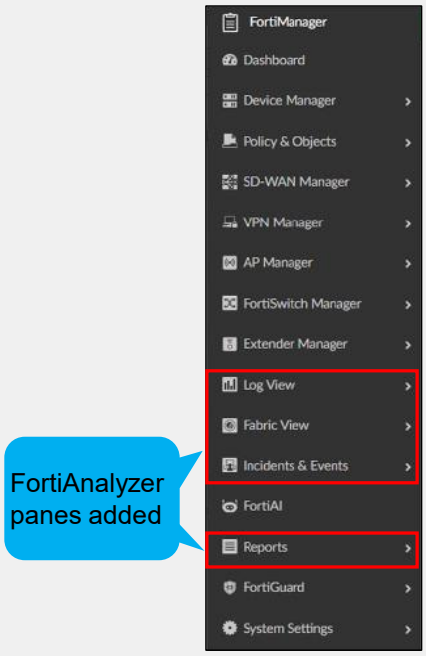
FortiManager can manage multiple FortiAnalyzer devices, but each FortiAnalyzer must be in its own ADOM. You can add the same FortiAnalyzer to more than one ADOM. When you do this, the FortiAnalyzer features and visibility in the ADOM are limited to the logging devices included in that ADOM.

Note that you cannot enable advanced ADOM mode when FortiManager is managing FortiAnalyzer. Advanced ADOM mode is discussed in this course.

FortiManager With FortiAnalyzer Features

- Enable FortiAnalyzer features manually to make FortiManager a logging and reporting device
  - More CPU, memory, and disk space are required for the additional functions
- Log rate and daily log quota restrictions are in place
  - FortiManager supports up to 150 logs per second only
  - FortiAnalyzer-related licensing is not stackable
- FortiManager stores and manages logs
- Solution feasible for low volume of logs only
  - For example, a testing environment

If FortiAnalyzer features are enabled, you cannot add FortiAnalyzer to FortiManager, and you cannot enable FortiManager high availability (HA)



FORTINET Training Institute

 9

FortiManager can act as a logging and reporting device for your network when you manually enable FortiAnalyzer features. Keep in mind that FortiManager requires additional resources (CPU, memory, disk space) to process and store logs and reports.

Additionally, logging rate restrictions considerably reduce the supported log rates compared to the capabilities of FortiAnalyzer. For example, the highest log rate FortiManager supports is 150 logs per second. However, FortiAnalyzer's lowest supported log rate is 500 logs per second, and it can reach 150,000 logs per second in high-end models.

Another restriction is that the licensing for FortiAnalyzer features is not stackable. For these reasons, this solution is feasible only for environments that have a low volume of logs. For example, it could be used for testing purposes. For high log volumes, you should use a dedicated FortiAnalyzer.

When you enable FortiAnalyzer features, all log and storage settings are configured on FortiManager. This means that you must specify how much disk space to use, and for how long to store the logs for each ADOM. You can monitor disk utilization for each ADOM and adjust storage settings for logs, as needed.

If FortiAnalyzer features are enabled, you cannot add FortiAnalyzer to FortiManager. You will also not be able to configure FortiManager HA.

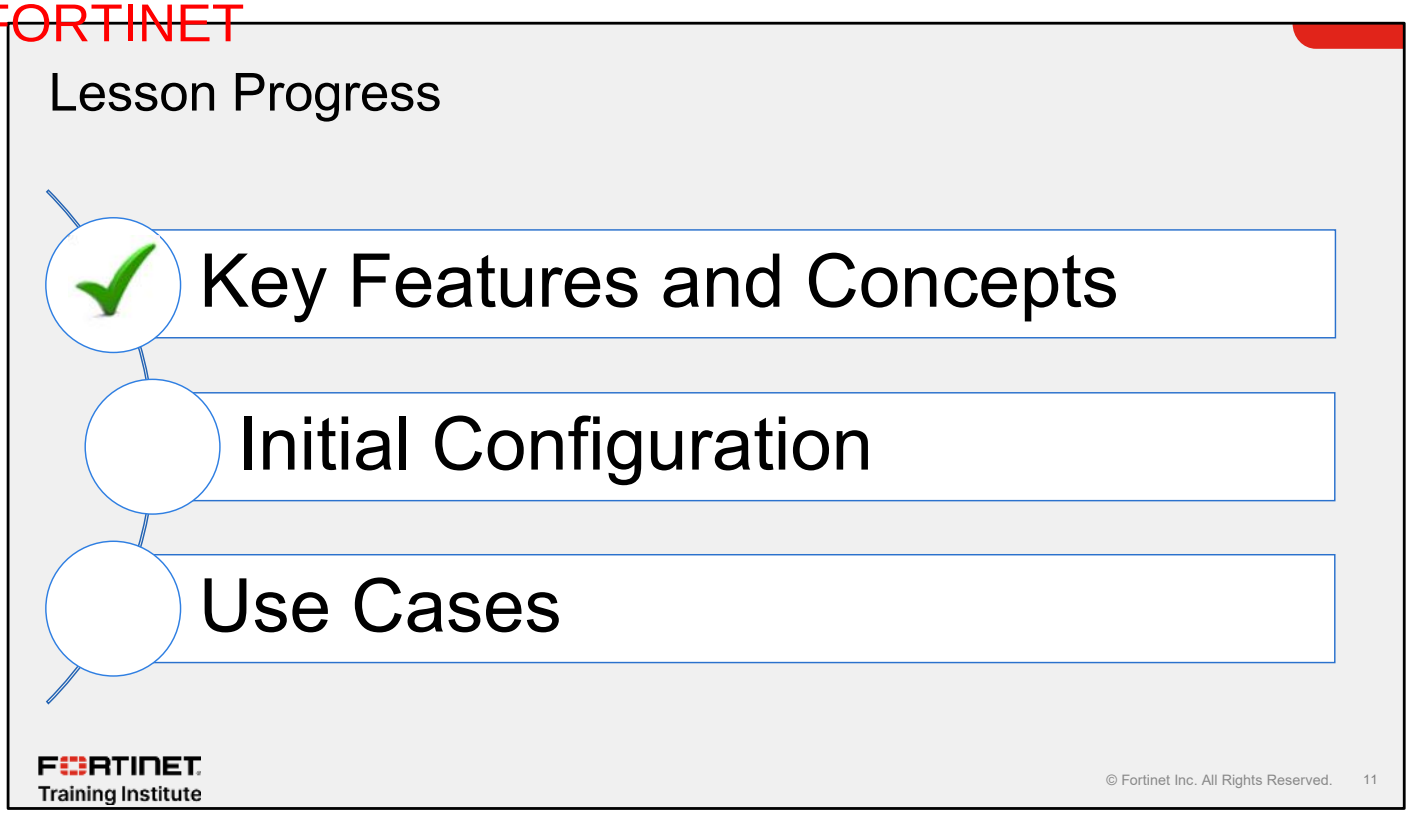
Knowledge Check

1. Which solution should you use in environments with a high volume of logs?
   - A. Enable FortiAnalyzer features manually on FortiManager.
   - ✓ B. Add and manage FortiAnalyzer from FortiManager.

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

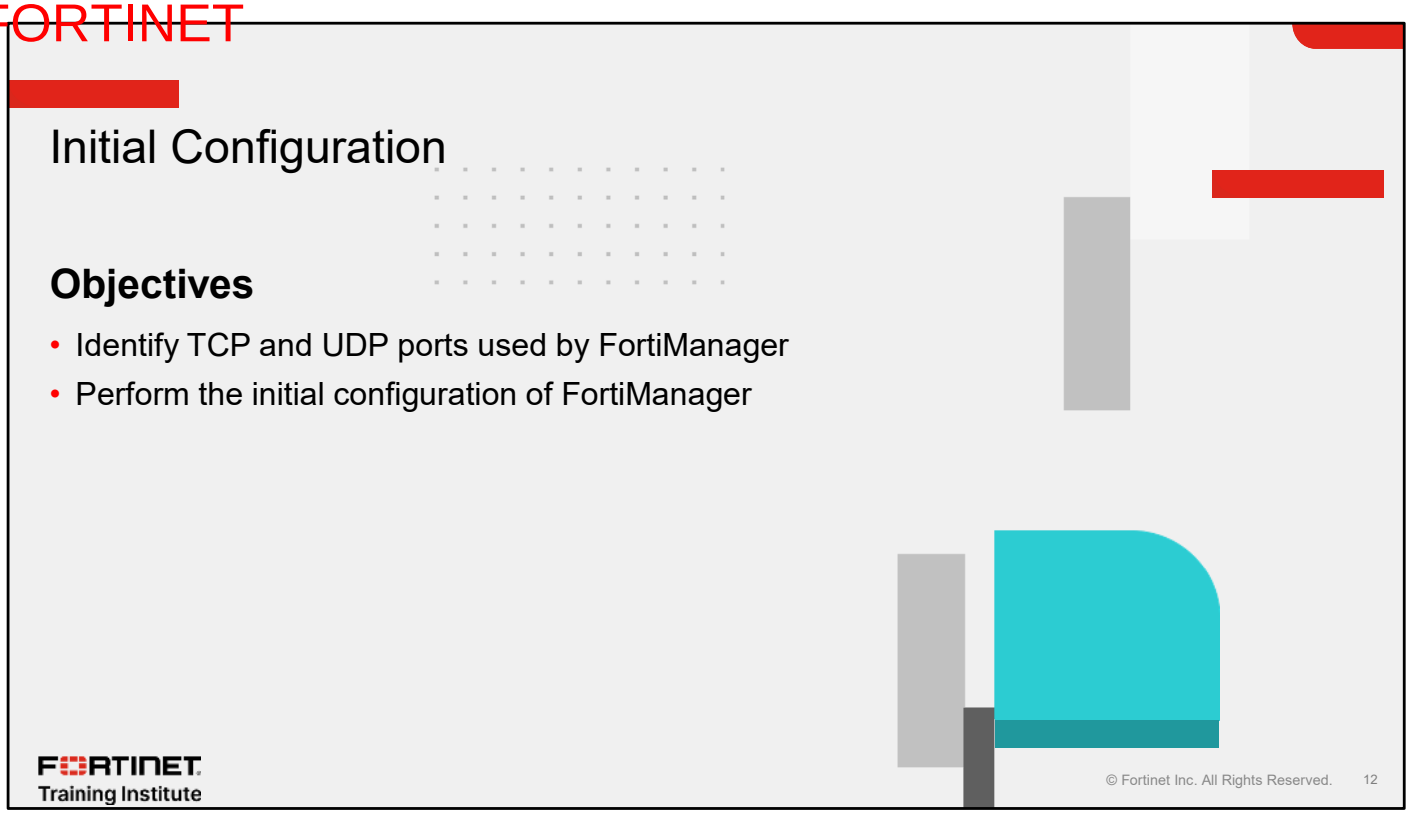
FORTINET Training Institute

 10



Good job! You now understand FortiManager key features and concepts.

Now, you will learn how to initially configure FortiManager.

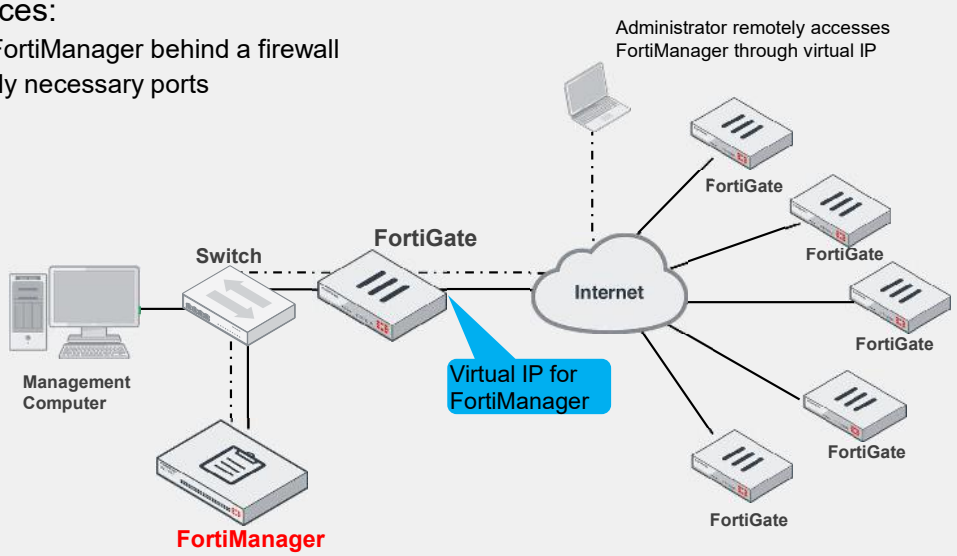


After completing this section, you should be able to achieve the objectives shown on this slide.

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

FortiManager Placement and Connectivity

- Best practices:
  - Deploy FortiManager behind a firewall
  - Allow only necessary ports



FORTINET Training Institute

 13

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. If administrators or remote FortiGate devices will make inbound connections to FortiManager from outside your local network, such as from the internet, create a virtual IP (VIP).

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

FortiManager Ports Used to Manage FortiGate

- FortiManager uses many ports to perform its functions
- Knowing which ports FortiManager uses helps when troubleshooting FortiManager network issues
- The table below shows the ports FortiManager uses to manage FortiGate devices
  - FortiManager uses the entries marked with an asterisk only when it acts as a local FortiGuard server

Functionality	Protocol and Port(s)
Incoming ports	
Web filter queries, antivirus, and IPS updates*	UDP 53, UDP/TCP 8888, TCP 80
Antispam*	UDP/TCP 8889
Registration for license validation and UTM updates (antivirus, IPS)*	TCP 8890, TCP 443
FortiGuard and FortiClient web filter and email filter*	TCP 8900, TCP 443
Outgoing ports	
Antivirus and IPS push updates*	UDP 9443
Incoming and outgoing ports	
FGFM management	TCP 541 (IPv4), TCP 542 (IPv6)

* Used only when FortiManager acts as a local FortiGuard server

FORTINET Training Institute

 14

Knowing which ports FortiManager uses can help you analyze, diagnose, and resolve common network issues. This is especially true if FortiManager is deployed behind a firewall.

FortiManager uses many TCP and UDP ports to perform tasks. The table on this slide includes some of the ports that FortiManager uses to manage FortiGate devices. Visit `https://docs.fortinet.com` to see the complete list of ports.

By default, the standard management ports are:

- HTTP: port 80 (TCP)
- HTTPS: port 443 (TCP)
- SSH: port 22 (TCP)

Security Recommendations

- Deploy FortiManager in a protected and trusted private network
- Use secure communication, even in a private network (HTTPS or SSH)
- Configure trusted hosts
- If access from the outside is required:
  - Open only the ports necessary for secure communications
  - Set up special users and use only secure protocols (HTTPS/SSH)
- Use secure passwords and the password policy feature
- Check event logs frequently
- Configure the external syslog and email servers for quick notifications

FORTINET Training Institute

 15

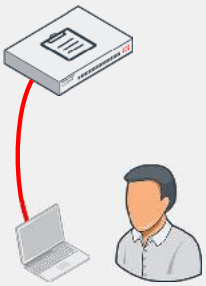
FortiManager manages all your Fortinet network security devices, so it is vital that you secure and protect FortiManager and FortiManager data.

Here are some security recommendations:

- Deploy FortiManager in a protected and trusted private network. You should never deploy directly on the internet.
- Always use secure connection methods for management: HTTPS for web-based management or SSH for CLI management. Fortinet strongly discourages using insecure methods like HTTP.
- Use trusted hosts to allow logins only from specific locations.
- If you must open outside access to the device so that remote devices can connect, open only the required ports. If you must open direct login access from the outside, you must set up dedicated user accounts for this purpose.
- Use secure, strong passwords and a password policy to enforce their use.
- You can enable and configure the 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.
  - **Expiration**: Specify the number of days a password is valid for. When the time expires, the administrator is prompted to enter a new password.
- Check event logs frequently.
- Configure the external syslog and email servers for quick notifications.

Factory Default Settings

- Use factory default settings to initially log in to FortiManager and begin your own network configuration.



- Default settings:
  - Port 1 is the default management port:
    - Port1 interface IP: `192.168.1.99/24`
    - HTTPS and SSH protocols are enabled for management access
    - Username: `admin`
    - Password: (blank)
    - You will be prompted to set a new password

- If you are deploying FortiManager VM in the cloud, the management IP address and its assignment depends on the provider you use

FORTINET Training Institute

 16

It is important to know the factory default settings, such as the default username and password, the IP address of port1, netmask, and default supported management access protocols, so that you can initially connect and configure FortiManager for your network.

Different FortiManager models have different numbers of ports, but port1 is the management port and will always have the IP address `192.168.1.99` configured by default.

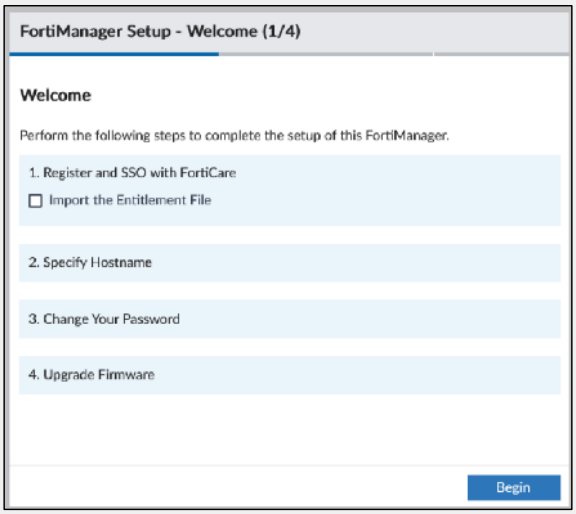
If you are deploying a FortiManager in the cloud, the management IP address and its assignment depend on the cloud provider you use.

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 username *`admin`* and a blank password.

After you log in for the first time, the **FortiManager Setup wizard** opens.

FortiManager Setup Wizard

- When you first access FortiManager, The **FortiManager Setup** wizard opens
- The **FortiManager Setup** wizard lets you perform the following actions:
  - Register and enable SSO with FortiCare (required step)
    - Or import entitlement file
  - Specify a host name
  - Change your password
  - Upgrade the firmware



FORTINET Training Institute

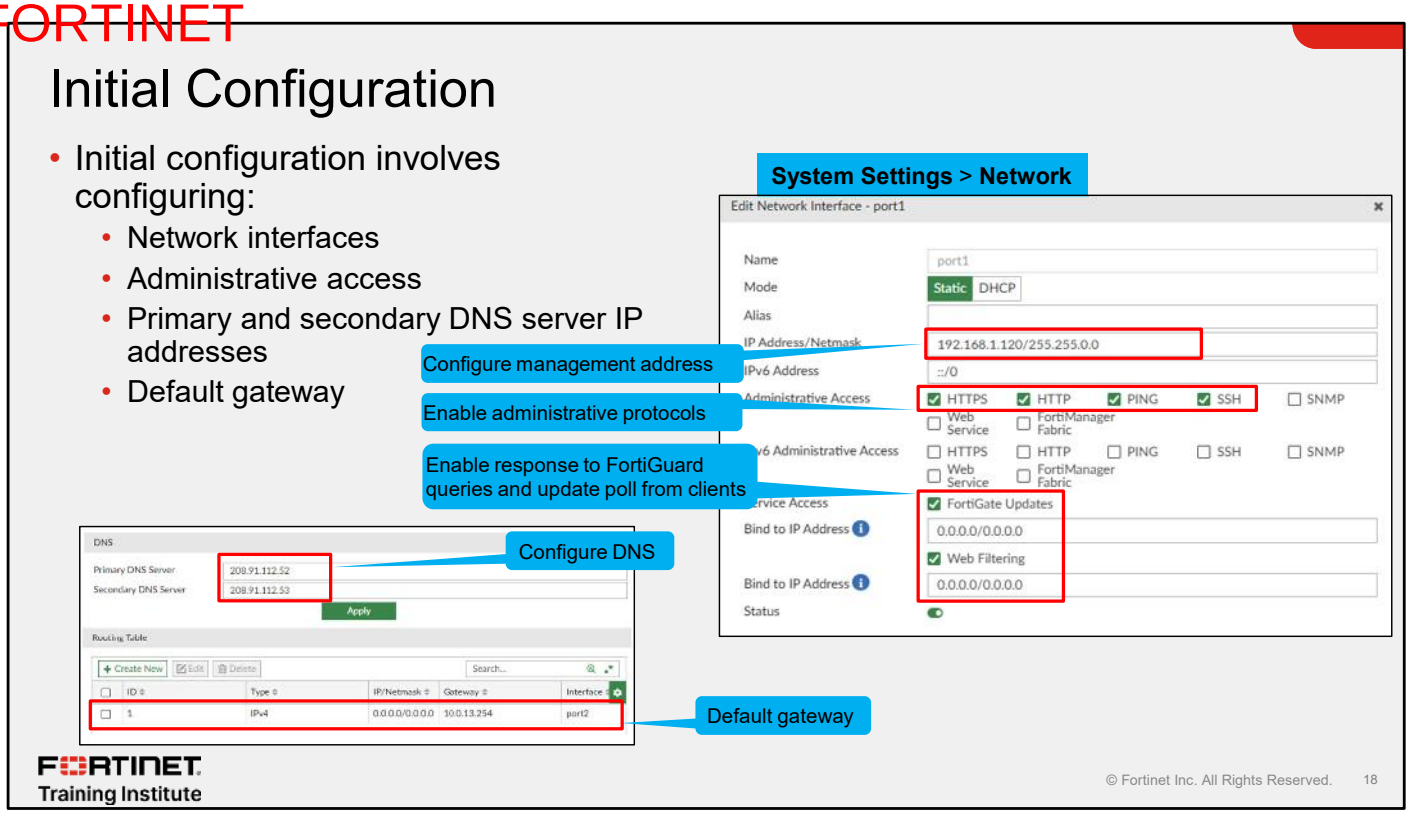
 17

When you log in to FortiManager for the first time, the **FortiManager Setup** wizard opens to help you set up FortiManager by performing the following actions:

- Register with FortiCare and enable FortiCare single sign-on (SSO).
- Specify a host name.
- Change your password.
- Upgrade the firmware.

The **FortiManager Setup** wizard requires that you complete the **Register and SSO** *with FortiCare* step before you can access FortiManager . This step requires internet access, unless FortiManager is operating in a closed network, in which case, you must request account entitlement files from Fortinet Customer Service and Support, and then upload the files using this wizard, or later from the FortiGuard pane.

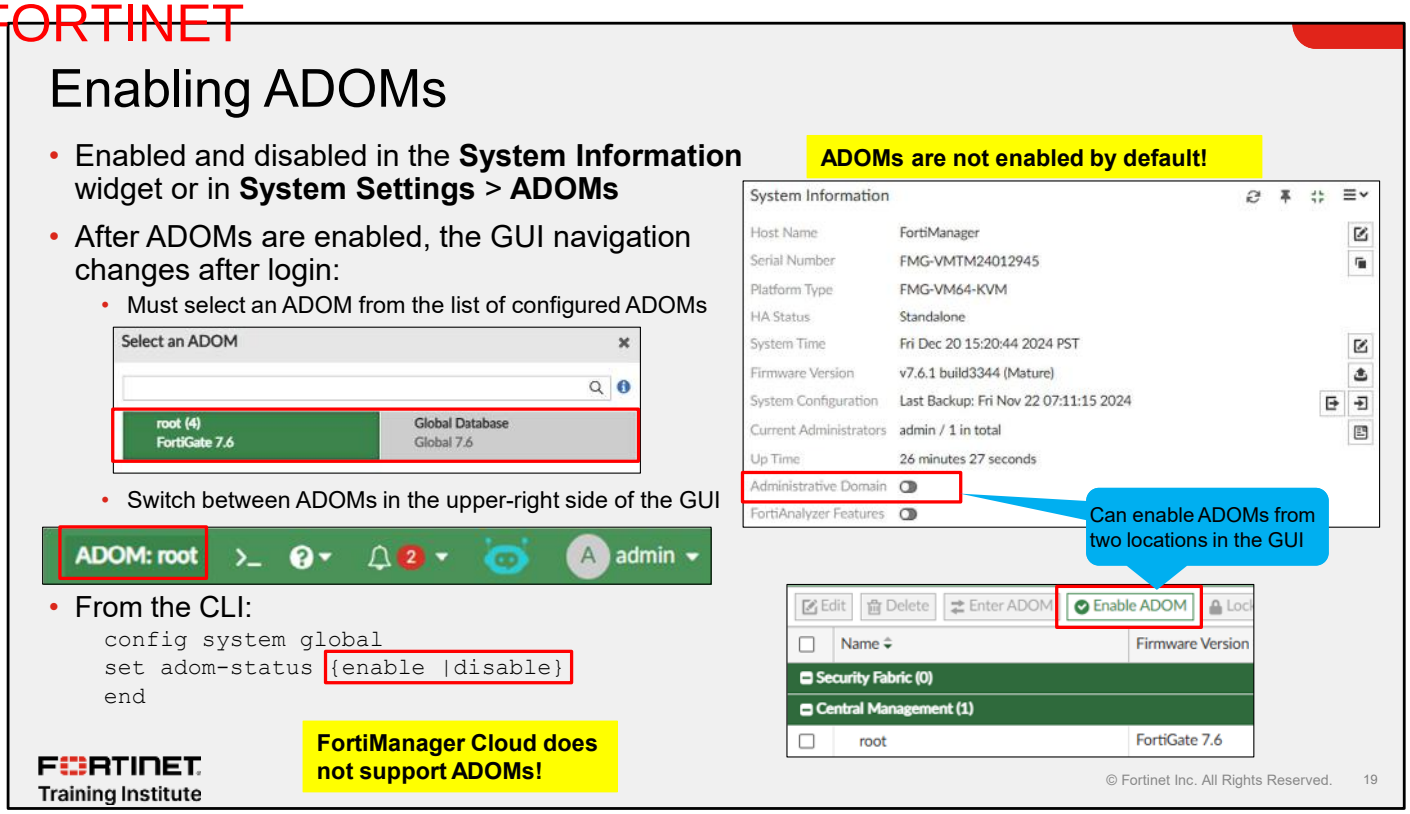
After you complete all of the steps in the wizard, the wizard no longer opens when you log in to FortiManager.



The initial configuration of FortiManager is very similar to FortiGate. To configure FortiManager for your network, you must set the IP address and netmask, select supported administrative access protocols, and specify a default gateway. 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 accordingly. The IP address must be a unique static IP address. Additionally, enter the IP address of the next hop router, and specify your DNS servers. By default, FortiGuard DNS servers are configured in the **DNS** window, to help guarantee connectivity for FortiGuard downloads and queries. However, 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 each interface. This includes FortiGate updates and web filtering. By default, all services to managed devices are enabled on port1 and disabled on other ports.



ADOMs are not enabled by default and can be enabled (or disabled) only by an administrator that has the Super_User profile.

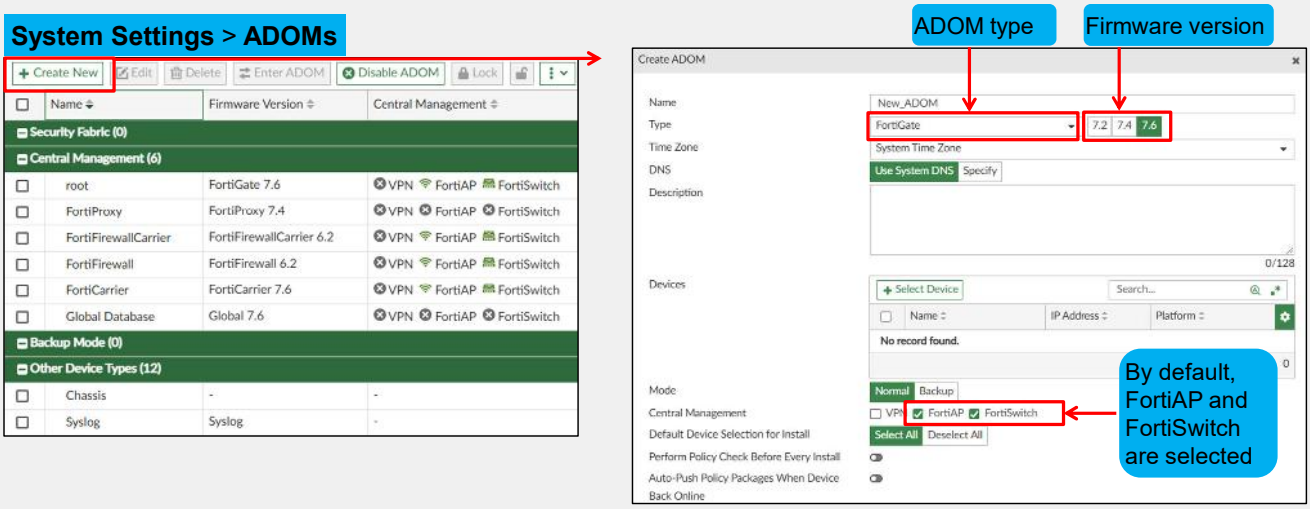
After you change the ADOM mode, the system logs you out so the it can reinitialize with the new settings. When you log in with ADOMs enabled, you must select the ADOM you want to manage from the list of configured ADOMs. You can easily switch between ADOMs by clicking the ADOM list on the upper-right side of the GUI.

The maximum number of ADOMs varies by FortiManager model or VM license.

FortiManager cloud does not support ADOMs. For more information, see the *Limitations of FortiManager Cloud* document in the **FortiManager Cloud** section at www.docs.fortinet.com.

Creating ADOMs

- You can create a new ADOM in **System Settings** > **ADOMs**
  - Visible to administrators with the Super_User profile



FORTINET Training Institute

 20

With ADOMs enabled, administrators with the Super_User profile have access to the **ADOMs** page, where all default ADOMs and custom ADOMs created by the administrator appear.

If the default ADOMs do not fit your requirements, you can create your own.

The ADOM type you create *must match* the device type you are adding later. For example, if you want to create an ADOM for FortiGate devices, you must select **FortiGate** as the ADOM type. The exception to this rule is the **Fabric** type, which allows you to add FortiGate devices and other types of devices. Additionally, you must select the firmware version for each new ADOM. This is because different firmware versions have different features, and therefore may use different CLI syntax. Your ADOM settings must match the device firmware.

The default ADOM operation 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.

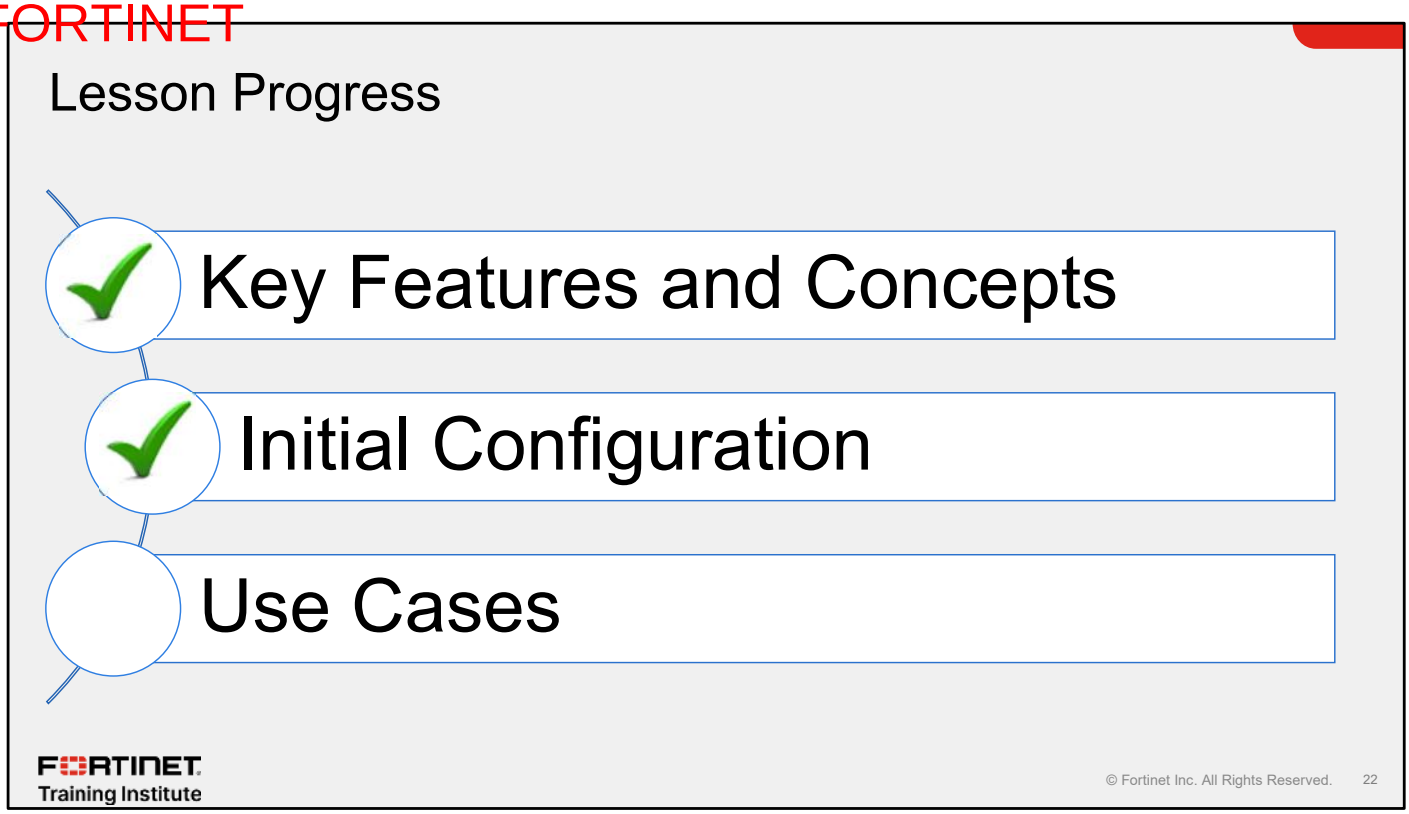
Knowledge Check

1. Which service access can you enable on a FortiManager interface?
   - ✓A. FortiGuard updates and web filtering
   - B. FortiSwitch and FortiAP

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

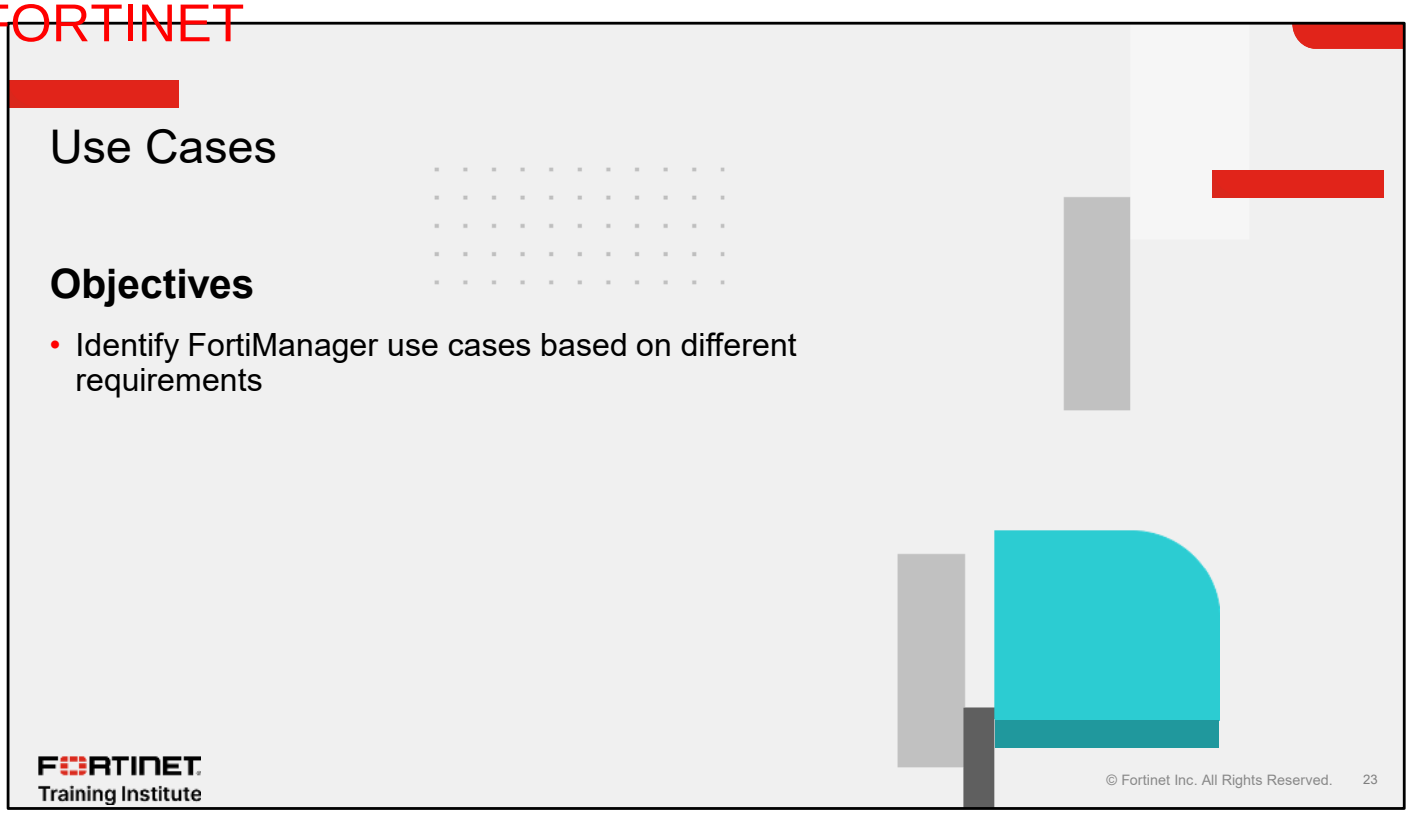
FORTINET Training Institute

 21



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

Now, you will learn about some use cases for FortiManager based on different organizations.



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

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

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

 24

One common FortiManager use case is managing large retail customers or distributed enterprises. These types of organizations often have many smaller customer premises equipment (CPE) devices in their branches, along with remote sites and multiple main locations. 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 drive or copy and pastes into the console. This basic configuration allows FortiGate to contact FortiManager, where the administrator can add that FortiGate to the appropriate device group or ADOM, and then send the full configuration to that FortiGate.

Use Case—MSSP

- Management of customer devices
- Characteristics:
  - Many smaller CPE devices or customer VDOMs on a large firewall platform in the data center
  - Customers typically have read-only access to their firewalls/VDOMs 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

 25

Another common use case involves Managed Security Service Providers (MSSP).

Carriers often have many powerful firewalls and require strict configuration control, which is achievable by restricting configuration from 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 difficult to understand and troubleshoot. So, periodically cleaning up orphan configuration objects is beneficial.

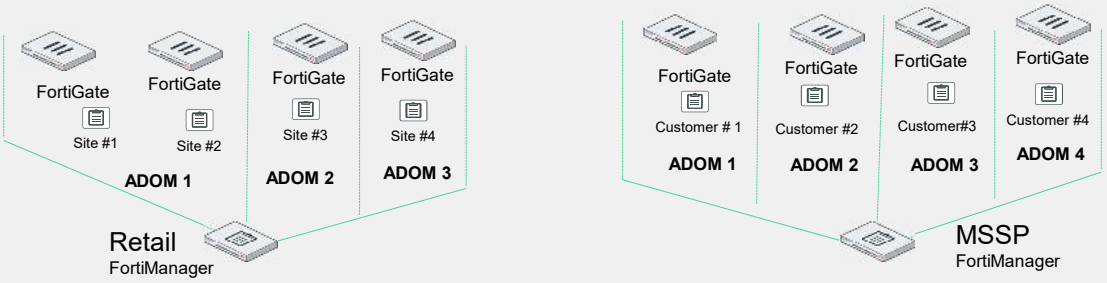
FortiManager allows MSSPs to avoid the overhead of perpetual licenses using the Fortinet VM On-Demand Program with auto scaling. When an auto-scale event is triggered, the public cloud platform launches a new FortiGate-VM that appears automatically on FortiManager as an authorized device in the Device Manager. When a scale-in event occurs, the device is automatically removed from FortiManager.

Requirements for Different Organizations

ADOMs and policy package structure varies by use case

- Use case—Retail
  - Single ADOM with one policy package for all devices

  or
  - Single or multiple ADOMs with multiple policy packages
- Use case—MSSP
  - Each customer has one or more dedicated ADOMs



FORTINET Training Institute

 26

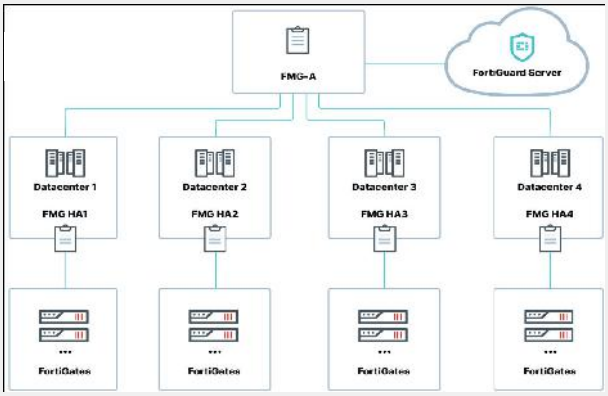
Organizations may use FortiManager ADOMs and policy packages differently.

In a retail organization, you may see a single ADOM with many FortiGate devices, or multiple ADOMs with one FortiGate each. In the case of MSSPs, each customer's FortiGate devices are placed in their dedicated ADOM.

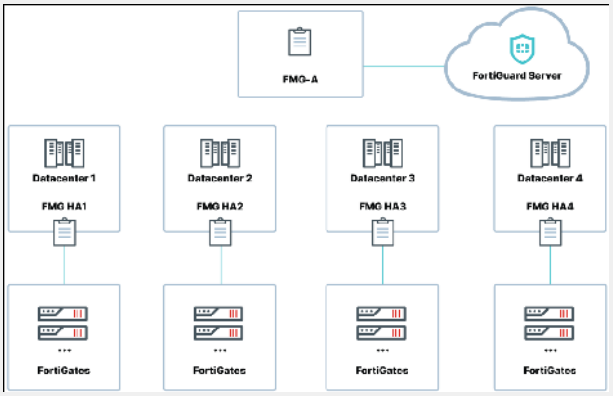
In this lesson, you will learn the practical skills necessary to manage devices for diverse organizations.

Closed Network Topologies

- Cascade mode
  - Only FMG-A has internet access and downloads the updates from FortiGuard
  - Other FortiManager devices download the updates directly from FMG-A



- Air gap mode
  - Only FMG-A has internet access and downloads the updates from FortiGuard
  - There is no connection between FMG-A and the other FortiManager devices
  - FMG-A exports the downloaded packages
  - Other FortiManager devices import the packages



FORTINET Training Institute

 27

You can operate FortiManager as a local FortiGuard Distribution Service (FDS) server for managed devices with no internet connectivity.

More complex scenarios may require the use of several FortiManager devices. This slide illustrates two possible topologies that can be used in such scenarios.

In both examples, only one FortiManager is connected to internet, and it downloading the updates from FortiGuard. There are two modes for distributing the FortiGuard updates from FortiManager to the rest of the devices:

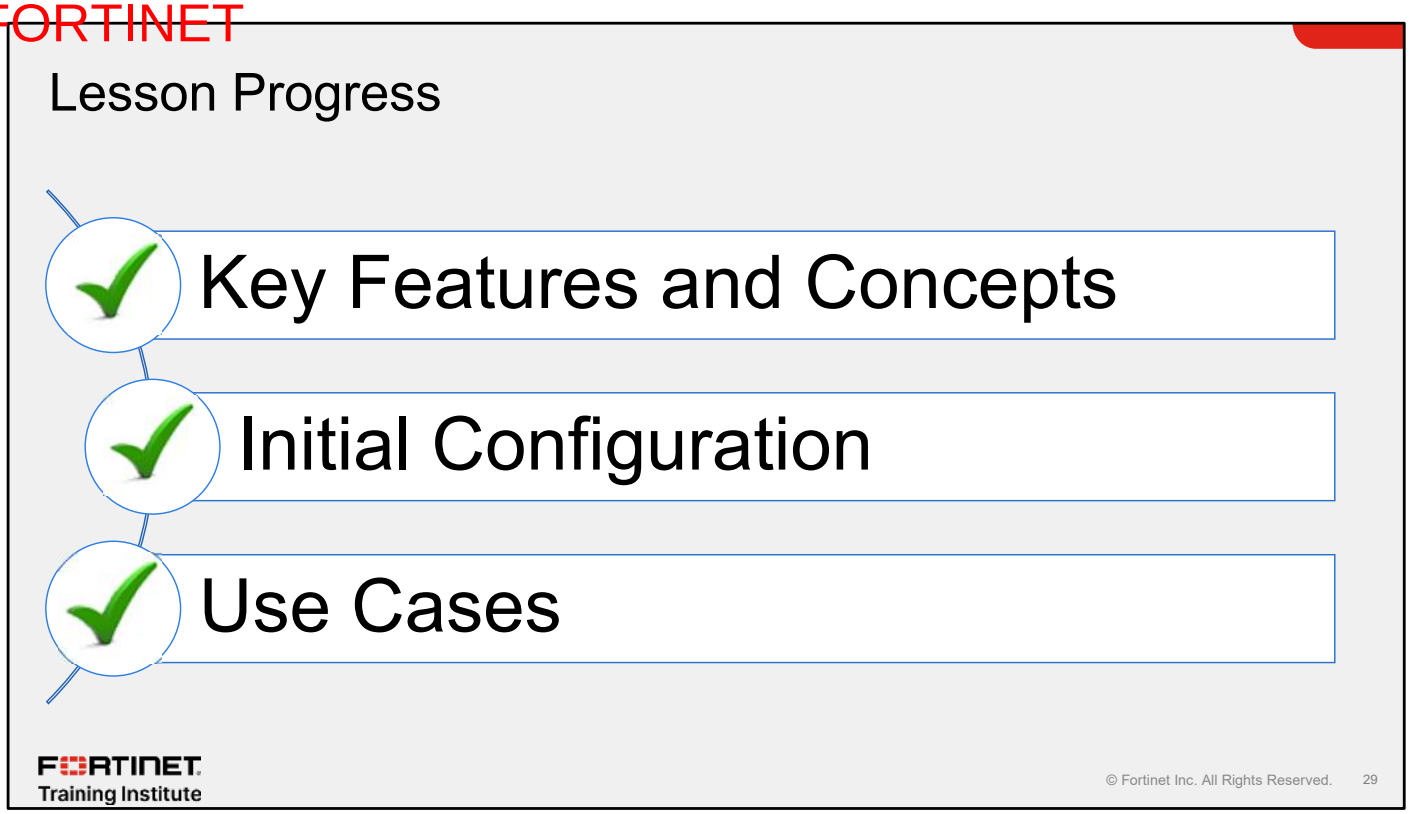
- Cascade mode: The main FortiManager device is connected to the other devices, and they download the updates directly from the main FortiManager device. FortiGate devices can then download the updates from their associated FortiManager device.
- Air gap mode: There is no connection between the main FortiManager device and the rest of the devices, so the downloaded packages must be exported and then imported into the other FortiManager devices. FortiGate devices can then download the updates from their associated FortiManager.

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.

FORTINET Training Institute

 28



Congratulations! You have completed this lesson. Now, you will review the objectives that you covered in this lesson.

Review

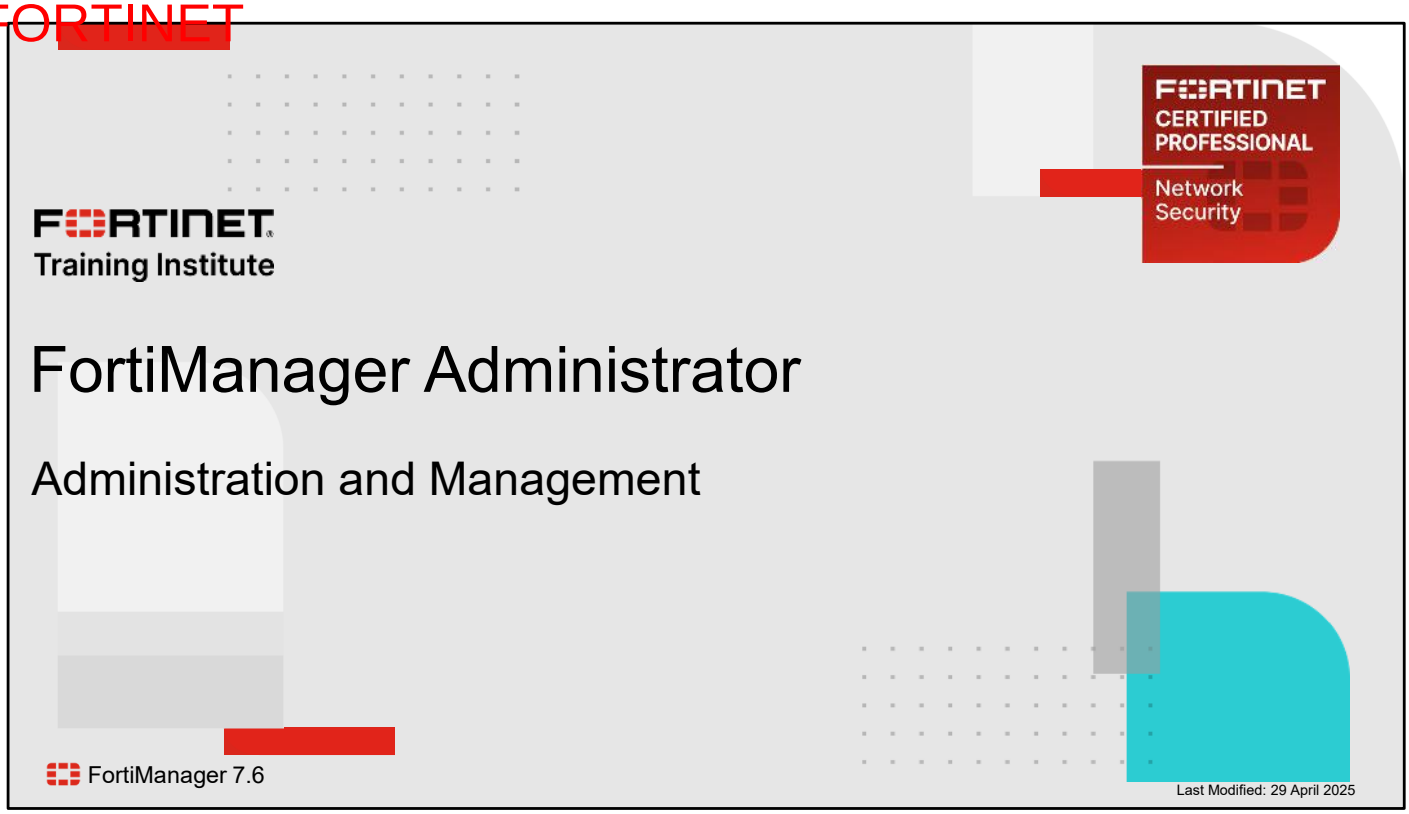
- ✓ Describe the purpose of FortiManager and its key features
- ✓ Describe the management module framework
- ✓ Describe the management task cycle
- ✓ Identify TCP and UDP ports used by FortiManager
- ✓ Perform the initial configuration of FortiManager
- ✓ Identify FortiManager use cases based on different requirements

FORTINET Training Institute

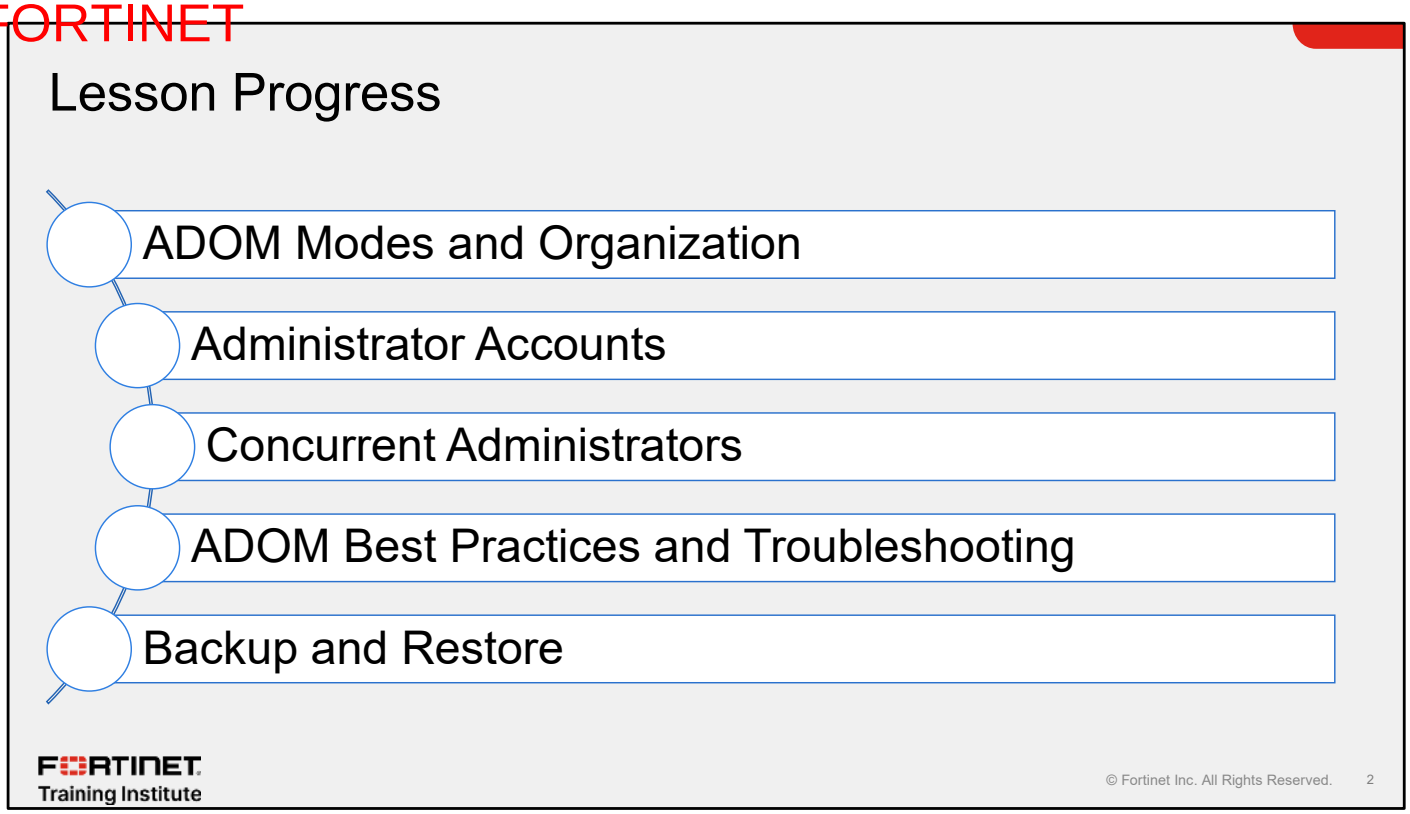
 30

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

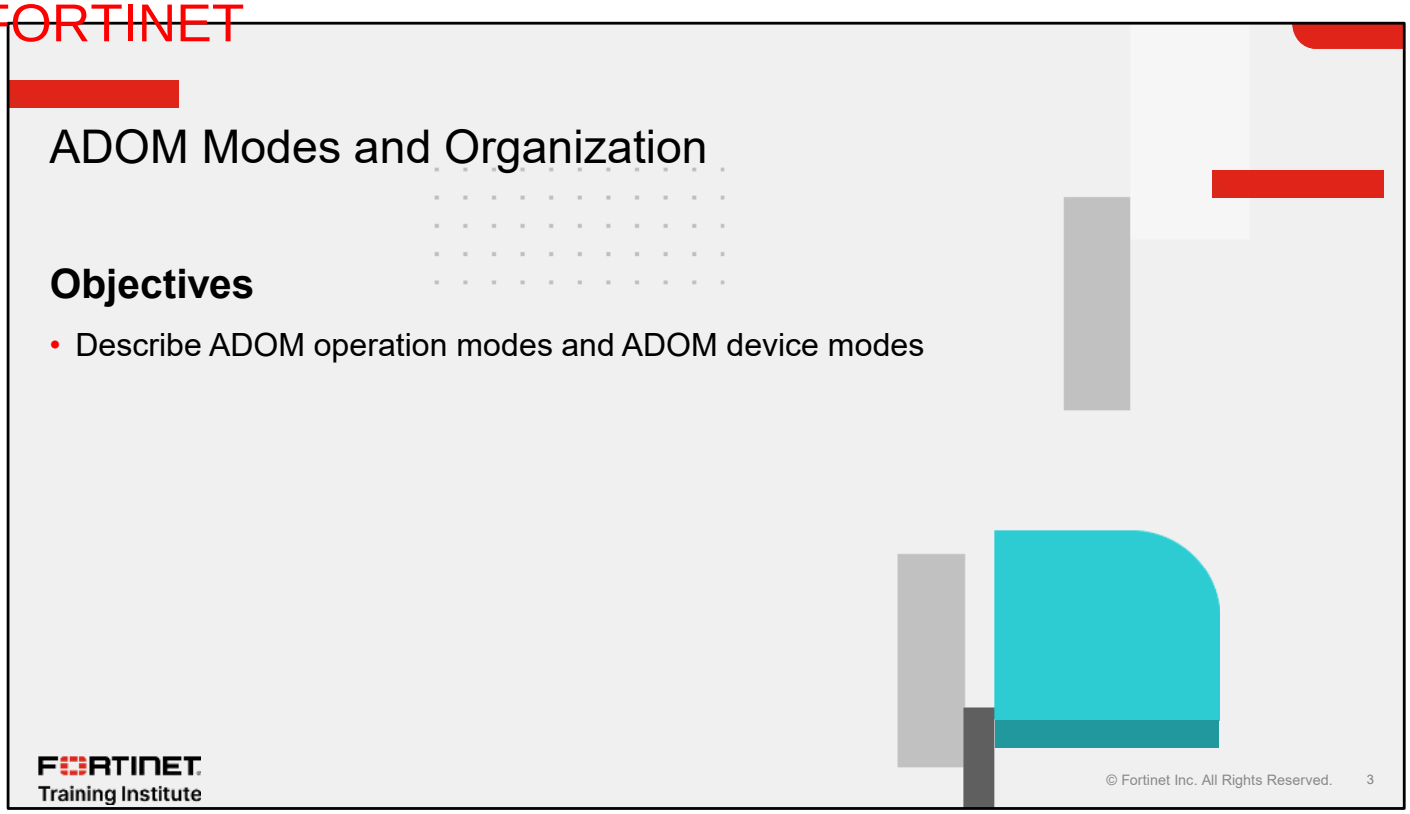
By mastering the objectives covered in this lesson, you learned the basics of FortiManager and how to use it in your network.



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 ADOM locks, administrative access controls, and configuration backup and restore.



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



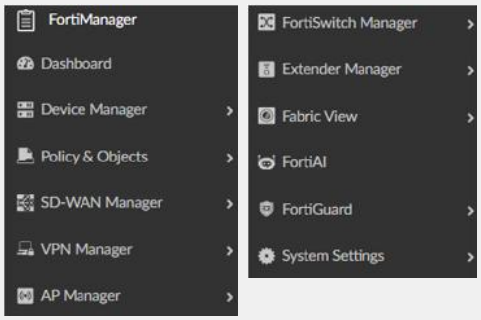
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in administrative domains (ADOM), you will be able to organize FortiGate devices effectively within FortiManager.

ADOM Operation Modes

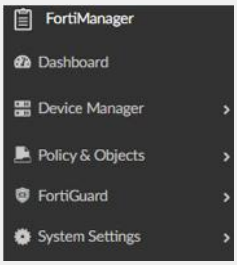
Normal mode:

- Default mode
- ADOM is *read/write*
- All management panes available
- Can make configuration changes to ADOMs and managed devices



Backup mode:

- ADOM is read-only
- Not all management panes available
- Must make changes directly on managed devices
- Only scripts can be used to make changes from FortiManager to the managed devices



Do not confuse ADOM normal operation mode with normal device mode!

FORTINET Training Institute

 4

When you create or configure ADOMs, you can choose between two operation modes: normal or backup.

By default, ADOMs run in normal operation mode which keeps all management panes available. An ADOM in normal operation mode 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 to each managed device through the FortiGate CLI or GUI.

You can configure ADOMs in backup operation mode if all configuration changes must be done directly on the managed devices and you want to use FortiManager only for revision control and tracking purposes.

When in backup operation mode, an ADOM is *read-only*, and some management options are not available while others are restricted. For example, in the **Device Manager** pane, you can add and delete devices, but the device-level settings are not available for configuration and installation.

In backup operation 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, but they 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.

To make configuration changes from FortiManager to managed devices while in backup mode, you must use the script feature. Additionally, if you make changes directly on the managed device, those changes need to meet specific conditions for the device to send the configuration revision to FortiManager. For example, if you make a configuration change, and then you log out of or reboot the device, a configuration revision is sent.

ADOM Device Modes

- ADOMs have two device modes: Normal (default) and Advanced
  - **System Settings** > **Advanced** > **Misc Settings**

Default device mode: **Normal**

- Normal
  - You can add a FortiGate device and its VDOMs to a single ADOM only
- Advanced
  - You can assign different VDOMs from the same FortiGate to different ADOMs
  - Applies globally to all ADOMs

Do not confuse ADOMs Normal operation mode with Normal device mode!

FORTINET Training Institute

 5

An ADOM can work in 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.

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 complex management scenarios, and it is recommended for advanced users only.

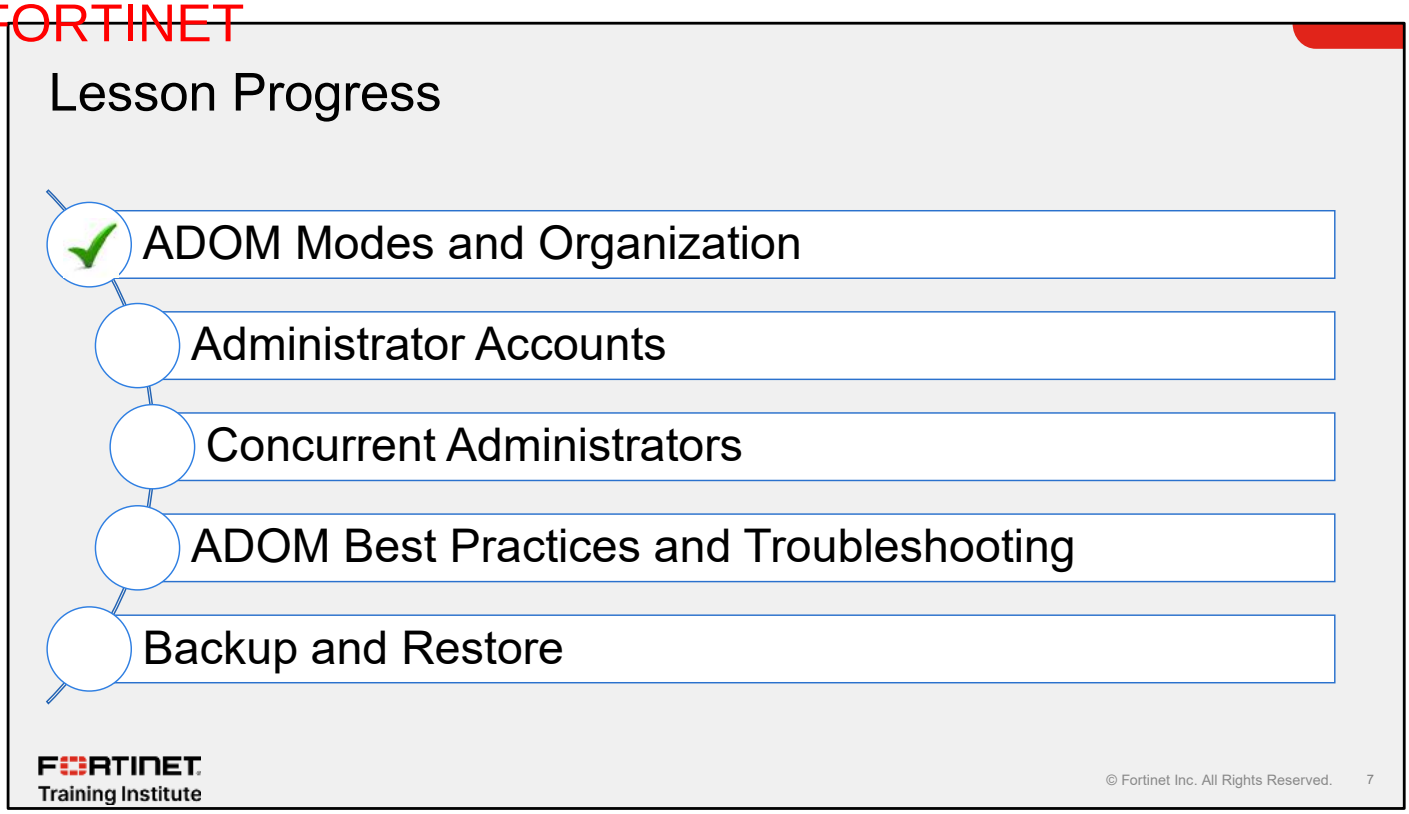
Knowledge Check

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.

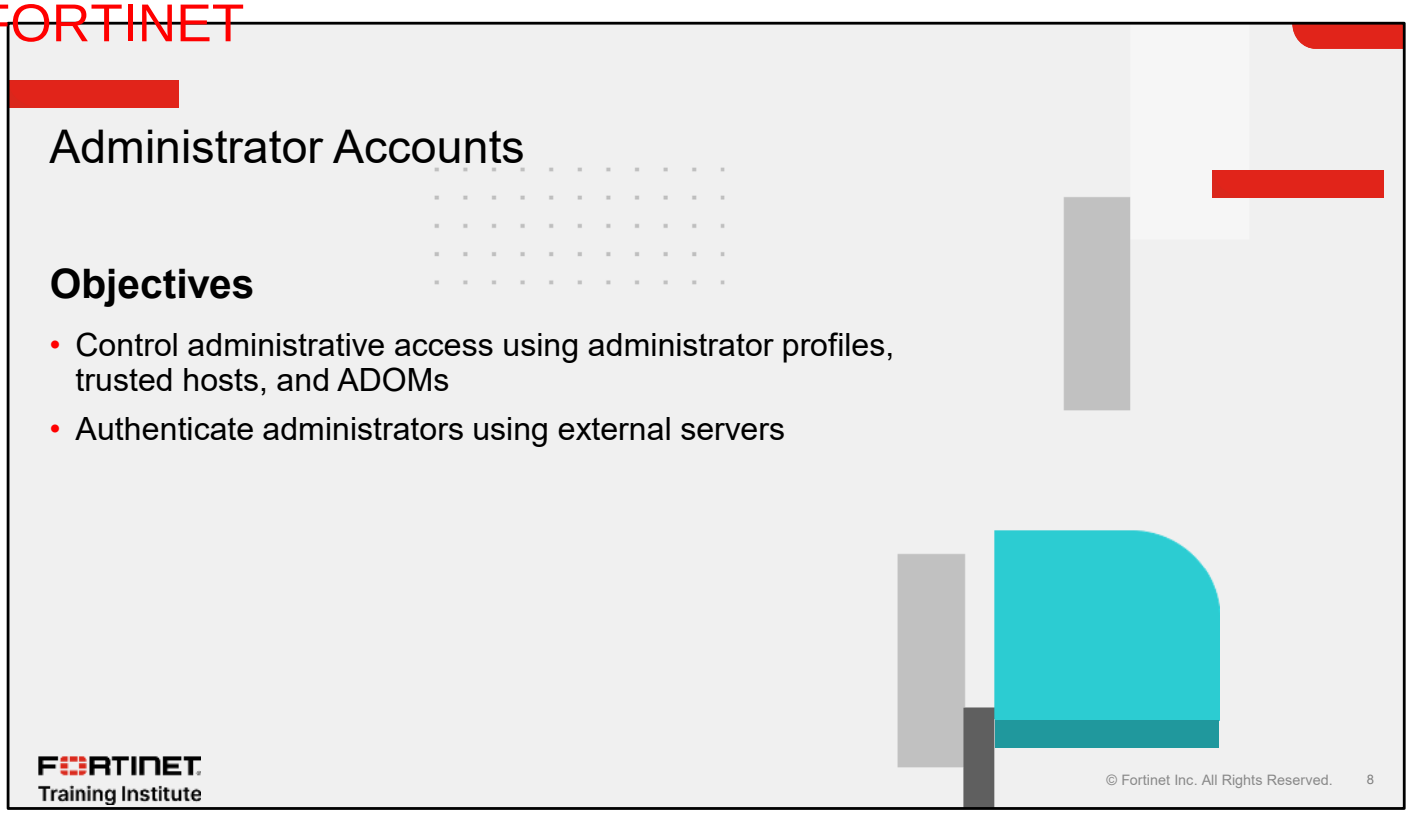
FORTINET Training Institute

 6



Good job! You now understand ADOMs.

Now, you will learn about administrator accounts on FortiManager.



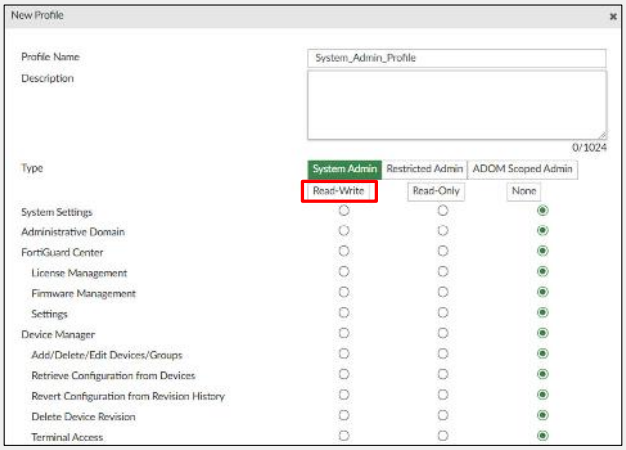
After completing this section, you should be able to achieve the objectives shown on this slide.

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.

Types of Administrator Profiles

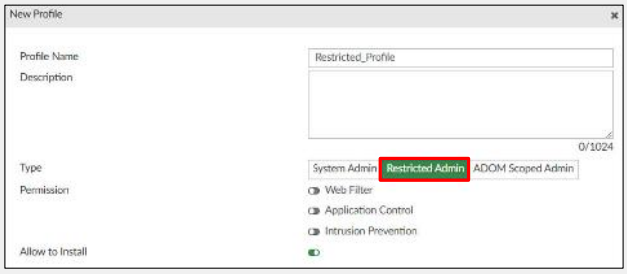
System Admin

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



Restricted Admin

- 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

 9

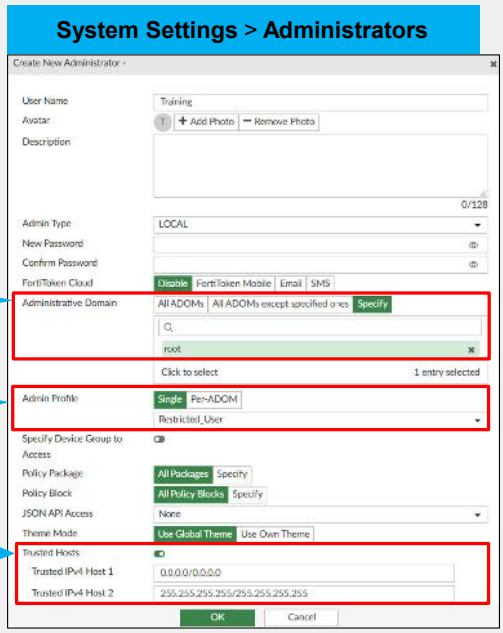
You can configure administrator profiles in one of two types: **System Admin** and **Restricted Admin**. Only administrators with full system permissions can modify administrator profiles.

For the **System Admin** type, you can modify one of the predefined profiles, or create a new custom profile. 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.

Profiles with the **Restricted Admin** type allows you to delegate administrators the management of web filtering profile, IPS sensors, and application sensor associated with their ADOM. When a restricted administrator logs in to the FortiManager, they enter the **Restricted Admin Mode**.

Multiple Administrators and Security

- You can divide administrative tasks among multiple employees by creating additional administrator accounts
- Several methods to control administrator access
- Most used access control methods are:
  - ADOMs
  - Administrative profiles
  - Trusted hosts



FORTINET Training Institute

 10

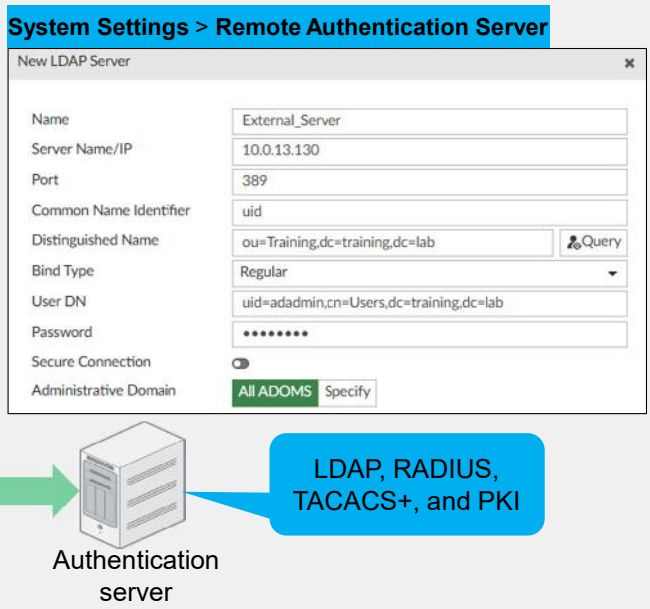
Depending on your deployment, you may want to divide FortiManager administrative tasks among multiple employees by creating additional administrator accounts.

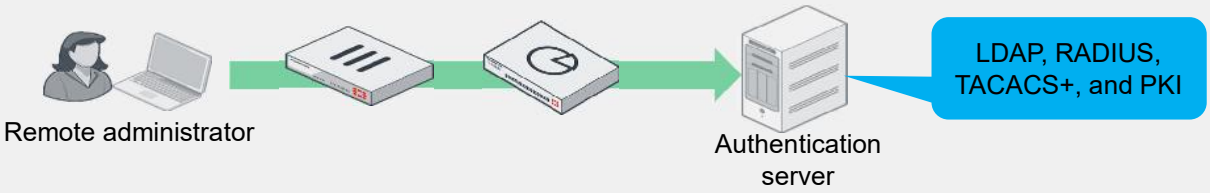
You can control and restrict administrator access using several methods, but the following are the most used:

- ADOMs: Administrators have access to only those ADOMs to which they are assigned.
- Administrative profiles: The level of access is determined by the administrative profile selected. When the administrators are restricted to specific ADOMs, you can assign different profiles for each ADOM, or the same profile for all ADOMs.
- Trusted hosts: This option restricts administrators to log in only from specific IP addresses or subnets. The trusted hosts you define apply to both the GUI and the CLI when accessed through SSH. This feature is available for IPv4 and IPv6 addresses.

External Validation of Non-Local Administrator Logins

- You can configure external servers to validate your administrator logins (non-local users)
  - LDAP, RADIUS, TACACS+, and PKI can verify administrator credentials
  - Must configure server entries for each authentication server in your network





FORTINET Training Institute

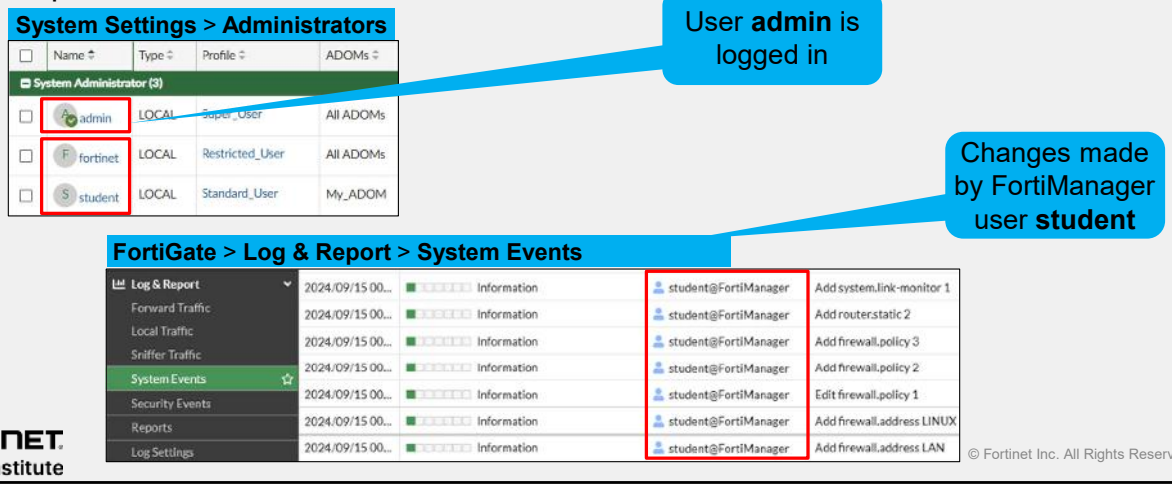
 11

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 public key infrastructure (PKI) as means of verifying the administrator credentials.

Additionally, you can configure two-factor authentication using FortiAuthenticator or FortiToken cloud. Refer to the *FortiManager Administration Guide* for more details.

Monitoring Administrator Sessions

- You can monitor currently logged in administrator accounts
  - Logged in → green check mark
  - Logged out → no check mark
- Only the default **admin** administrator or administrators with Super_User profile can see the complete list of administrators



FORTINET Training Institute

 12

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

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

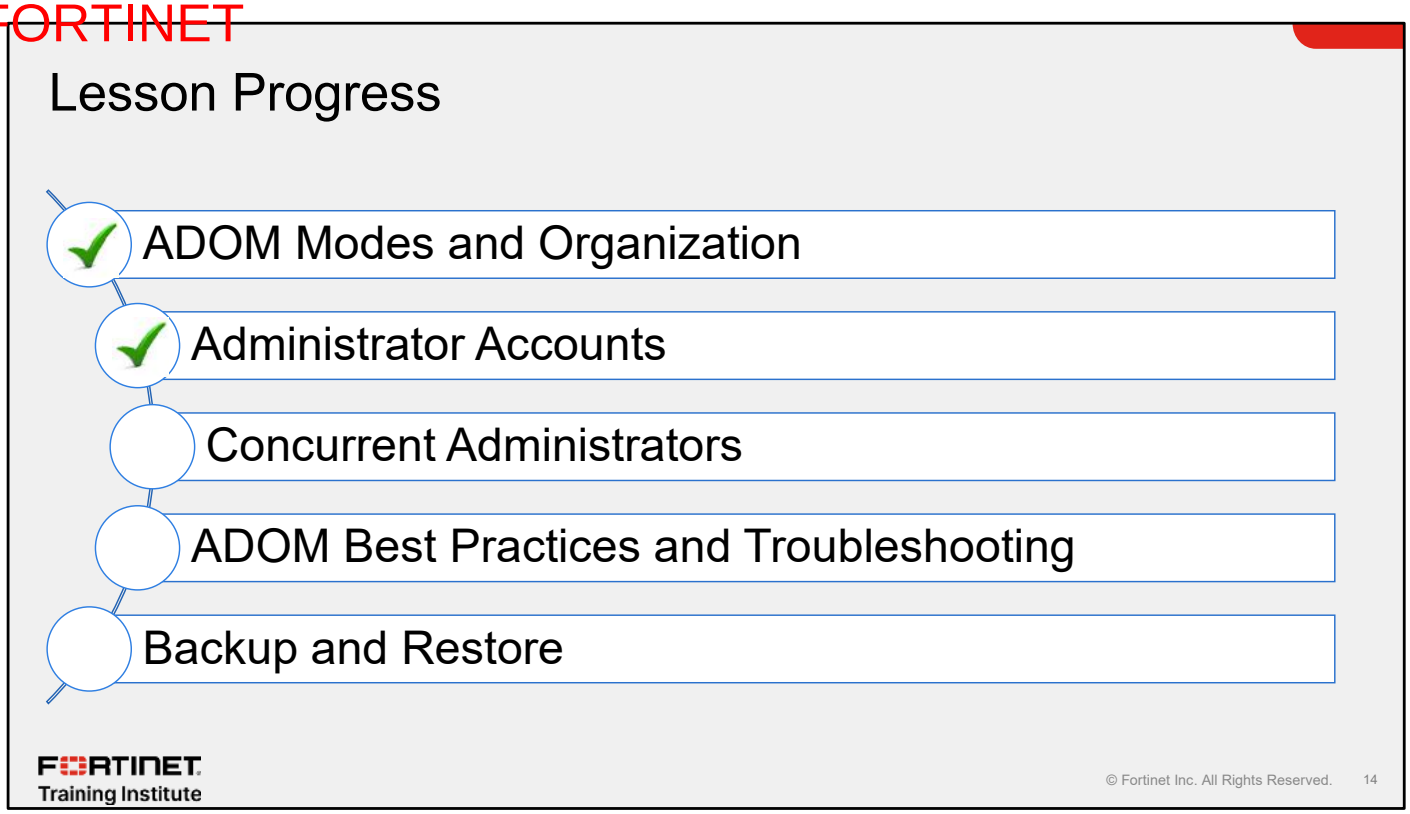
Knowledge Check

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

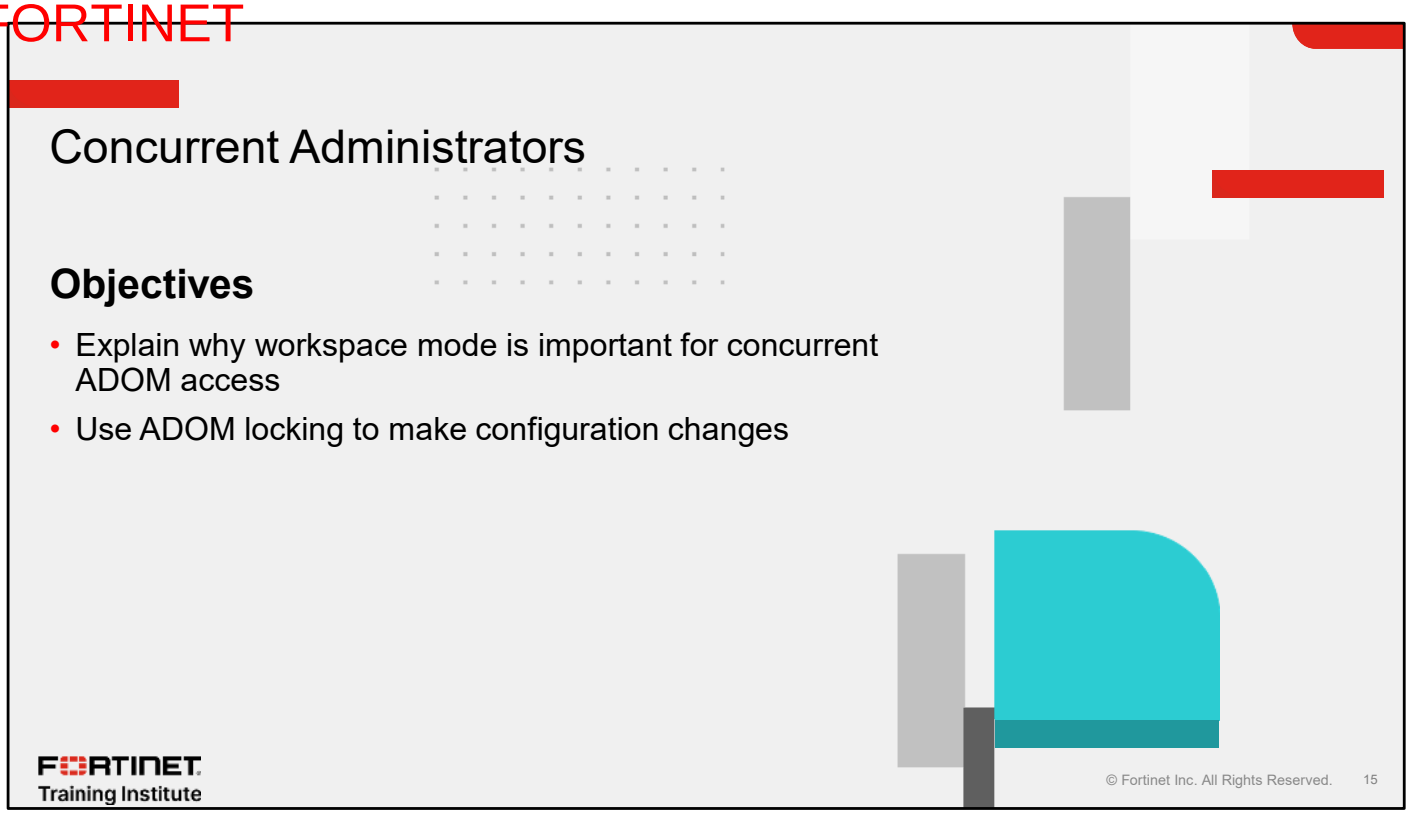
FORTINET Training Institute

 13



Good job! You now understand administrator accounts.

Now, you will examine concurrent administrators on FortiManager.



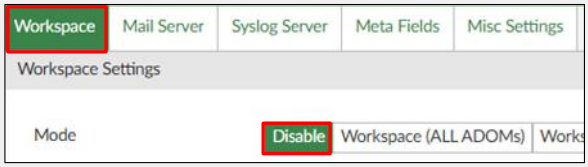
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using ADOM, device, or policy package locking, you will be able to better safeguard the administration and management of FortiManager and the managed devices.

Concurrent ADOM Access—Workspace Default

- By default, multiple administrators can log in and make changes in the same ADOM
  - This occurs because workspace mode is set to **disabled** out of the box

```
get system global
.
.
workspace-mode : disabled
```



- This concurrent access may cause conflicts if two or more administrators try to change the same setting at same time

System Settings > Administrators

Name	Type	Profile	JSON API Access	ADOMs
admin	LOCAL	Super_User	None	All ADOMs
student	LOCAL	Standard_User	None	My_ADOM
fortinet	LOCAL	Super_User	None	All ADOMs

These two accounts can make changes that conflict with each other

FORTINET Training Institute

 16

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

Usually this is acceptable, especially if you configured administrator profiles with non-overlapping permissions. However, the probability of two administrators changing the same setting in a network with many devices is still possible and should be avoided. The solution for such a scenario is to enable workspace mode.

Enabling Workspace Mode

- You can enable workspace mode from the GUI and from the CLI

System Settings > Advanced > Workspace


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

```
config system global
set workspace-mode per-adom
end
```

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

- You can choose from three options:
  - Workspace (ALL ADOMs)
  - Workspace (Per-ADOM)
  - Workflow (ALL ADOMs)
- Optionally, you can enable **Per-Policy Lock**

Always notify other administrators before enabling workspace mode so they can save their work and avoid losing unsaved data

FORTINET Training Institute

 17

You can use the CLI or the GUI to enable workspace mode and prevent concurrent ADOM access. This allows administrators to lock entire ADOMs, as well as specific devices, policy packages and objects.

You have the following three options:

- **Workspace (ALL ADOMs)**: All ADOMs can be locked.
- **Workspace (Per-ADOM)**: Only ADOMs configured for workspace mode can be locked.
- **Workflow (ALL ADOMs)**: In addition to locking ADOMs, this mode is used to ensure that all changes are reviewed and approved by authorized administrators before they are applied.

Optionally, you can enable **Per-Policy Lock**, which allows you to lock individual policies.

Effects of Enabling Workspace Mode

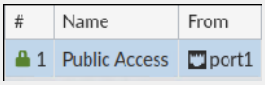
- Disables concurrent read/write access to locked items
- Read/write access for only *one* administrator—all others have read-only access
- Once enabled, you can create locks at different levels:
  - ADOM

  - Specific devices

  - Policy packages

  - Objects

  - You can lock individual policies if you enable **Per-Policy Lock**.



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

If another administrator locked devices or policy packages, you cannot lock the ADOM containing those devices or policy packages

FORTINET Training Institute

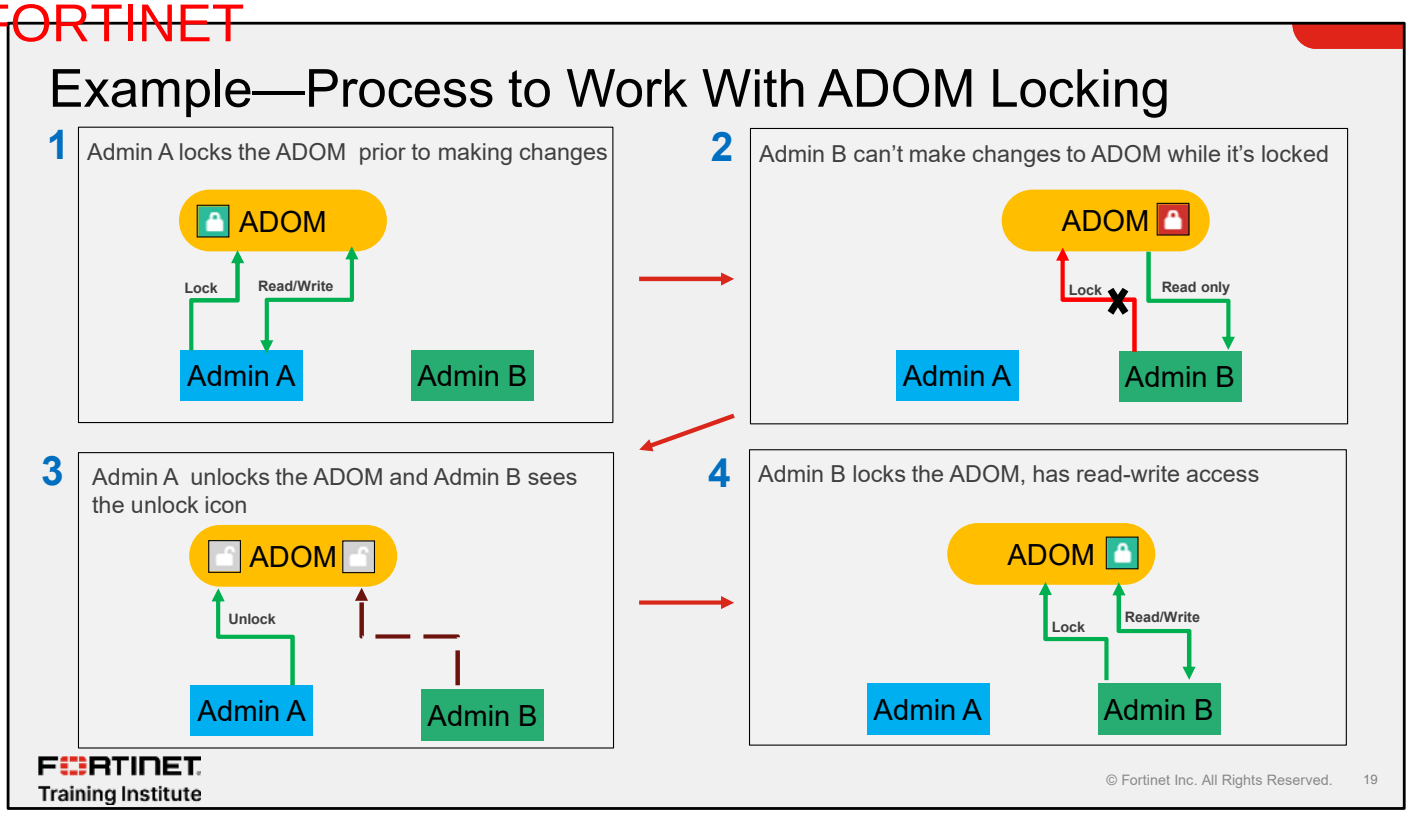
 18

Enabling workspace mode allows you to lock different items in FortiManager, effectively preventing concurrent read/write access to any locked item. Only the administrator that initiated the lock has read/write access to that item, while all other administrators have read-only access.

You can lock entire ADOMs, as well as specific devices, policy packages, objects, and individual policies.

After you make all required configuration changes, you can unlock the item manually. Another way that you can release the locks is to log out of FortiManager.

When you lock an ADOM, all existing locks on devices and policy packages that you created within that ADOM are removed. Additionally, if another administrator locked devices or policy packages, you cannot lock the ADOM that contains those devices or policy packages.

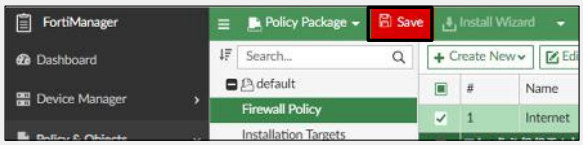


The example in the slide shows an example of the process of working with locked ADOMs when workspace mode is enabled.

1. Prior to making changes, Admin A locks the ADOM. A closed lock icon with a green background 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 closed lock icon with a red background on the ADOM. Admin B has read-only access to that ADOM and cannot make changes.
3. When Admin A finishes making changes, he saves the changes and then unlocks the ADOM. The icon changes to an open lock 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 accordingly. Admin B now has read-write access and can safely make changes without risk of conflicts.

Locking an ADOM (Workspace Mode)

- ADOMs can be locked in upper-right corner of GUI
  1. Select ADOM to be locked
  2. Click lock icon before making changes
     - If you made changes on the managed device configuration on FortiManager, you must save changes prior to installing them



  3. Click the lock icon again to unlock the ADOM

Open lock icon = ADOM unlocked

Closed lock icon with green background indicates an ADOM locked by you

Closed lock icon with red background indicates an ADOM locked by another administrator

FORTINET Training Institute

 20

To enable exclusive read/write permission, and make changes to an ADOM, you *must* lock the ADOM.

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:

- Open lock icon: The ADOM is currently unlocked.
- Closed lock icon with green background: The ADOM is locked by you. You can make changes in that ADOM.
- Closed lock icon with red background: The ADOM is locked by another administrator. You have read/only access and must wait for the ADOM to be unlocked before you can make changes.

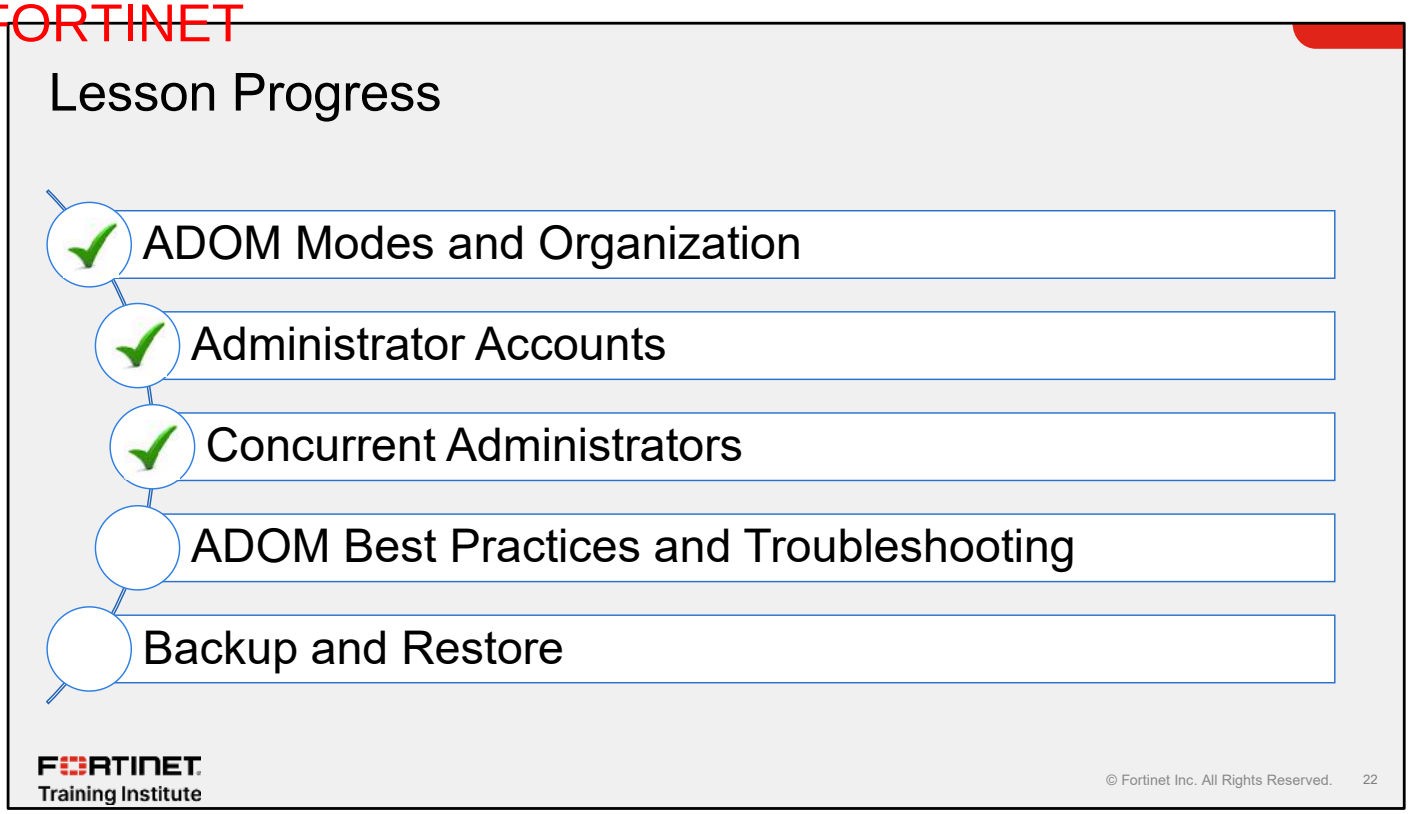
Knowledge Check

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.

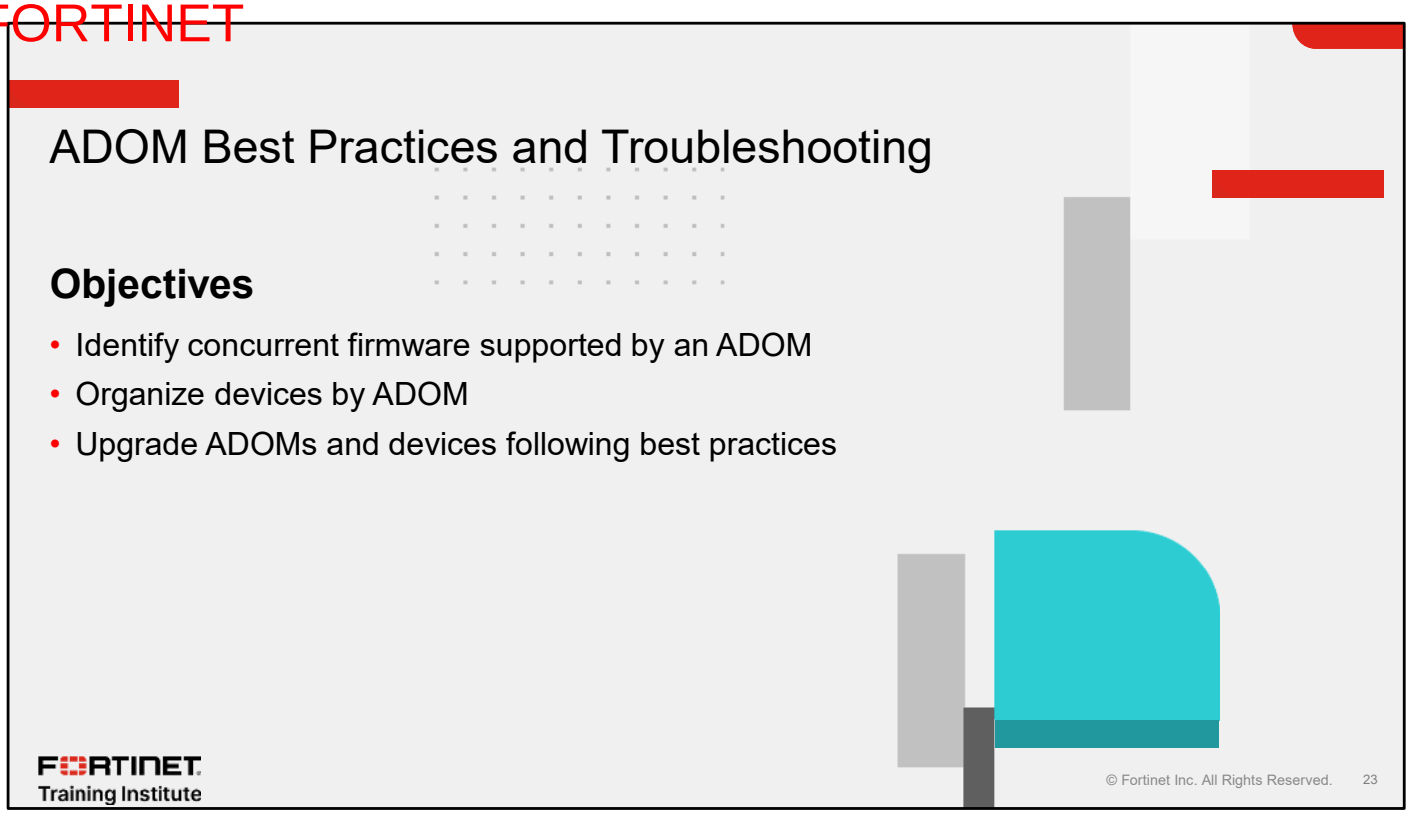
FORTINET Training Institute

 21



Good job! You now understand how you can use workspace mode to handle concurrent administrator sessions.

Now, you will learn about ADOM best practices and troubleshooting.



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.

Supported ADOM Versions

- Each ADOM is associated with a specific firmware version
  - Allows devices to share a common database to ensure compatibility
- The ADOM version determines which device firmware is supported by FortiManager
  - Support varies depending on the FortiManager version. Refer to the specific documentation for details
- FortiManager 7.6.2 supports ADOM versions 7.2, 7.4, and 7.6 as follows:

ADOM version	Device management support
7.2	Manage devices with firmware versions 7.2 and 7.4
7.4	Manage devices with firmware versions 7.2 and 7.4
7.6	Manage devices with firmware versions 7.2, 7.4, and 7.6

You should avoid using multiple firmware versions in the ADOM.

FORTINET Training Institute

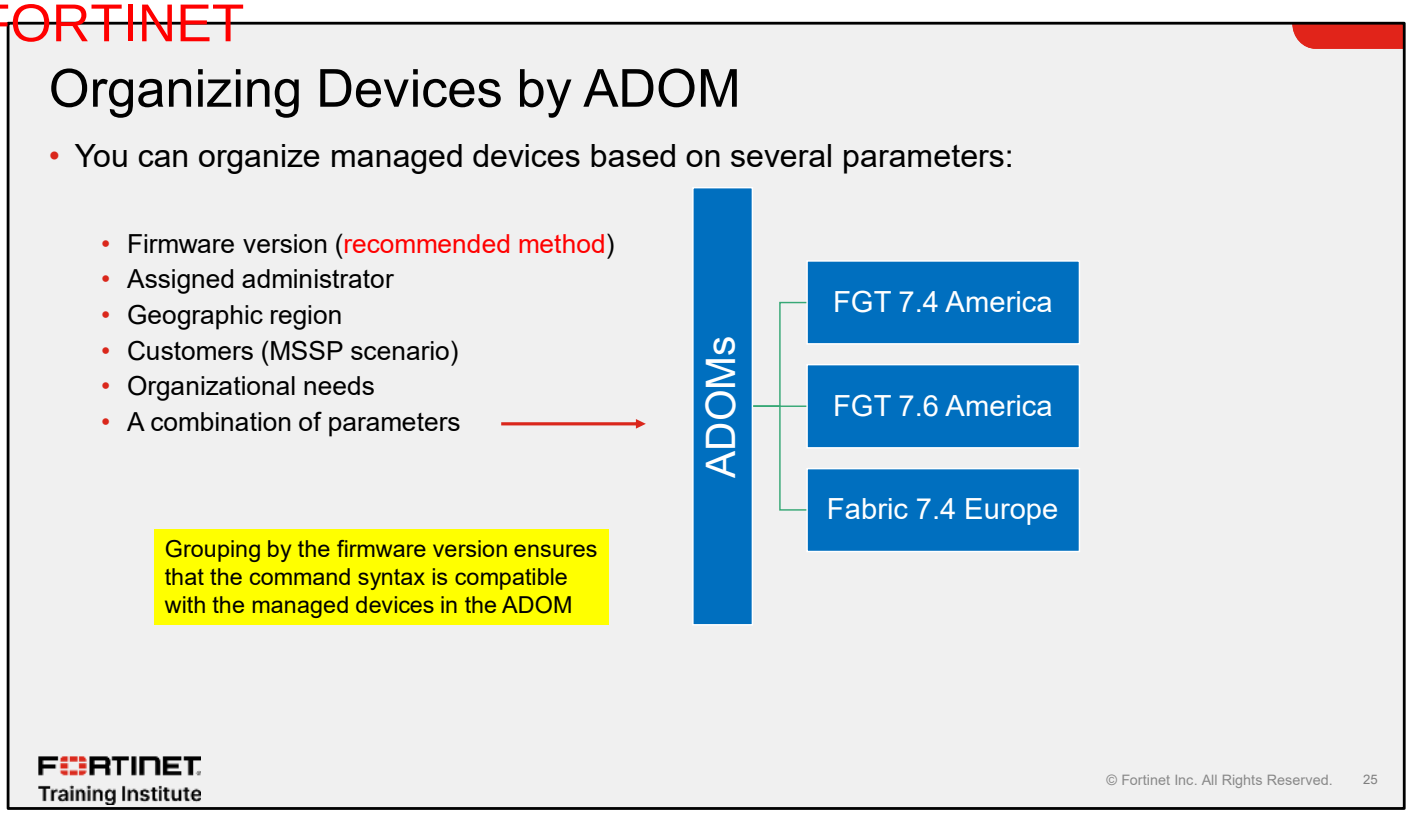
 24

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

Some ADOM versions can also manage FortiGate devices that are using earlier or later firmware versions. For example, in FortiManager 7.6.2, the 7.6 ADOM can manage FortiGate devices on firmware versions 7.6.x, 7.4.x and 7.2.x. Therefore, the devices on those firmware versions can share a common FortiManager database.

In the case of having multiple FortiOS firmware versions on the same ADOM, it is recommended to use separate ADOMs instead. The compatibility of multiple FortiOS on the same ADOM is performed on a best-effort basis, some features of the FortiOS firmware may be restricted due to configuration syntax.

Also note when you upgrade the FortiManager firmware version the existing ADOMs are not automatically upgraded.



Before designing your ADOM structure, verify the maximum number of ADOMs and the maximum number of managed devices that your FortiManager model supports. You can find this information in the **License Information** widget, or by using the `get system status` command.

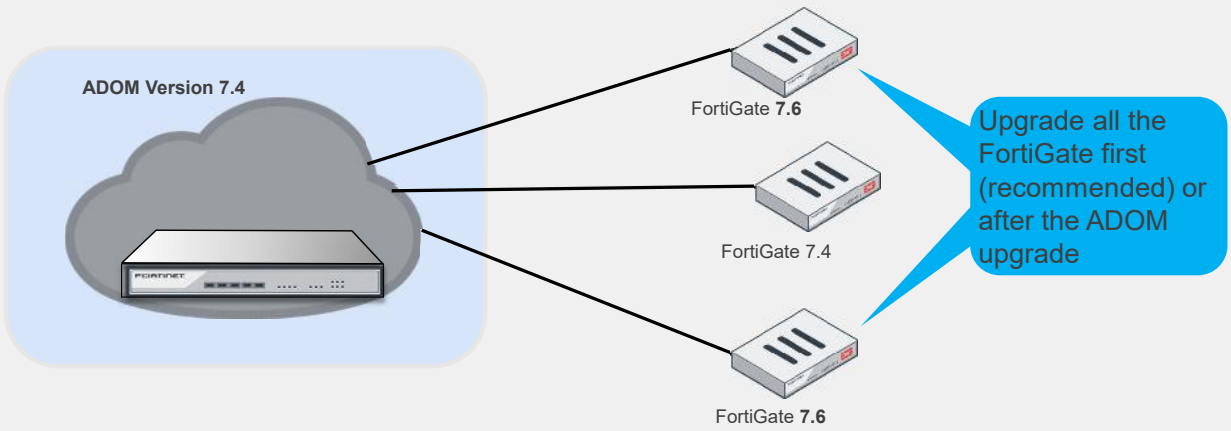
You should use a scheme that simplifies management. For example, you could organize your devices by:

- 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 7.6, you can group these devices in a version 7.6 ADOM. This is the recommended method for grouping devices.
- Assigned administrators: You can group devices into separate ADOMs and assign them to specific administrators.
- Geographic regions: You can group all devices for a specific geographic region into one ADOM.
- Customers: You can create a dedicated ADOM for each customer.
- Organizational needs: You can group devices based on their department or function. For example, you can create dedicated ADOMs for production, development, and test networks.

When you organize managed FortiGate devices, it is highly recommended that you group them based on their FortiOS firmware version. This is because valid command syntax varies by firmware version, which affects script compatibility and other features. For example, if you have FortiGate devices running FortiOS 7.4 and FortiOS 7.6 firmware in the same region, you should create an ADOM for each firmware version.

ADOM Upgrade

- You can upgrade the ADOM before, or after you have upgraded the firmware of all the devices it contains
- It is recommended to upgrade all devices first, and then upgrade the ADOM



FORTINET Training Institute

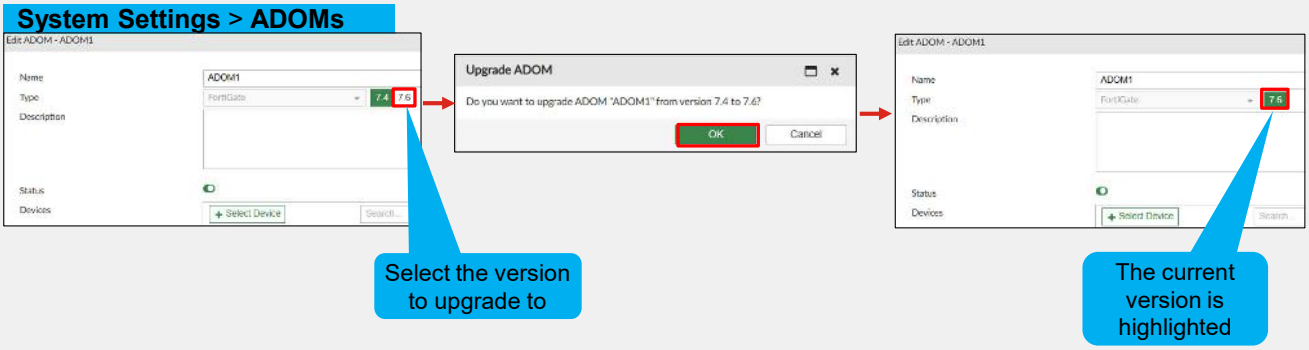
 26

You can upgrade the ADOM version before or after updating all devices in that ADOM. However, it is recommended to upgrade the devices first, and then upgrade the ADOM.

Note: If there are many ADOM revisions, FortiManager requires more system resources, and the ADOM upgrade can take more time to complete. You will learn about ADOM revisions later in this course.

One-Click ADOM Upgrade

- You can upgrade an ADOM in **System Settings** > **ADOMs**
  - Right-click the ADOM, and then select **Upgrade,** or edit the ADOM
  - Can upgrade to one version higher at a time



You must upgrade the **Global Database** ADOM first if global objects are referenced in the ADOM

FORTINET Training Institute

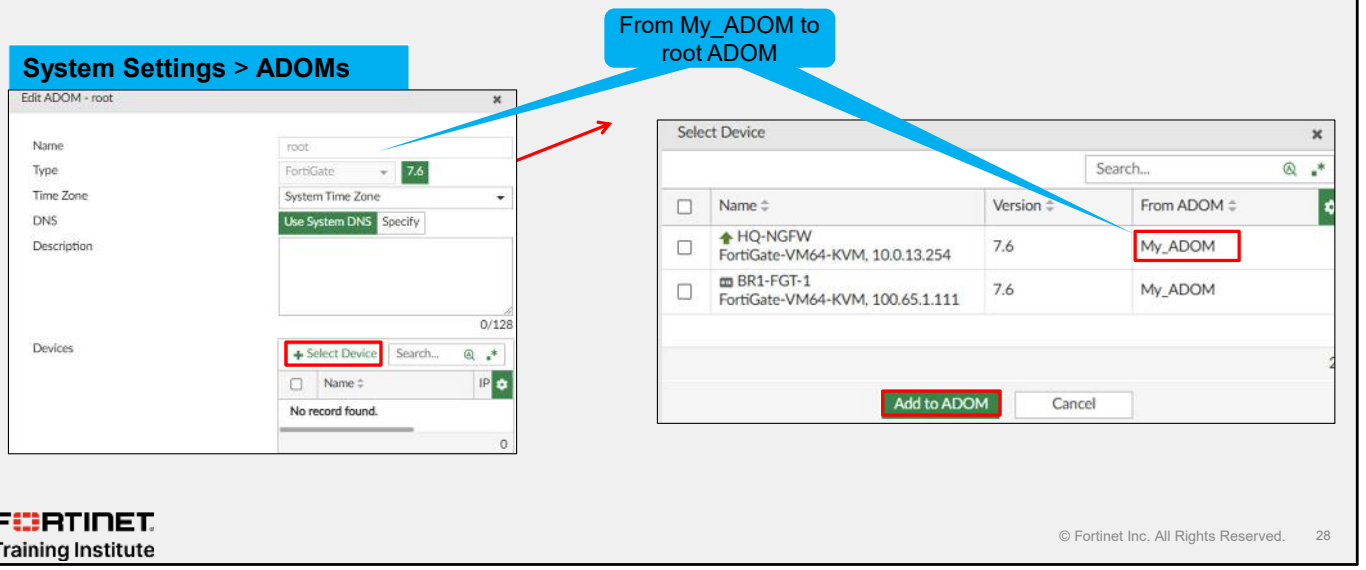
 27

You can upgrade the ADOM in **System Settings** > **ADOMs**. You can upgrade an ADOM one version at a time. For example, you can upgrade an ADOM running version 7.2 to version 7.4 first, and then repeat the process to upgrade it to version 7.6.

The upgrade process only updates database of the selected ADOM. If the ADOM is using global ADOM objects you must upgrade the global ADOM database to same version first; otherwise, you will lose some of the configuration.

Moving Registered Devices Between ADOMs

- Can move devices between ADOMs after registration
  - By default, restricted to administrators with Super_User access



FORTINET Training Institute

 28

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

ADOM Best Practices—Before and After Upgrades

Before upgrades

- Install any pending device settings and policy package changes, or retrieve the device configuration
- 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 changes to be installed are acceptable

Device migrated to different ADOM

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

FORTINET Training Institute

 29

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 examine 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.

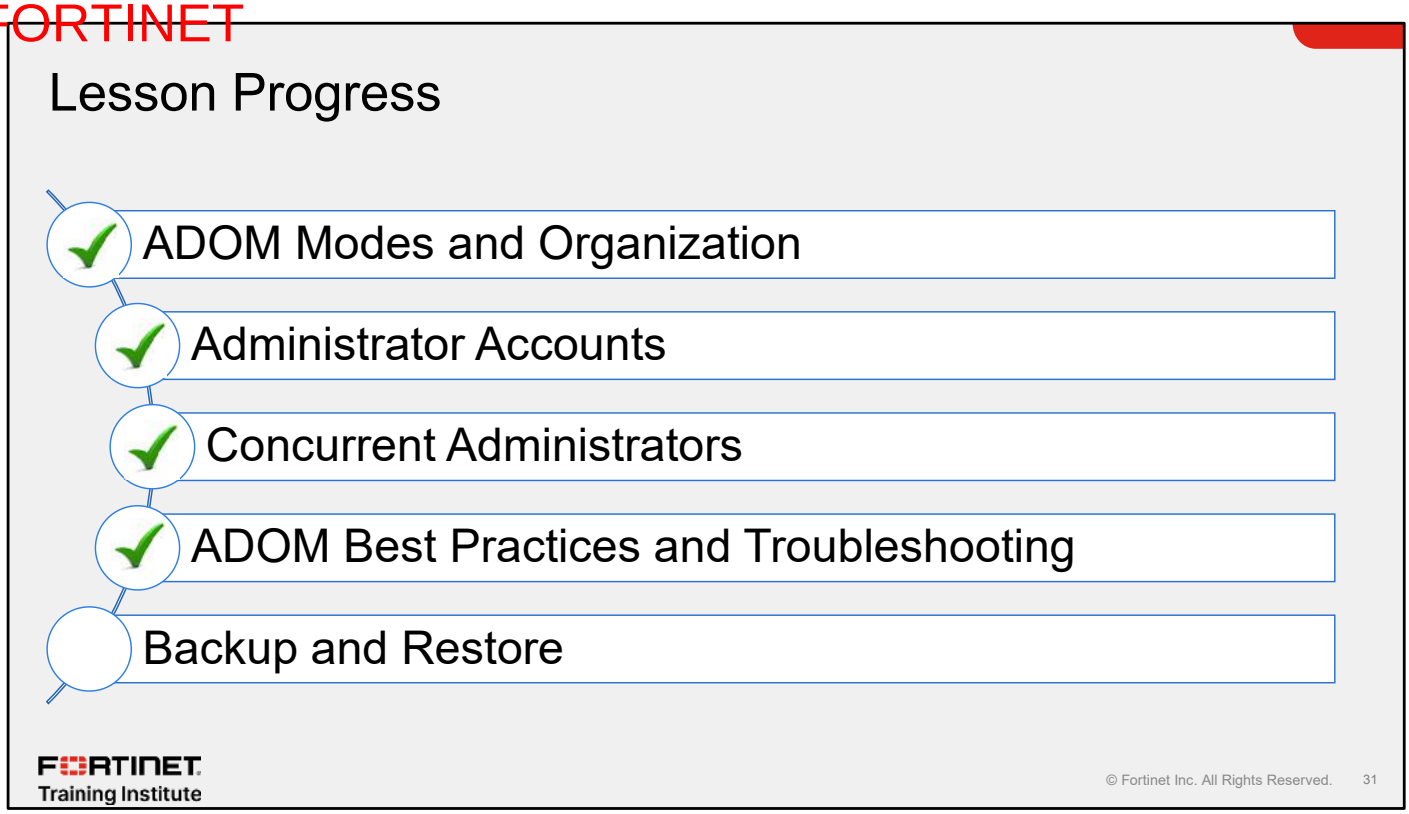
When you move devices from one ADOM to another ADOM, shared policy packages and objects do not move to the new ADOM. You will need to import policy packages from managed devices.

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. Check the installation preview to identify any changes caused by the upgrade

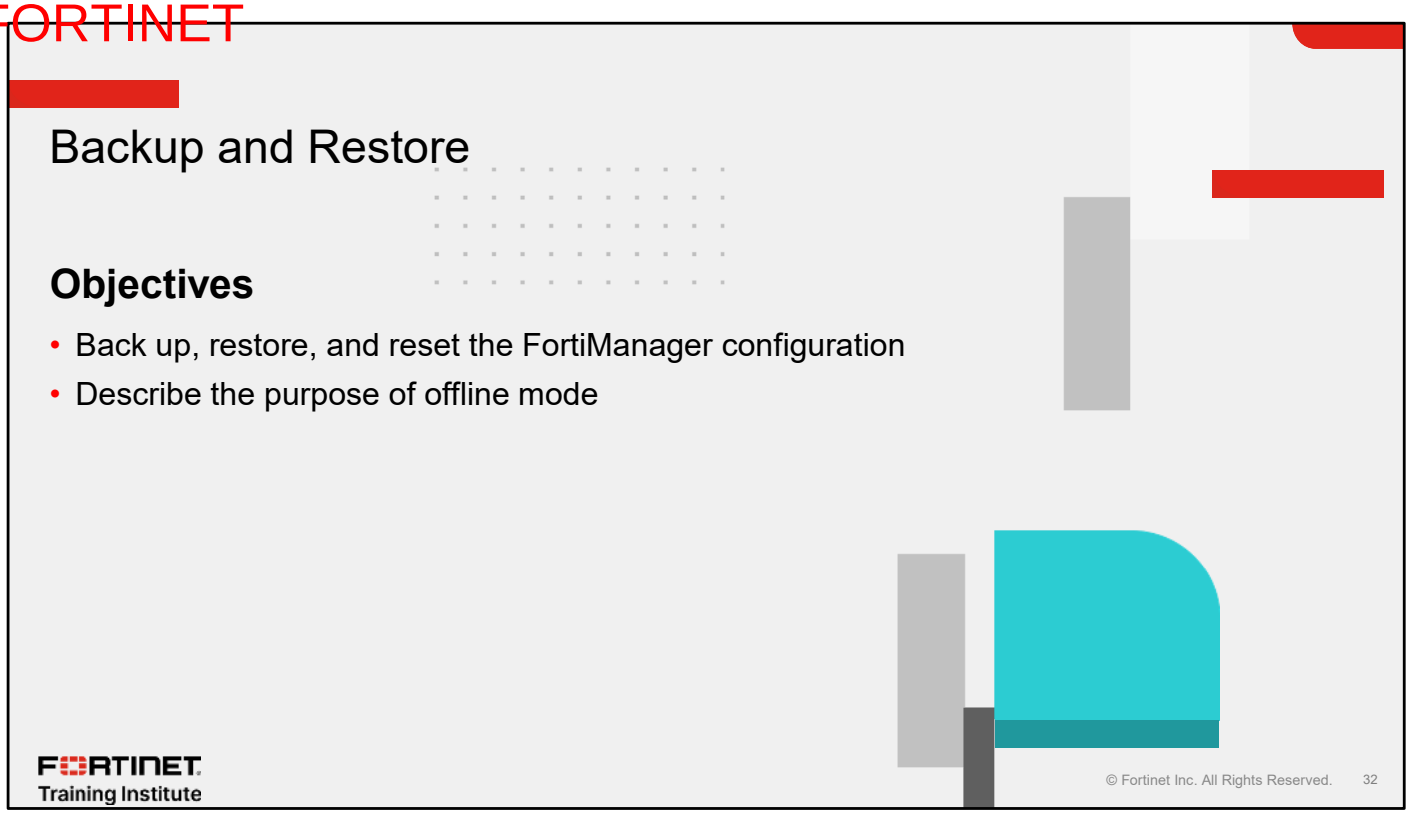
FORTINET Training Institute

 30



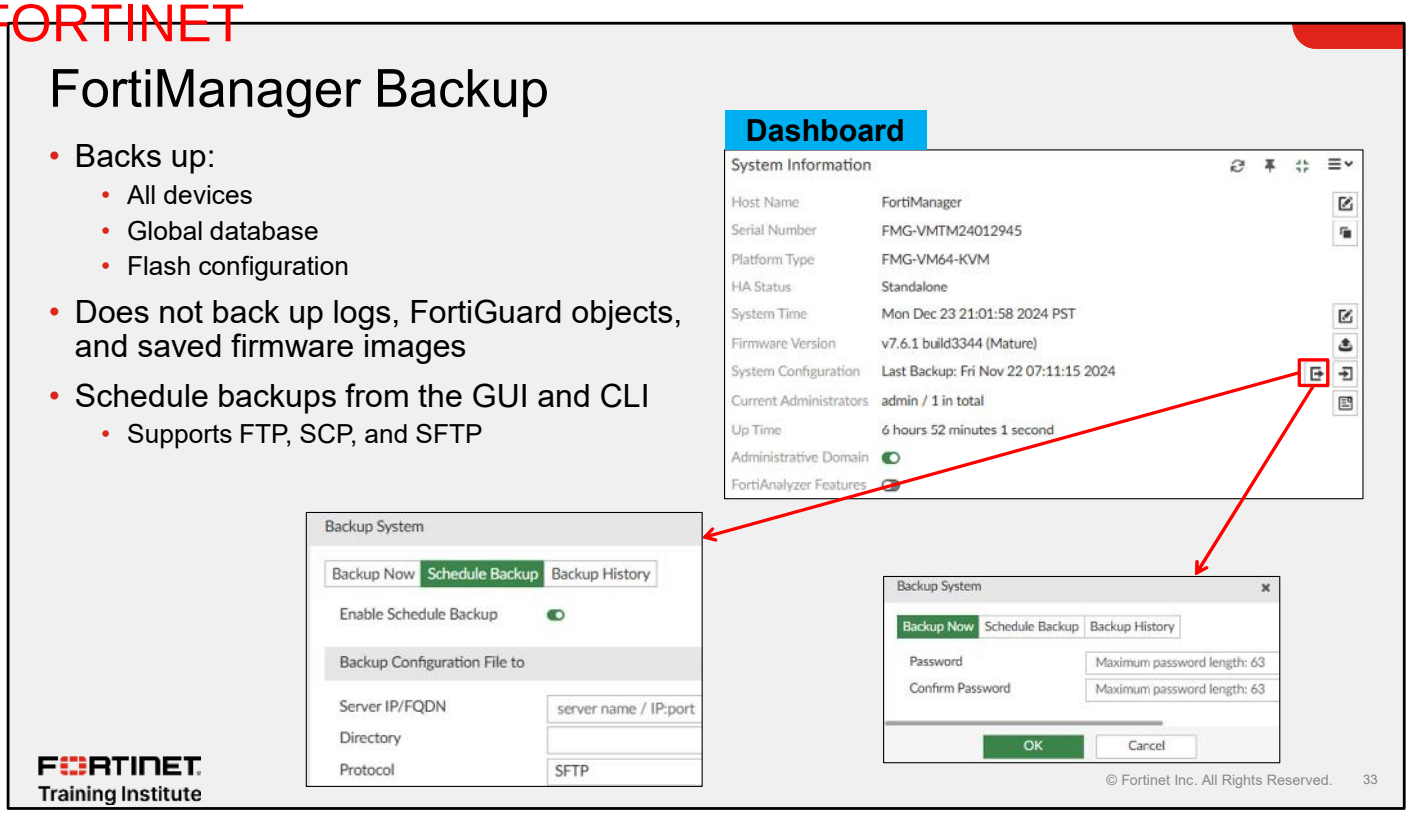
Good job! You now understand ADOM best practices and troubleshooting.

Now, you will learn about backup and restore on FortiManager.



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 a working 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.



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. Note that 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.

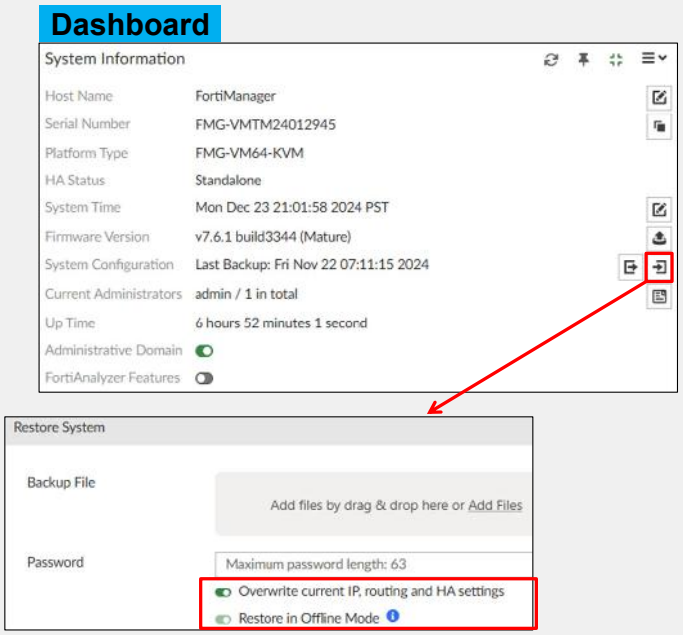
You can schedule backups at regular intervals using the GUI and the CLI.

After performing a backup, you can view the backup history to see all backups performed on FortiManager.

You can restore the configuration from any of backup you performed.

Restoring a FortiManager Configuration

- Reboots FortiManager
- Supports restore from GUI and CLI



FORTINET Training Institute

 34

You can restore the FortiManager configuration using the GUI or CLI. When you perform a restore, FortiManager restarts, and the changes take effect.

The two options in the **Restore System** window are:

- **Overwrite current IP, routing and HA settings**: By default, this option is enabled. If FortiManager has an existing configuration, restoring a backup overwrites 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 current HA and network settings.
- **Restore in Offline Mode**: By default, this option is enabled and grayed out—you cannot disable it. While restoring a backup, 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 device.

Migrating a FortiManager Configuration

You can migrate the 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 command:

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

FORTINET Training Institute

 35

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 the configuration are simple. You need to back up the configuration on the first FortiManager model, and then run the `exec migrate all-settings` command on the second FortiManager.

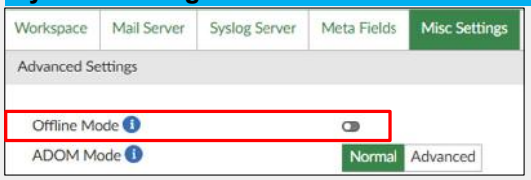
If the original FortiManager has databases from FortiGuard (antivirus, antispam, webfilter, etc.), they will not be included in the configuration file. After migrating, export the packages from the original FortiManager and import them to the other FortiManager.

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

Offline Mode

- Disabled by default
- Enabling offline mode disables FGFM management protocol (TCP 541)

System Settings > Advanced > Misc Settings



- By default, offline mode is enabled when a backup is restored

```
FMG-VM64 # get sys status
Platform Type       : FMG-VM64-KVM
Platform Full Name  : FortiManager-VM64-KVM
..
..
Offline Mode        : Enabled
```

FORTINET Training Institute

 36

By default, offline mode is disabled, allowing FortiManager to manage the devices.

When you perform a configuration restore, FortiManager restarts in offline mode, which effectively disables the FortiGate-FortiManager (FGFM) protocol. You can manually enable or disable offline mode in **System Settings** > **Advanced** > **Misc Settings**.

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

How to Reset Settings

- Back up, then reset using the local console
- Resetting all settings will
  - Reset FortiManager to factory default settings
  - Erase the configuration on flash, including IP addresses and routes
  - Disconnect all the sessions and reboot FortiManager

```
execute reset all-settings
```

- Reset all configurations except IP address and routing configuration

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

- Format command will
  - Delete all databases and logs, and repartition the hard disks

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

FORTINET Training Institute

 37

If you need to factory reset FortiManager, connect using the console port and use the appropriate command.

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

The `execute reset all-except-ip` command resets everything except IP addresses, so you can keep your network connection settings.

The `execute 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.

Formatting your disks destroys only the file system tables; the 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 formatting process to overwrite the hard disk with random data.

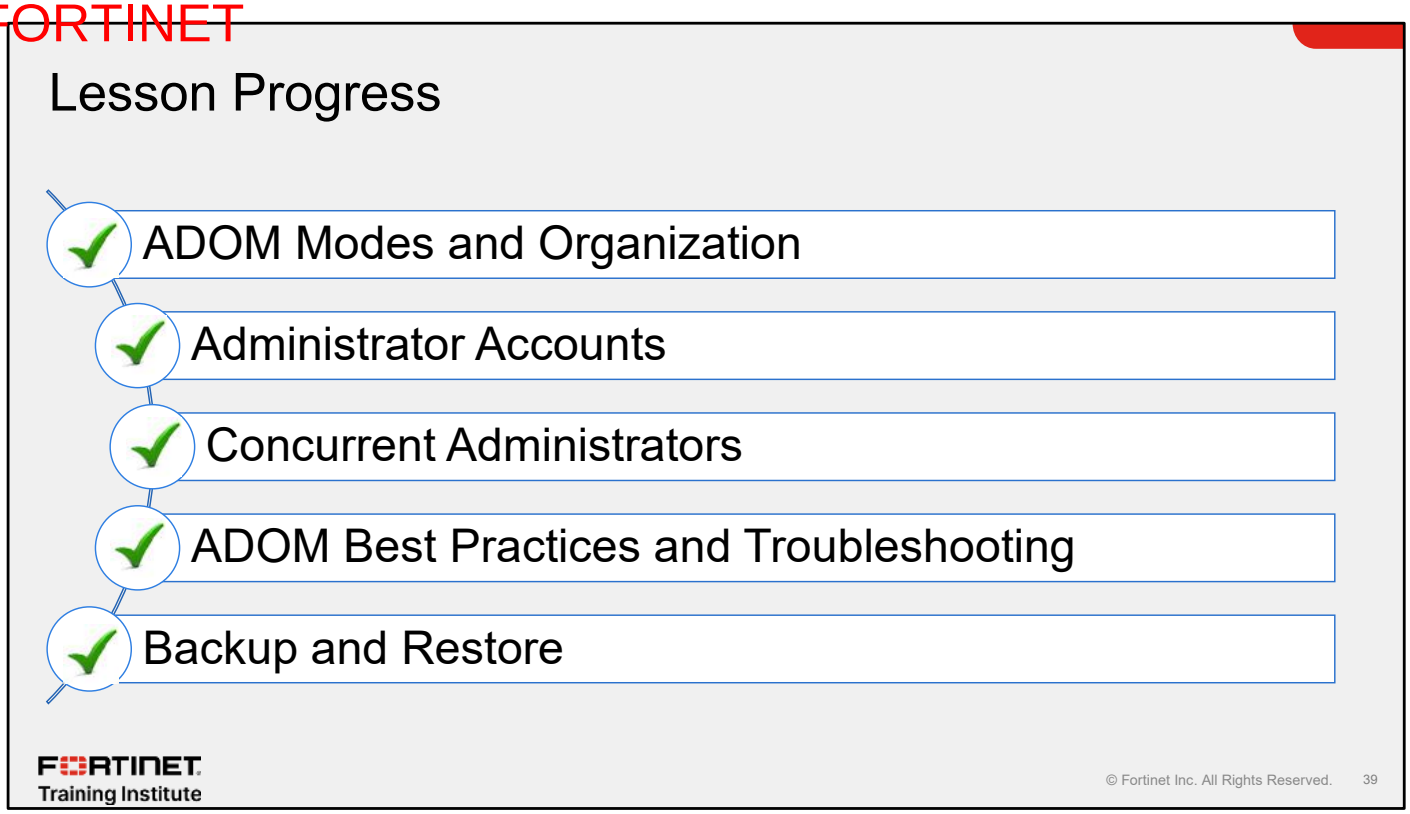
Knowledge Check

1. Which information is included when you perform a FortiManager backup?
   - A. Logs and firmware images
   - ✓B. The global database and all devices

2. Which statement about scheduled backups of FortiManager is true?
   - ✓A. Scheduled backups support FTP, SCP, and SFTP.
   - B. Scheduled backups can be configured using the CLI only.

FORTINET Training Institute

 38



Congratulations! You have completed this lesson.

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

Review

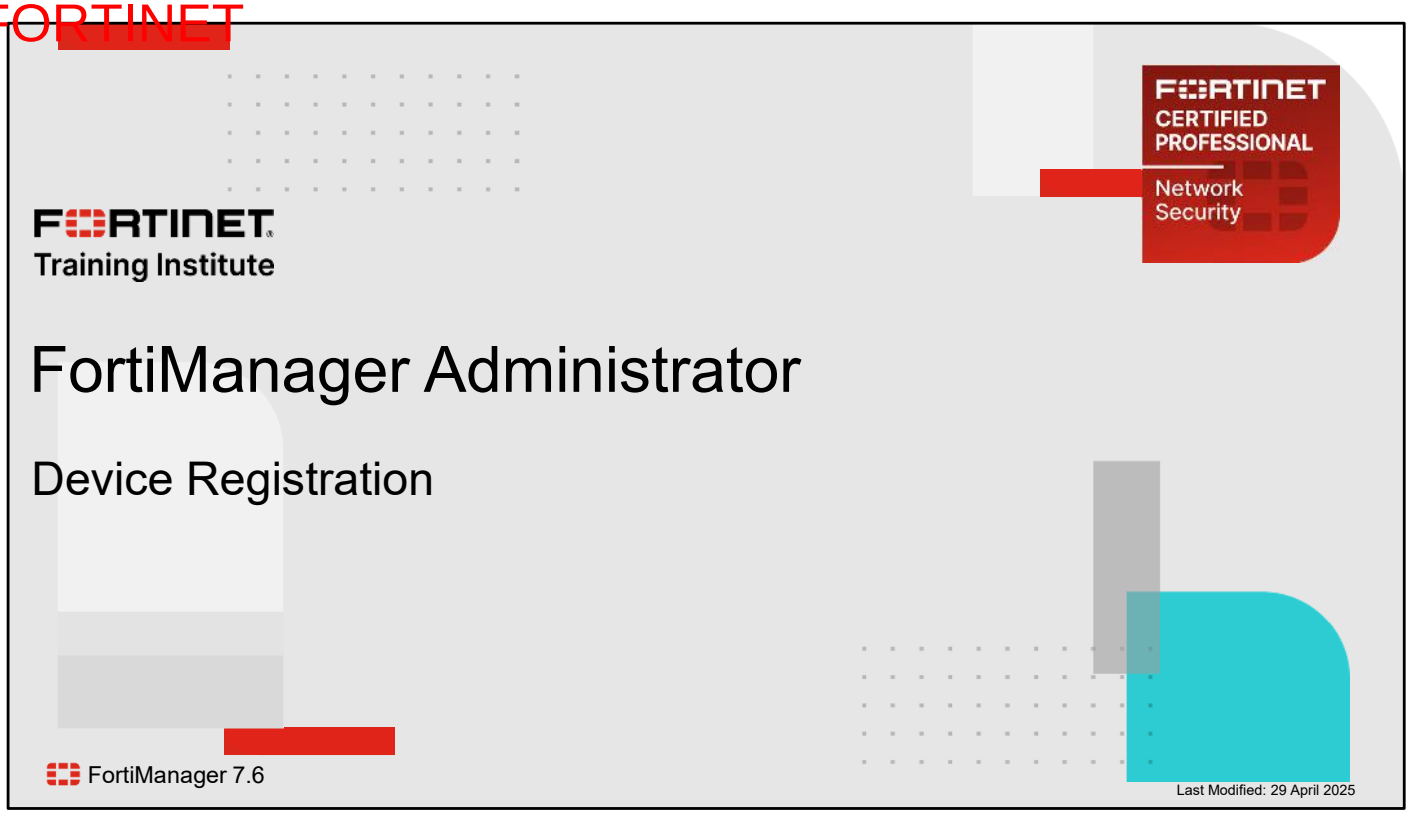
- ✓ Describe ADOM operation modes and ADOM device modes
- ✓ Control administrative access using administrator profiles, trusted hosts, and ADOMs
- ✓ Authenticate administrators using external servers
- ✓ Explain why workspace mode is important for concurrent ADOM access
- ✓ Use ADOM locking to make configuration changes
- ✓ Identify concurrent firmware supported by an ADOM
- ✓ Organize devices by ADOM
- ✓ Upgrade ADOMs and devices following best practices
- ✓ Back up, restore, and reset the FortiManager configuration
- ✓ Describe the purpose of offline mode

FORTINET Training Institute

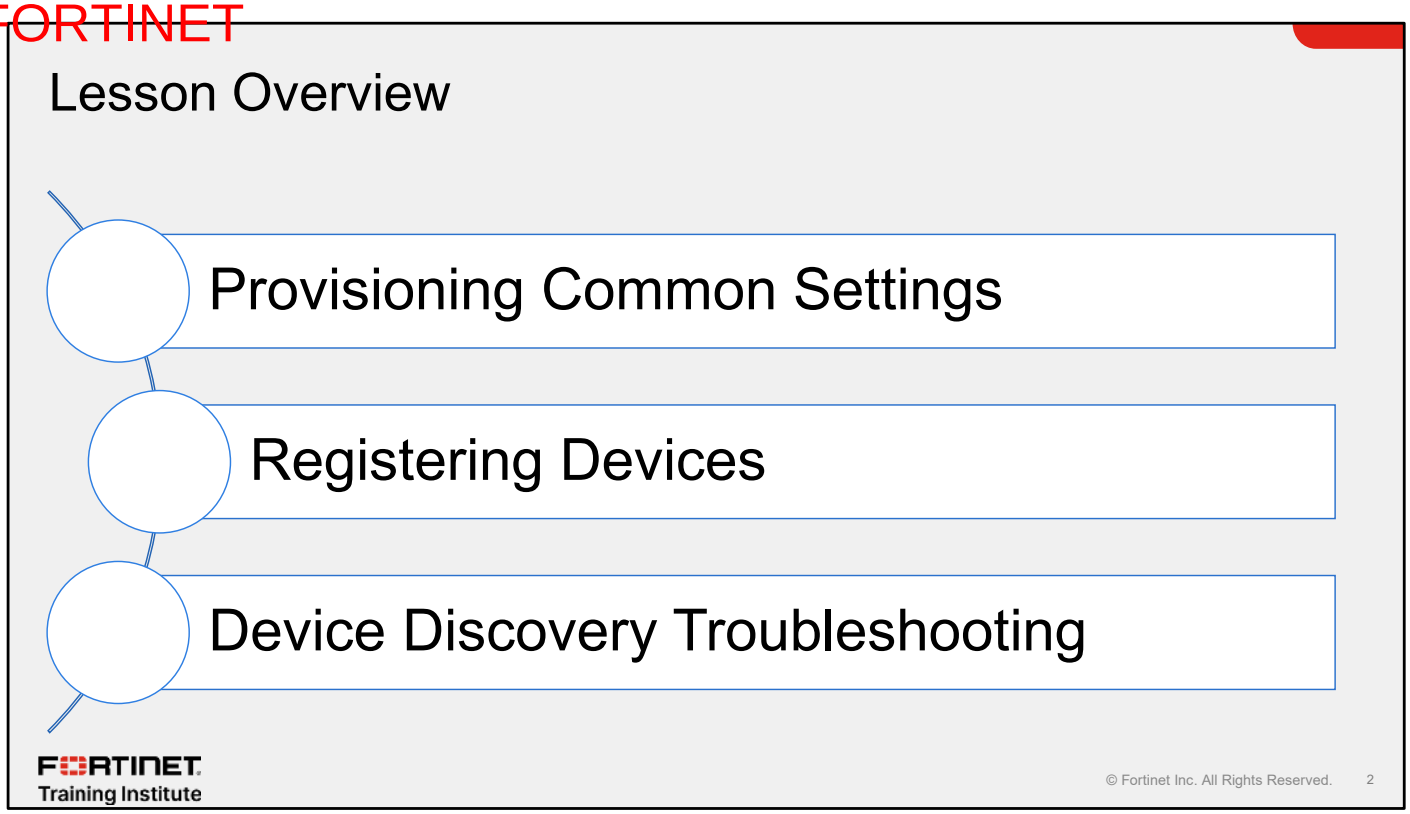
 40

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

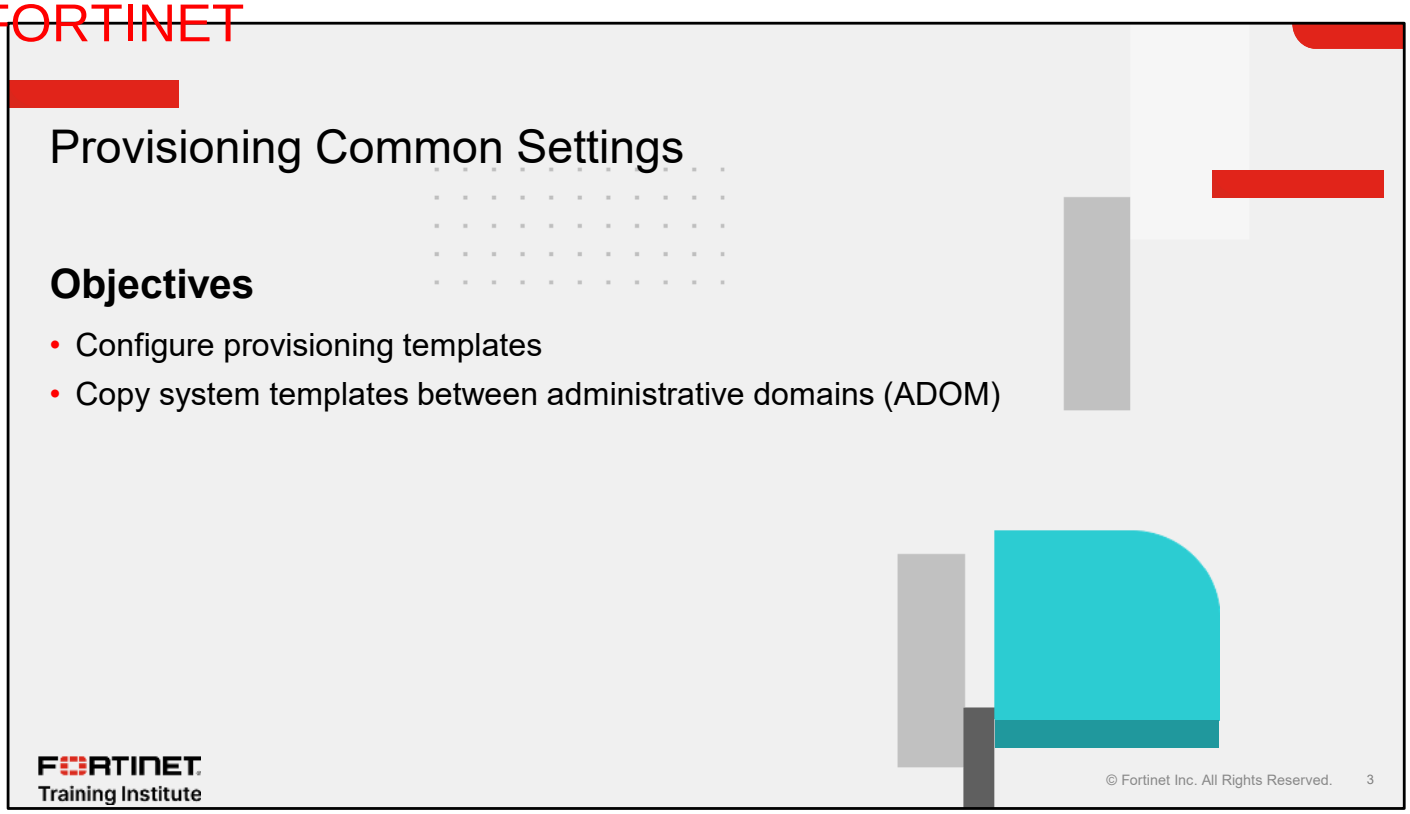
By mastering the objectives covered in this lesson, you learned how to set up and administer FortiManager. You also learned how to use features that are critical for day-to-day use, such as ADOM locks, administrative access controls, and configuration backup and restore.



In this lesson, you will learn about the primary functions of the device manager, and how to register FortiGate devices on FortiManager.



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



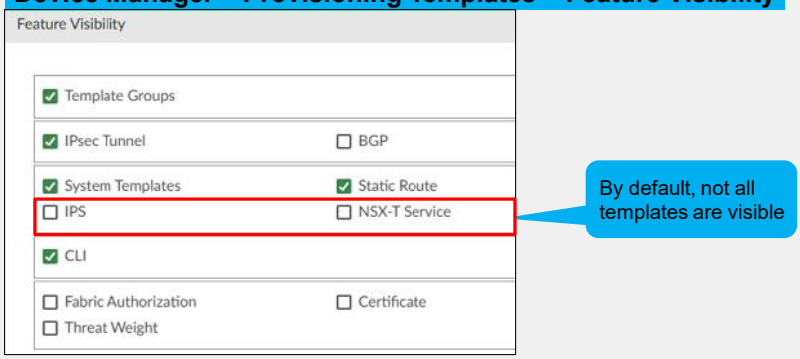
After completing this section, you should be able to achieve the objectives shown on this slide.

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

Provisioning Templates

- Templates allow you to apply common device settings to many devices
  - You can modify and reapply settings when needed
  - Some templates are based on common device settings:

Device Manager > Provisioning Templates > Feature Visibility



- You can create template groups if multiple templates are frequently applied to the same devices

FORTINET Training Institute

 4

Provisioning templates allow you to create profiles that contain device-level settings. These templates facilitate the configuration of identical device-level settings across many devices. You can edit and reapply the templates as needed. Note that by default, only some of the templates are visible. You can choose which templates are visible by selecting them under **Feature Visibility**.

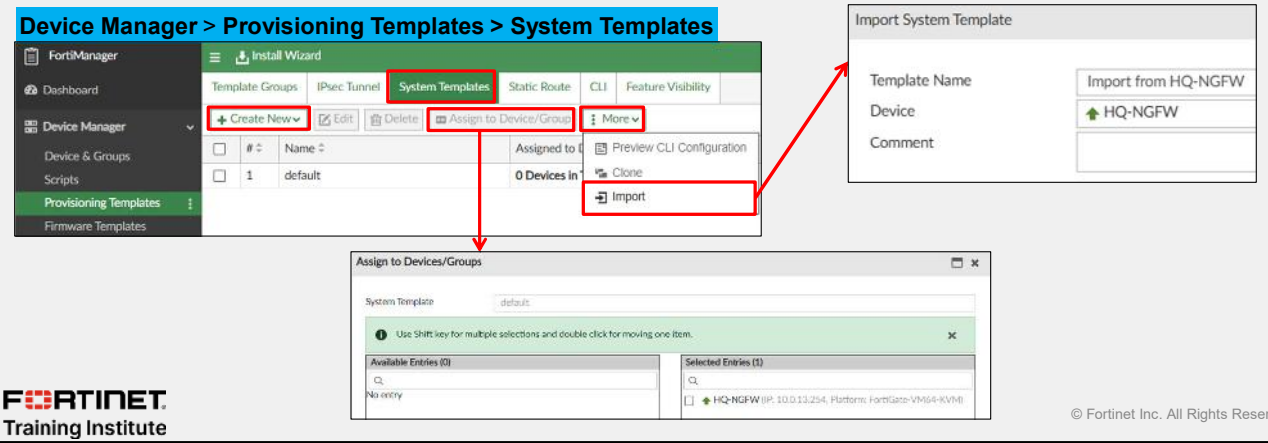
FortiManager includes many templates for commonly encountered scenarios, such as system templates, IPsec tunnel, SD-WAN, and several more.

The name of each template indicates its purpose. For example, you can use system templates to create and manage common system-level settings for the managed devices, and SD-WAN templates **to** configure SD-WAN for one or more devices. Refer to the *FortiManager Administration Guide* for more details.

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

System Templates

- Subset of model device configuration—system-level settings
  - Configure or modify common settings
- You can:
  - Create new templates
  - Inherit the system settings of a managed device using the import feature
  - Associate managed devices with existing templates



FORTINET Training Institute

 5

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

You can create a new system template and configure the settings in the included widgets, or you can import the settings from a specific managed device to inherit the system-level settings of that managed device.

You can use the **Assign to Device/Group** button to associate devices with a template.

Applying these templates to multiple devices within the same ADOM facilitates identical device-level settings across all those devices.

Copying System Templates Between ADOMs

- Each ADOM has its own system templates
- You can export templates from one ADOM to another ADOM
  - Useful when same set of templates is required by devices in different ADOMs
- Steps
  - Export template from first ADOM

In the CLI *templates* are referred to as *profiles*

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

Use *?* to find the profile-id

  - Import template to second ADOM

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

- Example: exporting system template from ADOM1 and importing it to ADOM2

```
execute fmprofile export-profile ADOM1 5244 Training
output dump to file: [/tmp/Training]

execute  fmprofile import-profile ADOM2 5595 /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 template in other ADOM

FORTINET Training Institute

 6

You can export and import system templates from one ADOM to another ADOM using the CLI. To avoid unexpected results, both ADOMs should be running the same firmware version.

The first step is to export the system template from the original ADOM with the `execute fmprofile export-profile` command, and then you can import that profile into the other ADOM with the `execute fmprofile import-profile` command.

An example of these steps is shown on this slide.

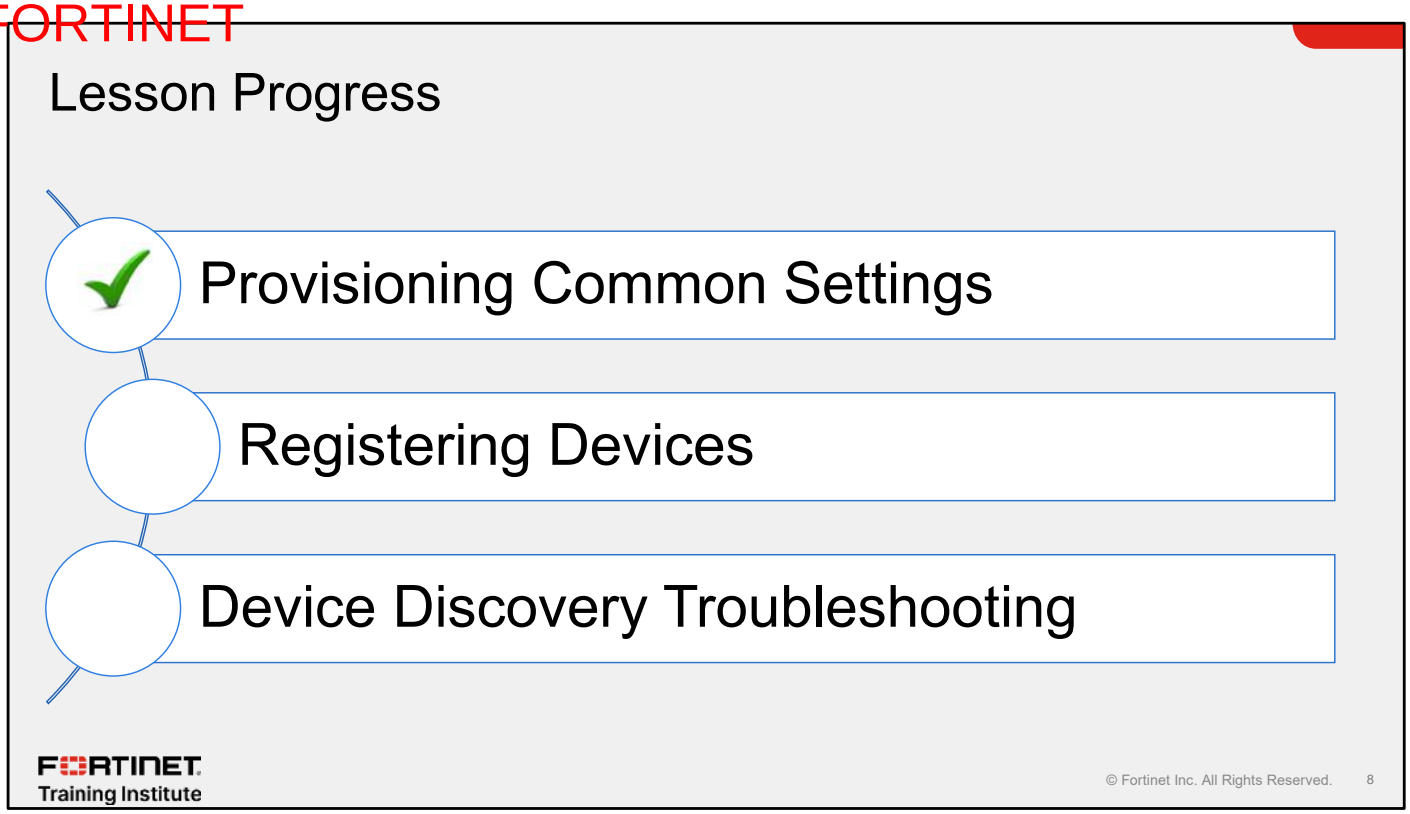
Knowledge Check

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. You can use existing policy packages in multiple devices assigned to the template.
   - ✓B. You can use the same template across devices in multiple ADOMs.

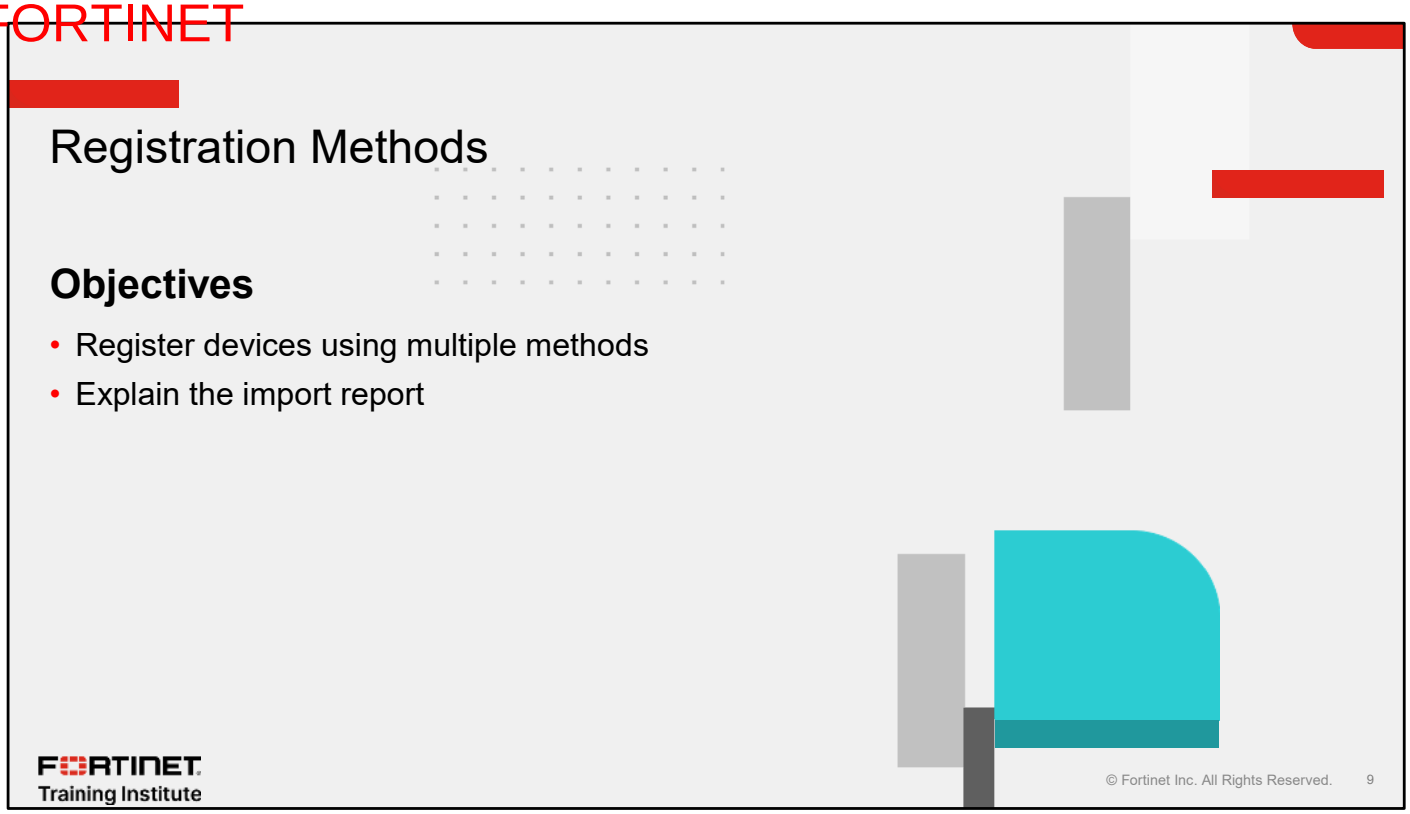
FORTINET Training Institute

 7



Good job! You now understand how to configure provisioning templates to apply common settings to several devices.

Now, you will learn about device registration methods.

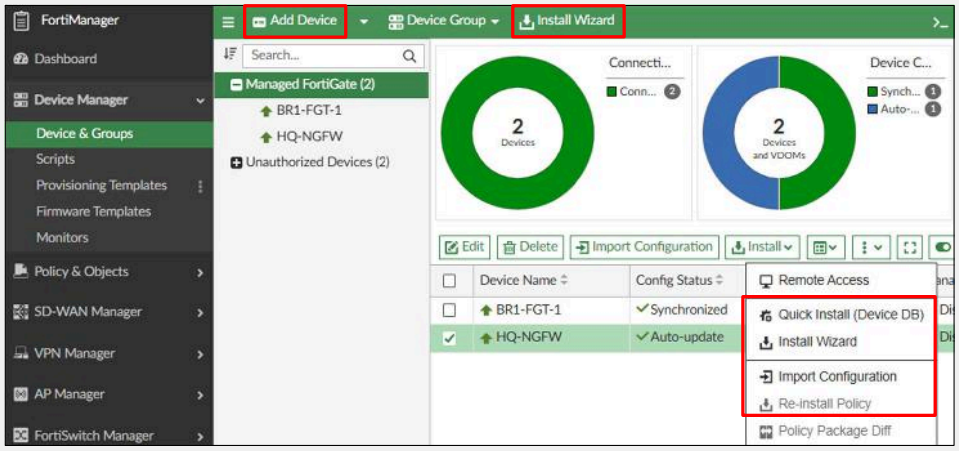


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in device registration, you will be able to add devices to FortiManager for management and administration.

Wizards

- Assist with various tasks
- Main wizards:
  - Add Device
  - Install Wizard
  - Import Configuration
  - Re-install Policy
  - Quick Install (Device DB)



FORTINET Training Institute

 10

Under **Device & Groups** you can find several 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**: Adds devices to central management and imports their configurations.
- **Install Wizard**: Installs changes to device settings and/or policies 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***:* Imports interface mapping, policy database, and objects associated with the managed devices into a policy package under the **Policy & Objects** pane. You can run it while using the **Add Device** wizard and at any time from the managed device list.
- **Re-install Policy***:* Installs the policy package already assigned to the device quickly. It also shows you a preview of the changes that will be installed on the managed device.
- **Quick Install (Device DB)**: Pushes device configuration from the FortiManager device layer to a FortiGate device. This operation does not have an installation preview, and you cannot cancel this operation.

You can access these wizards from the top bar in the GUI, or by right-clicking your device under **Managed FortiGate**.

Methods of Device Registration

Method 1: **Add Device** wizard

1. The FortiManager administrator uses the **Add Device** 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 creates a registration request
2. The FortiManager administrator accepts (or denies) the request

FORTINET Training Institute

 11

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

The first method involves the FortiManager **Add Device** 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).

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 online, and devices not yet online (add model device)
  - Add FortiGate HA clusters
  - Import devices from a CSV file
- 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

 12

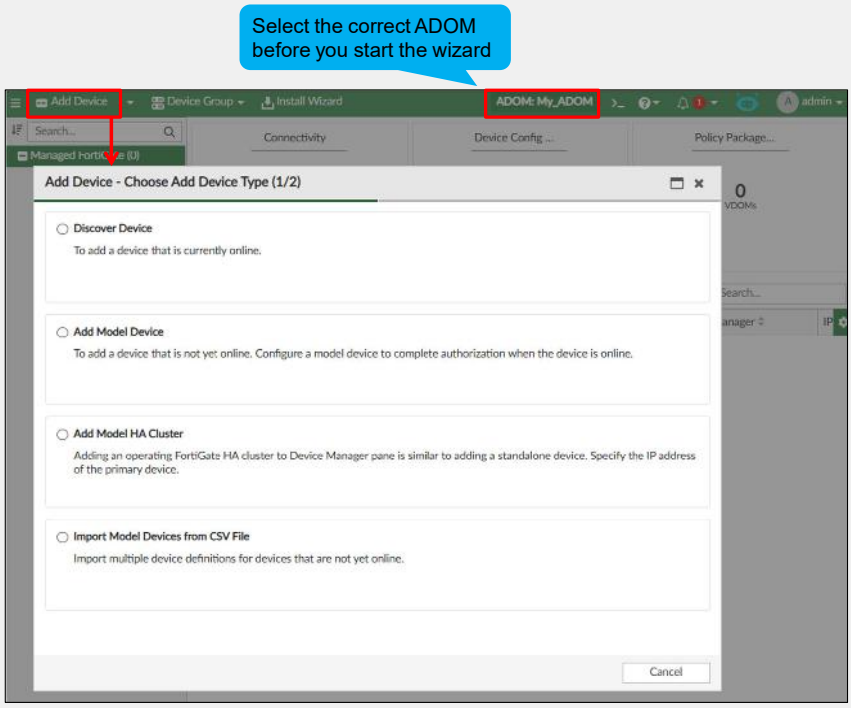
Using the **Add Device** wizard, you can add a FortiGate device with an existing configuration (which includes its firewall policies) or add a new FortiGate device that is not yet online. FortiGate is usually provisioned with a *call home* configuration, which is the minimum configuration needed to reach 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.

This wizard also allows you to add FortiGate HA clusters and devices from a CSV file.

When you import a device that has an existing configuration, you can choose to import the device firewall policies into a new policy package (which you can rename). Objects share the common object database for the 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.

Add Device Wizard

- Add a device through Device Manager
- If you created a custom ADOM based on the device type you are registering, switch to the custom ADOM before you add a device using the wizard



FORTINET Training Institute

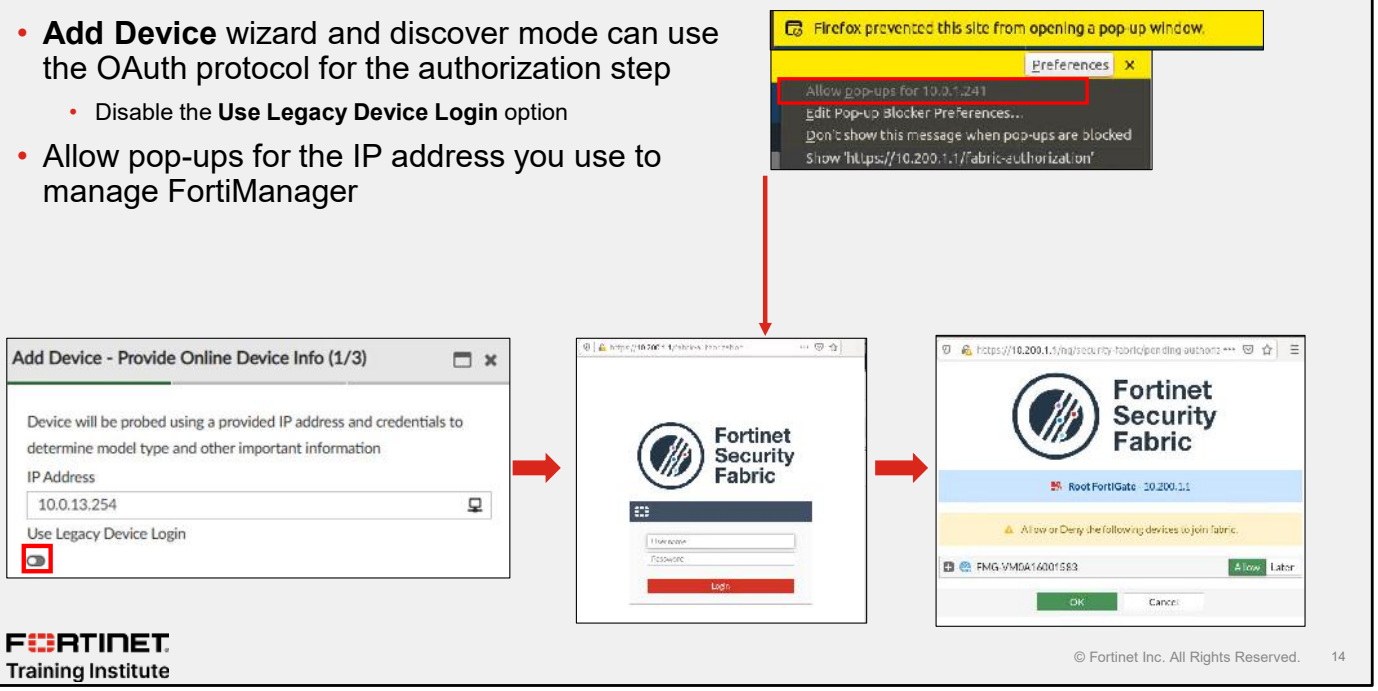
 13

With the **Add Device** wizard, the FortiManager administrator proactively initiates and, ultimately, performs the device registration. This method requires that the administrators know specific details about the device that they are registering.

You can launch the wizard from the **Device & Groups** pane by clicking **Add Device** on the top bar. If you have enabled ADOMs and want to add the device to a specific ADOM, select that ADOM from the ADOM list before starting the **Add Device w**izard.

Add Device Wizard—Discover Device and the OAuth Protocol

- **Add Device** wizard and discover mode can use the OAuth protocol for the authorization step
  - Disable the **Use Legacy Device Login** option
- Allow pop-ups for the IP address you use to manage FortiManager



FORTINET Training Institute

 14

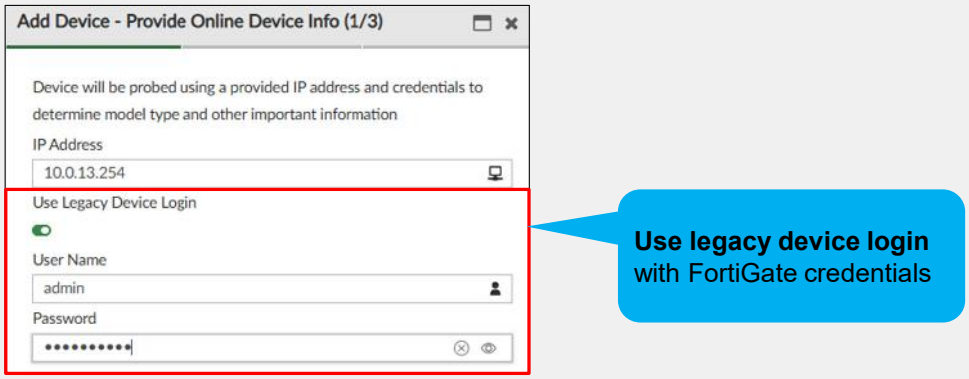
To use the **Add Device** wizard and discover mode with the OAuth protocol, you must type in the IP address of the FortiGate management port, and make sure the **Use Legacy Device Login** option is disabled. After you click **Next** to continue, the following actions occur:

1. FortiManager connects to the online FortiGate device.
2. A window opens to let you log in to FortiGate as part of the authorization process. Note that you must allow pop-ups for the FortiManager page to be able to continue.
3. When FortiManager connects to FortiGate, it retrieves the FortiOS management IP address and management port.

Depending on your network topology, it is possible that FortiManager can access the FortiGate management IP, but the management computer you use cannot. To ensure this method works you must specify a management IP address and port on FortiOS that can be reached from the management computer you use to connect to FortiManager.

Add Device Wizard—Discover Device—Legacy Login

- Enter the FortiGate IP address and login credentials
- Must provide credentials with full read-write permissions on the FortiGate device
- This allows FortiManager to fully discover and install configuration changes to the managed device



FORTINET Training Institute

 15

As an alternative to using the OAUTH method, 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 or older, you must use the legacy login.

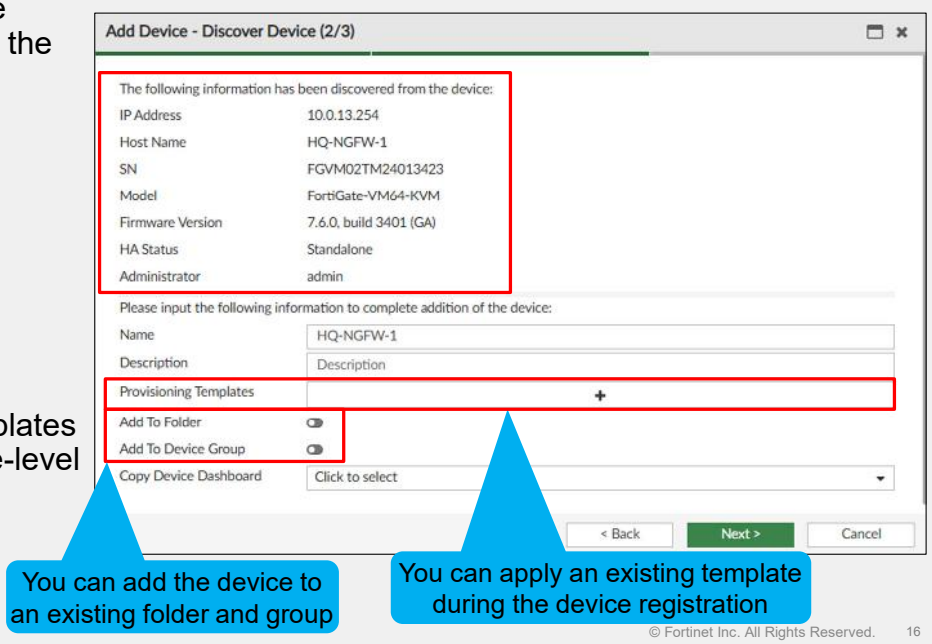
The legacy login method is useful for certain topologies where the management computer used to connect to FortiManager cannot connect to the FortiGate device.

You use the **Use Legacy Device Login** options to add an existing device. Here, you must enter the login credentials for the FortiGate device—IP address, username, and password.

To fully discover the device and add the full configuration, the login credentials that you enter must have full read-write *access* on FortiGate. This also allows FortiManager to install the required configuration on the managed FortiGate.

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

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



FORTINET Training Institute

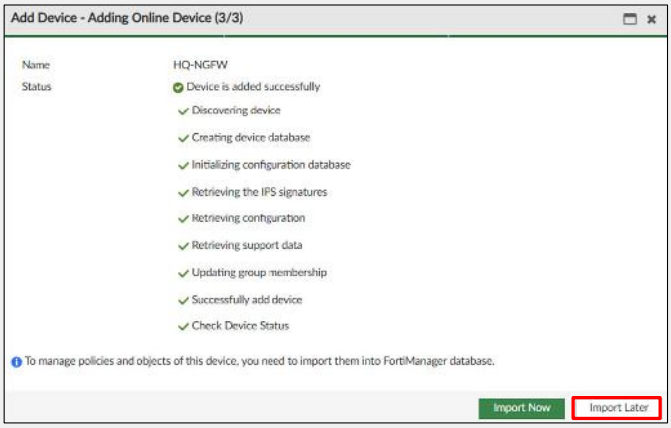
 16

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

Administrators can apply an existing provisioning template to new devices as they are being added to FortiManager. Templates save time by removing the need to repeat common configuration settings multiple times.

Add Device Wizard—Import Options

- Discovers and creates the initial configuration file
  - Retrieves support contract and IPS signatures
- Choose when 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 Configuration** wizard



FORTINET Training Institute

 17

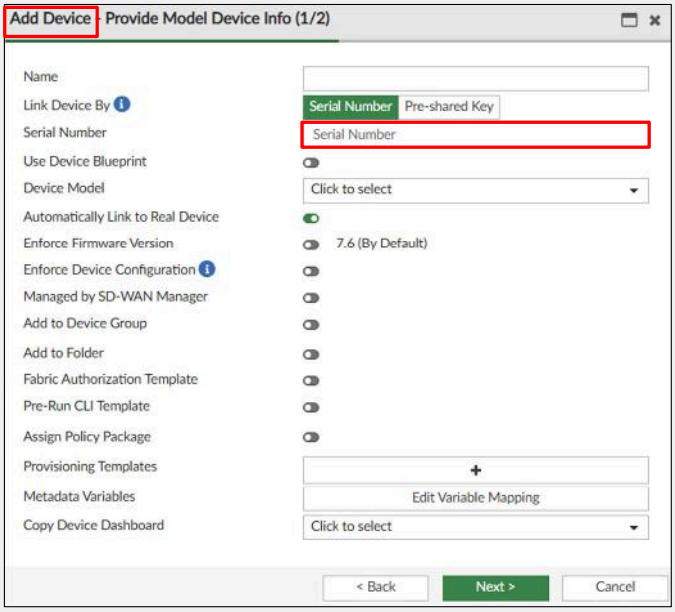
In the next step, FortiManager checks the addition of the FortiGate device and creates the initial configuration file in the revision history. This is the full configuration that contains all used and orphaned objects along with the firewall policies on FortiGate. It also checks the support contract, 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 a new 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. The firewall policy and objects are not imported into **Policy & Objects**. You can import these later using the **Import Configuration** wizard.

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
- You can link a device by either:
  - Its serial number
  - A pre-shared key
- Zero-touch provisioning involves the following general steps:
  - Add model device and configure settings in FortiManager
  - Connect FortiGate to the network and configure it for central management
  - Confirm deployment is successful (it may take several minutes)



FORTINET Training Institute

 18

The second option in the **Add Device** wizard is **Add Model Device**, which allows you to add a device that is not yet online. This option is intended for new FortiGate deployments, where no pre-existing configuration must be preserved. The configuration you create with this option in FortiManager is associated with the model device and overwrites the configuration of the FortiGate after it is registered.

You can link to the real device using one the following two methods:

- **Serial Number**: The serial number of the device you want to add.
- **Pre-shared Key**: A unique pre-shared key for each device you want to add. Useful when the exact device model is not known.

With both options you can select several parameters that will be applied to the managed device once it is registered.

Model Device—FortiGate Configuration (CLI)

- Execute the following commands on the FortiGate side:
  - Step 1

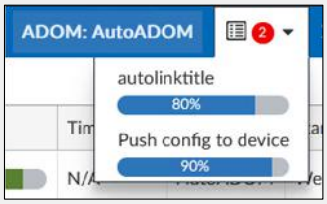
```
config system central-management
set type fortimanager
set fmg <FortiManager IP>
end
```

At this point, the FortiGate device shows in FortiManager as:
- Unauthorized in the *root* ADOM if you used a pre-shared key
- Unauthorized in the assigned ADOM if you used a serial number

  - Step 2

```
execute central-mgmt register-device
<fmg-serial-no> <pre-shared key>
```

FortiManager starts the registration process, as well as the application of any configuration associated with the device. This may take several minutes to finish.



FortiGate is registered in the ADOM where you configured the device model

The pre-shared key in step 2 is required in all cases. You can type any string when the serial number is used in the model device configuration.

FORTINET Training Institute

 19

You can use the GUI and the CLI to send a registration request from FortiGate. Regardless of the device model option you use, you must configure the central management type as `fortimanager`, and point to the IP address of the FortiManager using the command sequence shown on this slide as step 1.

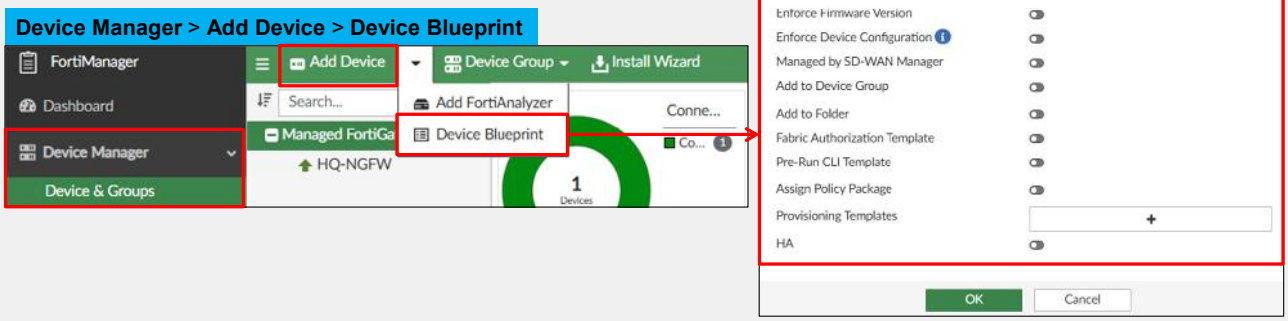
After the first step, if a pre-shared key was used in the model device, FortiGate shows as an unregistered device in the *root* ADOM. If the serial number was used, FortiGate shows as an unregistered device in the ADOM where it was pre-staged.

The second and final step consists of running the `execute central-mgmt register-device` command on FortiGate. This command requires the FortiManager serial number and a pre-shared key. The pre-shared key must match the value used when the device model was added. However, if the model device used the serial number, you can type any text as the pre-shared key since the device authentication uses the serial number instead.

If all parameters are correct, the FortiGate device is registered in the ADOM where you configured the device model.

Add Device Wizard—Device Blueprints

- A device blueprint simplifies configuration of certain device settings, including:
  - Device groups
  - Configuring pre-run templates
  - Policy package
  - Provisioning templates



FORTINET Training Institute

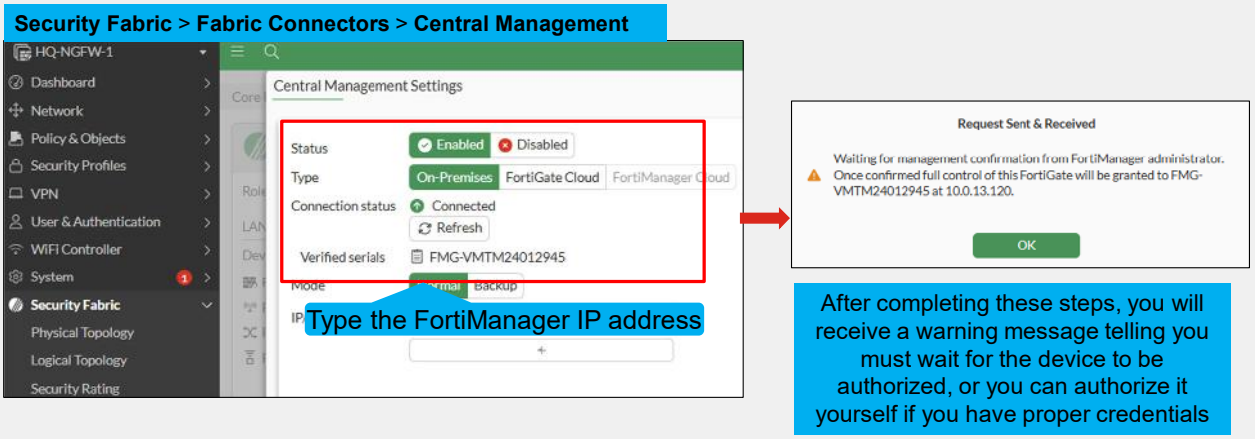
 20

You can 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.

Devices that are assigned a blueprint are automatically configured with the settings specified by that blueprint when they are added to FortiManager.

Method 2—Request From Supported Device

- Configure the central management setting to point to FortiManager



You don't need to enable the FGFM access in any port when FortiGate initiates the registration request

FORTINET Training Institute

 21

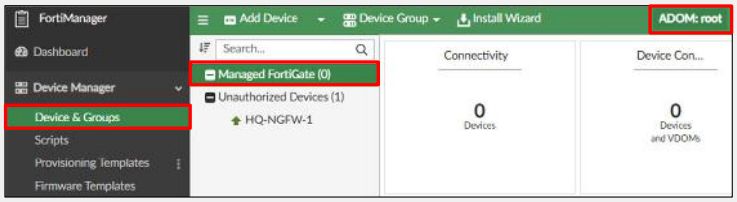
To initiate a registration request from FortiGate, you must configure the central management settings with the FortiManager IP address.

After this, a window opens stating that the management request has been sent to FortiManager. Click **OK** to open the **FortiManager Status** window, where you can authorize the FortiGate device if you have the proper credentials.

The example on this slide shows the configuration in the GUI but you can also use the CLI.

Unauthorized Devices

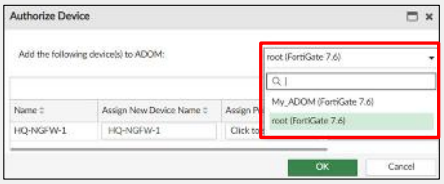
- Unauthorized devices requesting registration appear under **Device & Groups**
  - If ADOMs are enabled, unauthorized FortiGate devices appear in the **root** ADOM



- Can enable automatic registration—the default is disabled

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

- Can add FortiGate to a different ADOM



FORTINET Training Institute

 22

After the request is made from the supported device, it appears under **Device Manager** > **Device & Groups** > **Unauthorized Devices** on the FortiManager root ADOM.

The FortiManager administrator should review the details of the unauthorized device and, if satisfied, authorize the device. Finally, authorizing a device does not create a policy package automatically. For that reason, you must run the **Import Configuration** wizard to import the device firewall policy into a new policy package.

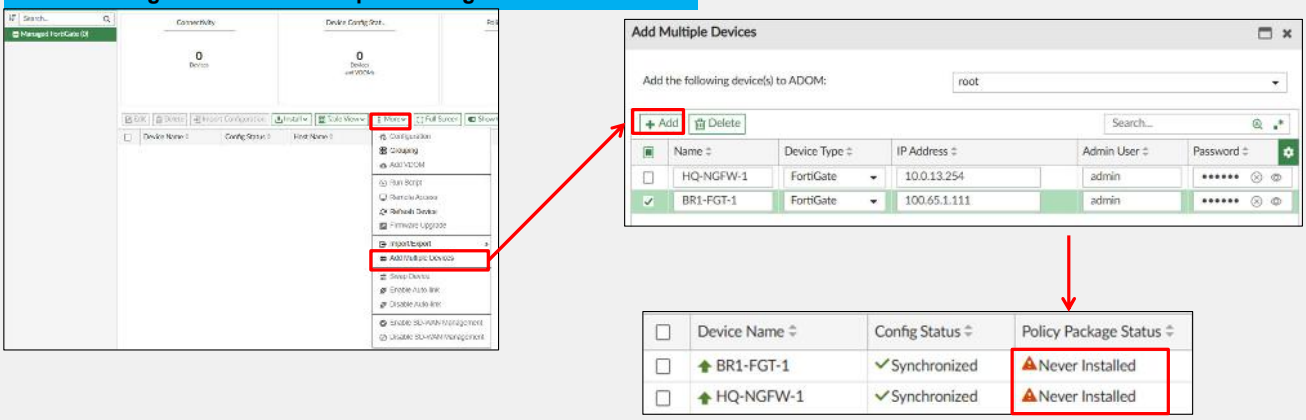
If ADOMs are enabled, the device appears in the **root** ADOM by default, and you can authorize FortiGate to join a different, previously created ADOM.

Optionally, you can enable automatic authorization of unauthorized devices from the FortiManager CLI.

Add Multiple Devices

- Can add multiple devices from the **Device Manager**
- Policy package must be imported after devices are added

Device Manager > Device & Groups > Managed FortiGate > More



FORTINET Training Institute

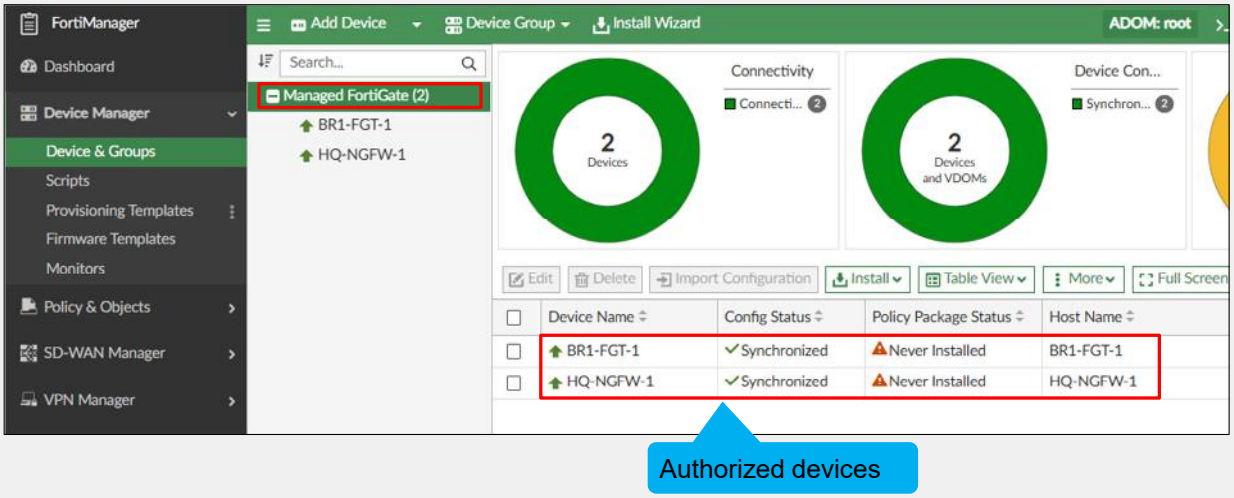
 23

If you need to add multiple FortiGate devices at the same time you can use the **More** button under **Manage Devices**. You can click **Add** and enter the IP address, username, and password of each FortiGate device that you want to add.

Like in the case of adding an unauthorized device, policy packages are not automatically created. You must run the **Import Configuration** wizard to import the device firewall policies into a new policy package.

Viewing Authorized Devices

- **Device Manager** lists all authorized (and unauthorized) devices



FORTINET Training Institute

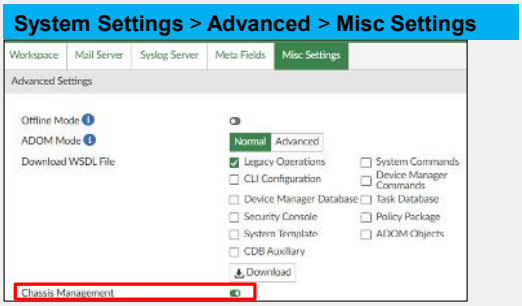
 24

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

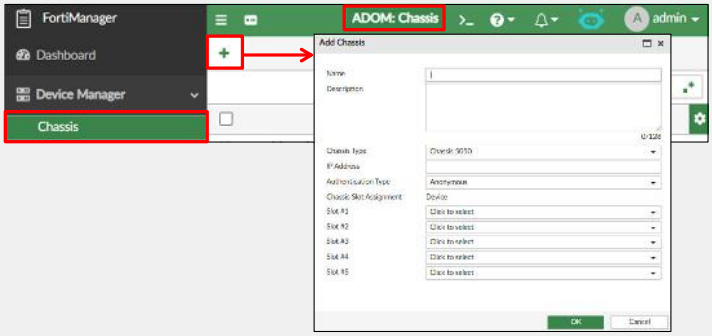
Chassis Management

Some FortiManager devices support chassis management

- Enable chassis management under **System Settings** > **Advanced** > **Misc Settings**



- Added under default chassis ADOM
  1. Type the IP address of the shelf manager running on the chassis
  2. You can select FortiGate, FortiCarrier, or FortiSwitch as a slot



FORTINET Training Institute

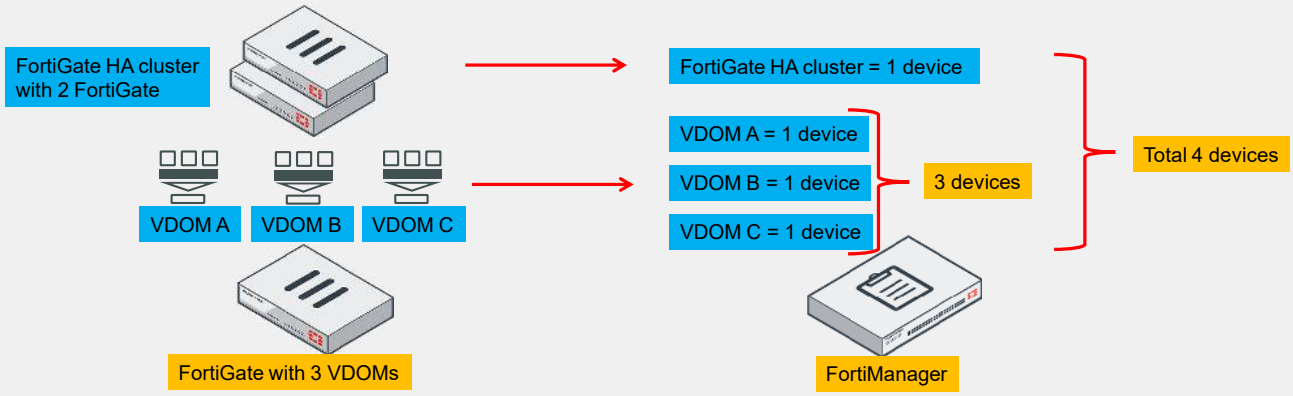
 25

Some FortiManager models can work with the Shelf Manager to manage the FortiGate 5000 series chassis. To do so, you first must enable **Chassis Management** on **System Settings** > **Advanced** > **Misc Settings**. 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, power entry modules (PEM), fan tray, shelf manager, and shelf alarm panel (SAP).

Device Count on FortiManager

- Maximum number of managed devices/VMs is determined by model and license
  - Check product data sheet model limits
- Each FortiGate HA cluster counts as one device
- Each VDOM counts as one device



FORTINET Training Institute

 26

FortiManager physical devices or VMs support a limited number of managed devices. That number depends on the FortiManager model and license.

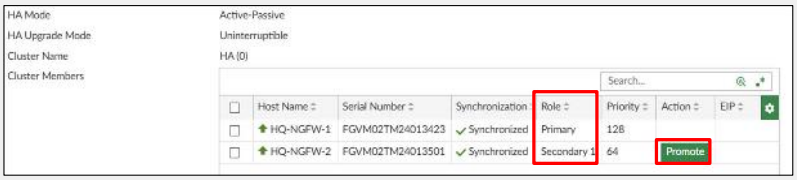
A FortiGate high availability (HA) cluster counts as a single managed device in FortiManager. This is because the bulk of the configuration relates to the firewall policies and objects, and devices in the cluster are running the same configuration.

When using VDOMs, each one counts as one managed device. This is because each VDOM is logically a separate firewall and has its own configuration.

On the example on the slide, there is a FortiGate cluster with two device members, and another FortiGate with three VDOMs. This yields a total of four devices managed by FortiManager. Note that in this example the physical FortiGate is not managed by FortiManager.

Considerations When Managing FortiGate HA Clusters

- A FortiGate cluster is managed as a single device
- You can use `diagnose dvm device list` to see the cluster members
- FortiManager reports the FortiGate HA sync status received from the cluster
- The FortiGate HA configuration is read-only in FortiManager
  - **One exception**: You can promote a secondary device to be the primary device



- Local changes to the cluster configuration do not cause an out-of-sync state in FortiManager
- You should not use the `ha-mgmt-interface` or the standalone management VDOM to establish the FGFM connection

FORTINET Training Institute

 27

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 cluster device members.

FortiManager reports the FortiGate HA synchronization status it receives from the cluster, allowing you to identify possible network issues. You need to refresh the GUI session to see the most up-to-date status information.

FortiManager has read-only access to the FortiGate HA configuration. However, you can promote a secondary cluster member to become the primary from FortiManager.

FortiGate configuration changes concerning HA parameters do not modify the system checksum for FortiManager (`get system mgmt-csum`) and do not cause an out-of-sync state.

It is not recommended that FortiGate devices in an HA cluster use the ha-mgmt-interface or the standalone management VDOMs to establish the FGFM connection since they are designed specifically to manage the cluster directly.

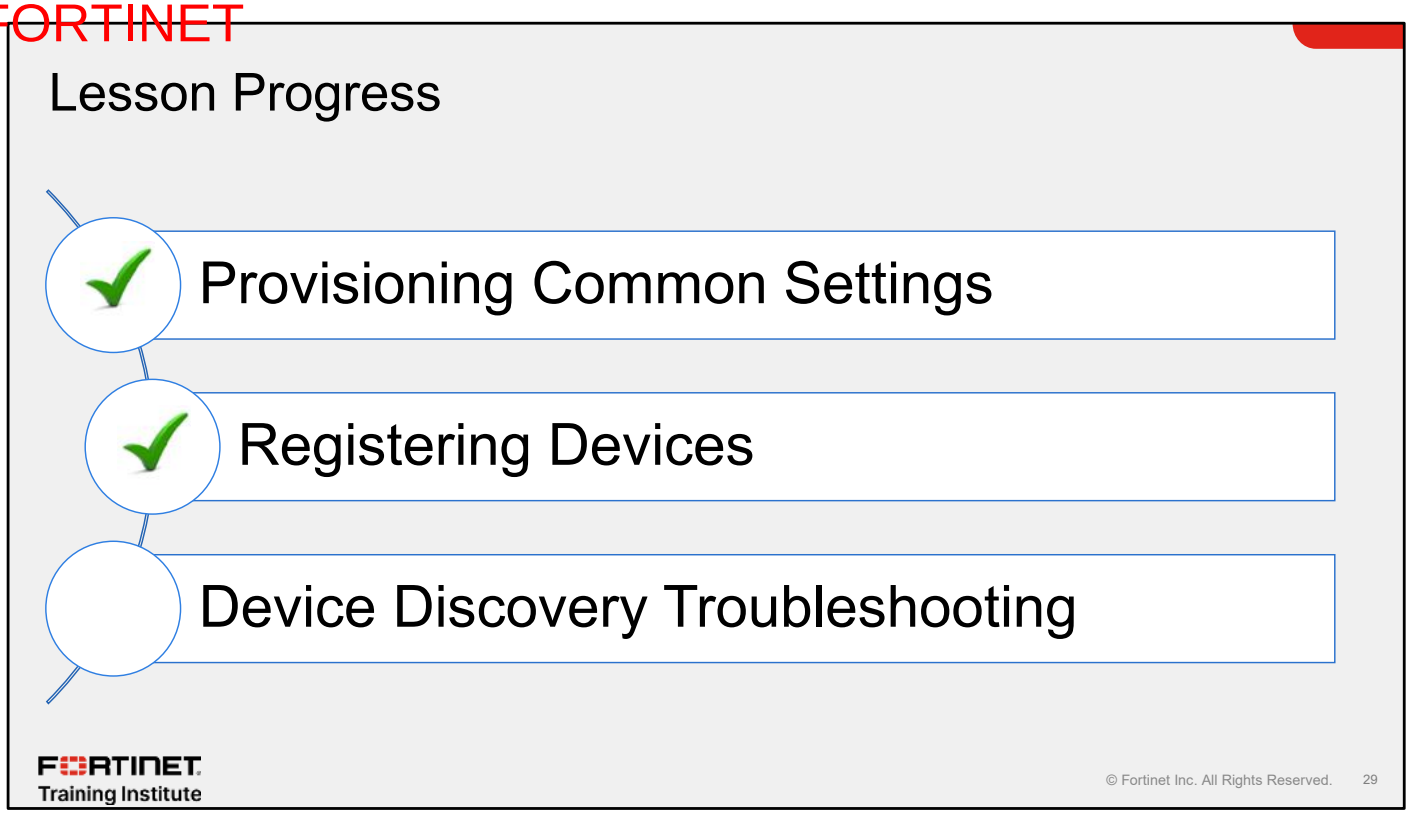
Knowledge Check

1. Which combination of methods can you use to link the model device to the real device?
   - ✓ A. IP address and serial number
   - B. Serial number and pre-shared key

2. Which information can you obtain with the `# diagnose dvm device list` command?
   - ✓ A. The individual cluster members of the FortiGate HA cluster
   - B. A list of pending device configuration changes

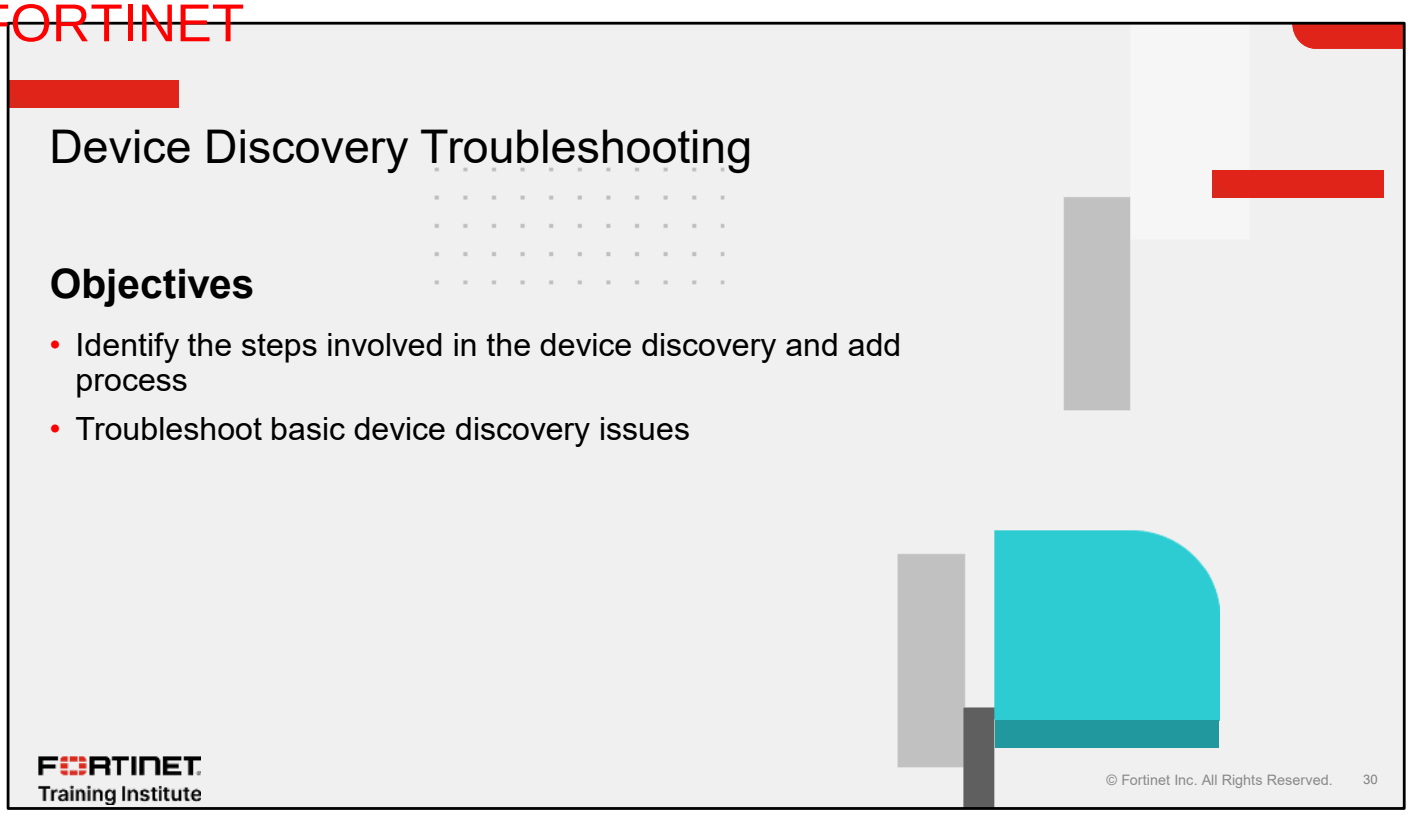
FORTINET Training Institute

 28



Good job! You now understand how you can register devices on FortiManager.

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



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.

FGFM Management Protocol

- An FGFM daemon runs on both:
  - In FortiGate: process `fgfmd`
  - In FortiManager: process `fgfmsd`
- Secure communication tunnel uses port TCP 541
  - Established between FortiManager and all managed FortiGate devices
  - TCP-based, therefore supports port-based NAT
- The protocol must be 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 of the FortiGate

FORTINET Training Institute

 31

The management protocol FGFM runs on both FortiGate (`fgfmd`) and FortiManager (`fgfmsd`). FortiManager and FortiGate create a secure tunnel using 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 must enable the **FMG-Access** setting for each interface facing FortiManager.

Once you have configured the management tunnel, it can be established in either direction—by FortiManager or by the managed FortiGate device. FortiManager uses link-level addressing from the `169.254.0.0/16` subnet for the tunnel. 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.

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 executed to obtain minimal information to start modeling the device
  2. Adding
     - Various other configuration details are obtained through CLI commands. The configuration is retrieved and stored in the device database
- The FGFM tunnel is initiated by either of the following:
  - By FortiManager, during add and discovery process
  - By FortiGate, if a management request is sent by FortiGate

FORTINET Training Institute

 32

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

1. Discovery: In this step, FortiManager sends a `get system status` 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 device database.

The secure FGFM tunnel can be initiated by either device, FortiGate or FortiManager, depending on the registration method used.

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 authorized.

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 "10.0.13.254"
end
..
get ips rule status
get ips decoder status
get application name status
```

Discovery of device

The adding process starts here

Command to check hard disk changes on FortiGate

Setting FortiManager serial number and IP address

Retrieving IPS signature information

FORTINET Training Institute

 33

When FortiManager is discovering and adding FortiGate, it sends several commands to FortiGate to get its complete information. This slide shows only some of those commands.

To see the complete list of commands, you can run the `diagnose debug cli 8` command on FortiGate, while you add it to FortiManager.

Basic Discovery Failure Checklist

What to investigate	Common solutions
Does the FortiManager administrator have sufficient privileges to add FortiGate?	Check the FortiManager administrator profile
Is FortiManager in offline mode?	Disable offline mode in the system settings
Are the FortiGate parameters correct in the **Add Device** wizard?	Confirm that the FortiGate IP address, credentials, serial number, and pre-shared key are correct
Is FGFM access on FortiGate interface disabled?	Enable FGFM access on the FortiGate interface facing FortiManager

- Additionally, you can check if the required ports are open in all intermediary devices and run the `diagnose sniffer packet` command to examine the traffic sent and received

FORTINET Training Institute

 34

Refer to this basic checklist if FortiManager is having issues discovering FortiGate devices:

- Verify that you have sufficient administrator privileges in FortiManager to add a FortiGate device.
- Verify that offline mode is disabled. Remember that offline mode is enabled after a configuration restore.
- Verify that parameters like credentials, IP address, serial numbers, and pre-shared keys are correct in the **Add Device** wizard.
- Verify that FGFM access is enabled on the FortiGate interface facing FortiManager.

Additionally, you can check if the required ports are open in all intermediary devices and run the `diagnose sniffer packet` command to examine the traffic sent and received.

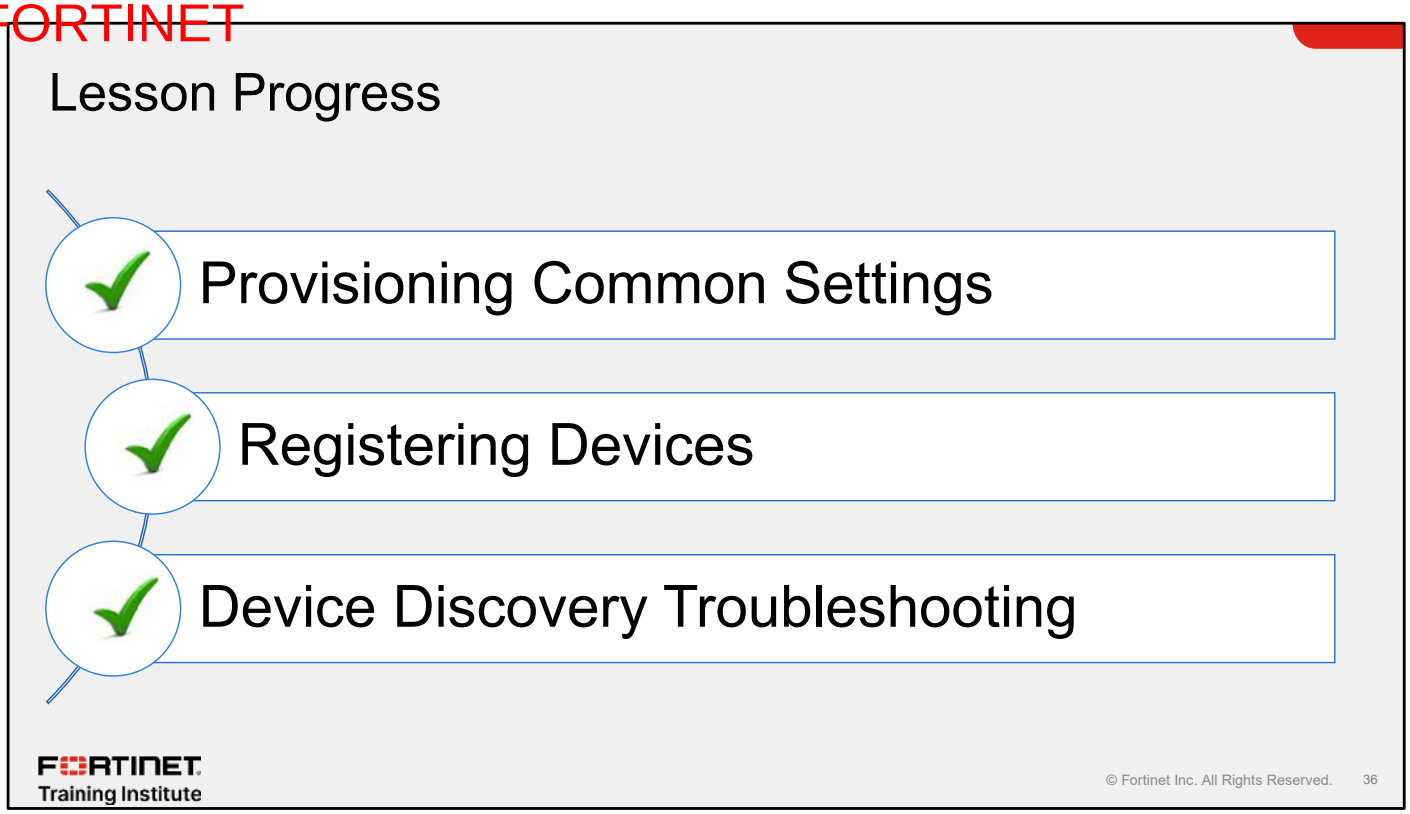
Knowledge Check

1. Where do you enable FGFM access on FortiGate?
   - ✓A. At the FortiGate interface level
   - B. At a FortiGate fabric connector

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

FORTINET Training Institute

 35



Congratulations! You have completed this lesson.

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

Review

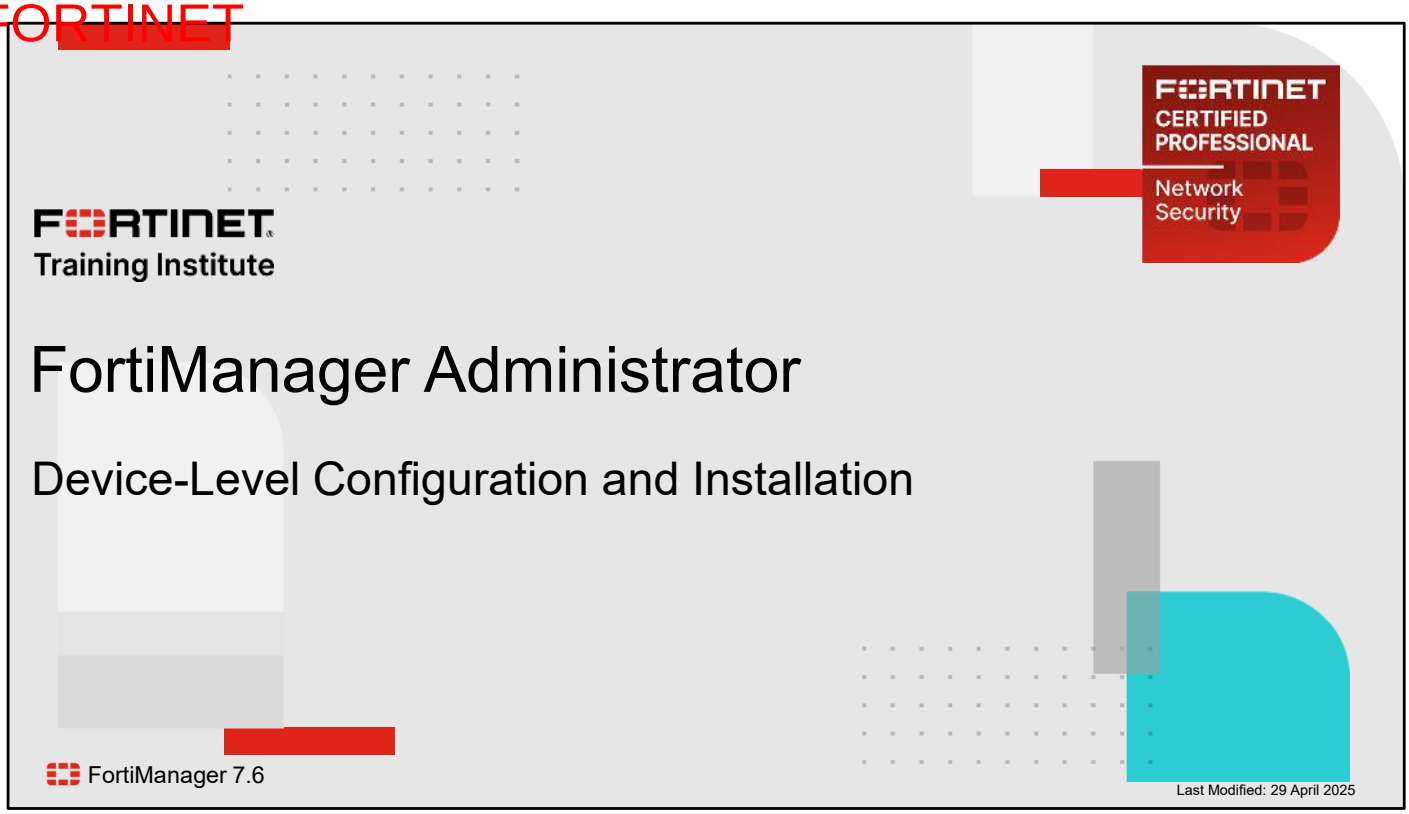
- ✓ Configure provisioning templates
- ✓ Copy system templates between ADOMs
- ✓ Register devices using multiple methods
- ✓ Explain the import report
- ✓ Identify the steps involved in the device discovery and add process
- ✓ Troubleshoot basic device discovery issues

FORTINET Training Institute

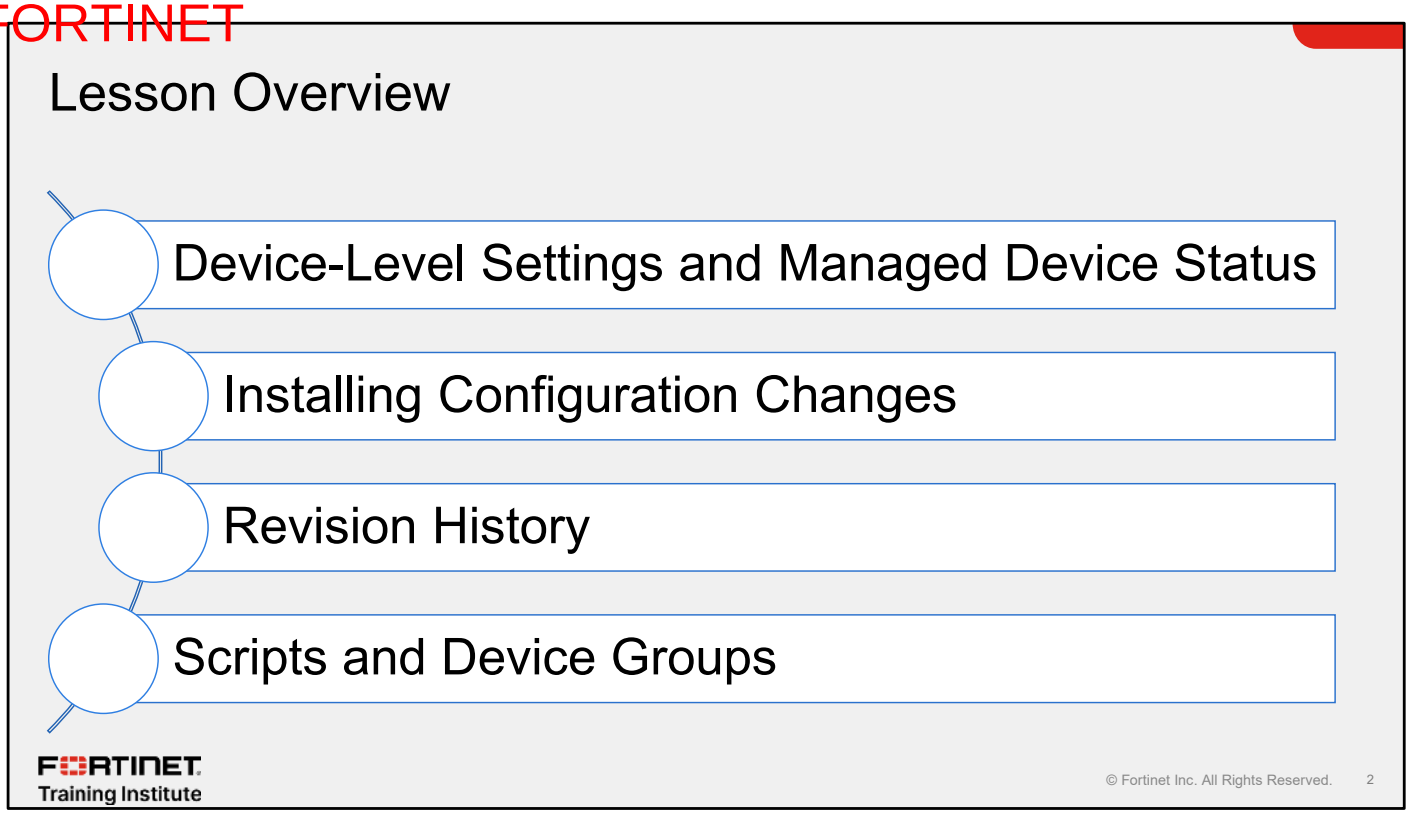
 37

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

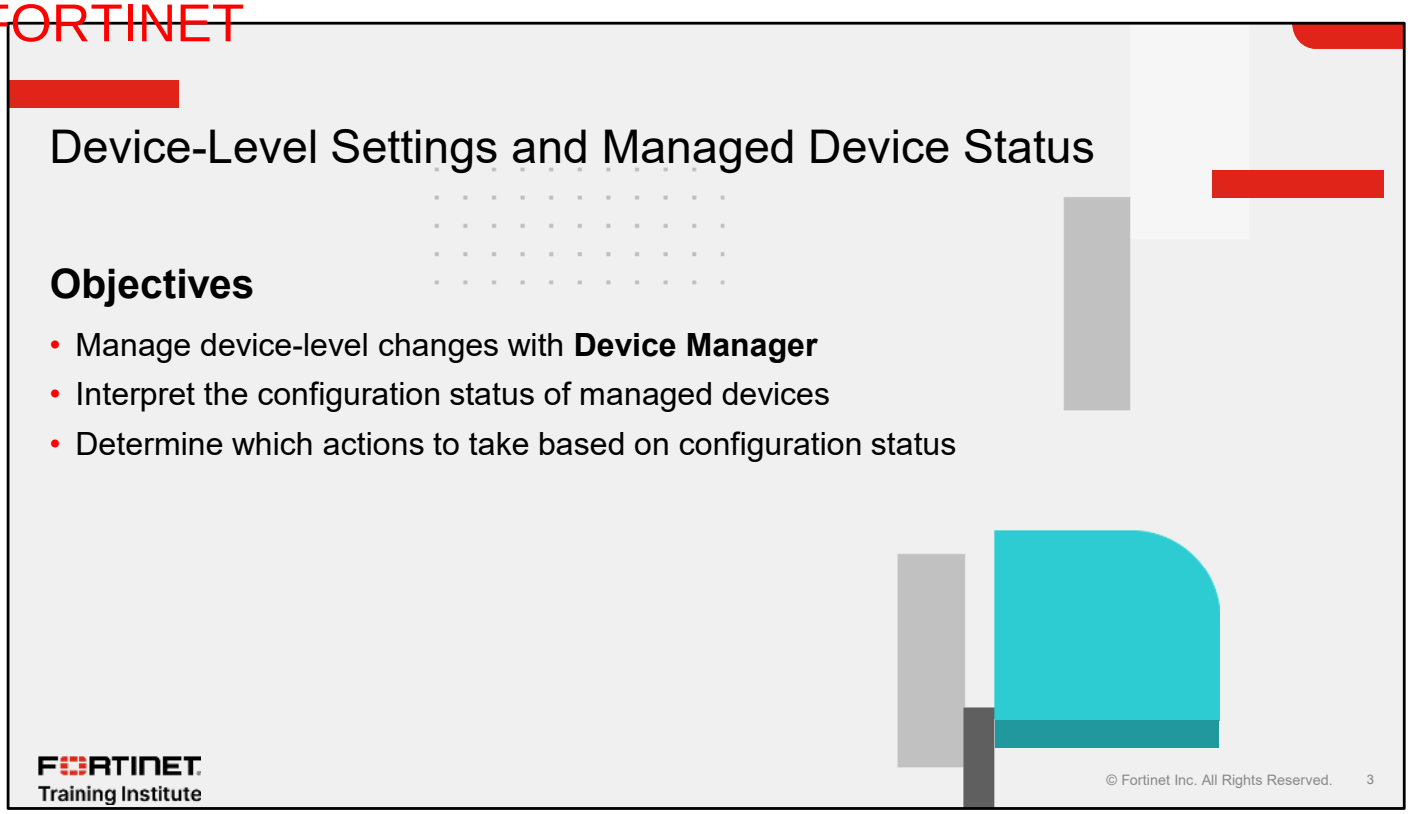
By mastering the objectives covered in this lesson, you learned about the primary functions of the device manager, and how to register FortiGate devices on FortiManager.



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 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.



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

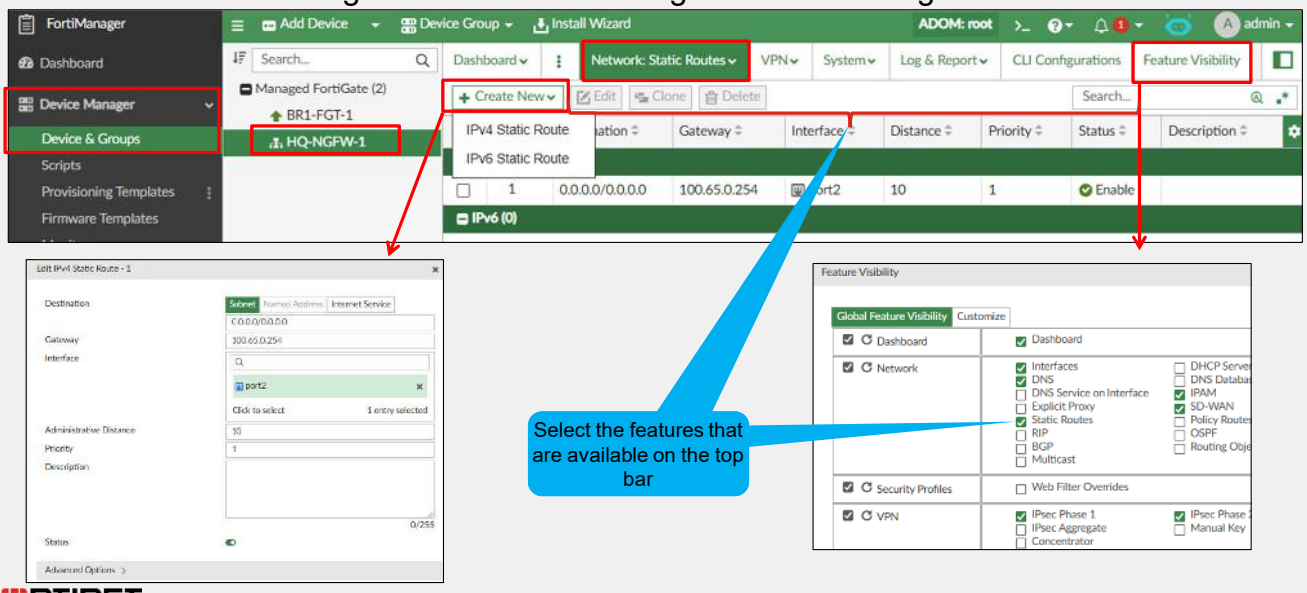


After completing this section, you should be able to achieve the objectives shown on this slide.

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.

Device-Level Settings

- You can view and configure device-level settings for each managed device



FORTINET Training Institute

 4

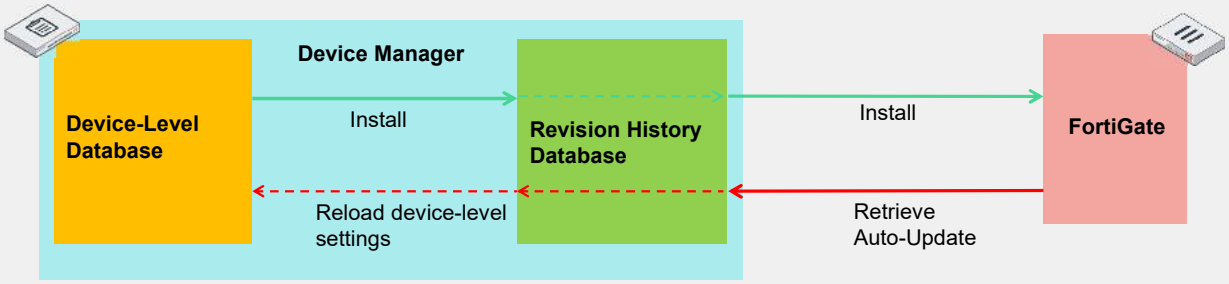
You can configure device-level settings by selecting the desired device under **Device & Groups** > **Managed FortiGate**. You can manage the available settings by selecting them from the toolbar, which includes tabs to configure network, VPN, and system settings, among others. Most of the settings that you find here have a one-to-one correlation with the options that you would see if you logged in locally using the FortiGate GUI or CLI.

When you make changes to device-level settings, you must install them in order to apply them. You will learn about installing configuration changes in this lesson.

You can choose the options that you want to hide or show on the toolbar. The available options are determined by the features supported by the device and the firmware version.

Managed Device Status

Config Status	Device-Level DB and Revision History DB	Revision History DB and FortiGate	Recommended action
Synchronized and Auto-update	✓	✓	Nothing, all sync
Modified	×	✓	Install changes →
Out of Sync	✓	×	← Retrieve changes
Conflict	×	×	← Retrieve changes Install changes →
Unknown	?	?	← Retrieve changes



FORTINET Training Institute

 5

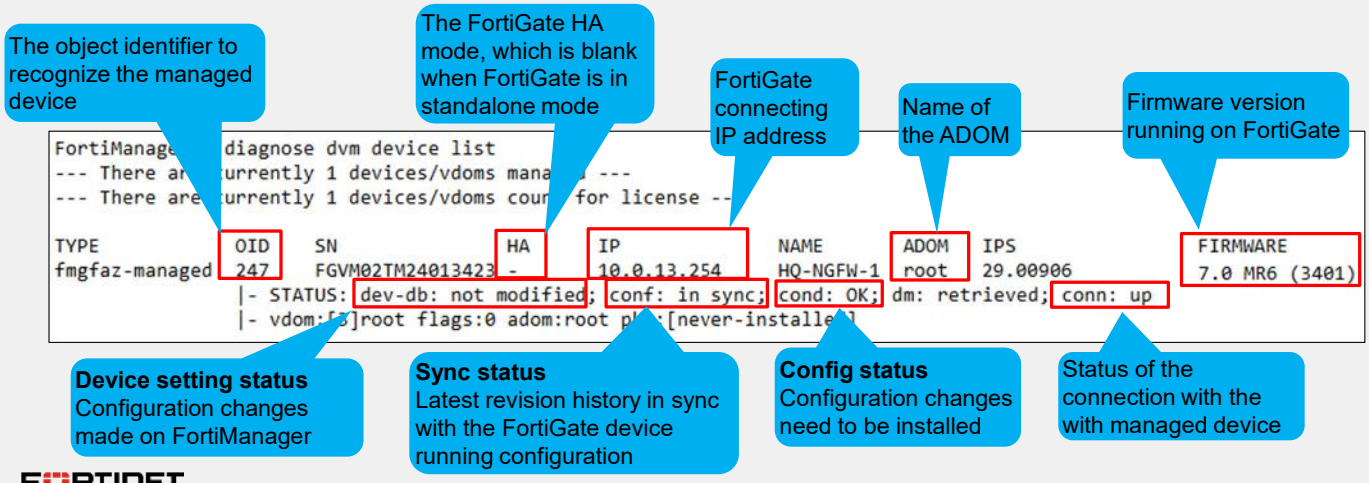
This diagram shows the different statuses a managed FortiGate can have. FortiManager keeps FortiGate configurations in the revision history. FortiManager compares the latest revision history with the FortiGate configuration to provide the configuration statuses. FortiManager also compares the latest revision history with the FortiGate device-level database, 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 on FortiManager. Device statuses are as follows::

- **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 FortiManager.
- **Conflict**: An installation failed. This status can also indicate that changes made locally on Fortigate were not retrieved and changes were made on FortiManager. To resolve this conflict, you can retrieve the configuration or install the changes from FortiManager.
- **Unknown**: The FortiManager is unable to determine the synchronization status because FortiGate is not reachable or due to a partial install failure. It is recommended that you perform a retrieve from FortiManager.

Device List

- Use the `diagnose dvm device list` command to display details of all managed and unregistered devices
- The configuration of each FortiGate is stored in a separate device-level database (**dev-db**)



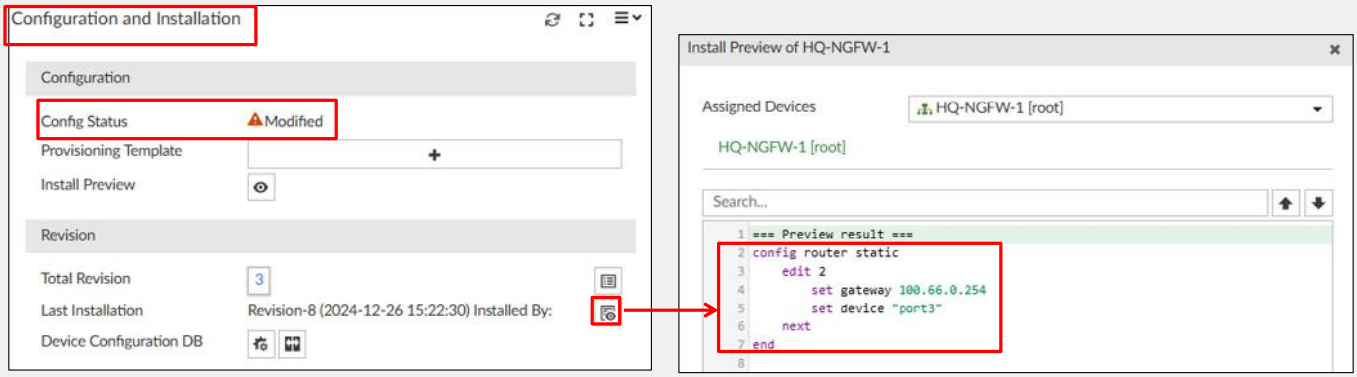
The `diagnose dvm device list command` provides the list of all devices managed by FortiManager, as well as any unregistered devices. Registered VDOMs are also listed here. This output provides the serial number, connecting IP address, firmware, high availability (HA) mode, status for device-level settings and policy packages, and more.

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

Finally, this command also shows whether the FortiGate-FortiManager (FGFM) communication protocol tunnel between FortiGate and FortiManager is up or down.

Installation Preview

- Displays device-level changes made on FortiManager
  - Example: adding a new static route
  - Does not display ADOM-level changes
- Changes have not been installed on the managed device



FORTINET Training Institute

 7

You can view the changes made to the device database on FortiManager by clicking **Install Preview** in the **Configuration and Installation** widget. The preview includes the exact commands that will be installed on FortiGate during the next installation.

This slide shows a new static route that will be pushed to FortiGate during the next installation. Because a configuration change was made, but it still hasn't been installed on the device, the **Config Status** is **Modified**.

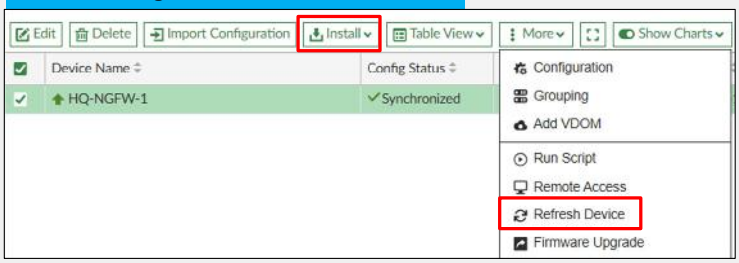
FGFM Session List and Refresh Connection

- Use the `diagnose fgfm session-list` command to display the status of FGFM tunnels for all managed devices
  - Includes the link-local IP address used in the tunnel

```
FortiManager # dia fgfm session-list
        HQ-NGFW-1(247) sn(FGVM02TM24013423) ip(10.0.13.254)
                state(tunnel) tunnel(169.254.0.4) uptime:Thu Dec 26 15:22:14 2024
        Session count = 1 (tunnel 1)
```

- Click **Refresh Device** to reestablish the connection
  - Recovers basic information about the managed device

Device Manager > More > Refresh Device



FORTINET Training Institute

 8

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-local addresses assigned by FortiManager to FortiGate devices for management traffic.

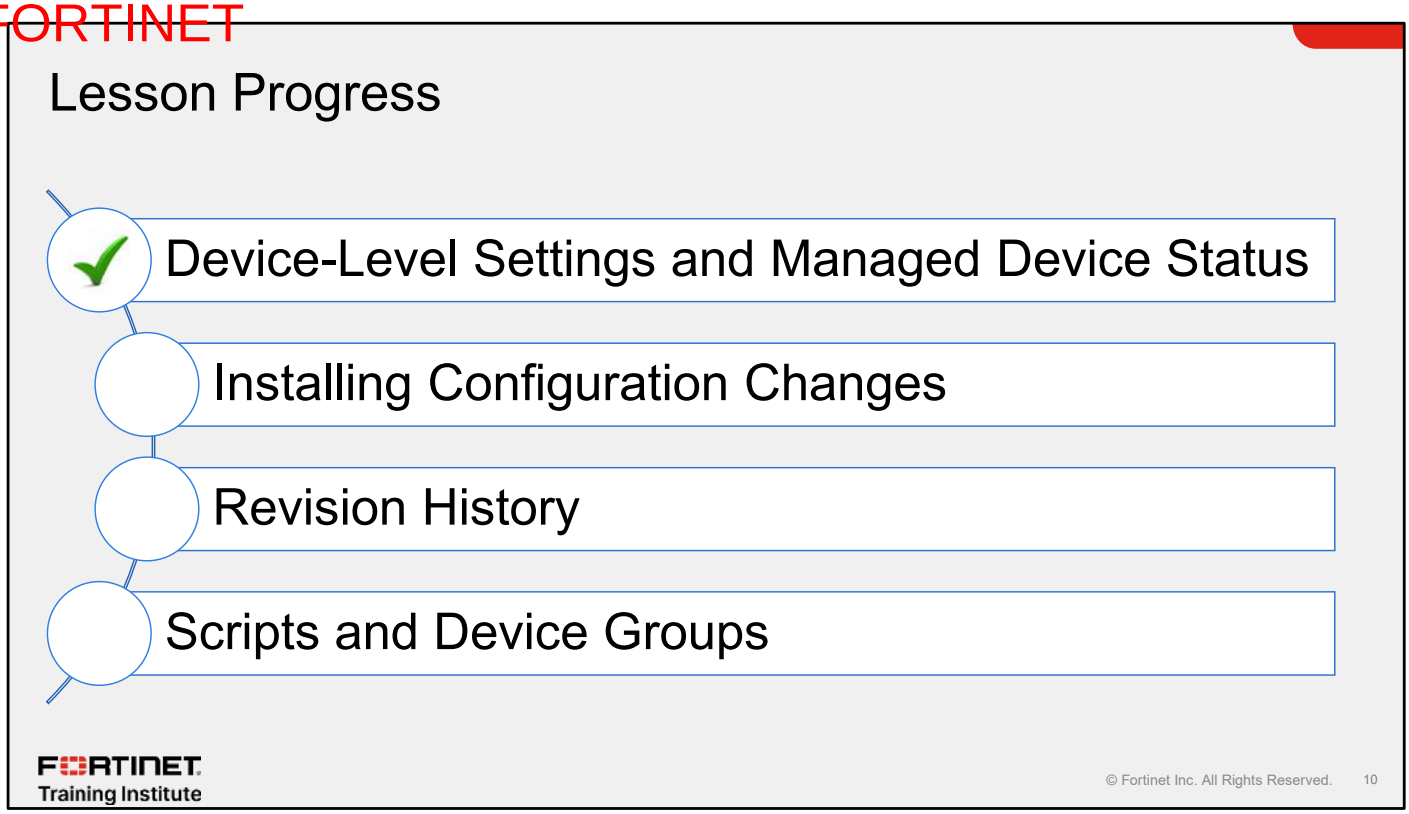
If you need to reestablish the connection between the selected device and FortiManager, you can use the **Refresh Device** option to update the device status and retrieve basic information about the managed device, such as serial number, firmware version, support contracts, and FortiGate HA cluster member information.

Knowledge Check

1. How does FortiManager determine that 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 a configuration status of **Modified** indicate?
   - A. Configuration changes made directly on FortiGate were automatically updated on FortiManager.
   - ✓B. Device-level configuration changes were made on FortiManager for the managed device.

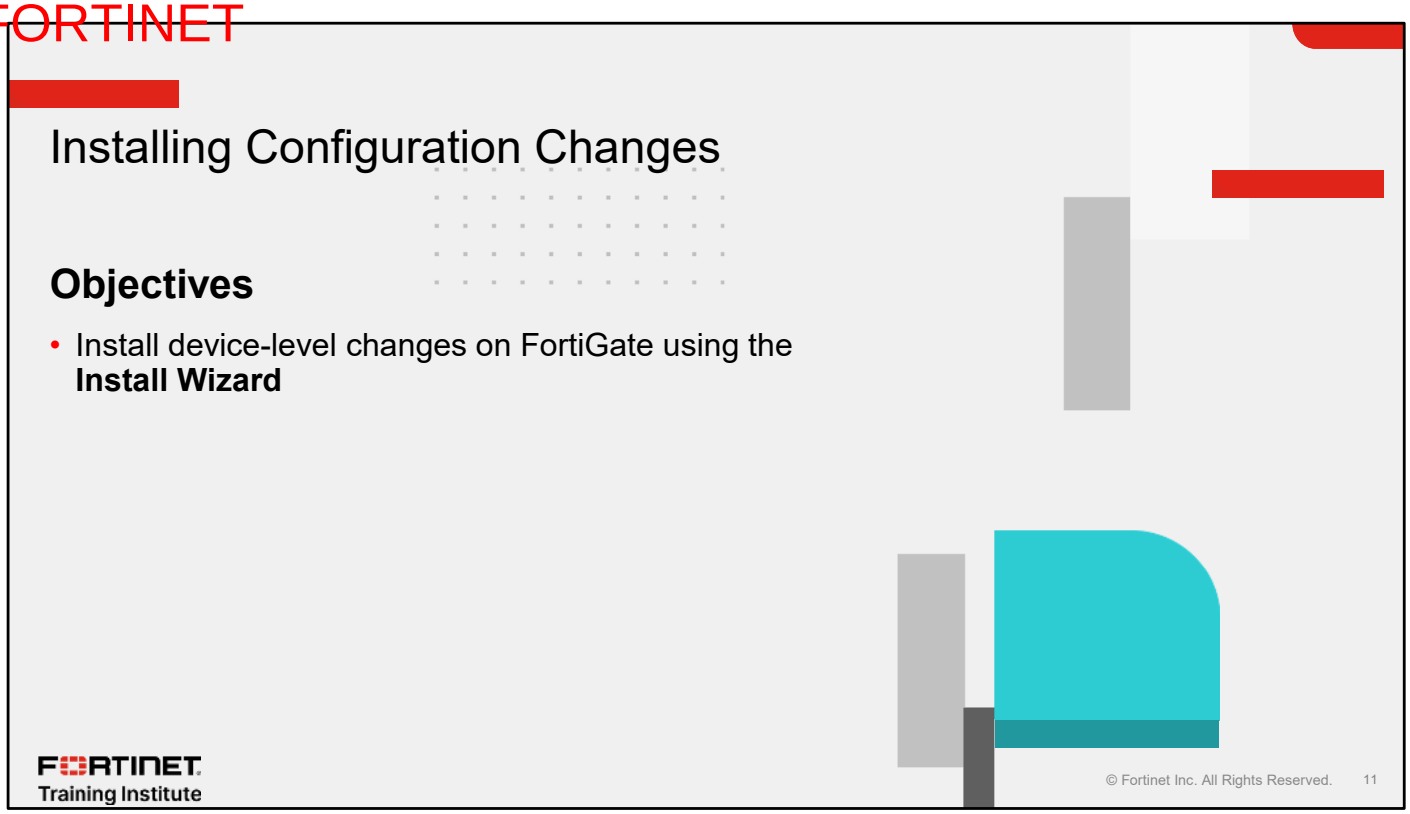
FORTINET Training Institute

 9



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

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

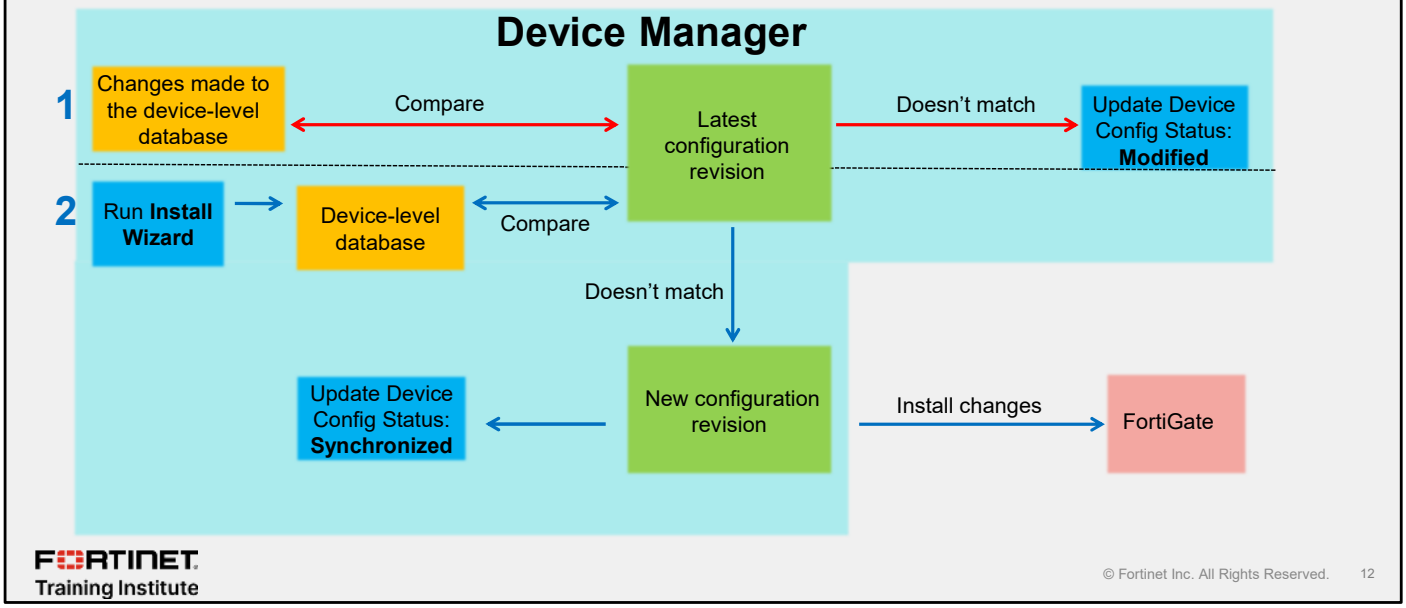


After completing this section, you should be able to achieve the objective shown on this slide.

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

Device Status and Installation Process

- What happens when you make changes and install them from FortiManager?



FORTINET Training Institute

 12

This slide shows what happens when the configuration status of a managed FortiGate is updated after you make a change on FortiManager, as well as the process that takes place when you run the **Install Wizard** to install those changes.

FortiManager keeps FortiGate configurations in the revision history. The latest revision history is compared with the FortiGate configuration to provide the configuration status and the status is updated if needed.

When you install a new configuration, FortiManager compares the latest configuration revision with the changes made on FortiManager. If they are different, FortiManager creates a new revision and installs the changes on the managed device.

Installing Device Settings

- Use the **Install Wizard** to apply the new settings on one or more FortiGate devices
- Two options are available:

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

 13

Configuration changes you make on the **Device Manager** do not take immediate effect—you must install them. Until you install the changes, the configuration status of the device remains as **Modified**. You use the **Install Wizard** to install changes.

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

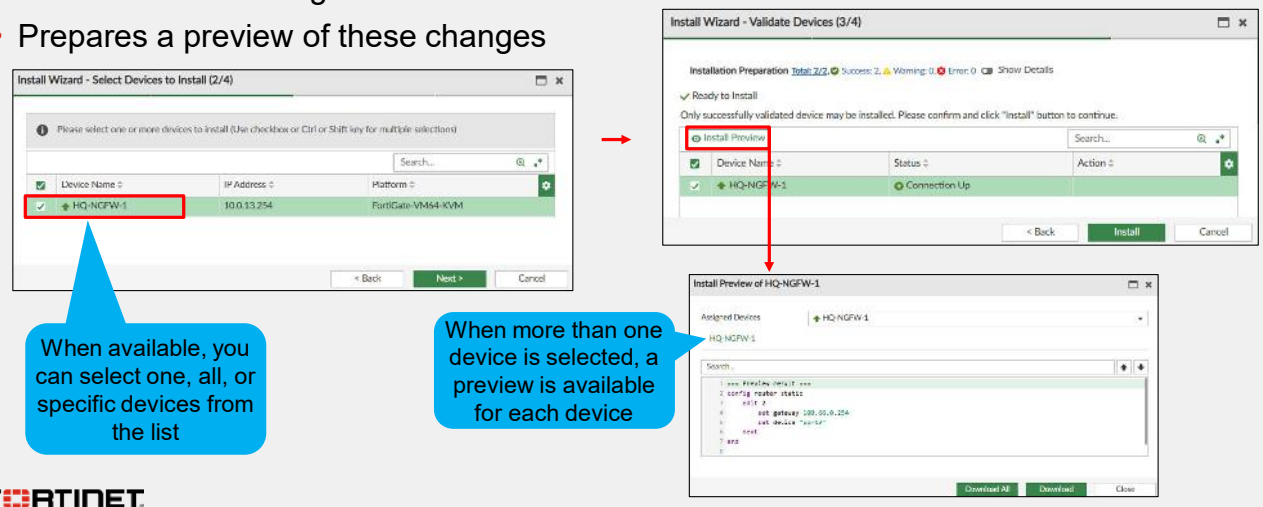
If you choose **Install Device Settings (only)**, the wizard installs only device-level configuration changes made from FortiManager. If you have made changes to the device-level configuration and policies in the policy packages, you can choose **Install Policy Package & Device Settings**, which installs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

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

In the example on the slide, **Install Device Settings (only)** is selected. After the installation is complete, FortiManager and FortiGate will be back in sync, and the **Config Status** will change from **Modified** to **Synchronized**.

Install Wizard—Device Selection and Validation

- You must indicate where to install changes
- You can select multiple devices
- Verifies device settings that will be installed
- Prepares a preview of these changes



FORTINET Training Institute

 14

After you choose the installation type, you need to select the device on which you want to install the changes. If you have made device-level changes to multiple devices on **Device Manager**, you can select multiple devices on which to install those changes.

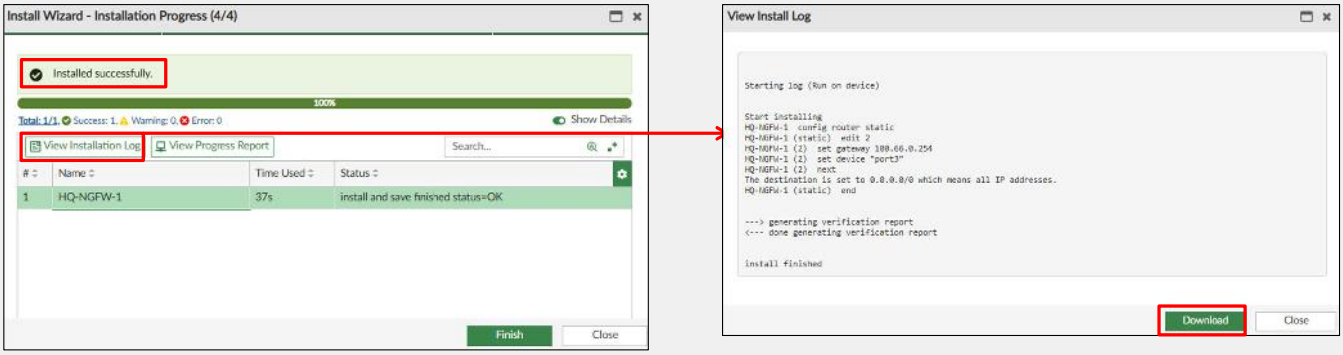
The next step is validation. The **Install Wizard** checks the device settings and compares them with the latest running revision history. At this point, you can click **Install Preview** to view the configuration changes that will be installed on the managed FortiGate. You can click **Download** to download the preview. The file is saved in a TXT file.

As a best practice, you should always preview and verify the changes before you commit them 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.

Install Wizard—Installation

- Indicates where changes were installed
- Indicates the installation status
- Provides **Install Log**



FORTINET Training Institute

 15

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

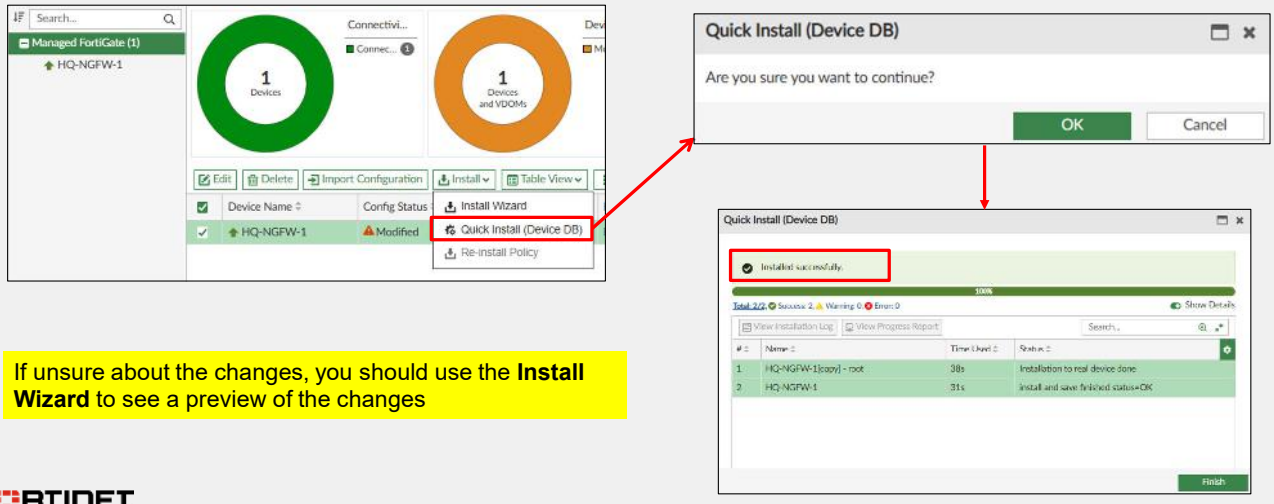
The log also shows any errors or warnings that occurred during the installation process. Click **View Installation Log** to view the configuration changes installed on the managed FortiGate. If the installation fails, the installation log provides an indication of the stage where the failure occurred.

Optionally, you can download the installation log for your records, or to use it as a reference for future installations.

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

Managed FortiGate—Quick Install (Device DB)

- Installs device-level changes on FortiGate without launching the **Install Wizard**
- Does not provide an installation preview



If unsure about the changes, you should use the **Install Wizard** to see a preview of the changes

FORTINET Training Institute

 16

The **Quick Install (Device DB)** option enables 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 before installing them. Administrators should be certain of the changes they intend to make before using this option because the installation can't be cancelled after the process is initiated.

If you are not sure about the changes, you must use the **Install Wizard** to preview changes before committing them.

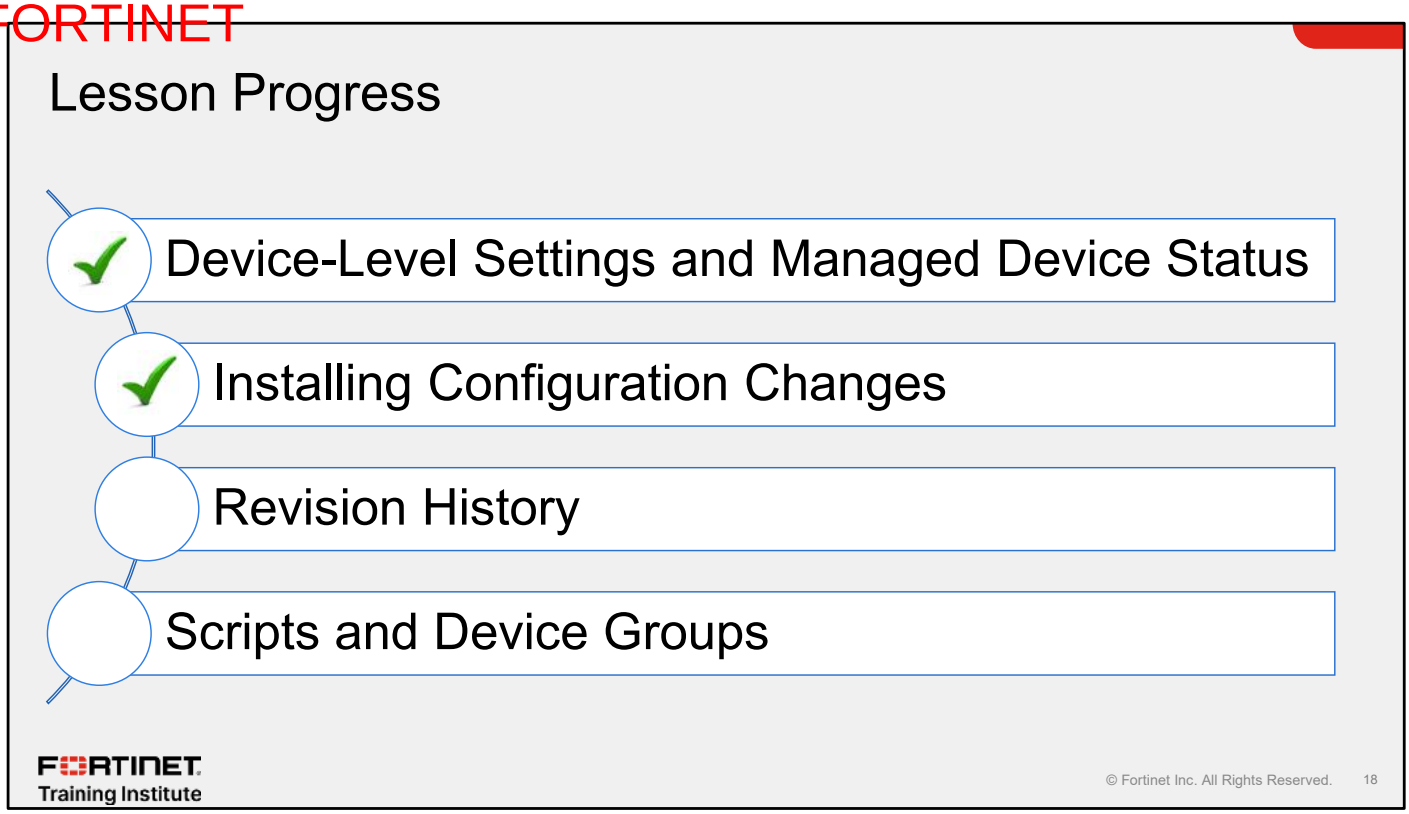
Knowledge Check

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 changes before installation?
   - ✓ A. **Install Wizard**
   - B. **Quick Install (Device DB)**

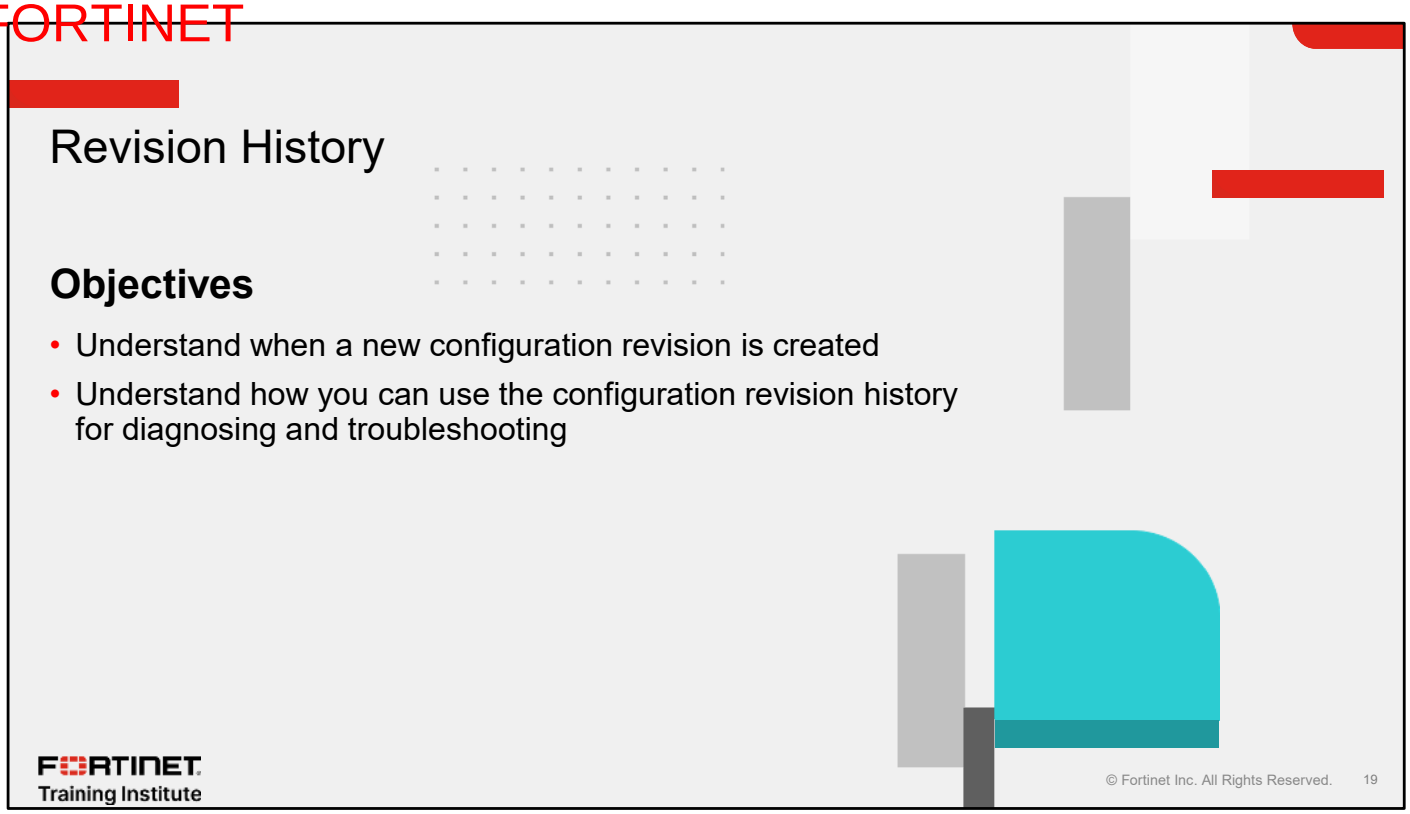
FORTINET Training Institute

 17



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 devices on FortiManager.



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

By demonstrating competence in using the configuration revision history, you will be able to diagnose and troubleshoot common issues related to FortiGate configuration changes.

Configuration Revision Creation and Troubleshooting

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

FORTINET Training Institute

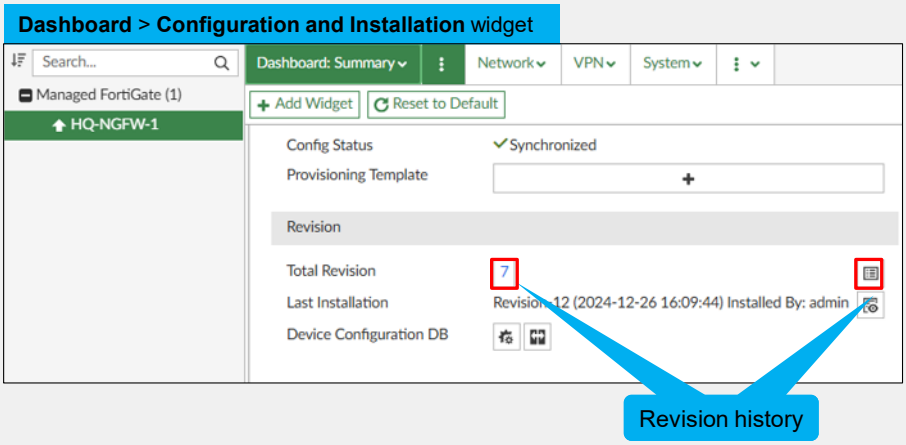
 20

Several operations, such as adding a device, installing changes, retrieving a configuration, or the occurrence of an automatic update cause the creation of a configuration revision.

FortiManager maintains a repository of the configuration revisions associated with its managed devices. This collection is the configuration revision history and allows the FortiManager administrator to examine configuration changes between revisions, view the installation history, and view which administrator or process created the new configuration revision. This is very useful for troubleshooting.

Revision History

- The repository stores all configuration revisions for devices
  - Tags each revision with an ID number
  - Identifies which administrator or process created the revision
- You can:
  - View the version history
  - Download the configuration
  - Compare different revisions
  - View the installation log
  - Revert the configuration

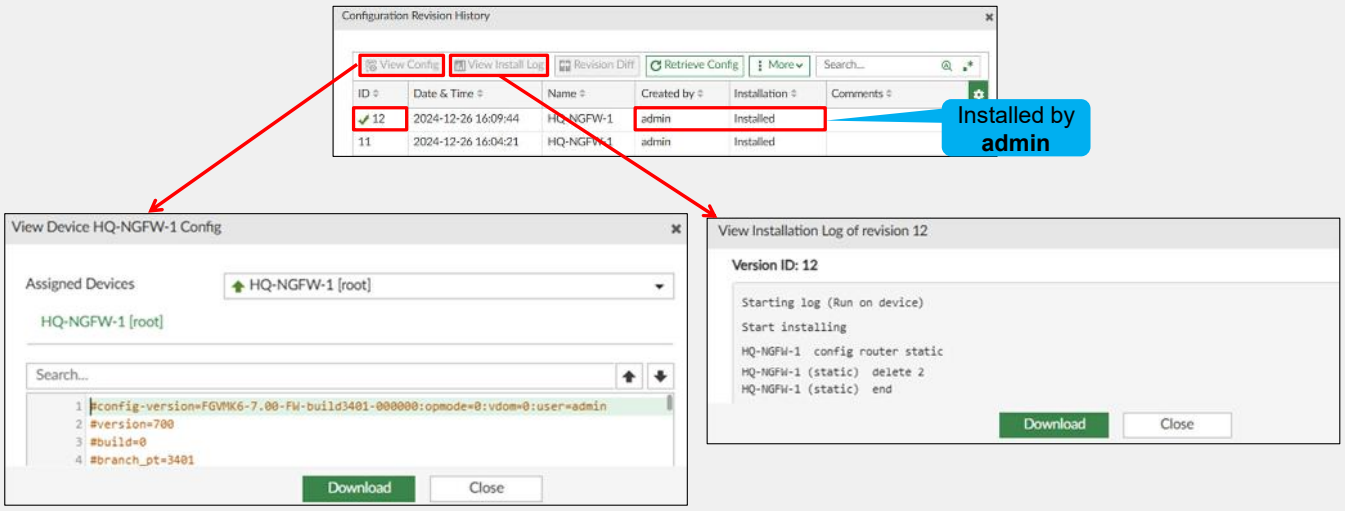


FORTINET Training Institute

 21

To examine the revision history, select the device and use the **Configuration and Installation** widget to view, download, or compare the differences between revisions.

Revision History—Viewing Configuration and Installation Details



FORTINET Training Institute

 22

Several important pieces of information are available when you examine the **Configuration Revision History**. The **Installation** and **Created by** columns provide details about the action, process, and administrator that created the revision.

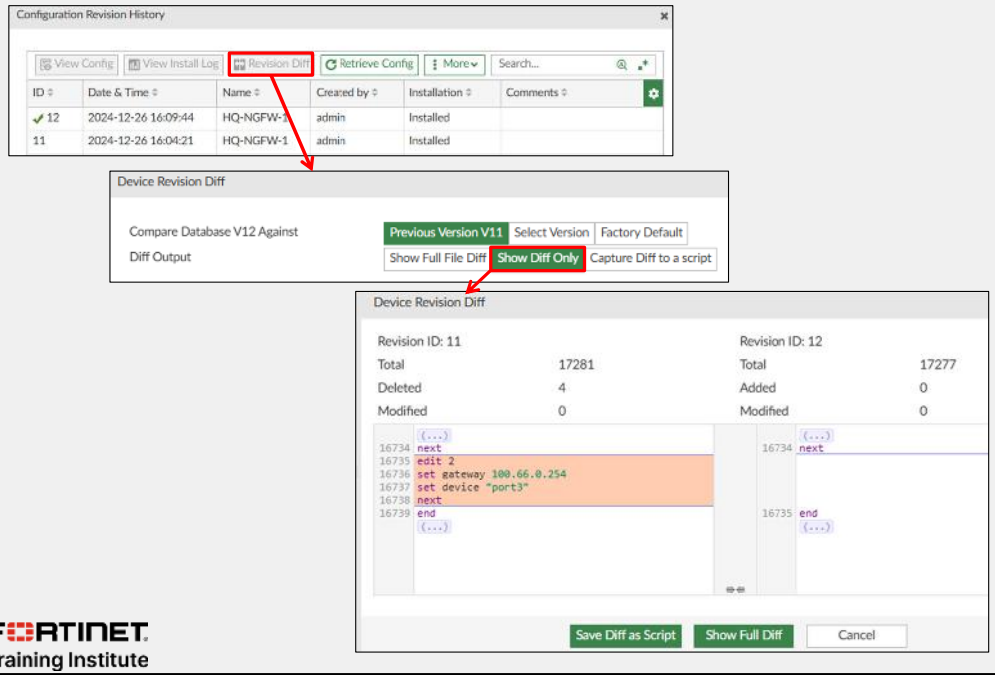
You can select any revision to view or download the corresponding configuration revision. This includes the complete configuration of the managed device, not just the device-level configuration.

You can also compare the differences between versions 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. You can choose to show the full configuration with differences, or just the differences like the example on this slide.

The **View Install Log** option is available only from entries with the status of **Installed**. You can use this option to see which commands were sent to and accepted by, the device, as well as the commands that were not accepted if any errors occurred.

You can download all of the configuration and installation details to a file. One way that you could use the information in the file to create configuration scripts.

Revision History—Revision Diff



FORTINET Training Institute

 23

Several important pieces of information are available in the **Configuration Revision History** window. The **Installation** and **Created by** columns provide details about the action, process, and administrator that created the revision.

You can select any revision to view or download the corresponding configuration revision. This includes the complete configuration of the managed device, not just the device-level configuration.

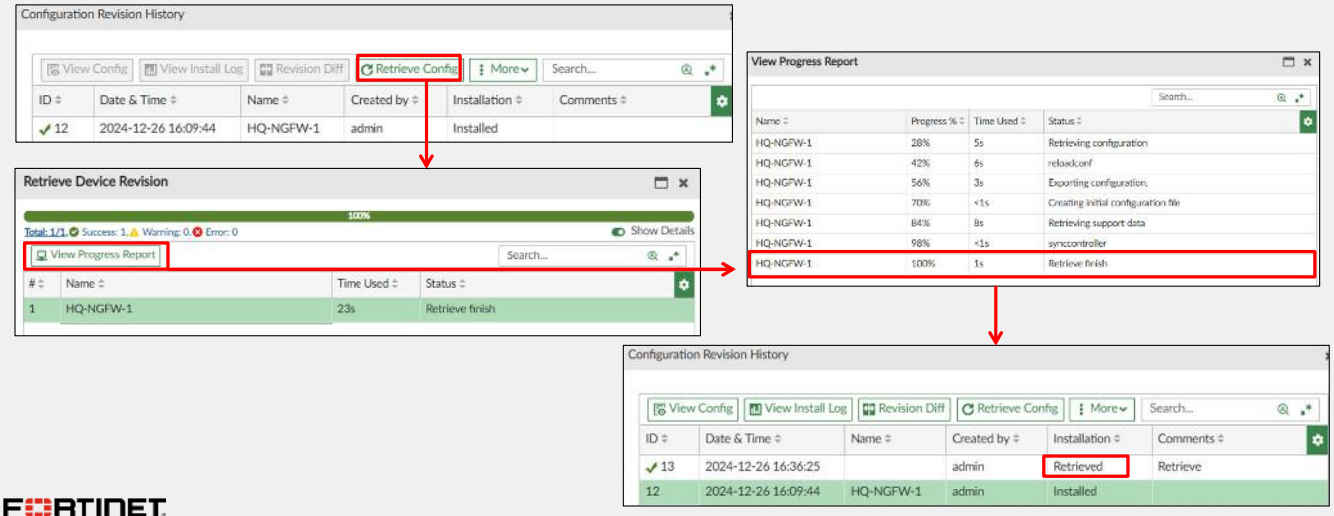
You can also compare the differences between versions by clicking **Revision Diff**. You can compare the revision history to a previous version, select a specific version, or compare it to the factory default configuration. You can choose to show the full configuration with differences, or just the differences, like the example on this slide.

The **View Install Log** option is available only from entries with the **Installed** status. The log shows which commands were sent to, and accepted by, the device, as well as the commands that were not accepted if any errors occurred.

You can download configuration revision information to a file. One way that you might use this information is to create a configuration script.

Revision History—Retrieve

- Retrieves the current configuration
- Updates FortiManager revision repository



FORTINET Training Institute

 24

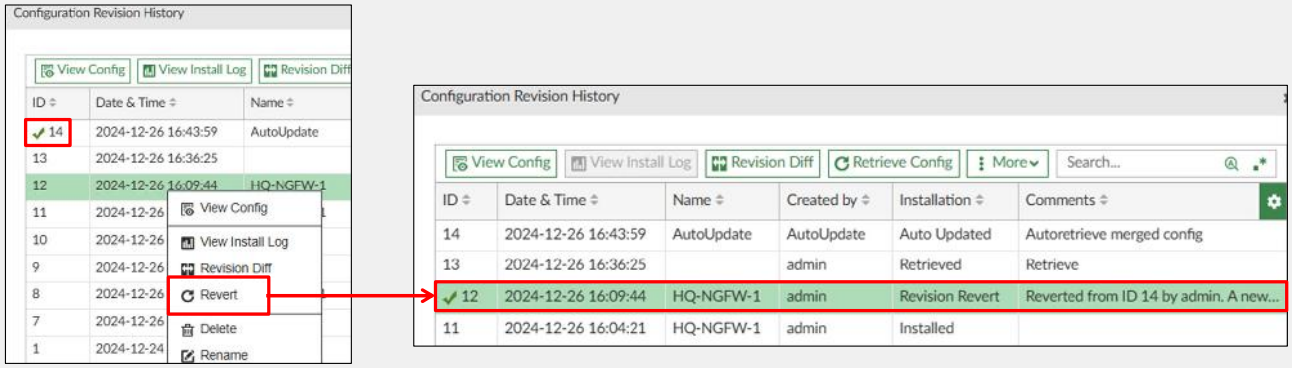
You can use the **Configuration Revision History** window, to create a new revision that is based on the current configuration of a managed device. When you click **Retrieve Config**, FortiManager retrieves the selected device configuration and creates a new revision.

You can use this option to resynchronize FortiGate with the FortiManager device database. After you retrieve the configuration, you must use the **Import Configuration** wizard to ensure the policy information is also synchronized.

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

Revision History—Retrieve (Contd)

- Usually, the top revision entry corresponds to the device manager database configuration, which is synchronized with the FortiGate configuration
- You can revert to a previous configuration revision
  - Reverts only the device database to the previous revision
  - Does not revert policies and objects—you must import them
- You must install reverted changes on FortiGate



FORTINET Training Institute

 25

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.

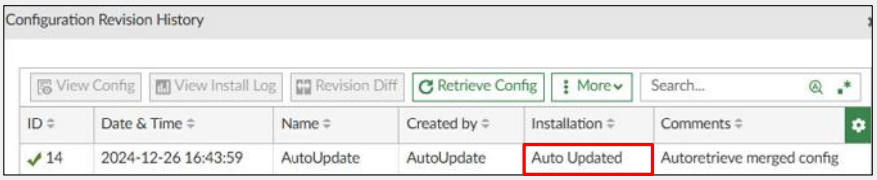
A revert operation reverts the device database configuration to a previous configuration state. You must install these reverted changes on FortiGate. FortiGate then creates a new revision entry which is a copy of the reverted revision and is synchronized with the FortiGate configuration.

You can revert to any previous revision by right-clicking the entry and then clicking **Revert**. The selected entry automatically updates the **Installation** column to **Revision Revert**. FortiManager also updates the **Comments** column with the number of the revision it is reverted from and indicating that a new revision ID will be generated on an install.

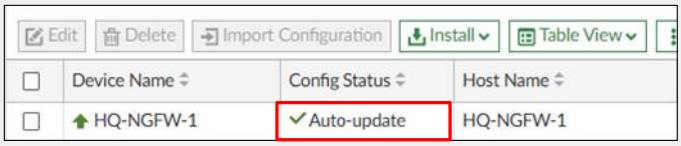
Performing a revert operation followed by an installation only reverts device-level changes and does not revert policy packages. To achieve full synchronization, you must run the **Import Configuration** tool on FortiManager to synchronize the policy package.

Revision History—Automatic Update

- Changing the configuration directly on a managed device creates a new revision



- **Config Status** is updated automatically in **Device Manager**



- You can disable automatic update behavior on the FortiManager CLI
  - Default enabled
  - FortiManager will still show a synchronized status, even if the configurations are different

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

FORTINET Training Institute

 26

By default, all changes made on a managed FortiGate device are automatically updated on FortiManager and reflected in revision history and configuration status of that device.

You can use the commands shown on this slide to disable the default automatic update behavior.

If you disable the automatic update, changes made to FortiGate will not cause updates to the FortiManger device-level database. FortiManager will still show a synchronized status, even if the configurations are different. Disable automatic updates only when you do not want FortiGate changes to override the FortiManager device-level database.

Resolving Device-Level Configuration Issues

- Retrieve the configuration of a managed device
- Modify the configuration locally on a managed device
- Install configuration changes on FortiGate after modifying the configuration on FortiManager
- Revert to the previous working configuration

FORTINET Training Institute

 27

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

- Retrieve the configuration of the managed device.
- Modify the configuration directly on the managed device.
- Modify the configuration on FortiManager and then install it on the managed device.
- Revert to a previous working configuration.

After every retrieve, auto-update, or revert operation, you must use **Import Configuration** to ensure the policy information is synchronized.

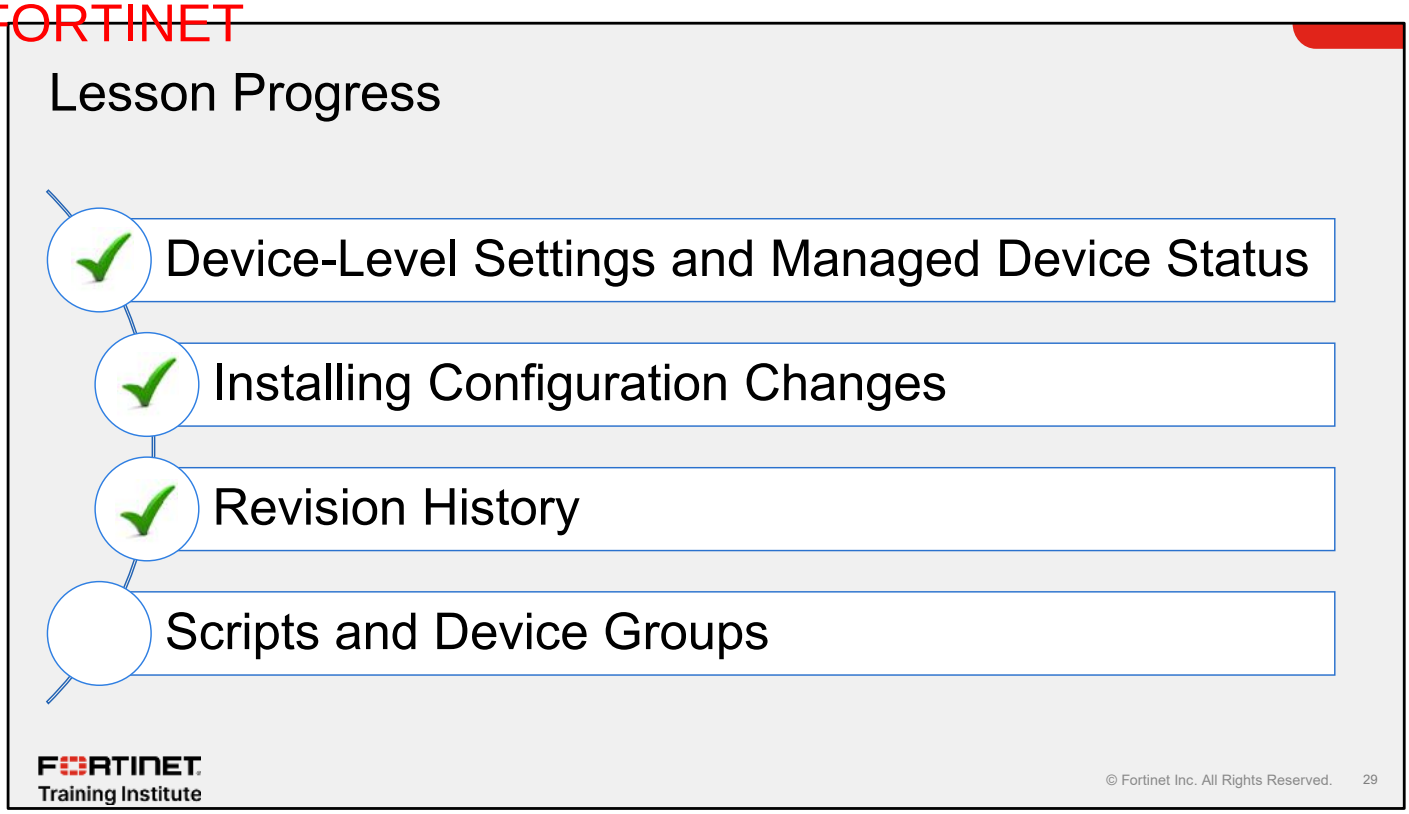
Knowledge Check

1. How can you use the revision history?
   A. To modify FortiManager system settings
   ✓B. To view and download a FortiGate configuration revision

2. How can an administrator use 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.

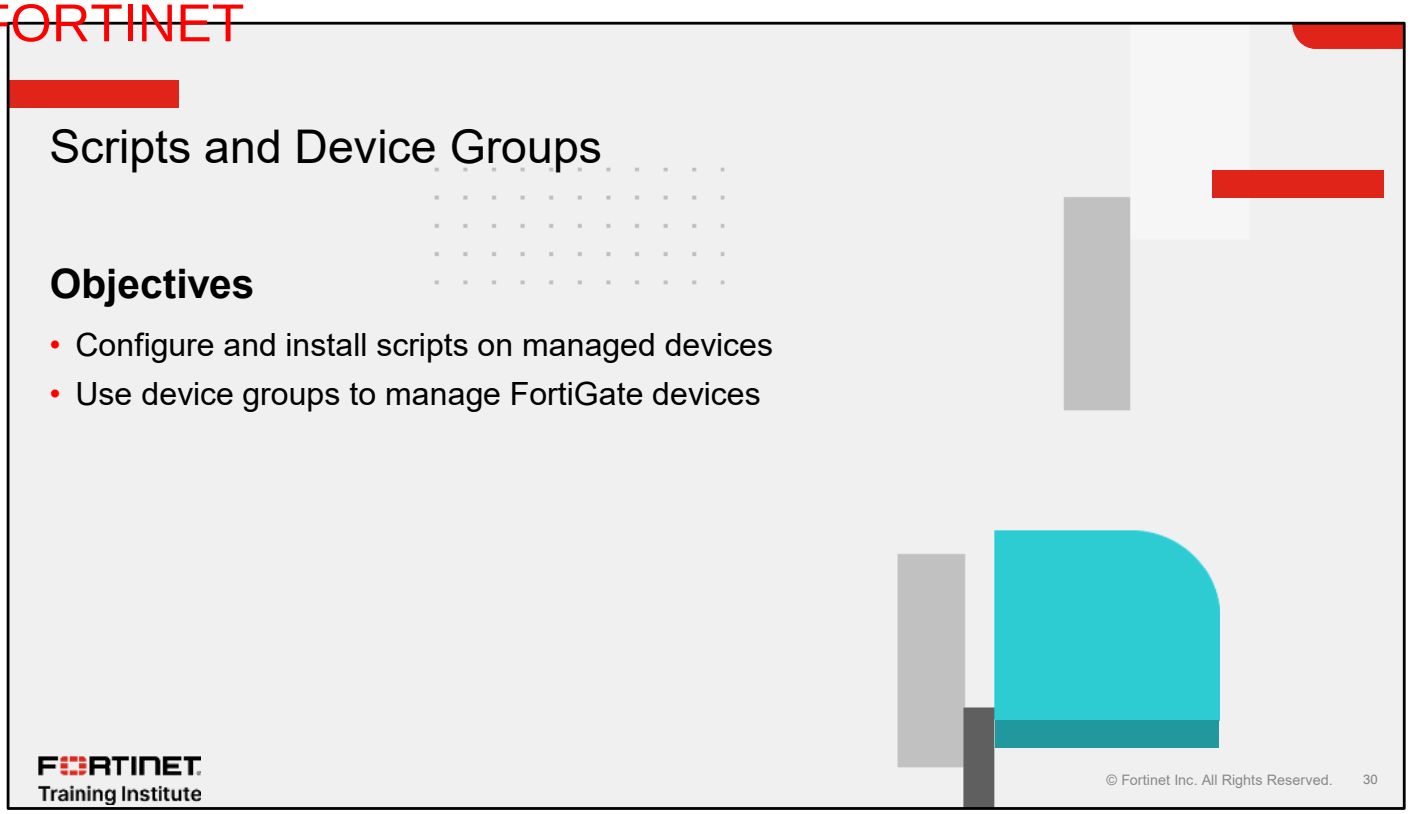
FORTINET Training Institute

 28



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

Now, you will learn about scripts and device groups.

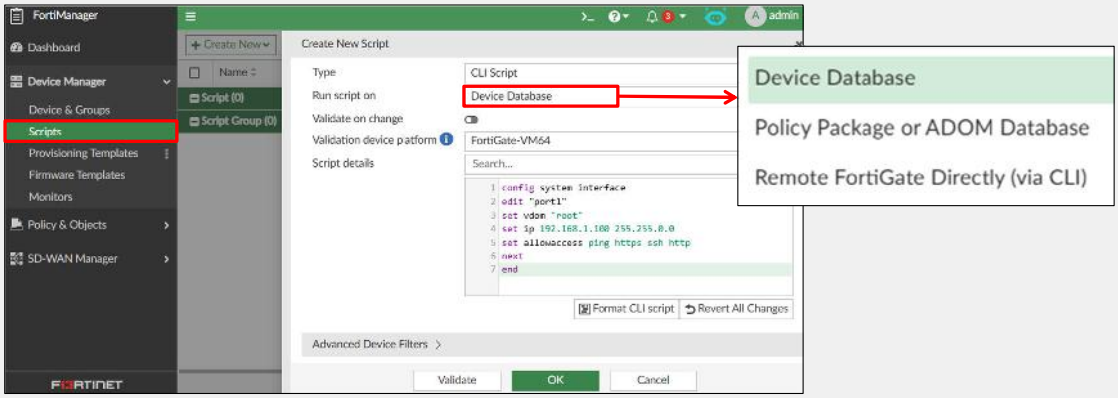


After completing this section, you should be able to achieve the objectives shown on this slide.

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

Scripts

- Automate and simplify bulk changes while ensuring consistency.



CLI scripts are enabled by default

FORTINET Training Institute

 31

You can use scripts to make configuration changes to multiple managed devices at once. By using scripts to automate and simplify bulk changes, you ensure a higher degree of consistency and a decreased chance of errors.

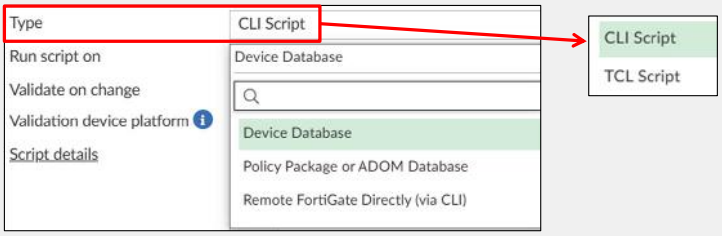
You can run scripts in three different locations. Choose where you run the script based on the changes you are making. :

- **Device Database**: Scripts are executed on the device database by default. When you run a script or make changes to the device database, you can view which configuration changes are sent to the managed device. After you run a script on the device database, you can then install the changes on a managed device using the installation wizard.
- **Policy Package or ADOM Database**: If a script contains changes related to ADOM-level objects and policies, run it on **Policy Package or ADOM Database** instead, and then install the changes using the installation wizard.
- **Remote FortiGate Directly (via CLI)**: When you execute a script directly on a device, the changes are automatically applied on the device. You do not need to take any further action to apply the changes; however, you cannot preview the changes before they are applied.

CLI scripts are enabled by default.

Type of Scripts

- CLI—A sequence of FortiGate CLI commands
- Tool Command Language (Tcl)—A dynamic scripting language that provides more functionality to your scripts, including global variables and decision structures



- Tcl scripts are not run through the FGFM tunnel like CLI scripts. They use SSH and require SSH authentication.

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

TCL scripts are enabled on the FortiManager CLI

FORTINET Training Institute

 32

FortiManager supports two types of scripts:

- CLI: These scripts include only FortiOS CLI.
- Tcl: These scripts allow for the use of global variables and decision structures. You must be familiar with Tcl and regular expressions to use it. For more information about Tcl scripts, visit: http://www.tcl.tk

To use Tcl scripts you must enable them using with the command shown on this slide.

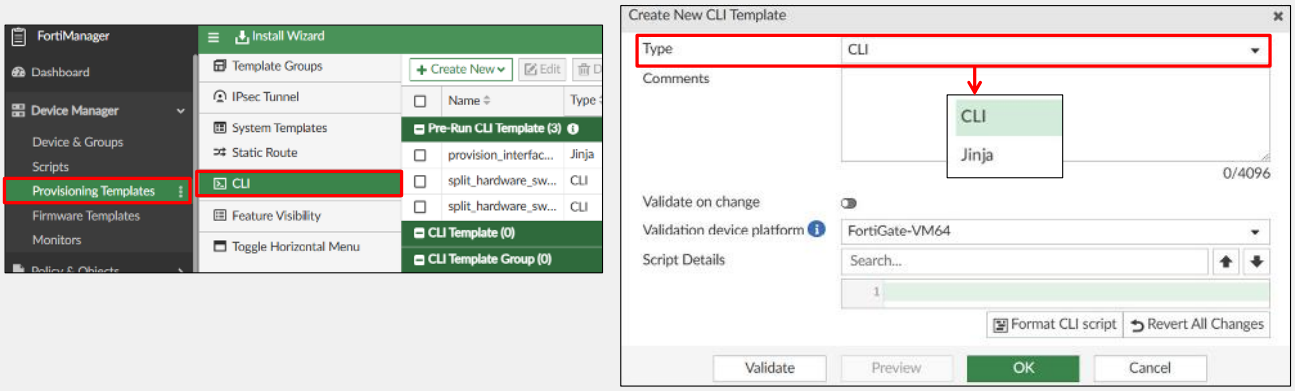
Note that Tcl scripts do not run through the FGFM tunnel like CLI scripts do. Tcl scripts use SSH to tunnel through FGFM and they require SSH authentication to do so. If FortiManager does not use the correct administrative credentials in the device manager, the Tcl script fails.

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.

CLI Templates

- Automate and simplify bulk changes while ensuring consistency



Jinja is enabled by default

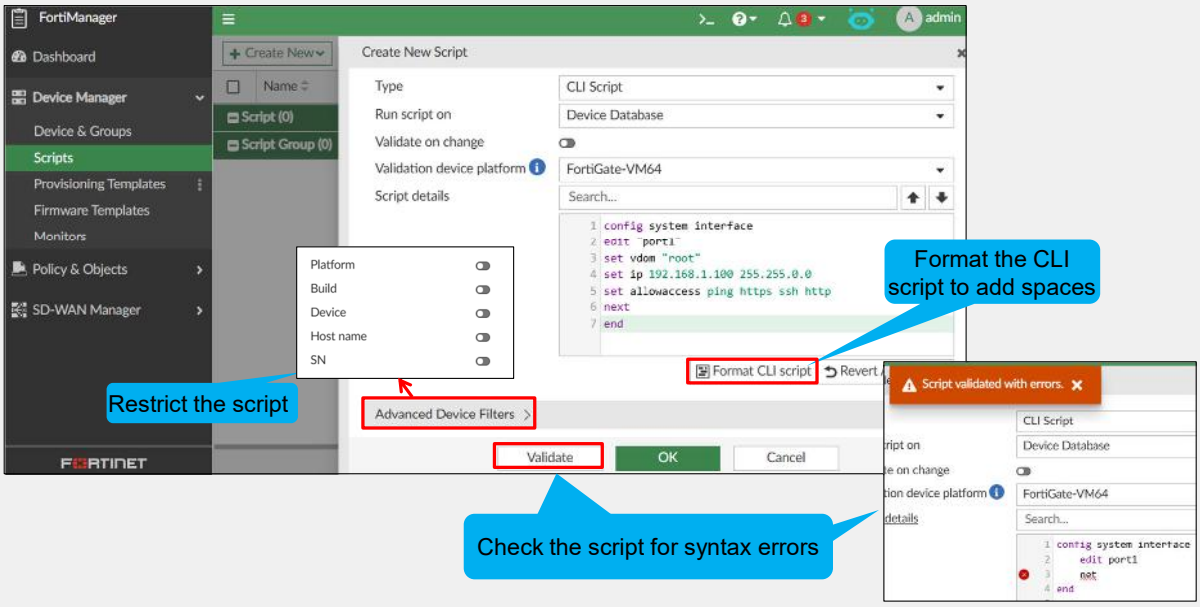
FORTINET Training Institute

 33

You can use CLI templates to make configuration changes to multiple managed devices at once. By using templates to automate and simplify bulk changes, you ensure a higher degree of consistency and a decreased chance of errors.

FortiManager supports two types of CLI templates. The standard CLI templates include only the FortiOS CLI commands that you would use on FortiGate. Jinja CLI templates include placeholders or variables, similar to Python. For more information, see the *Jinja Filters and Functions in CLI Templates* document in the **FortiManager** section at www.docs.fortinet.com.

Configuring Scripts



FORTINET Training Institute

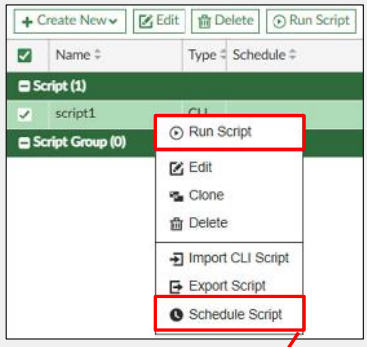
 34

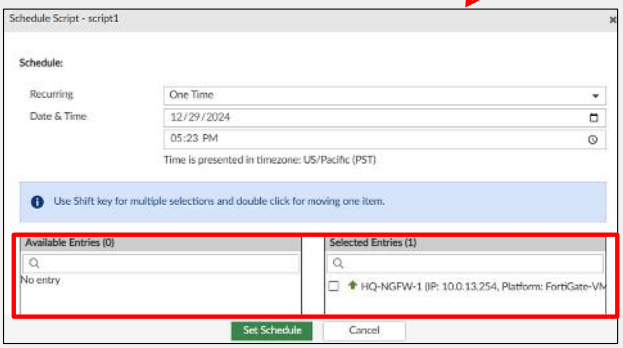
You can configure the following options on scripts:

- **Advanced Device** Filters allows you to restrict the scripts to run on managed devices, only if the device matches the set criteria. For example, you can limit the script to run on only a subset of the managed devices or on only devices running on a specific platform.
- **Format the CLI script** adds spaces at the beginning of the script lines for easy recognition of sublevel configurations.
- **Validate** checks for syntax errors, fixes issues, and adds a red circle next to the line number to show the error.

Running and Scheduling Scripts

- Two ways to execute scripts
  - Run scripts now
  - Schedule scripts
- Must perform and install when you run a script on the **Device Database** or the **Policy Package or ADOM Database**
- Can clone, export, or import scripts from a local computer
- Cannot schedule scripts to be run on **Policy Package or ADOM Database**





Confirm that the schedule feature is enabled on the CLI

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

FORTINET Training Institute

 35

You can run scripts manually by selecting **Run Script** or you can schedule them to run at a specific time. Scheduling scripts to run outside of business hours to avoid network interference is a common practice.

To schedule a script, right-click the script and then click **Schedule Script**. You cannot schedule scripts to run on **Policy Package or ADOM Database**.

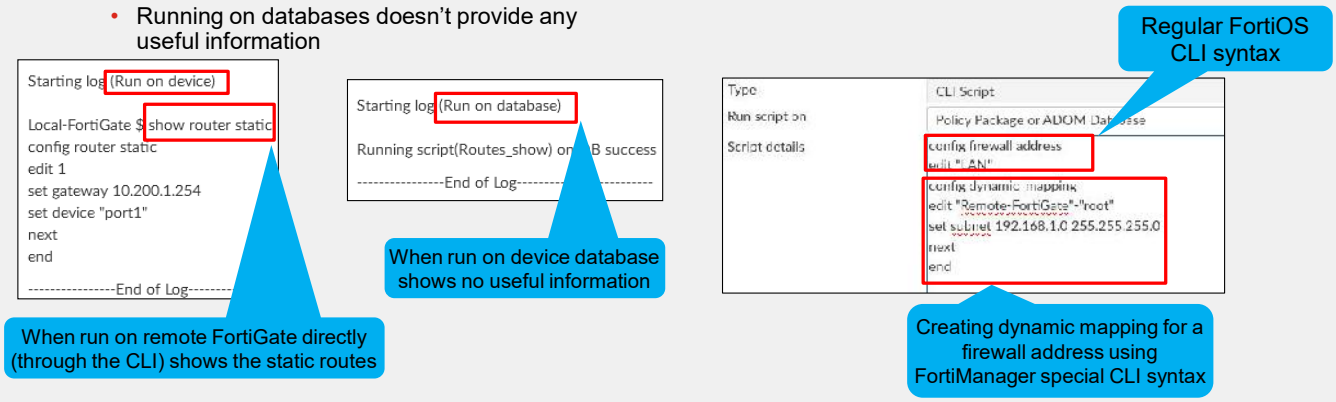
You can also edit, clone, delete and export scripts text files. You can import scripts as text files as well.

You can view the script running history in the **Configuration and Installation Status** widget of each managed device, as well as by clicking **System Settings** > **Task Monitor**.

Advanced Use of CLI Scripts

- Getting information from FortiGate
  - Typically involves one line of script to view FortiGate configuration
  - Output available on FortiManager GUI
  - These scripts should be run on **Remote FortiGate Directly (via CLI)**
    - Running on databases doesn't provide any useful information

- Special CLI syntax for dynamic mappings Used to create dynamic mapping for objects, interfaces
  - Must be run on **Policy Package or ADOM Database**



FORTINET Training Institute

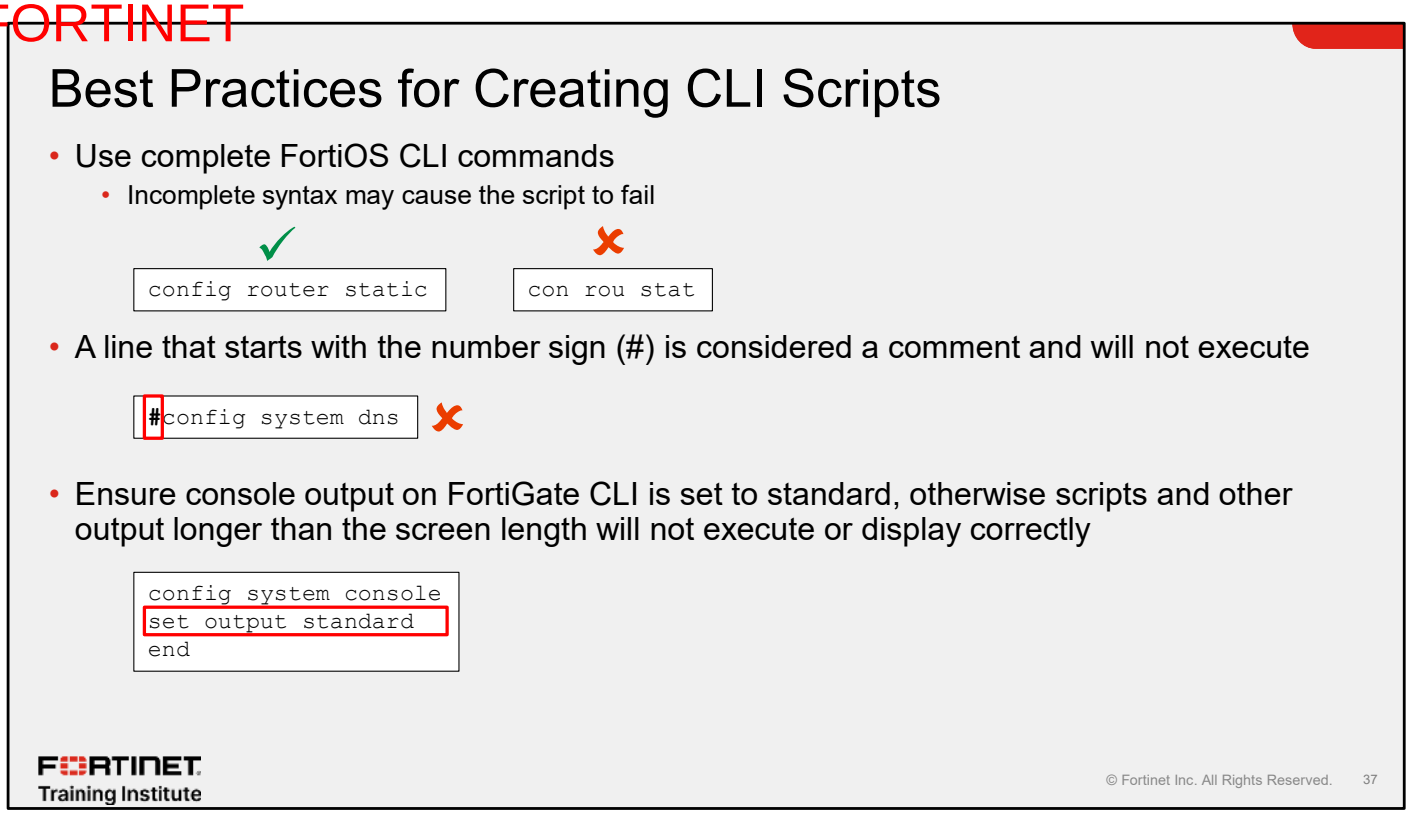
 36

You can also use scripts to get information from FortiGate. A script written for this purpose usually consists of a single line that uses a `show` or `get` command and should be set to run on **Remote FortiGate Directly (via CLI)**. If you run a script like this on the device database or the ADOM database, it does not provide any useful information or simply fails with an error.

FortiManager supports the dynamic mapping of interfaces and objects so that they can be used with multiple policy packages. You can configure dynamic mappings from the FortiManager GUI in the **Policy & Object** pane. But what if you need to configure dynamic mappings for hundreds of FortiGate devices for an address object or interface?

In cases like this, you can use a script that requires special CLI syntax that is applicable to FortiManager internally and is used to create dynamic mappings. Scripts like this are composed of two types of syntax:

- Regular FortiOS CLI syntax that defines the object
- Special FortiManager CLI syntax that creates the dynamic mapping for the defined object or interface defined.

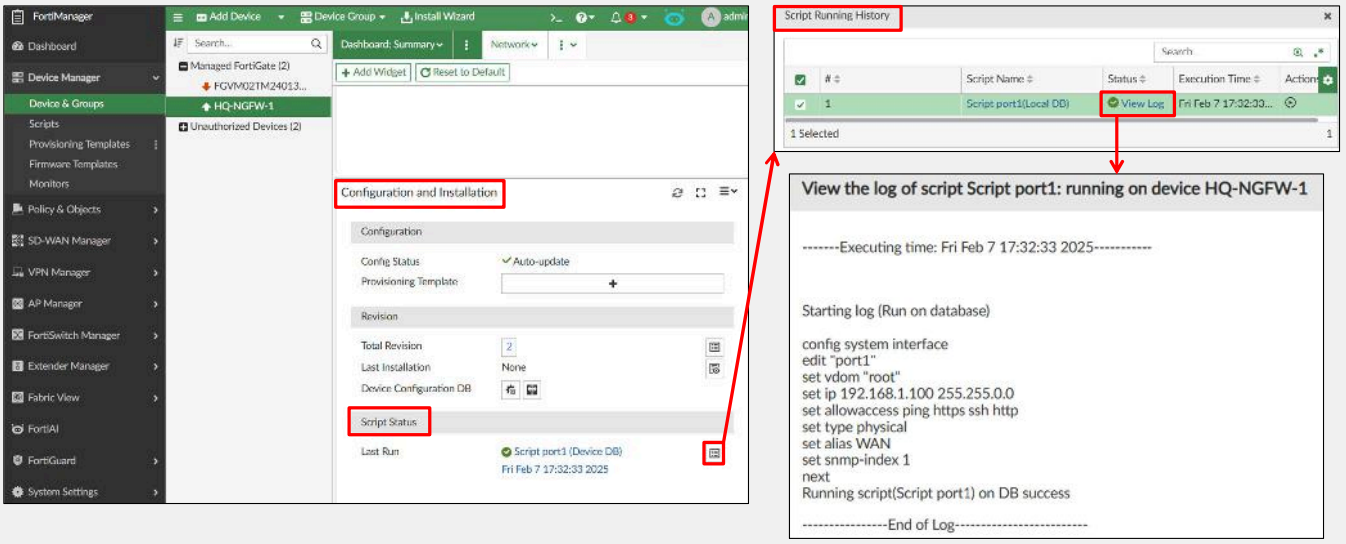


When you create CLI scripts, follow these best practices:

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

Best Practices for Creating CLI Scripts (Contd)

- Check the script running history



FORTINET Training Institute

 38

You can access to the entire running history of each FortiGate device.

Click **Device Manager** > **Device & Groups** > **Managed FortiGate** > **Select FortiGate** > **Dashboard** > **Configuration and Installation** > **Scripts Status** to find more about the **Script Running History**.

Common Script Execution Errors

Common errors	Common causes	Common solutions
`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, the script has no end statement FortiGate not synchronized with FortiManager	Check the script output Add an end statement Resync FortiGate by retrieving the 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

 39

The table on the slide includes common errors and causes of script failures. You can use this information to diagnose and troubleshoot script failure issues.

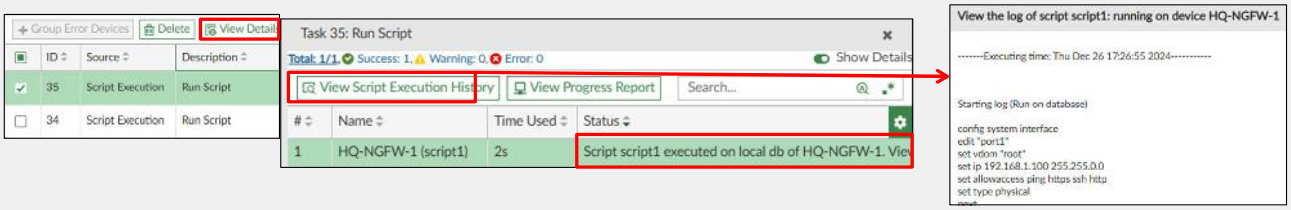
The common errors and causes of script failures are as follows:

- `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 a misspelled keyword or an incorrect command format.
- `unknown action`: Generally, this message indicates that the previous line of the script was not executed, causing the following CLI commands to fail to execute properly.
- `Device <name> failed-1`: This message 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 FortiGate is not synchronized with FortiManager.

To resolve these script issues, use the script history to examine which CLI commands are executed, and which commands are failing to execute.

Troubleshooting Scripts

- You can view the details of scripts from the script execution history available at:
  - **Configuration and Installation Status** widget of each managed device
  - **Task Monitor** under **System Settings**



- Execution details are also available in event logs
  - The following example shows two logs in raw format:

```
type=event subtype=dm pri=information desc="Script install status" user="admin" msg="script script1 successfully installed on HQ-NGFW-1" device="HQ-NGFW-1" adom="root" status="successfully" session_id=60442 operation="Install script" performed_on="HQ-NGFW-1" changes="script script1 sucessfully installed on HQ-NGFW-1" script="script1"

type=event subtype=dm pri=information desc="Script install status" user="admin" msg="Install script failed: Script script1 executed on local db of HQ-NGFW-1 failed. Reason: invalid value - [line 4] > sr" device="HQ-NGFW-1" adom="root" status="failed" session_id=60442
```

FORTINET Training Institute

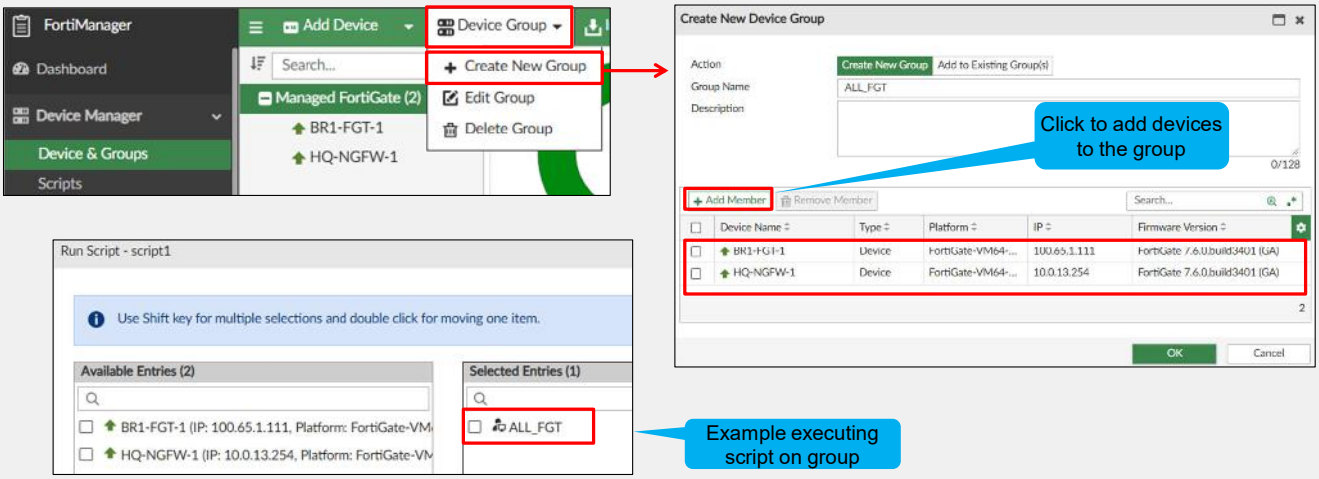
 40

When troubleshooting scripts, you can check the script execution history to see details about the script. This is available in the **Configuration and Installation Status** widget of each managed device, as well as by clicking **System Settings** > **Task Monitor**.

Additionally, you can examine details related to the script execution in event logs.

Device Groups

- Allow you to run an operation on multiple devices instead of a single device
  - For example, you can install device changes or run scripts on multiple devices at once
  - Useful when you are upgrading the firmware on a group of managed devices



FORTINET Training Institute

 41

You can create device groups in an ADOM to simplify management tasks. For example, you can provide 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 delete a device group, you must delete all devices from the group first. Similarly, to delete an ADOM, you must delete all device groups from that ADOM first.

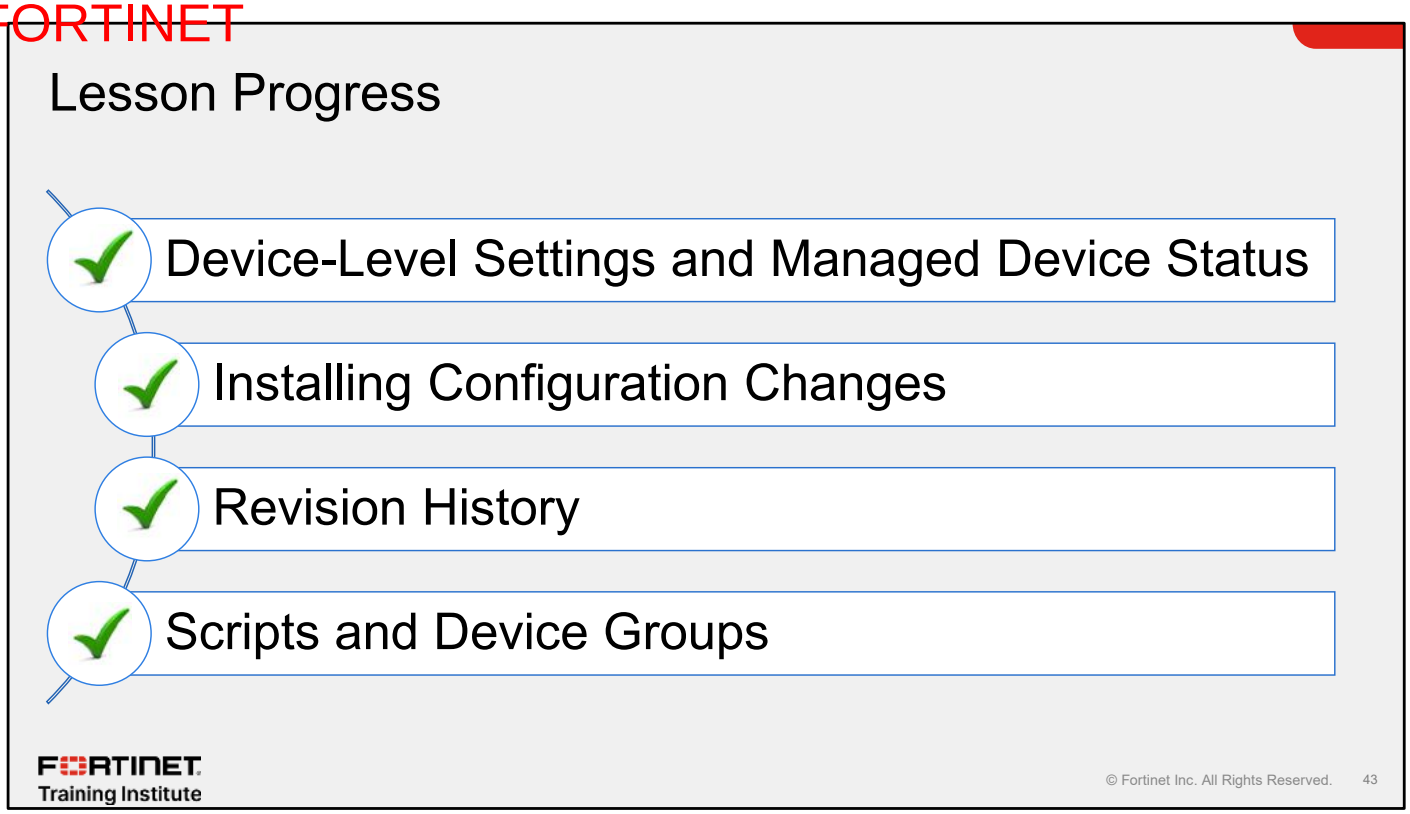
Knowledge Check

1. Which types of scripts can you create in FortiManager?
   - ✓A. CLI and Tcl scripts
   - B. Bash and Linux Shell scripts

2. Which status will a device have after you execute a script using the **Remote FortiGate Directly (via CLI)** option?
   - ✓A. **Auto-Updated**
   - B. **Modified**

FORTINET Training Institute

 42



Congratulations! You have completed this lesson.

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

Review

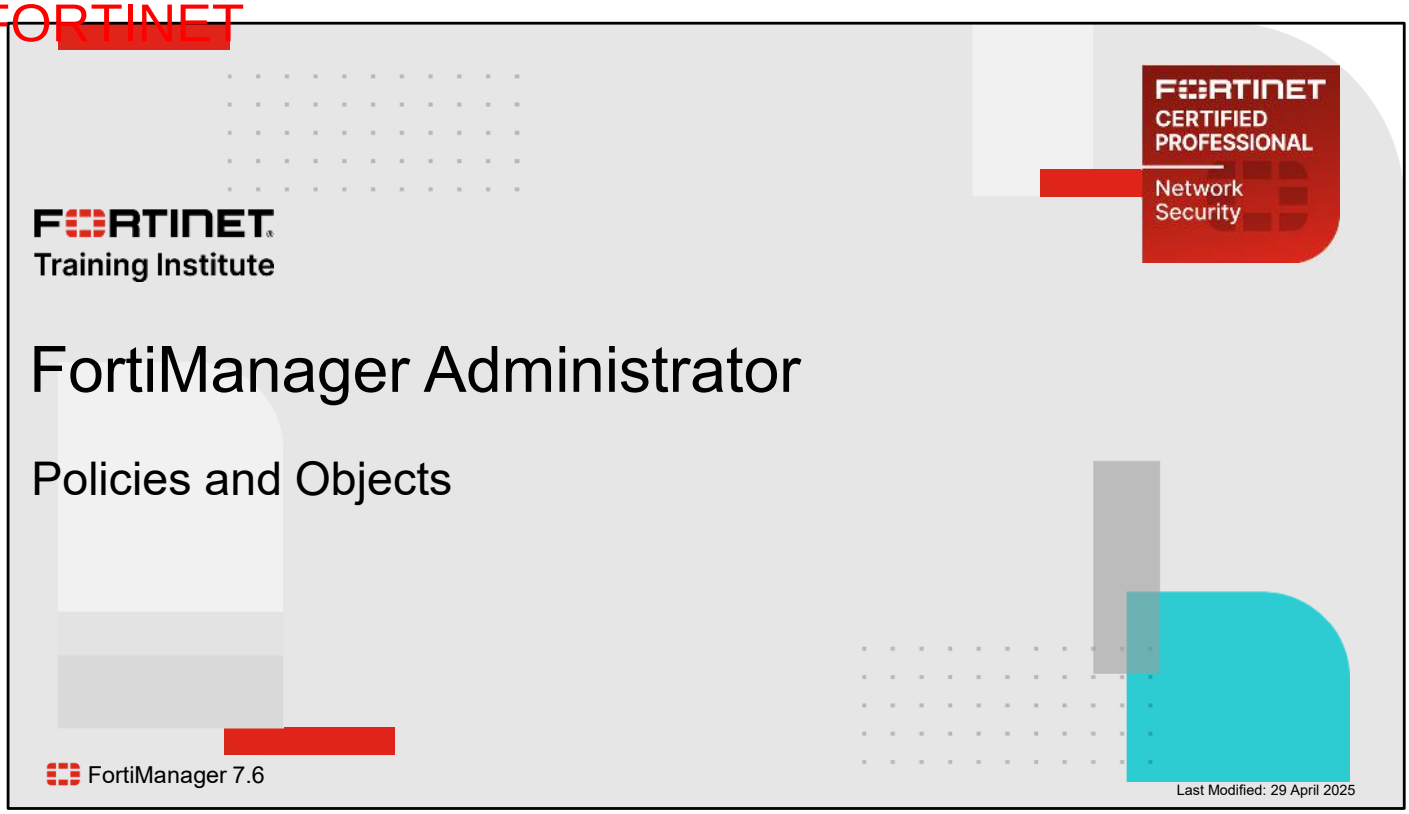
- ✓ Manage device-level changes with **Device Manager**
- ✓ Interpret the configuration status of managed devices
- ✓ Determine which actions to take based on configuration status
- ✓ Install device-level changes on FortiGate using the **Install Wizard**
- ✓ Understand when a new configuration revision is created
- ✓ Understand how you can use the configuration revision history for diagnosing and troubleshooting
- ✓ Configure and install scripts on managed devices
- ✓ Use device groups to manage FortiGate devices

FORTINET Training Institute

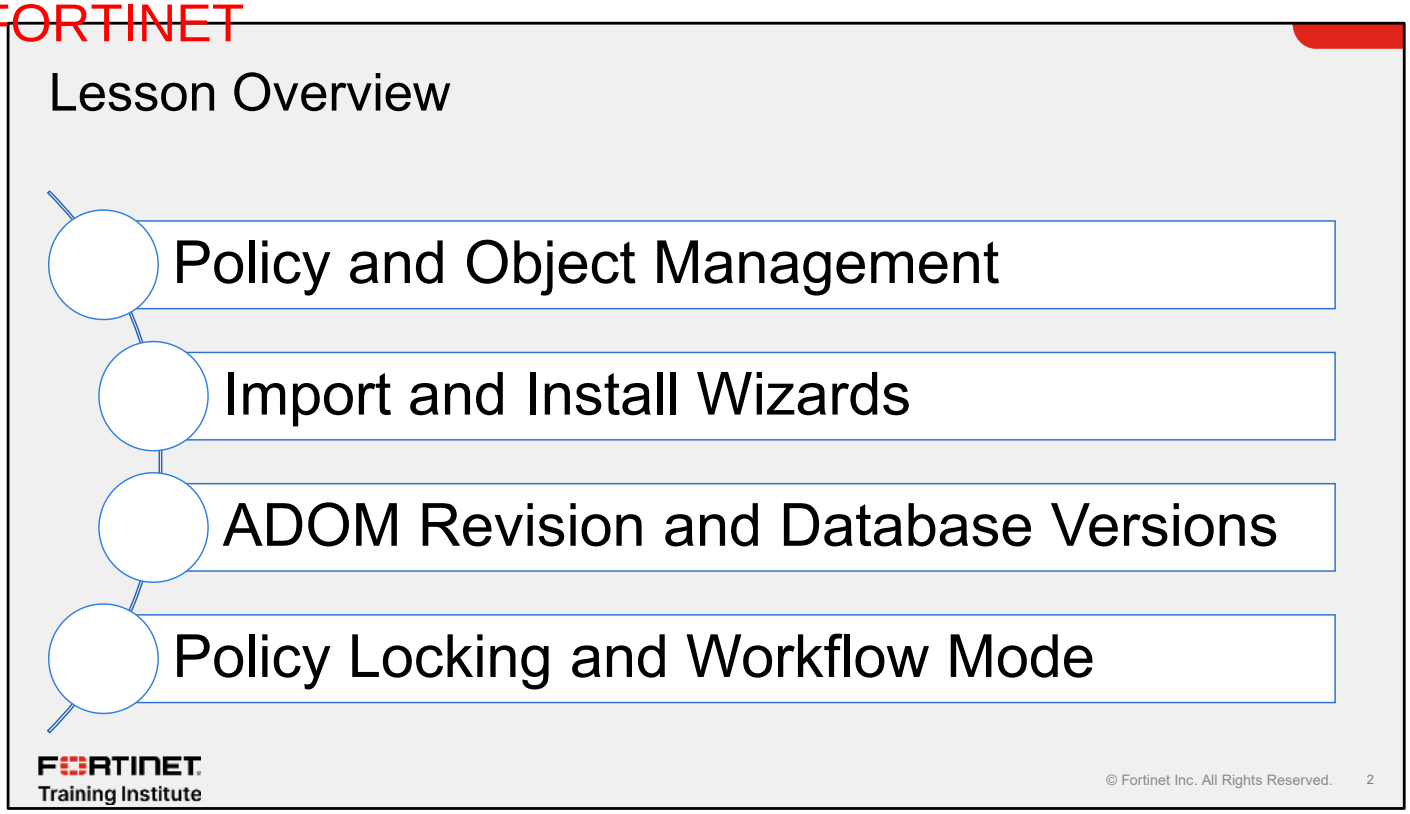
 44

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

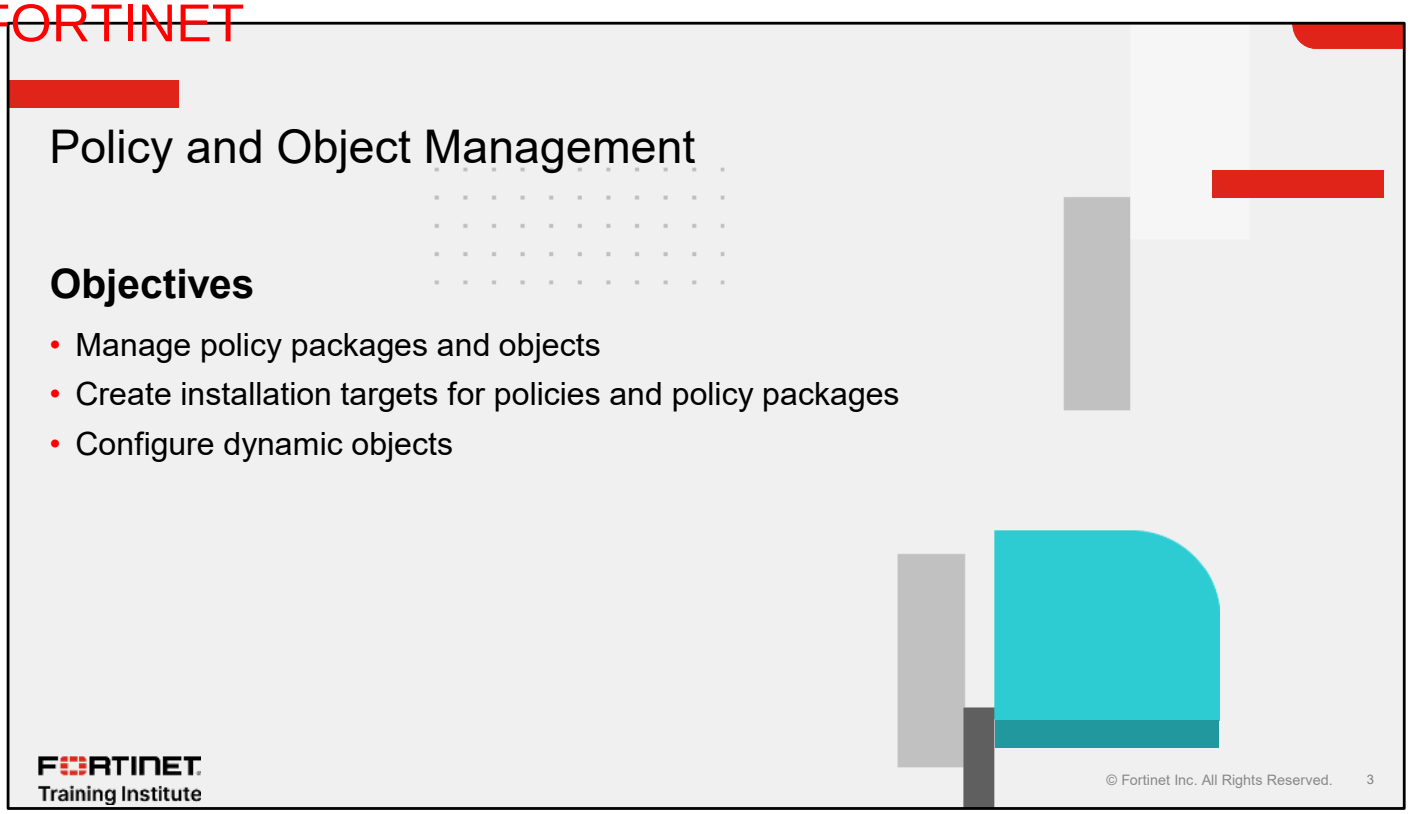
By mastering the objectives covered in this lesson, you learned how to configure device-level changes, understand the status of a managed FortiGate on FortiManager, and install changes to managed FortiGate devices. You also learned how to use the revision history for troubleshooting and the capabilities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



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

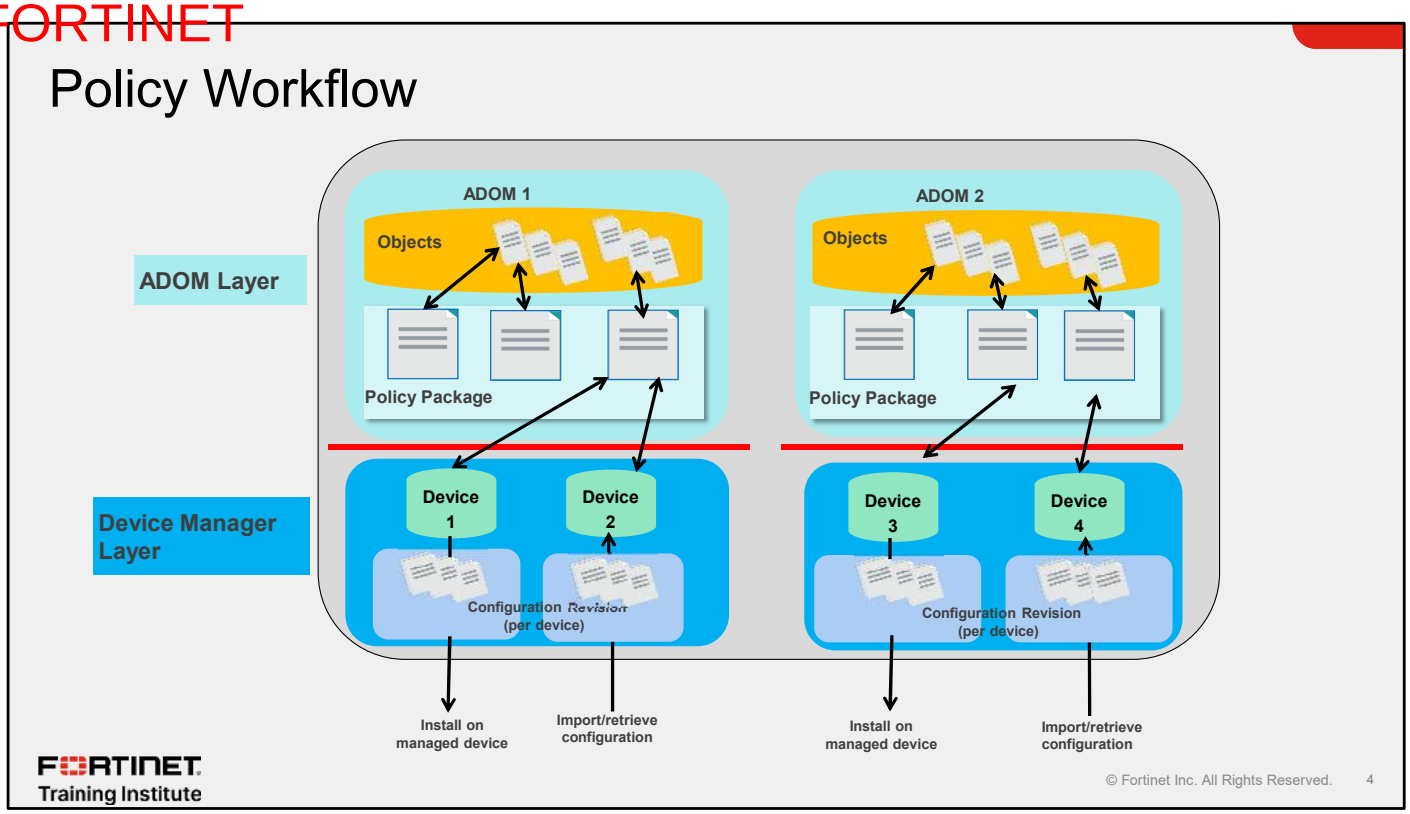


In this lesson, you will learn about the topics shown on this slide.



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.



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 **Firewall Objects** pane. Objects share the common object database for each ADOM. You can share objects among multiple policy packages in the ADOM.

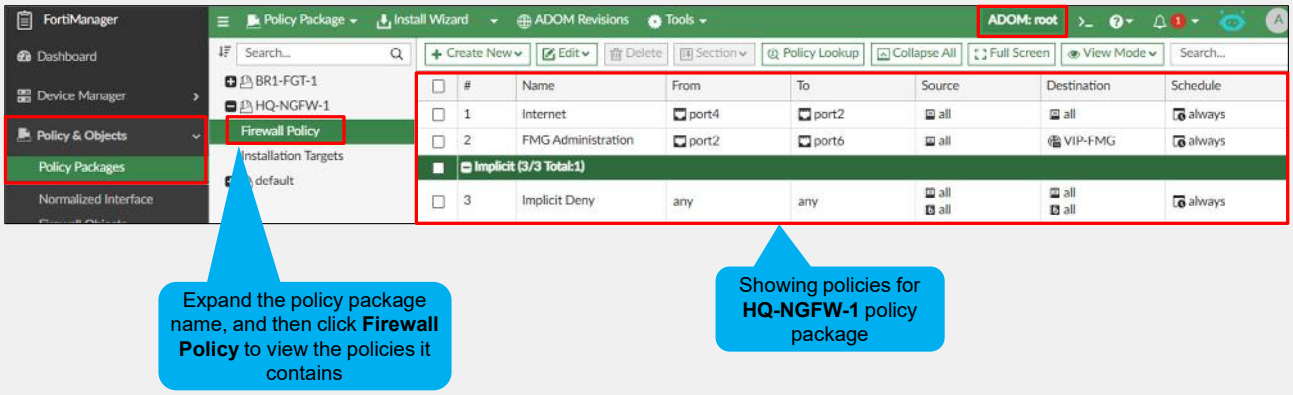
You can manage a common policy package for many devices in an ADOM, or have a separate policy package for each device. Policy packages allow you to maintain multiple versions of a rule set. For example, you can clone a policy package before you make changes, which allows you to preserve the previous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

Note that 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.

Policy Packages

- **Policy & Objects** > **Policy Packages**
- Create firewall policies in policy packages
- Displays all the policy packages for the ADOM



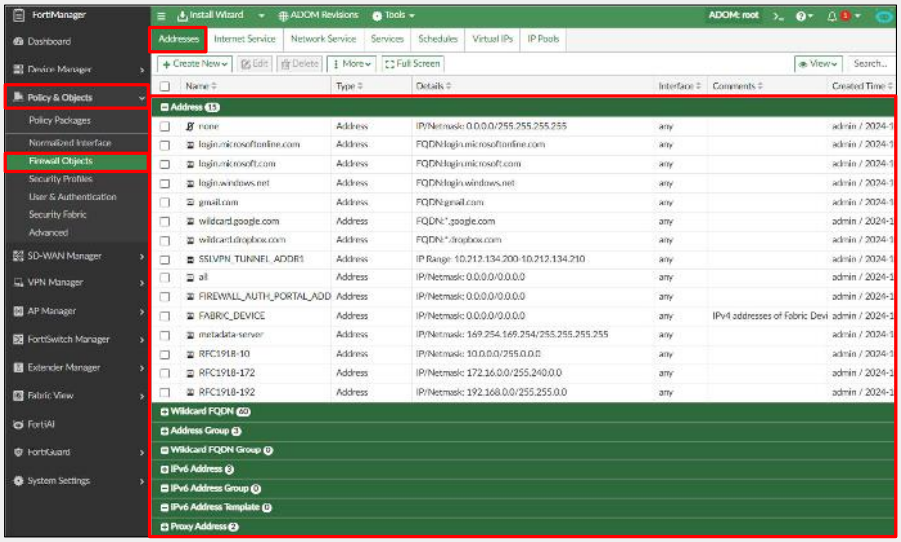
FORTINET Training Institute

 5

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 to 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.

Object Configurations

- **Policy & Objects** > **Firewall Objects**
- Firewall policies in policy packages refer to objects defined in the ADOM database



FORTINET Training Institute

 6

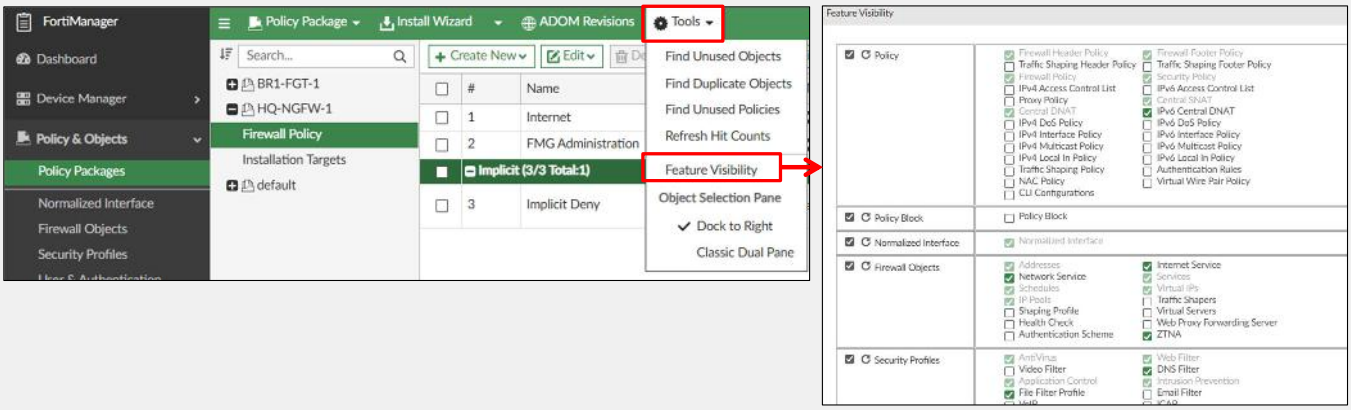
All objects in an ADOM are managed by a single database that is unique to that ADOM. Objects inside the database include firewall objects, security profiles, users, and devices, among others.

Objects are shared in the ADOM and can be used in 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 existing objects, click **Policy & Objects** > **Firewall Objects** and select the object type. On this slide, the **Addresses** tab is selected.

Feature Visibility

- **Policy & Objects** > **Feature Visibility**
- You can customize which features are visible on the different panes under **Policy & Objects**



FORTINET Training Institute

 7

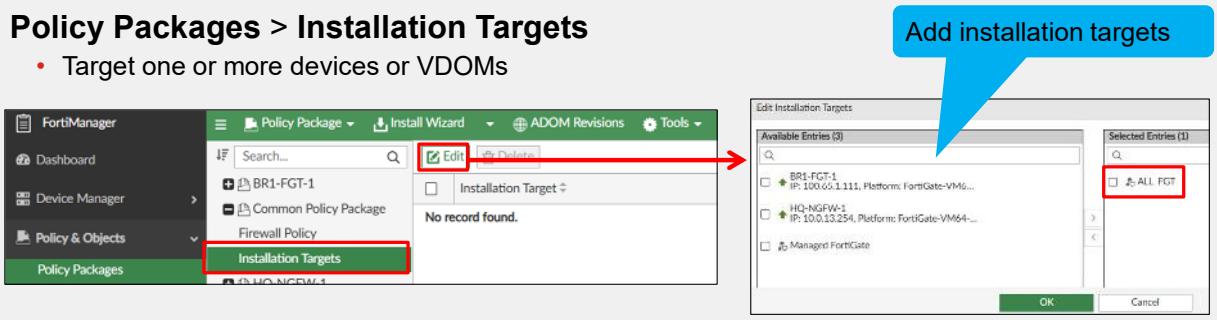
The **Feature Visibility** window allows you to display specific features on the GUI. The available options depend on the ADOM version and vary from one ADOM to another.

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

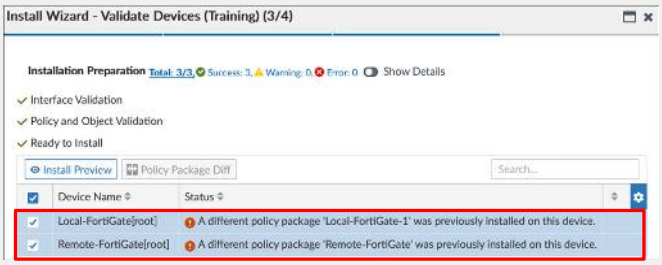
You can also enable additional firewall policy types such as NAT64, IPv6, and interface policies on the **Feature Visibility** window.

Installation Target

- **Policy Packages** > **Installation Targets**
  - Target one or more devices or VDOMs



- The **Install wizard** provides warning message with name of previous policy package assigned



FORTINET Training Institute

 8

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.

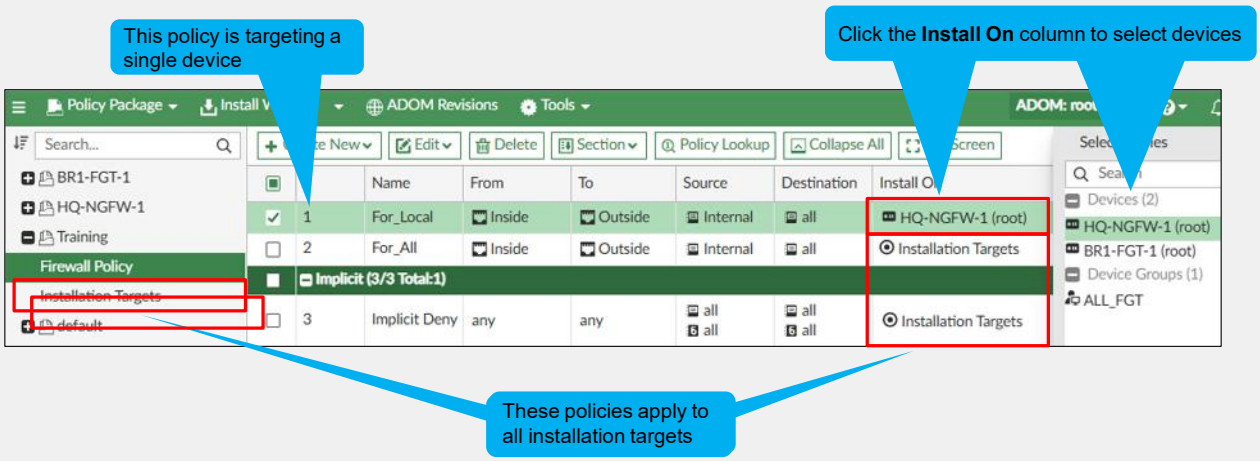
You can add, edit, or delete an installation target in the **Installation Targets** window.

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 in the **Device Manager** window, in the **Policy Package Status** column.

Installation Target—Per Policy

- Per-rule installation targets allow per-device exceptions for a shared policy package
- The **Install On** column allows you to target devices to add, remove, or set to defaults



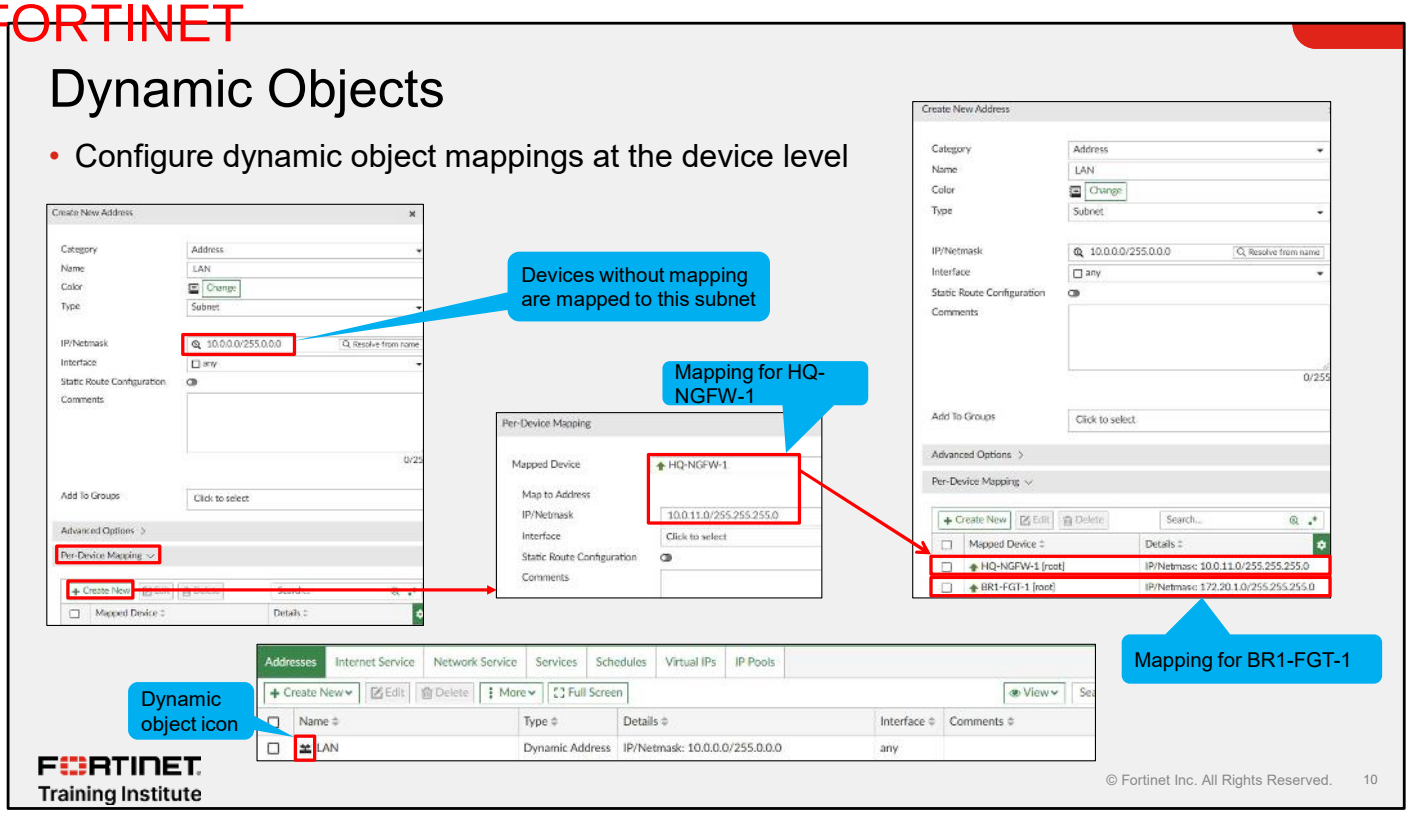
FORTINET Training Institute

 9

What if you need to share a policy package among many devices, but some of the policies in the package apply to only specific FortiGate devices?

You can set specific installation targets per rule in policy. In a policy, you use installation targets to add, remove, or set default devices for each rule.

Using installation targets, you can share a policy package among multiple devices, and define rules per device in the policy. In environments where many devices need to share common policies, share policies eliminate the need for multiple policy packages.



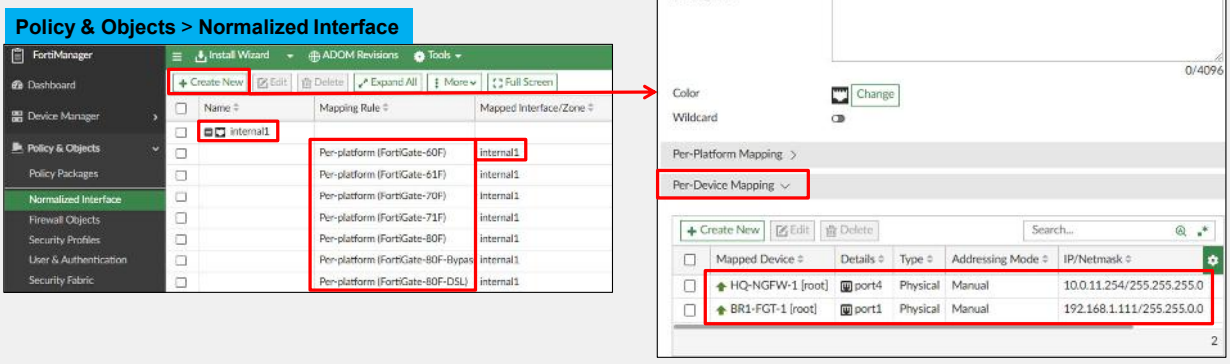
All objects in an ADOM are managed by a single database that is unique to the ADOM. Many objects now include the option to enable dynamic mapping. You can use dynamic objects to map a single logical object to a unique definition, per device. You can dynamically map common features such as *addresses,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

In the example shown on this slide, the dynamic address object **LAN** 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 **BR1-FGT-1**, the address object **LAN** refers to `172.20.1.0/24`, whereas for **HQ-NGFW-1**, the same object refers to `10.0.11.0/24`. The devices in the ADOM that do not have a dynamic mapping for **LAN** have a default value of `10.0.0.0/8`.

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

Interface Mapping

- Defines mapping rules for interfaces
- Interfaces are mapped per device, per platform, or both
- When the normalized interface is used in a policy, the per-device mappings have higher priority than per-platform mappings



FORTINET Training Institute

 11

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

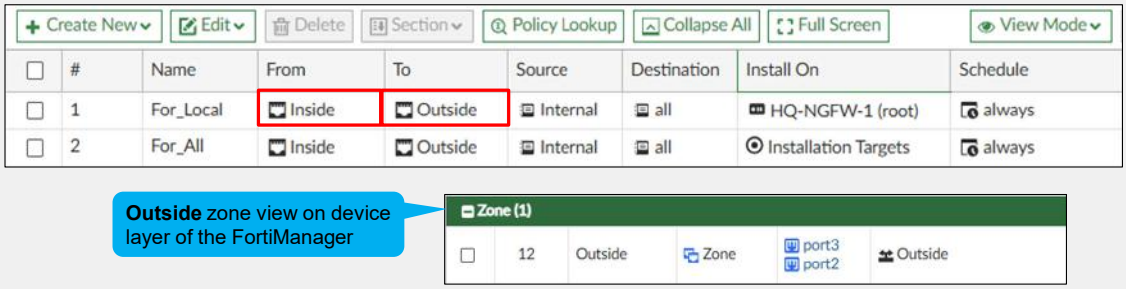
In the example shown on this slide, interface **internal1** is mapped to **internal1** for the platforms highlighted. Default per-platform mapping rules allow you to install policies on FortiGate devices without first creating custom mapping rules.

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 **port4** for HQ-NGFW-1 and to **port1** for **BR1-FGT-1**.

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

Example—Firewall Policy

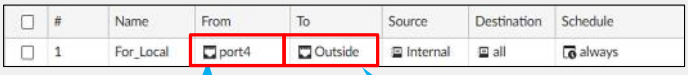
- Policy view of **Interface** and **Zone** on FortiManager

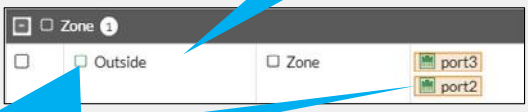


Outside zone view on device layer of the FortiManager

- Policy view of **Interface** and **Zone** on the managed FortiGate

Outside zone view on managed FortiGate





Inside is mapped to port4

Outside (includes port2 and port3)

Note that zones are represented with an icon that is different from interfaces

FORTINET Training Institute

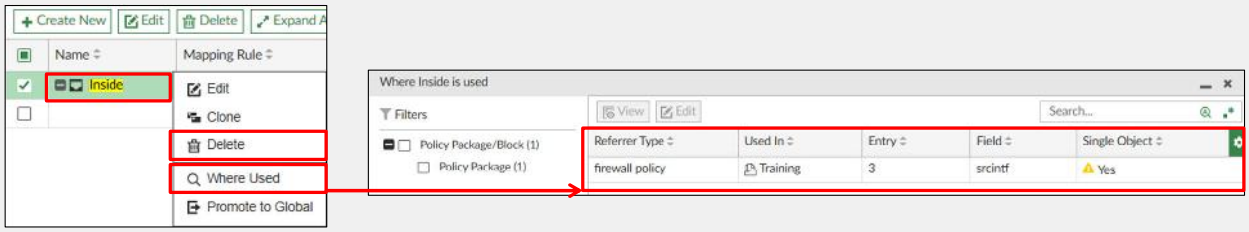
 12

In this example**, Inside** is mapped to **port4** on **HQ-NGFW-1**. Therefore, after a firewall policy is installed on the managed FortiGate, the **Inside** interface will appear as **port4**.

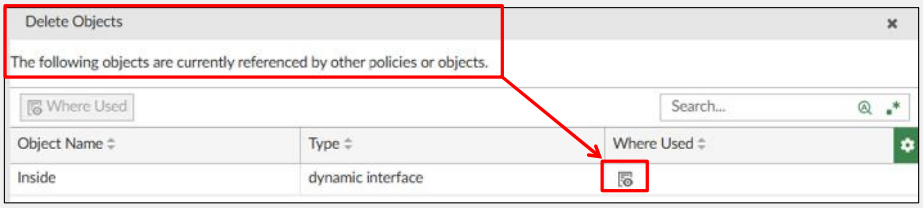
Outside, however, remains untouched, because it is installed on the device as a zone and the **port2** and **port3** interfaces are part of it.

Used Objects

- View where the used object is before deleting it



- However, if you delete an object that is referenced in a firewall policy, FortiManager will display a warning indicating the object is currently referenced by other policies or objects



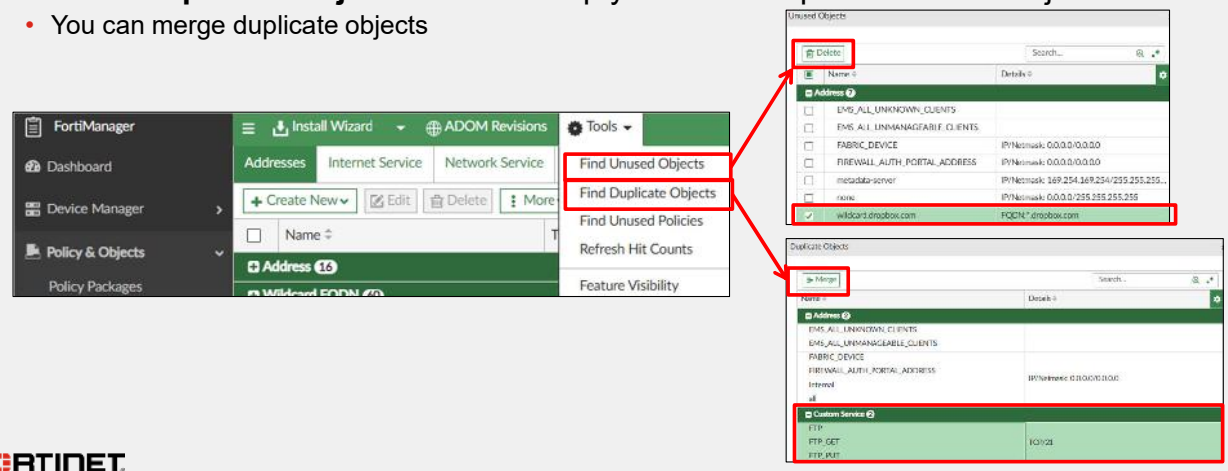
FORTINET Training Institute

 13

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 for this object, click **Where Used**. If the object that you want to remove is referenced by other policies or objects, you must change the policy or remove the object from the policy before deleting the object to prevent empty or null objects on the policy layer.

Find Unused and Duplicate Objects

- The **Find Unused Objects** tool displays all the firewall objects that are currently unused
  - Example: Address, service, virtual IP, IPPOOL, and so on
- Delete unused objects directly in the **Unused Objects** window
- The **Find Duplicate Objects** tool can help you locate duplicate firewall objects
  - You can merge duplicate objects



FORTINET Training Institute

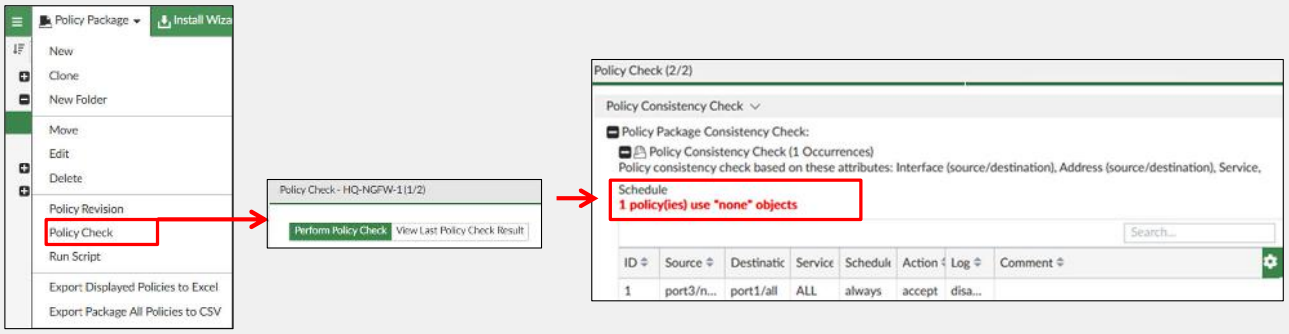
 14

Find Unused Objects is a built-in GUI tool that you can use to 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** window. This removes the selected object from the FortiManager ADOM objects database.

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. When duplicate objects are found, you can merge those objects, if needed.

Policy Check

- Looks for consistency and conflicts in the policy package
- Helps you to optimize firewall rules to potentially reduce the size of the policy package database



FORTINET Training Institute

 15

Policy Check provides recommendations only on which 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

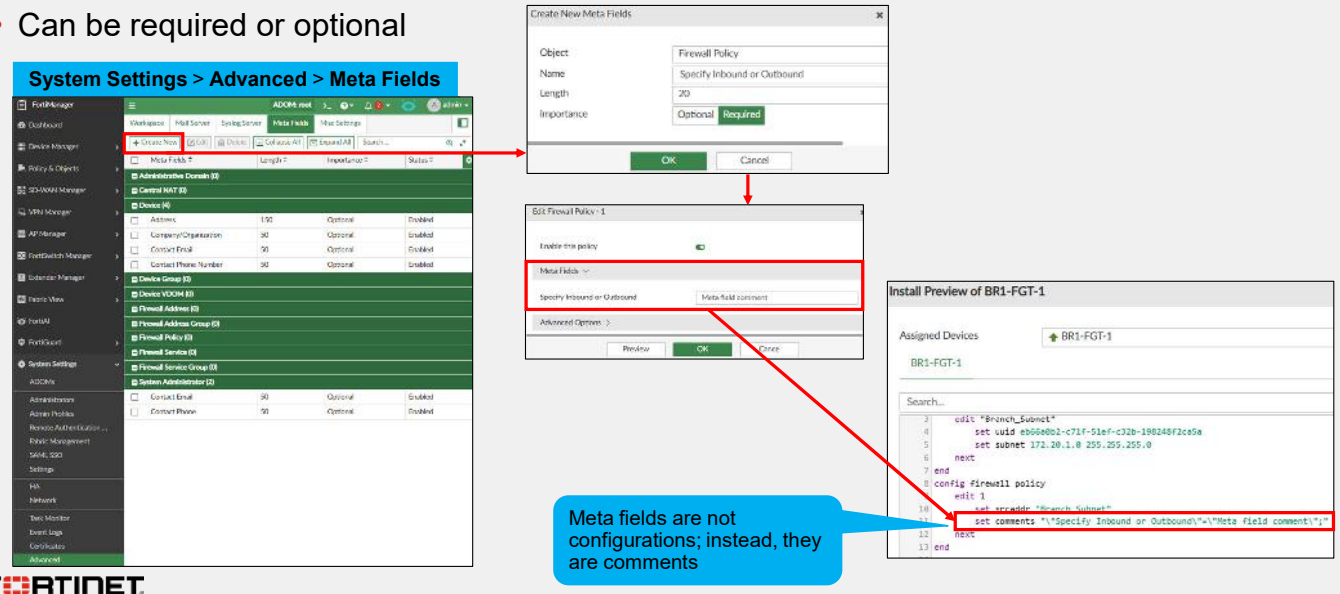
To perform a policy check, select a policy package, and then, in the **Policy Package** drop-down list, click **Policy Check**. In the **Policy Check** window, select one of the following options:

- **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, the policy with ID **1** uses a **none** object in its source field and must be fixed to allow traffic.

Meta Fields

- Allow administrator to add additional attributes to several FortiManager objects
- Can be required or optional



Meta fields allow administrators to add additional attributes to several types of objects and administrator accounts. 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 new meta field, you must choose a value for the following fields:

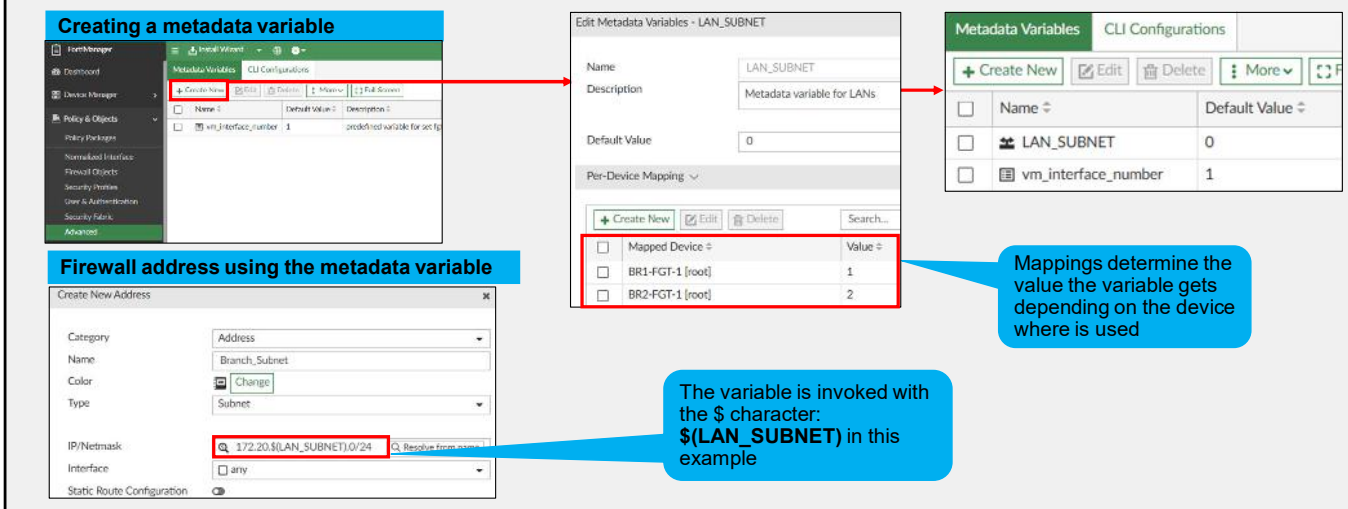
Object: allows you to select the object type this meta field applies to, such as administrative domain, firewall address group, firewall policy, central NAT, administrator, and so on.
Name: is the label used for this field.
Length: is the maximum number of characters allowed for the field.
Importance: determines if the field is compulsory or not.
Status: determines the availability of meta fields to select in the objects. This option is available only for non-firewall objects.

Meta fields cannot be used as variables in scripts or provisioning templates. Instead, you can use ADOM-level metadata variables for that purpose.

The example on this slide shows the creation of a new meta field for firewall policies. The new field is labelled **Specify Inbound or Outbound** and marked as required.

ADOM-Level Metadata Variables

- Metadata variables can be used as variables in scripts, templates, firewall address objects, IP pools, and virtual IPs VIP.
  - Available by default in the ADOM in which they were created only, but can be exported and imported



ADOM-level metadata variables can be used as variables in scripts, templates, firewall address objects, IP address pools, and VIPs.

Typing $ in the an object's field of an object with supported metadata variables displays the available metadata variables for the selection. Fields that support metadata variables are identified with a magnifying glass icon.

You can configure ADOM-level metadata variables by clicking **Policy & Objects** > **Advanced** > **Metadata Variables**.

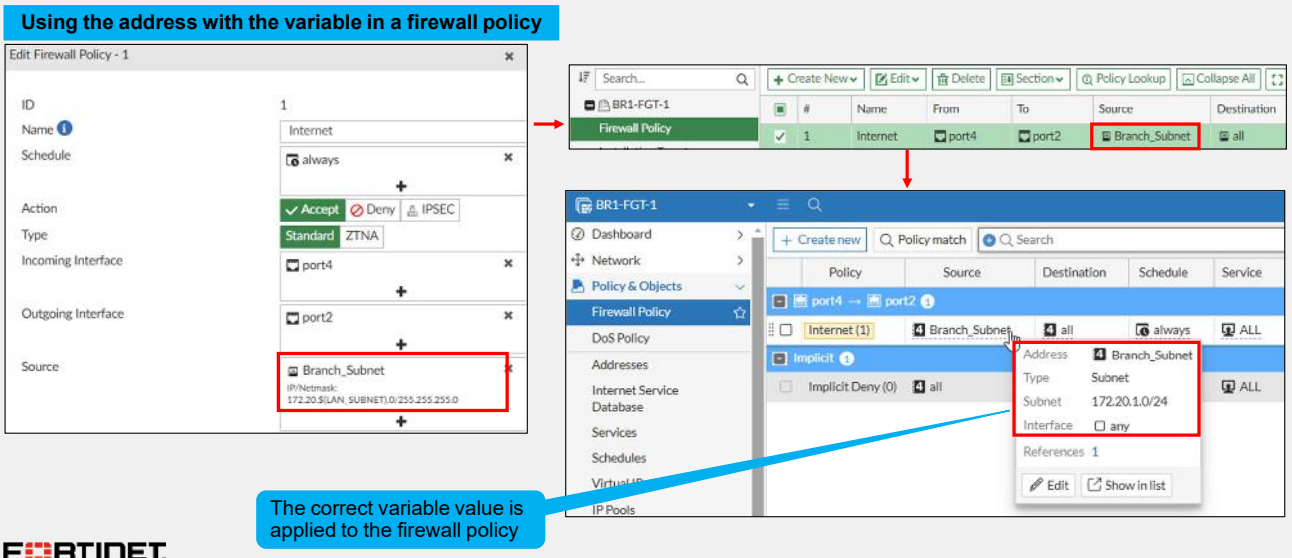
By default, metadata variables are available in only the ADOMs in which they were created. However, you can export them and then import them into another ADOM.

Metadata variables can also be created in the global database ADOM. When creating ADOM-level metadata variables in the global database, you can configure per-ADOM mappings to assign specific values to all devices within an ADOM.

The example on this slide shows the creation of a new metadata variable that refers to the subnet for each branch and how the new variable is used in a firewall address object.

ADOM-Level Metadata Variables (Contd)

- Example of a metadata variable applied to a firewall policy



FORTINET Training Institute

 18

The example on this slide shows a metadata variable being referenced in a firewall policy and how the variable value is adjusted based on the device the firewall policy is installed on. In this example, **Branch_Subnet** is translated to **172.20.1.0/24** for **BR1-FGT-1**. That is, the third octet becomes **1**.

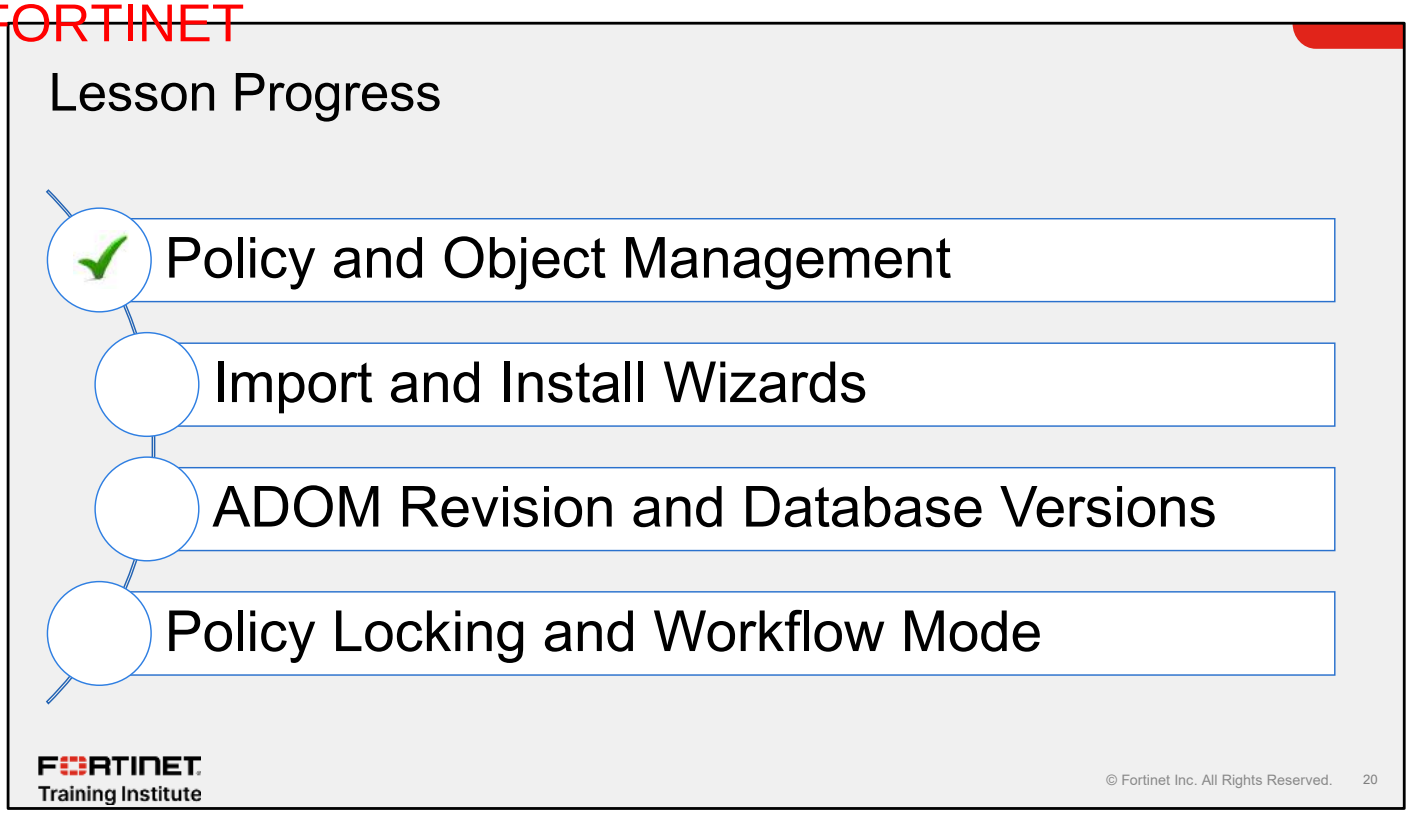
Knowledge Check

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 policy packages is true?
   - ✓A. A policy package can have multiple installation targets in an ADOM.
   - B. There can be only one policy package per ADOM.

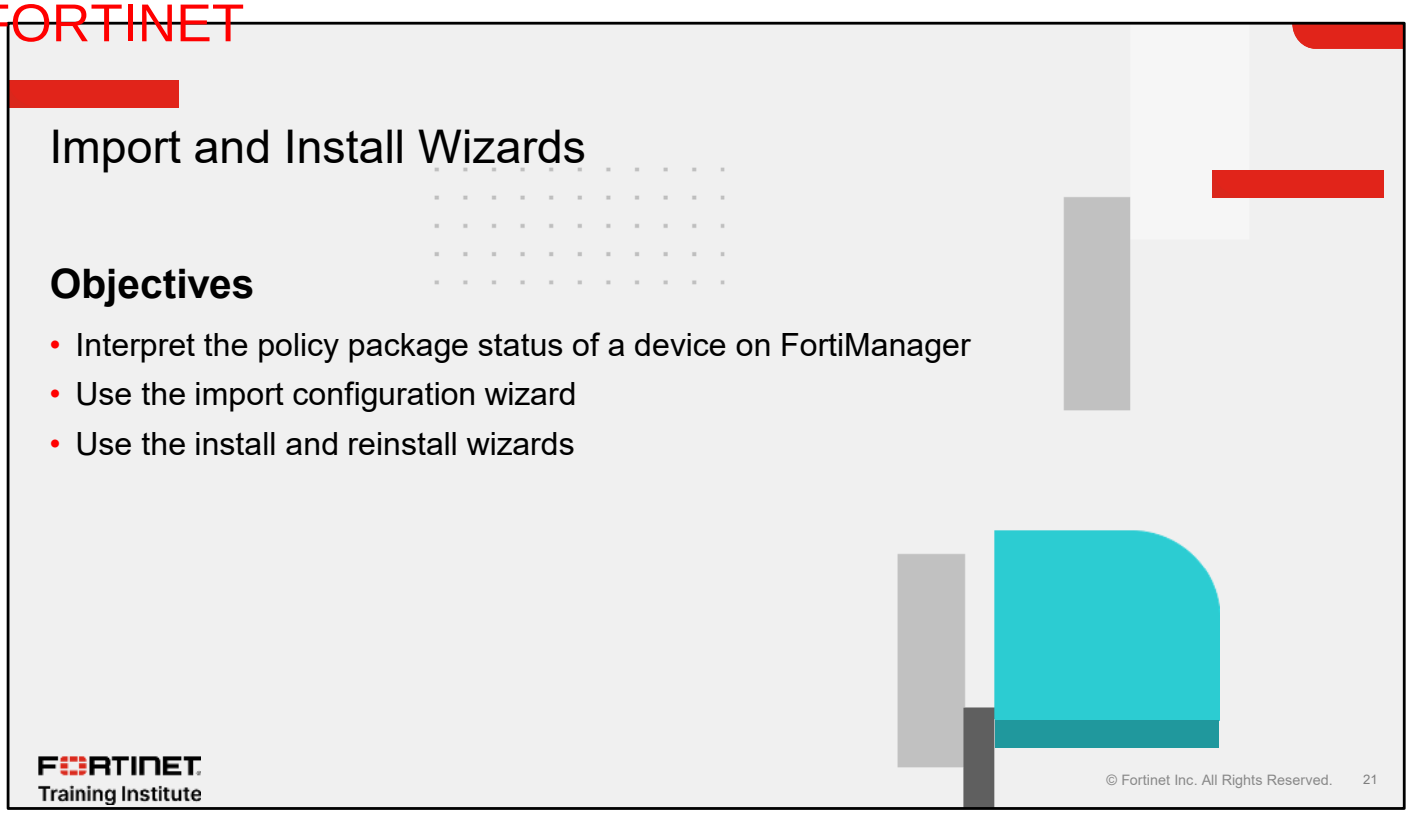
FORTINET Training Institute

 19



Good job! You now understand policy and object management.

Now, you will learn about import and install wizards.



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 you will be able to use various options to manage devices on FortiManager.

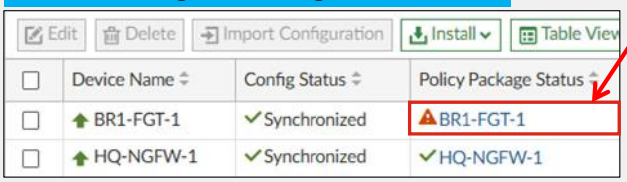
Policy Package Status

```
FortiManager # diagnose dvm device list
--- There are currently 2 devices/vdoms managed ---
--- There are currently 2 devices/vdoms count for license ---

TYPE            OID     SN               HA      IP              NAME        ADOM    IPS
FIRMWARE
fmgfaz-managed  284     FGVM02TM24013504 -       100.65.1.111    BR1-FGT-1   root    7.0 MR6 (3401)  N/A
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:root pkg:[modified]BR1-FGT-1

...
--- End device list ---
```

Device Manager > Managed FortiGate

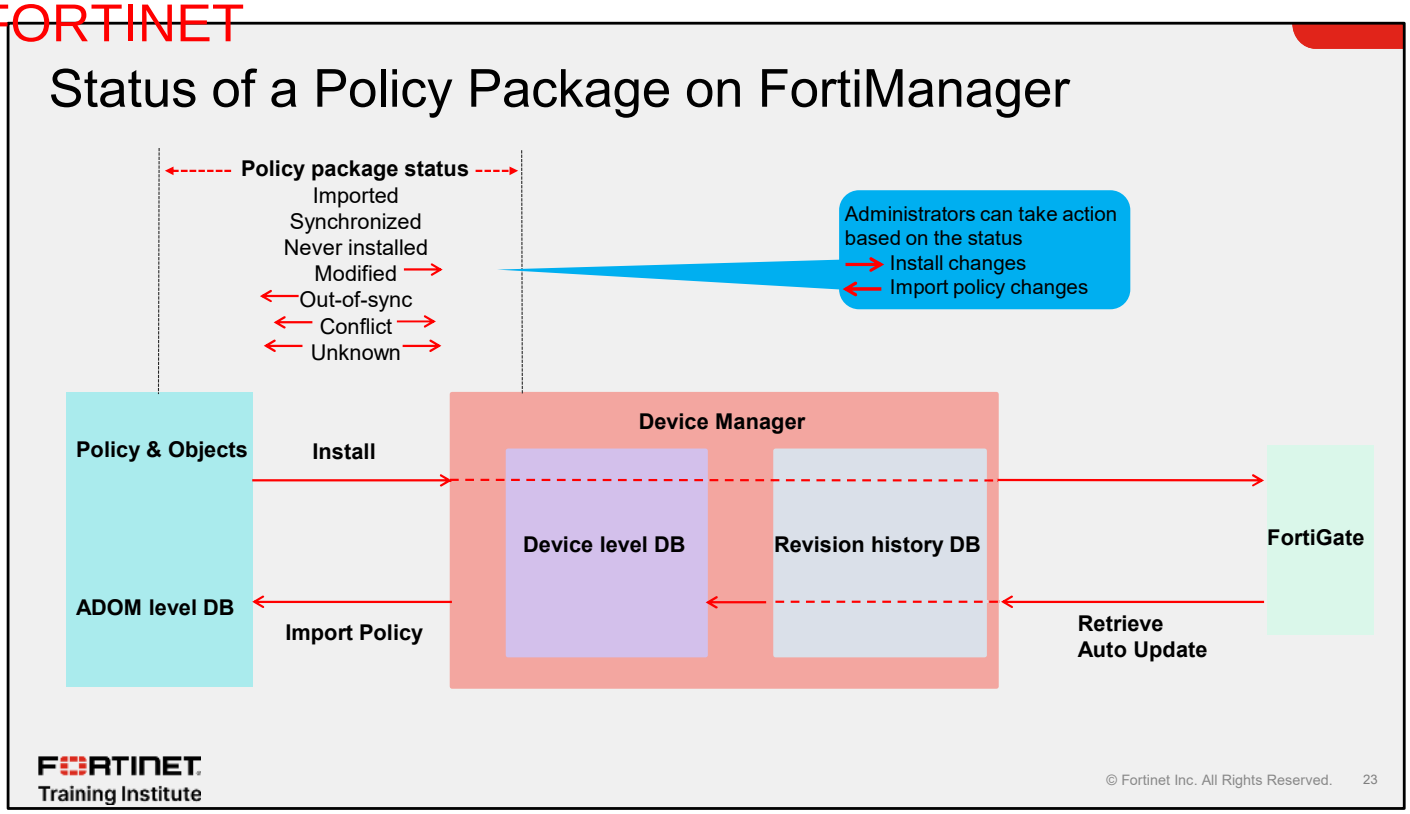


FORTINET Training Institute

 22

This 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.



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

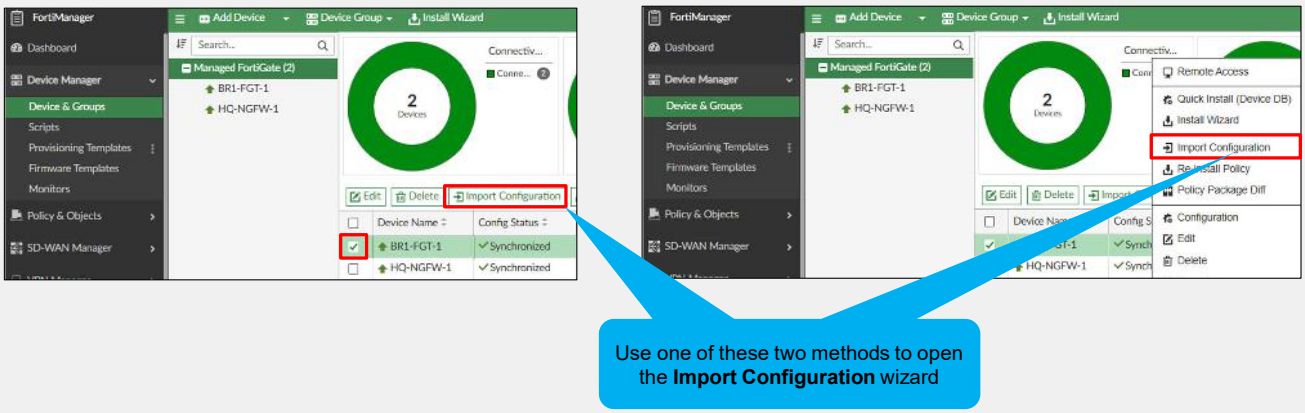
This slide shows the status of the policy package:

- **Imported:** indicates that a policy package was successfully imported for a managed device.
- **Synchronized:** indicates that policies and objects are synchronized between FortiManager and the managed device.
- **Never Installed:** indicates that the policy package was never created and it was never imported for a managed device.
- **Modified:** indicates that the policy package configuration has changed on FortiManager and changes have not been pushed to the managed device.
- **Out-of-sync:** indicates that 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:** indicates that you made policy configuration changes locally on FortiGate and did not import the changes into the policy package, and you also made the changes on FortiManager. Depending on the changes you made, you can either import a policy package or install the changes from FortiManager.
- **Unknown**: indicates that 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.

Import Configuration Wizard

- **Device Manager** > **Managed FortiGate**
  - Select the FortiGate device, and then click **Import Configuration**
  - Creates a new policy package, or can override an existing one, and imports objects
    - Objects imported are added to the ADOM object database



Use one of these two methods to open the **Import Configuration** wizard

FORTINET Training Institute

 24

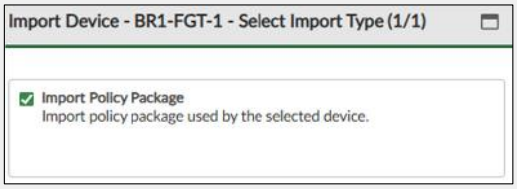
It is common for FortiGate to have a running configuration already. The **Import Configuration** wizard guides you through importing policies and objects into FortiManager. When you import a device configuration, you create a new policy package that does not interfere with other packages. However, objects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

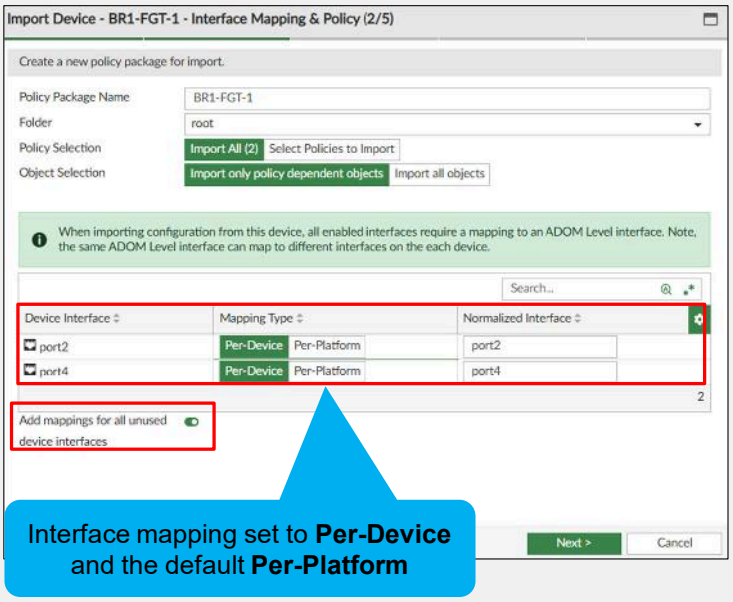
If you add an unregistered device to FortiManager, you must run the **Import Configuration** wizard after promoting the device.

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

Import Configuration Wizard—Interface Mapping and Policy

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





Interface mapping set to **Per-Device** and the default **Per-Platform**

FORTINET Training Institute

 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.

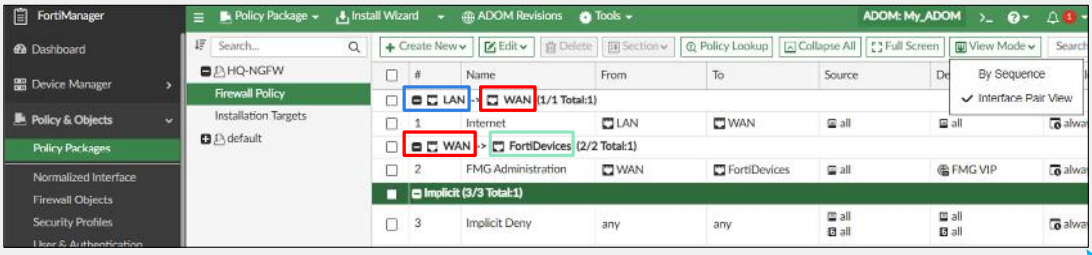
The wizard performs a policy search to find all policies in preparation for import into the FortiManager database. You may choose to import all firewall policies, or select specific policies to import. If you choose to import only specific policies into the policy package and later install policy changes, 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 unused objects that are not tied to policies locally on FortiGate in the next installation. 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.

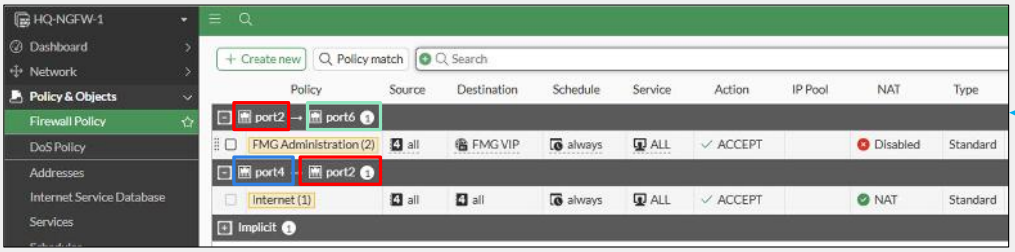
By default, the **Import All** and **Import only policy dependent objects** options are selected when you run the **Import Policy** wizard. As a word of caution, if you are managing many devices in an ADOM and select **Import all objects** for all devices, the object database will be filled with unused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

Policy View—FortiManager and FortiGate

- Policy view from FortiManager:



- Policy view from FortiGate:



port2 = WAN
port4 = LAN
port6 = FortiDevices

FORTINET Training Institute

 26

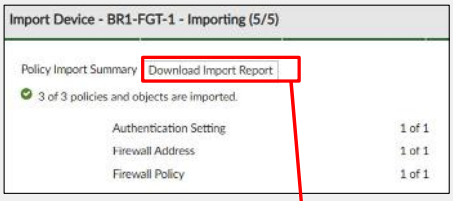
In the example on this slide, **port2** was renamed **WAN**, **port4** was renamed **LAN**, and **port6** was renamed **FortiDevices** in the interface mapping step of the wizard and the policy shows those custom interface names. However, on FortiGate, the policy shows **port2**, **port4**, and **port6**.

These mappings are called the **normalized interface**, and 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.

The **normalized interface** is useful when installing the same policy package to multiple managed FortiGate devices.

Import Configuration Wizard—Summary

- Imports objects into the ADOM database, policies into a policy package



- You can save the import report in TXT format

```
Start to import config from device(BR1-FGT-1) vdom(root) to adom(root), package(BR1-FGT-1)
"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=Branch_Subnet, oid=2266, new object)"
"firewall address",SUCCESS,"(name=HQ_SUBNET, oid=2267, new object)"
```

FORTINET Training Institute

 27

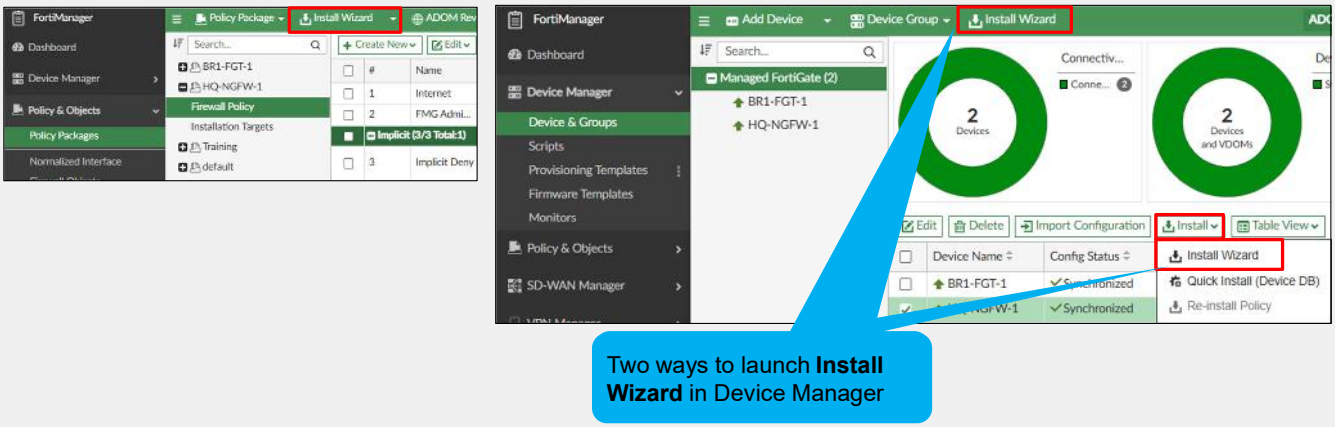
After the import is complete, the wizard provides the **Policy Import Summary** and the **Download Import Report**. You can download the import report, which is only available on the **Import Device** page. You can view the report using any text editor.

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.

Install Wizard

- Multiple ways to launch
- If you make configuration changes to a policy package, the policy package status changes to **Modified**



FORTINET Training Institute

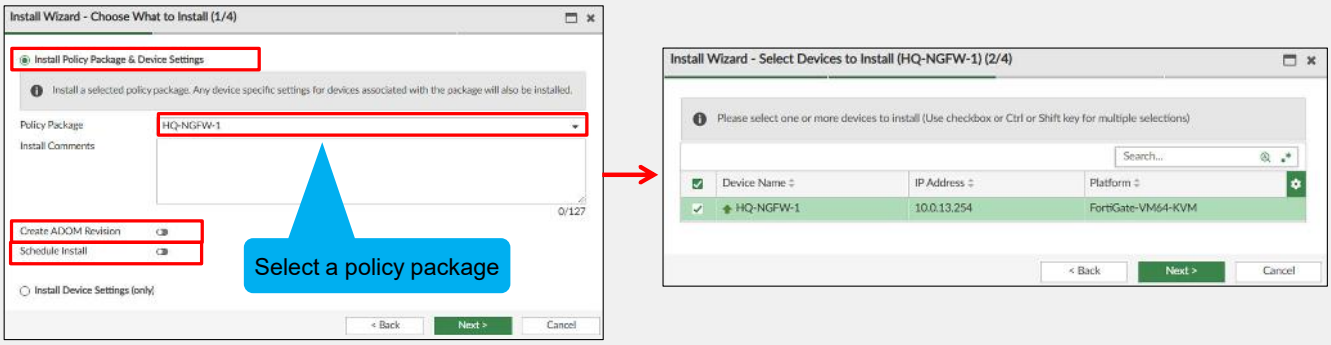
 28

After you make configuration changes to the policy package, the **Policy Package Status** is flagged as **Modified** on the **Device Manager** pane windows, as well as on the **Policy & Objects** pane. If you are using ADOMs, before you launch the wizard.

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 synchronized and the **Policy Package Status** changes from **Modified** to **Installed** (**Synchronized**).

Install Wizard—What to Install

- **Install Policy Package & Device Settings** allows administrators to install the policy package and device settings changes
- **Install Wizard** also provides the options to:
  - Create a configuration revision
  - Schedule push to remote device
- Select device to install the changes on



FORTINET Training Institute

 29

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

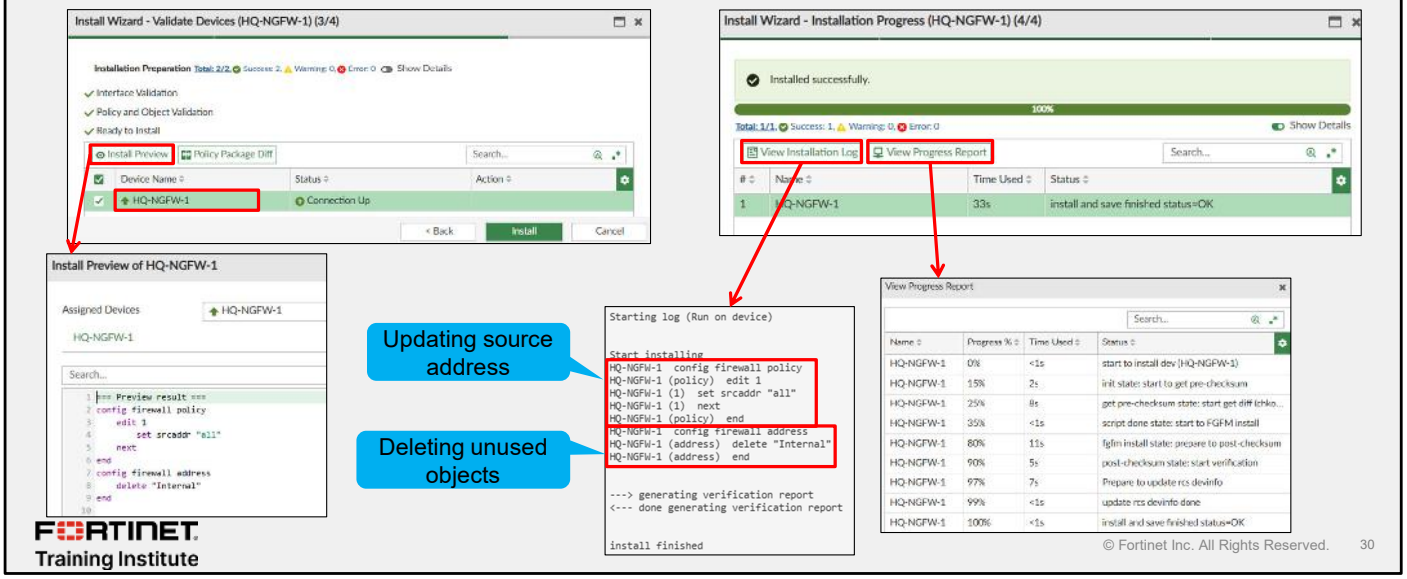
The policy package you select is displayed and you have the option to create a new ADOM revision for this installation. Note that an ADOM revision is a snapshot of the entire ADOM and not the changes specific to this policy package.

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.

Install Wizard—Validation

- Verifies the policy and device settings that will be installed and prepares a preview
- Indicates which devices the changes were installed on and installation status



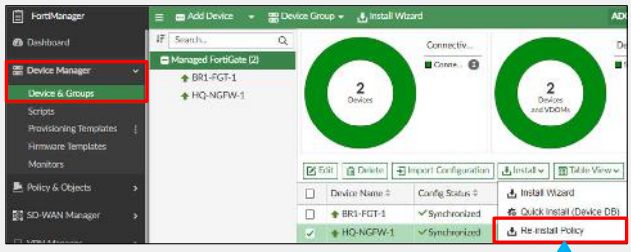
The next step in the wizard is validation. In this step, the wizard checks that the policy package selected is suitable for the installation targets selected, such as whether the interface mapping reference in the policy package is configured on the installation targets. If the validation fails, the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

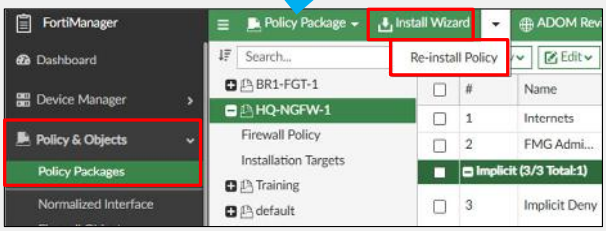
Reinstall

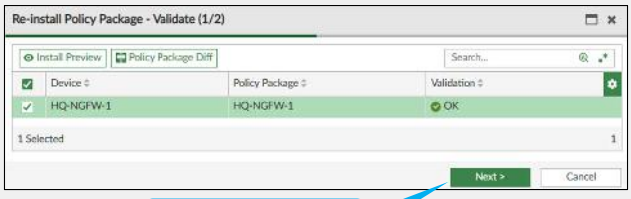
- Skips the **Install Wizard** but still provides an option to preview the installation



On **Device Manager** pane

On **Policy & Objects** pane





An administrator must perform policy installation first before the **Re-install Policy** option becomes available

Clicking **Next** will install the policy package

FORTINET Training Institute

 31

FortiManager also provides a **Re-install Policy** option. A reinstallation bypasses the wizard because the FortiGate and policy package are already selected. It offers an installation preview with an option to cancel. A reinstallation creates a new revision history and applies it to all selected installation targets.

The **Re-install Policy** option works only after the first policy installation. The option is unavailable if **Policy Package Status** is **Never Installed** for the managed device.

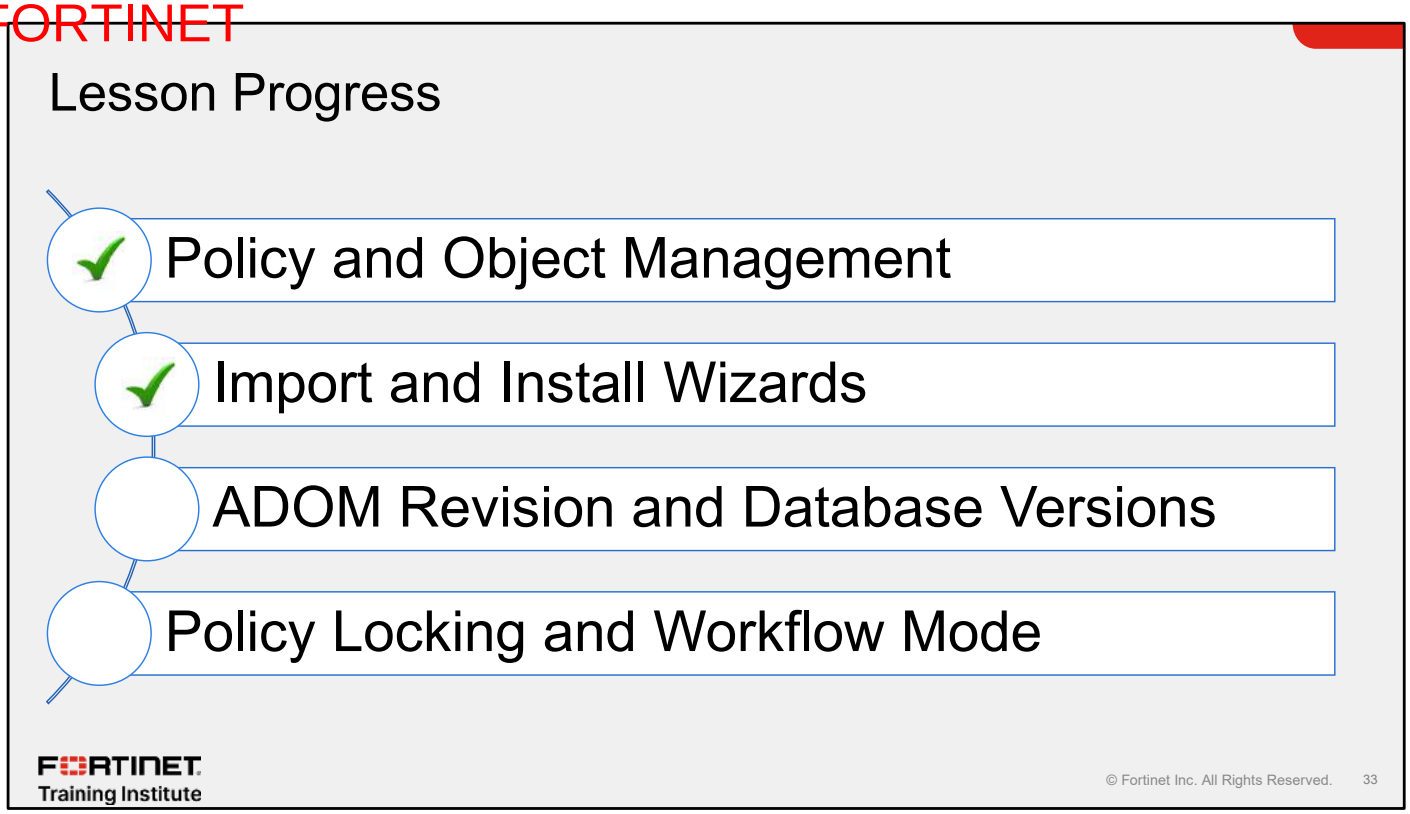
Knowledge Check

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. It can push a policy with fewer steps for quick policy change.
   - B. It can schedule a policy push.

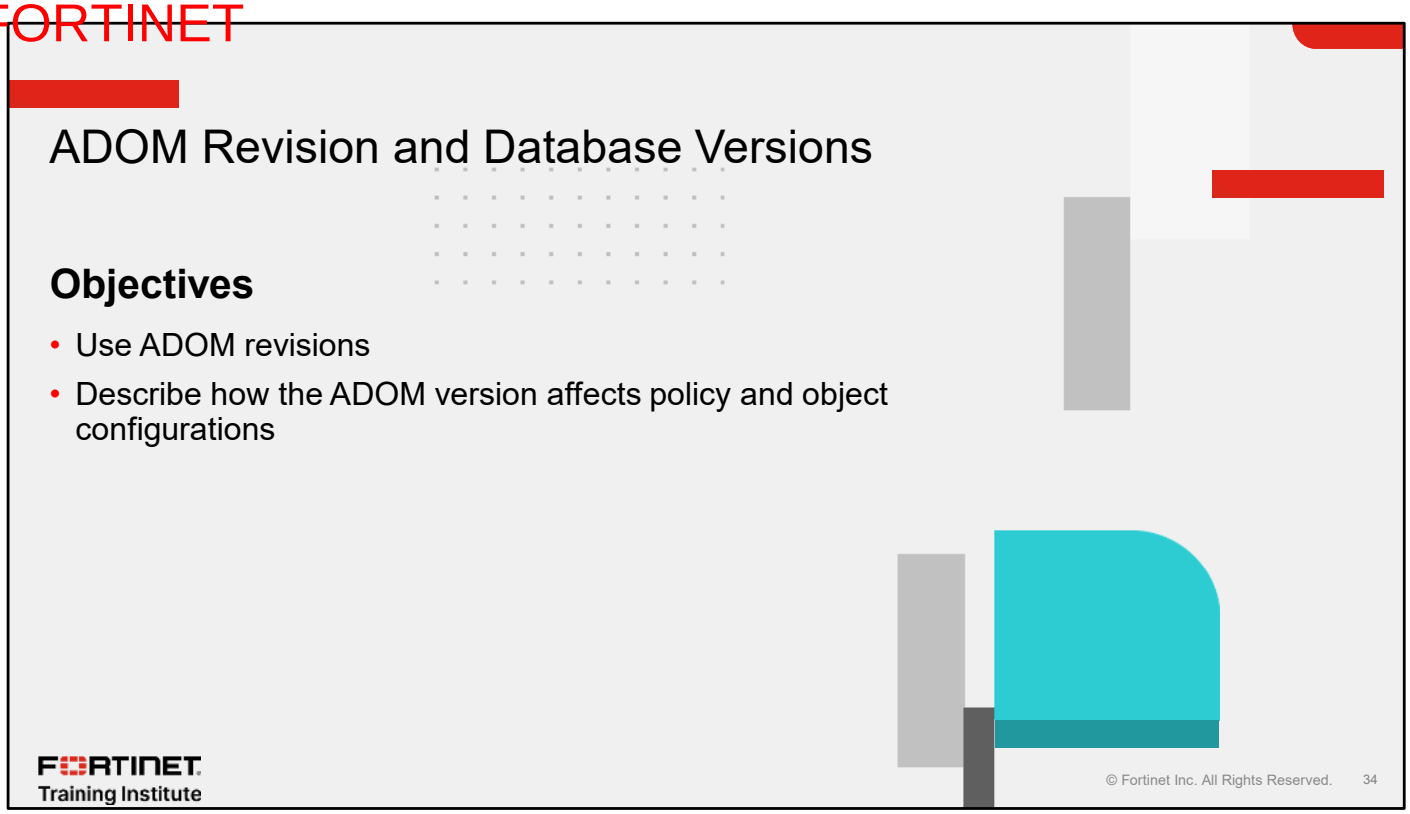
FORTINET Training Institute

 32



Good job! You now understand the FortiManager import and install wizards.

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



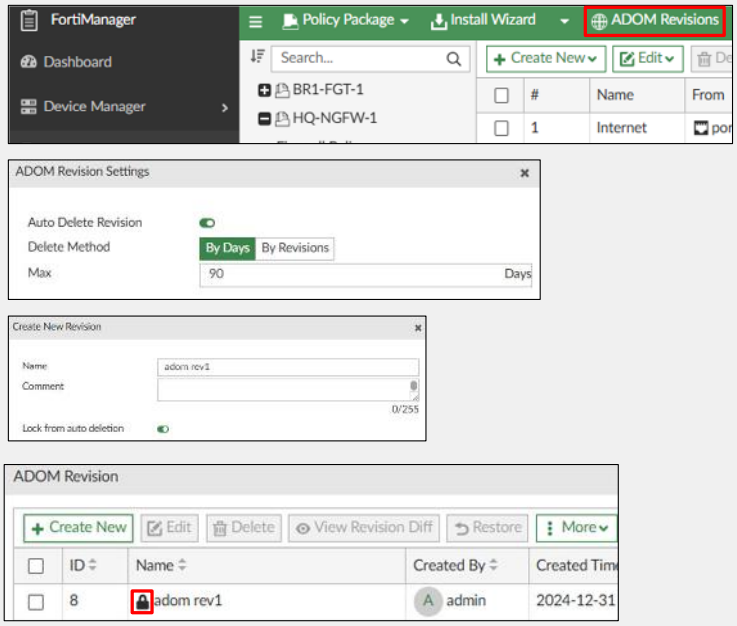
After completing this section, you should be able to achieve the objectives shown on this slide.

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

ADOM Revisions

- An ADOM revision creates a snapshot of all policy and object configurations for the ADOM
- The **ADOM Revision Settings** window provides access to autodeletion parameters
- You can lock revisions to prevent autodeletion

Warning: ADOM revisions can significantly increase the size of the configuration backup files



FORTINET Training Institute

 35

ADOM revisions allow you to save locally in FortiManager snapshots of the policy packages, objects, and VPN console settings contained in an ADOM.

When you create multiple ADOM revisions, you can view differences between them, or revert to a specific 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.

FortiManager can delete ADOM revisions automatically based on specified parameters as shown on this slide. Optionally, you can lock individual revisions to prevent them from being automatically deleted.

Note that ADOM revisions can significantly increase the size of the configuration backup.

Considerations Before Moving Devices to a New ADOM

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

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

  - Run scripts on the policy package or ADOM database
- Configuration of manager panes like VPN manager does not move
  - You must configure or reconfigure VPNs on the managed device

FORTINET Training Institute

 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 Configuration** 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 or run scripts on the policy package or ADOM database.

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

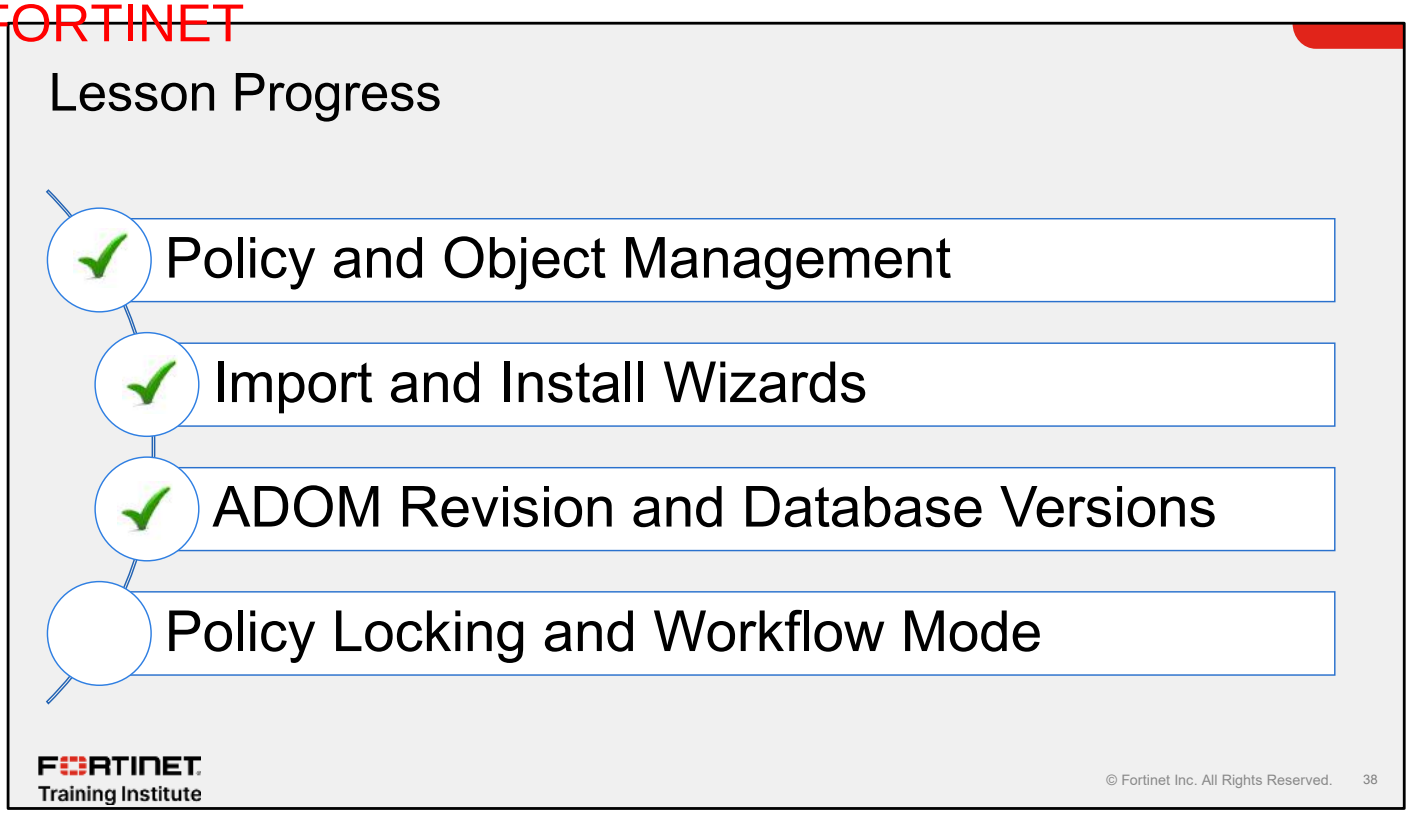
Knowledge Check

1. What is the 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

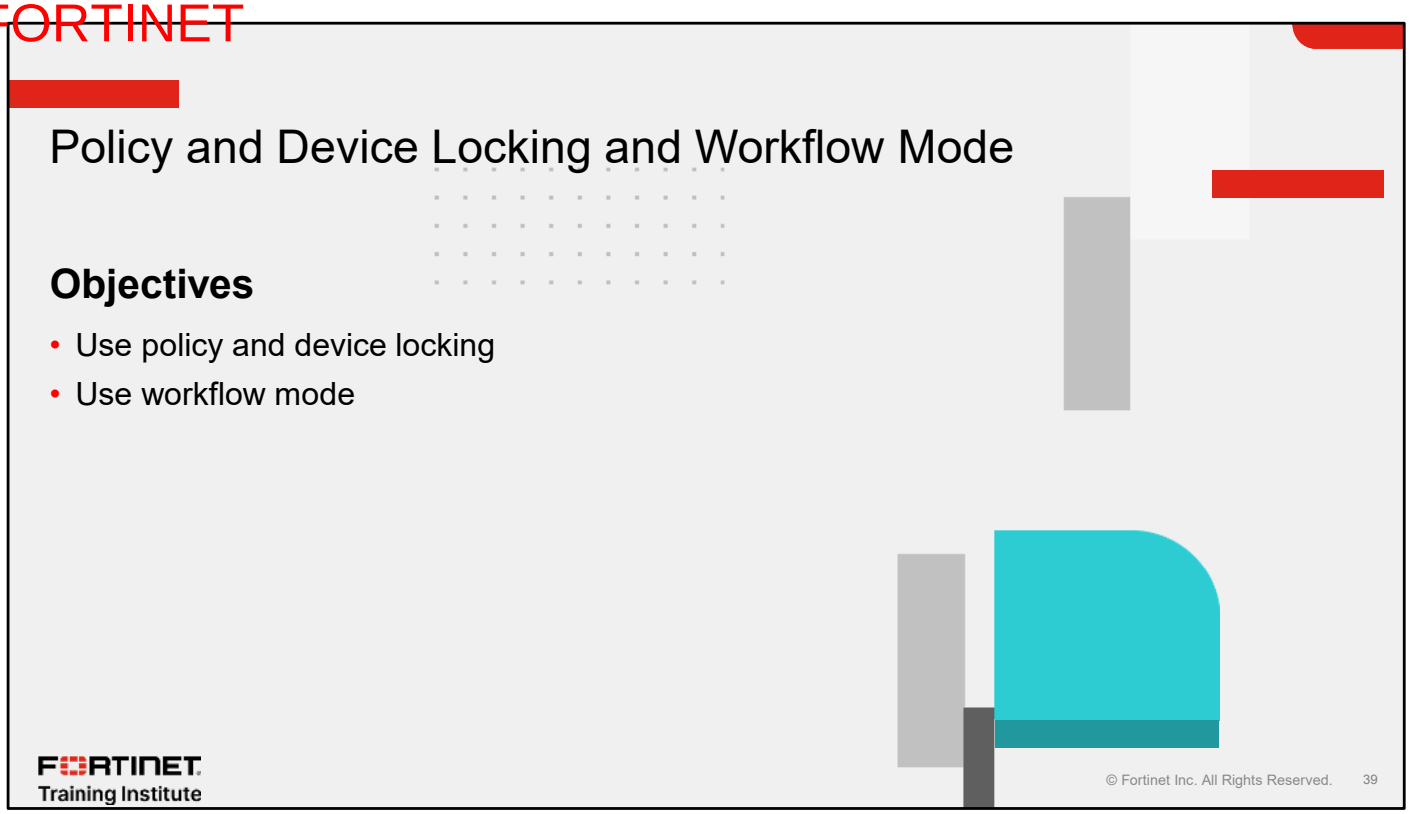
FORTINET Training Institute

 37



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

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

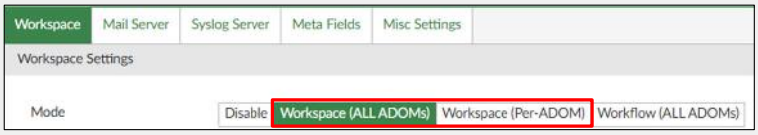


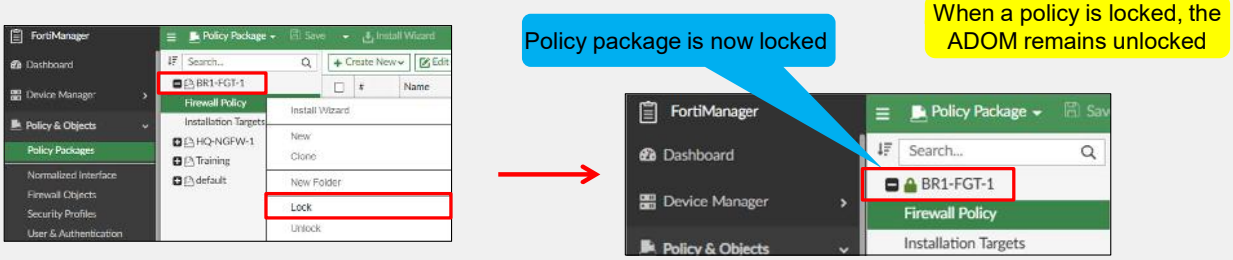
After completing this section, you should be able to achieve the objectives shown on this slide.

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.

Policy Lock

- Allows administrators to lock a single policy package instead of whole ADOM
  - Works in conjunction with `workspace-mode normal` or `workspace per-adom`
  - Locks only a policy package, not entire object database
  - You can edit locked policy package in a private workspace
  - Multiple administrators can lock and work on separate policy packages at the same time





FORTINET Training Institute

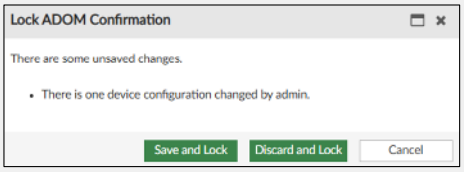
 40

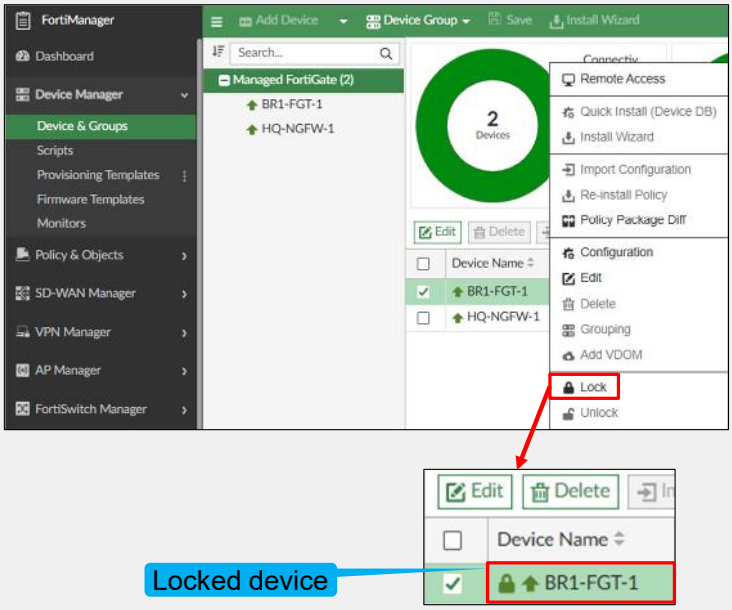
Policy locking is available in workspace normal and per-ADOM modes. Policy locking allows administrators to work on and lock a single policy package instead of locking the whole ADOM. You can lock either the whole ADOM or a specific policy package. Policy locking is an extension of ADOM locking, which allows multiple administrators to work on separate policy packages on the same ADOM at the same time.

Device Lock

- You can lock specific devices
  1. Right-click the device and select **Lock**
  2. Click **Save** after making all changes
  3. Click **Unlock** to unlock device
- System will remove individual device locks if you lock the ADOM

If you try to unlock a device or a policy package before saving your changes, a confirmation dialog box will give you the option to save or discard your changes





FORTINET Training Institute

 41

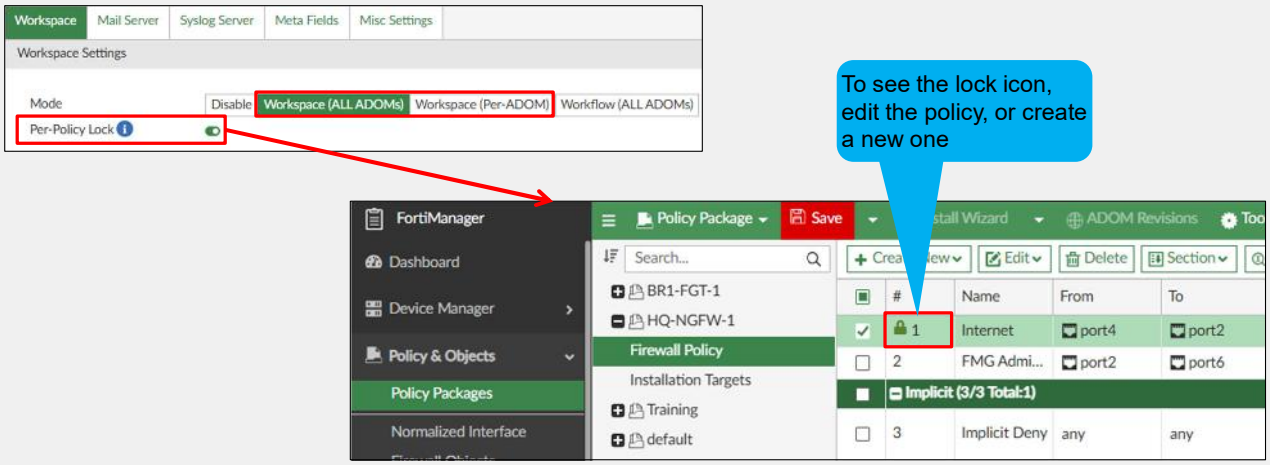
In workspace normal and per-adom modes, you can also lock specific devices to make changes to them. Other administrators will be unable to make changes to those devices until you unlock them, log out of FortiManager, or are forcibly disconnected when another administrator locks the ADOM that the device is in.

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

Keep in mind that you cannot lock individual devices if ADOMs are in advanced mode.

Per-Policy Lock

- 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



FORTINET Training Institute

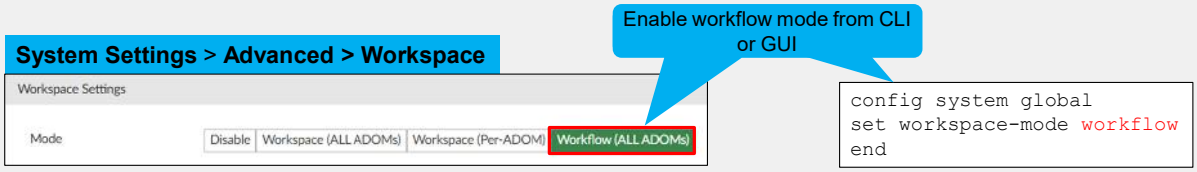
 42

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.

Workflow Mode

- Works together with ADOM locking
- Sessions can be created only on some of the management panes
  - Workflow is mostly used to make changes under **Policy & Objects**
- Allows you to control the creation, configuration, and installation of multiple settings
- All changes must be approved before they can be installed on a device
- Modifications made during a workflow session must be discarded or submitted for approval at the end of a session
- Rejected sessions can be repaired and resubmitted as new sessions for approval
- Management panes are initially read-only until an ADOM is locked



FORTINET Training Institute

 43

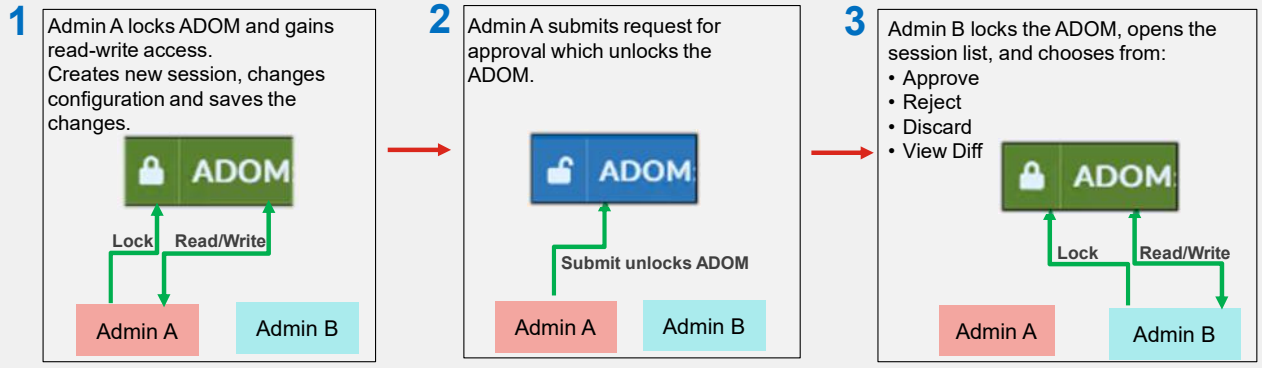
Instead of workspaces, you can use workflow mode. As with the other workspace modes, enabling workflow terminates all management sessions. You must notify other administrators to save their work to prevent any data loss. You can enable workflow mode on the CLI or GUI.

You can use workflow mode to control the creation, configuration, and installation of several settings. However, this feature is mostly used to control changes to 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.

Workflow Mode Process



FORTINET Training Institute

 44

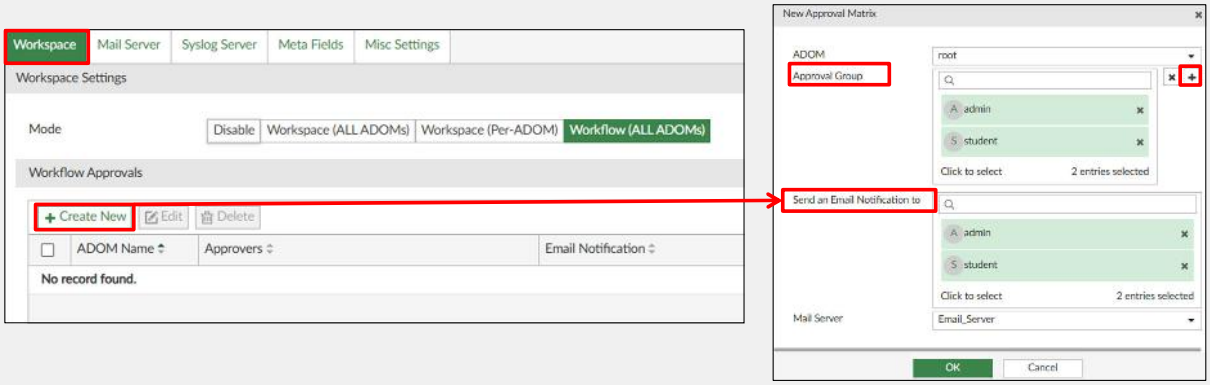
The graphic on this slide shows how to use workflow mode.

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.

Workflow Permissions

- An administrator must be part of an approval group before they can approve a session
  - Regardless of which administrator profile an administrator account is part of
  - Administrator will also need to have access to the ADOM in which the session was created in order to approve it
- On the GUI, the approval matrix must be configured before the workflow sessions are allowed



FORTINET Training Institute

 45

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.

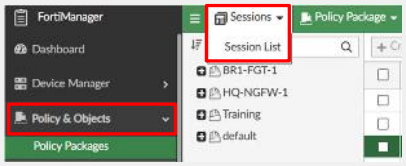
In the **Workflow Approvals** section, configure the workflow approval matrix using the following values:

- **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 in the **Mail Server** field.

Creating a New Workflow Session

- Select and lock ADOM

- Open session list



- Create new session

FORTINET Training Institute

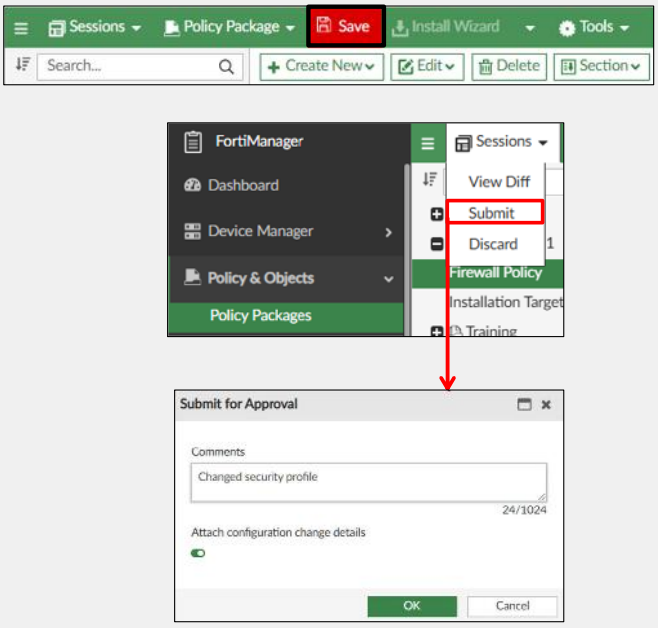
 46

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.

Submitting Workflow Sessions

- **Save** the session then submit changes
  - Session changes are discarded if administrator logs out without saving them
  - Saved sessions can be worked on at a later time
- The **Sessions** field also allows you to view a session diff
- After submitting changes for approval, ADOM returns to unlocked state

Save the session, then submit changes, or select **Submit** to automatically save and submit changes



FORTINET Training Institute

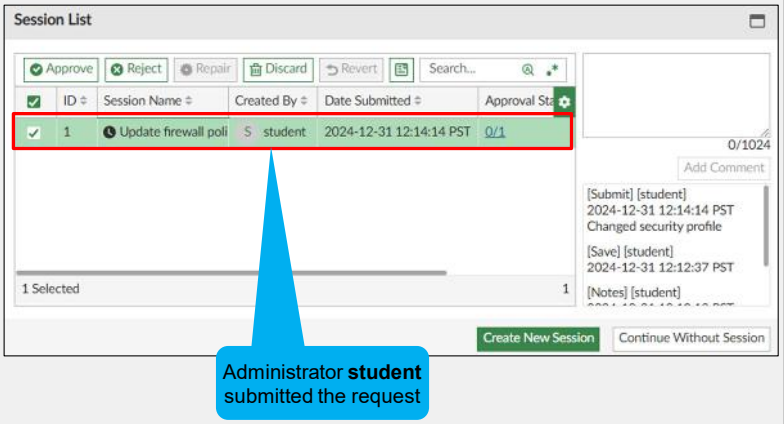
 47

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.

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**
- Actions available:
  - **Approve**
  - **Reject**
  - **Repair**
  - **Discard**
  - **Revert**
  - **View Diff**
- Rejected sessions can be resubmitted with proposed changes



FORTINET Training Institute

 48

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.

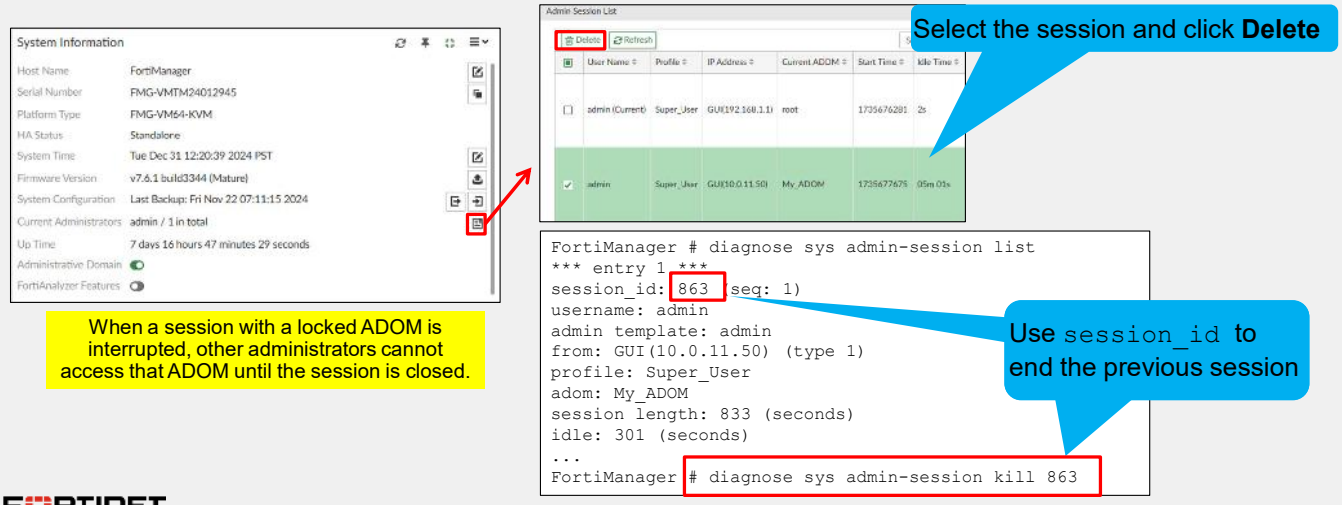
The approver administrator has several options available:

- **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.
- **Repair**: When a session is rejected, it can be repaired to correct the problems with it.
- **Discard**: The approval administrator doesn't agree with the changes and discards them. No further action is required.
- **Revert**: A previously approved session can be reverted, which undoes any existing later sessions. This creates a new session at the top of the session list that is automatically submitted for approval.
- **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 administrator user **student** submitted the request for approval.

Closing Sessions With Locked ADOMs

- FortiManager does not immediately close sessions that were unexpectedly interrupted
  - For example, when a computer crash occurs, or when you close the browser with the open session
- In these cases, sessions are closed after a timeout, or they must be manually deleted



FORTINET Training Institute

 49

When a FortiManager session is interrupted, such as a when the management computer crashes, or when you close a browser with an open GUI session, that session remains open for the system configured timeout, or until an administrator manually deletes it. When a session associated with a locked ADOM is interrupted, the read-write access to that ADOM is not possible for other administrators until the interrupted session is deleted.

You can delete administrator sessions on the GUI or the CLI as shown on this slide. After the session is deleted, the ADOM will be unlocked immediately.

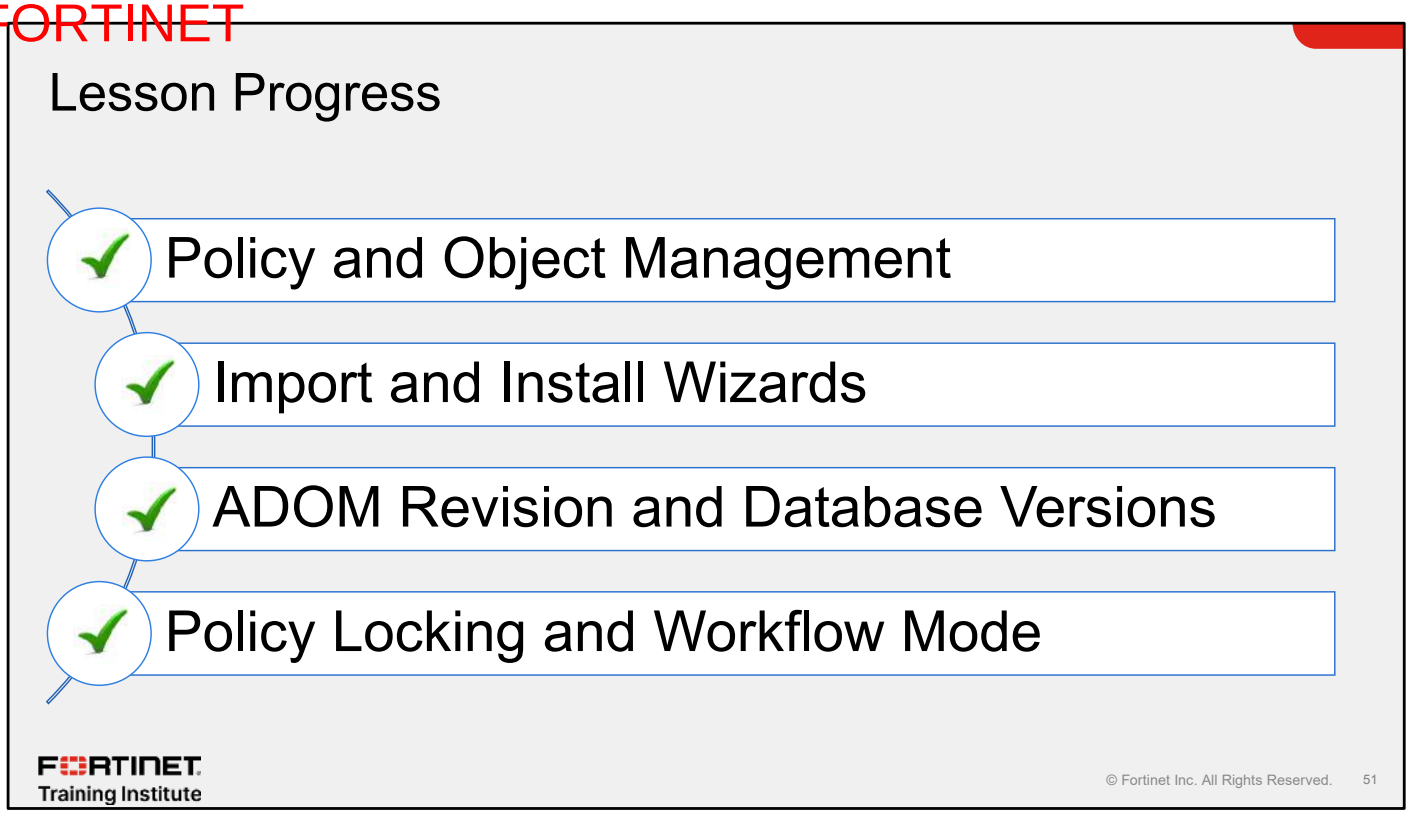
Knowledge Check

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 a 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

 50



Congratulations! You have completed this lesson.

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

Review

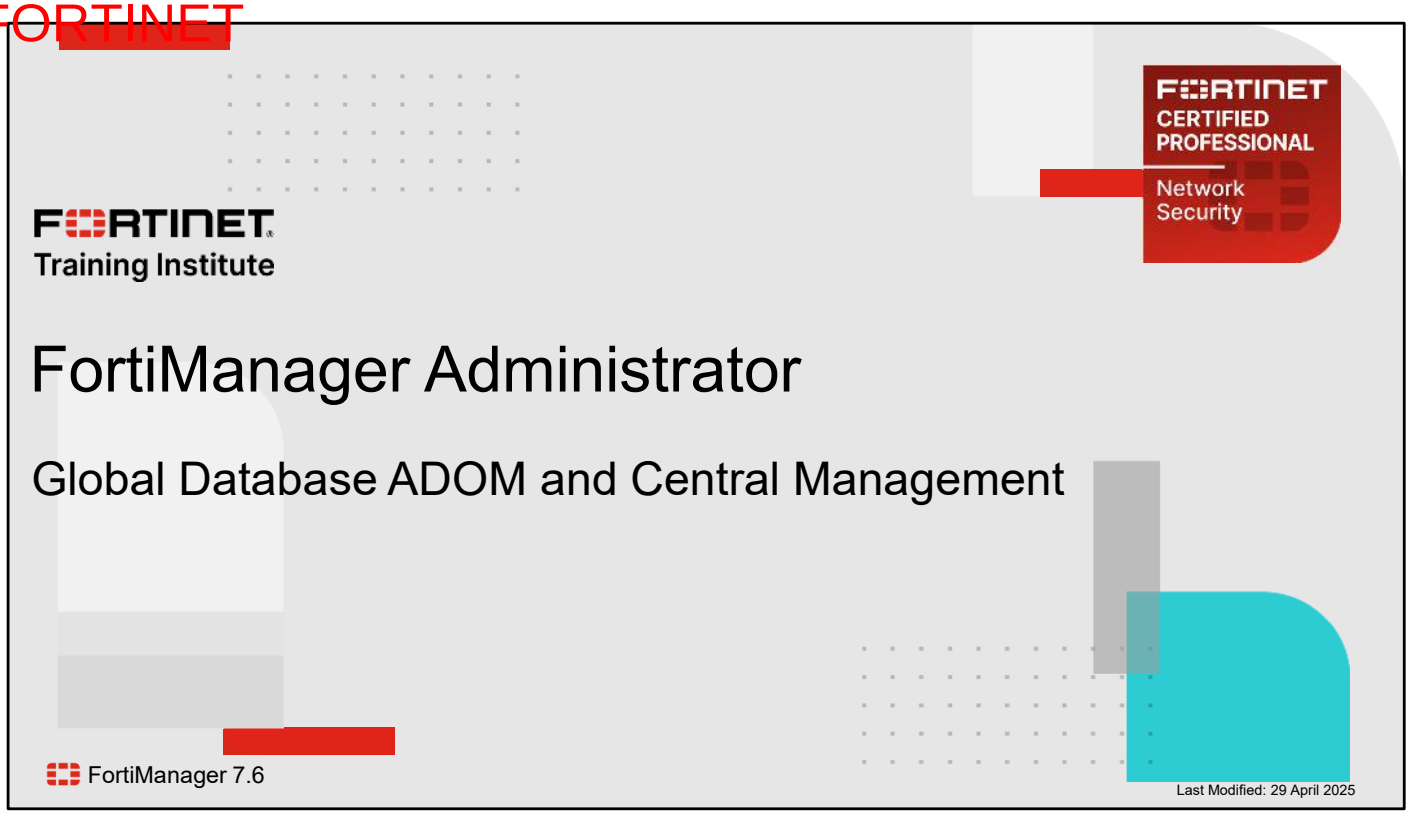
- ✓ Manage policy packages and objects
- ✓ Create installation targets for policies and policy packages
- ✓ Configure dynamic objects
- ✓ Interpret the policy package status of a device on FortiManager
- ✓ Use the import configuration wizard
- ✓ Use the install and reinstall wizards
- ✓ Use ADOM revisions
- ✓ Describe how the ADOM version affects the policy and object configurations
- ✓ Use policy and device locking
- ✓ Use workflow mode

FORTINET Training Institute

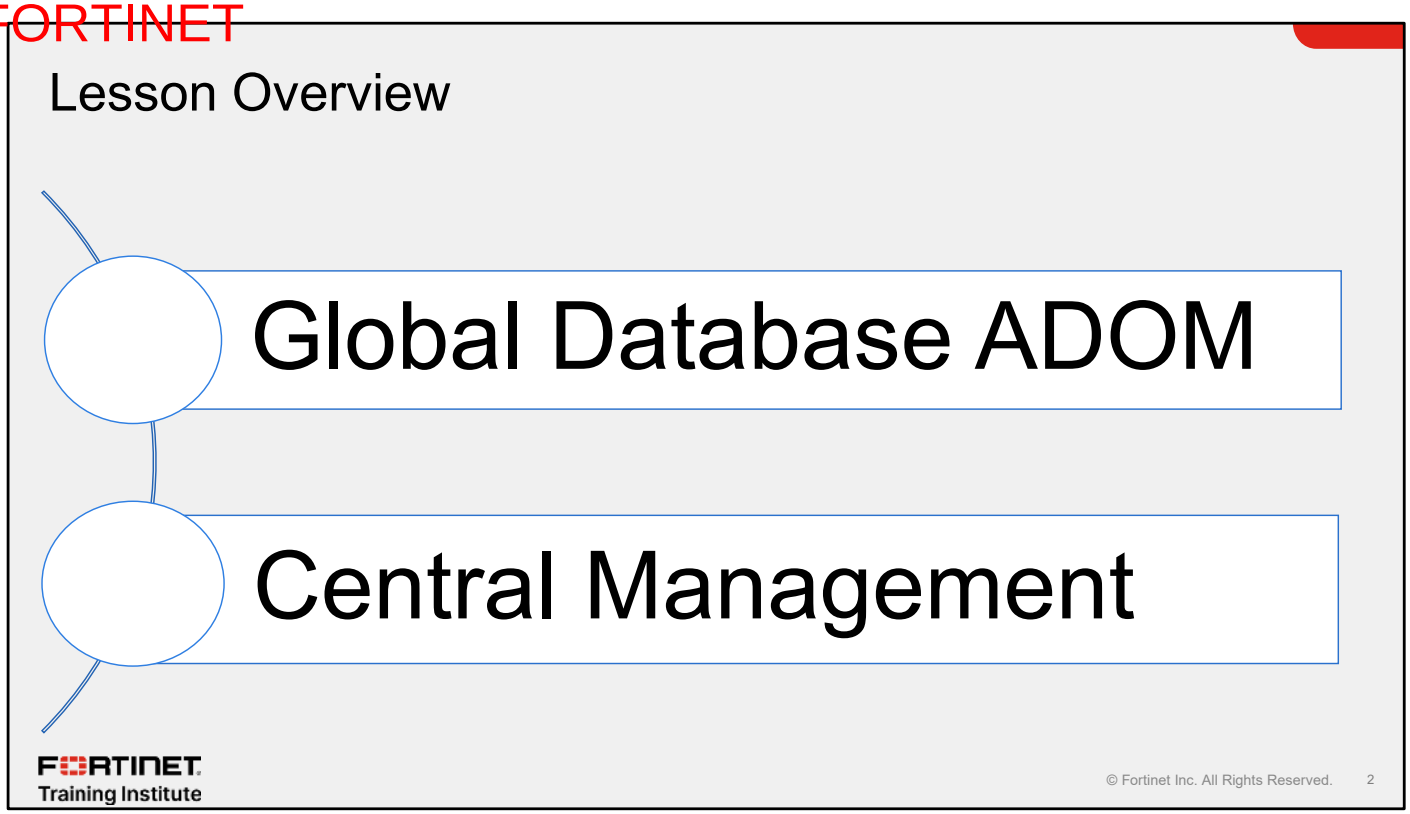
 52

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

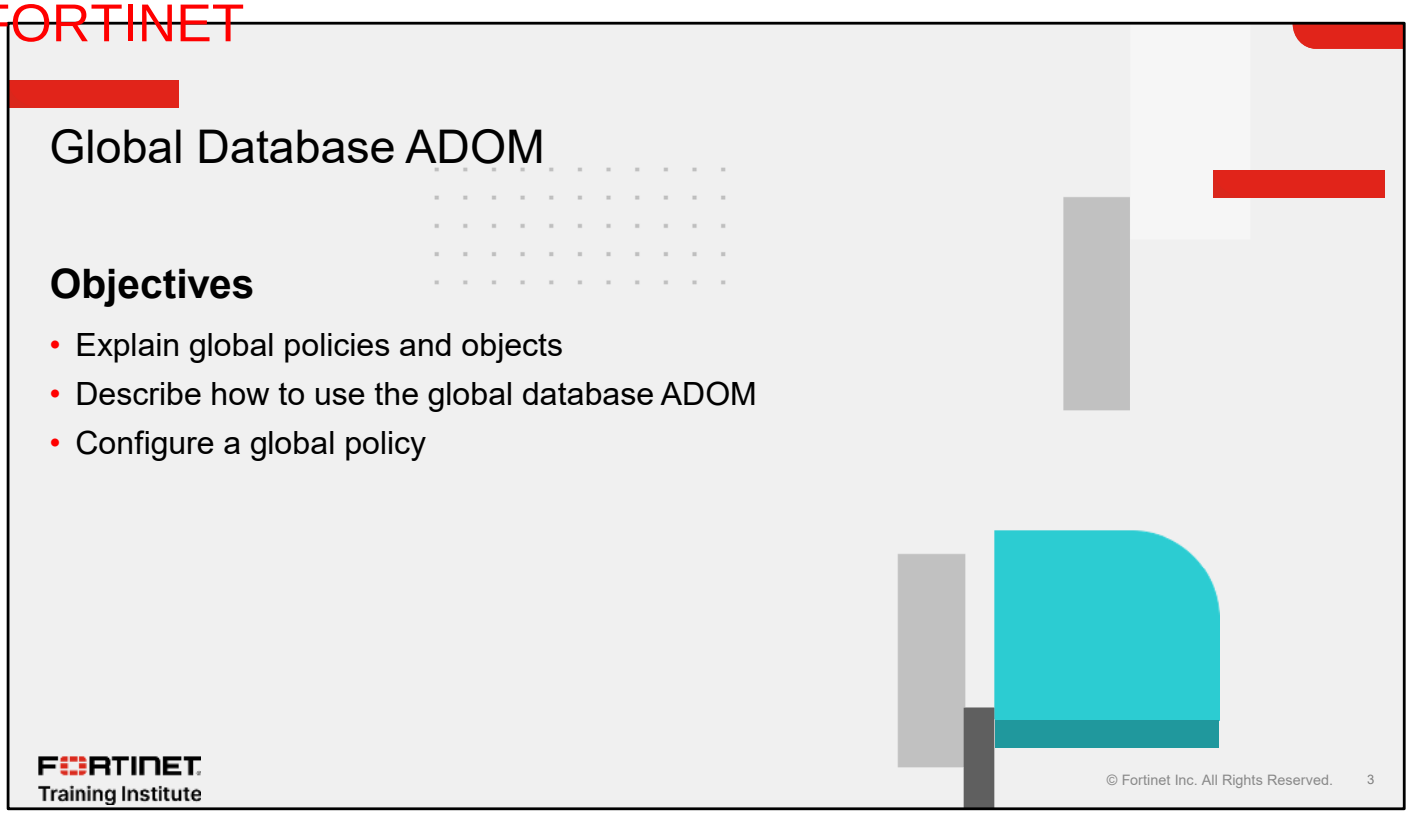
By mastering the objectives covered in this lesson, you learned how to manage policies and objects on FortiManager for FortiGate. You also learned how to configure policies and objects on FortiManager, and then install them on FortiGate.



In this lesson, you will learn about the global database ADOM and central management.



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

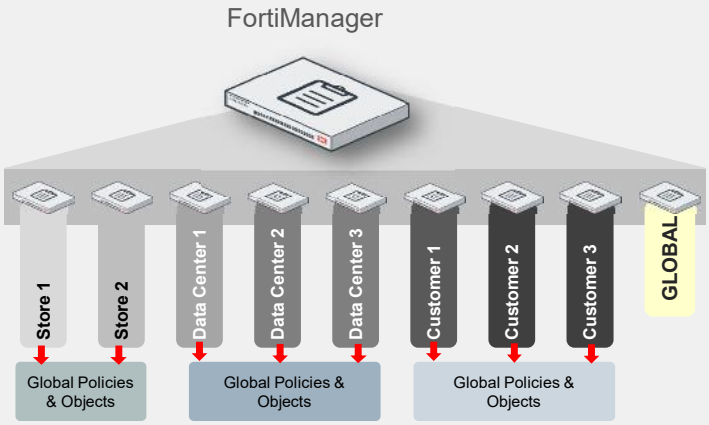


After completing this section, you should be able to achieve the objectives shown on this slide.

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

Shared Global Policies and Objects

- Global policies and objects are shared among all ADOMs



FORTINET Training Institute

 4

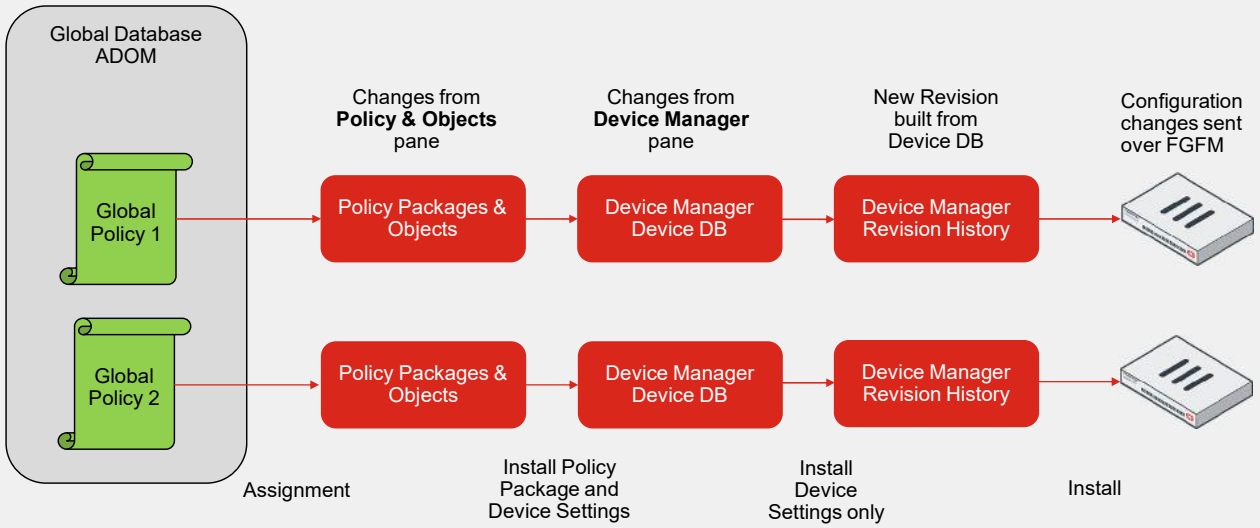
Global policies and objects allow administrators to push firewall policies to some or all ADOMs. You must explicitly assign global policy packages to specific ADOMs on which administrators want to install similar policies.

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.

Global Database ADOM

- Contains global objects, and header and footer policies



FORTINET Training Institute

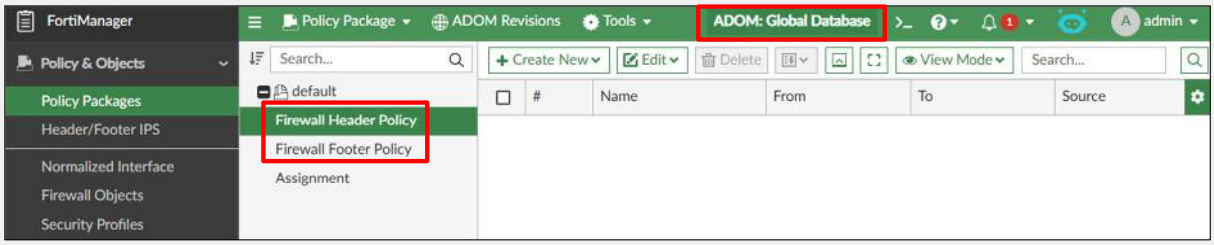
 5

You can use header and footer policies to wrap policies in individual ADOMs. 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.

Global Database ADOM—Policy Types

- 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

 6

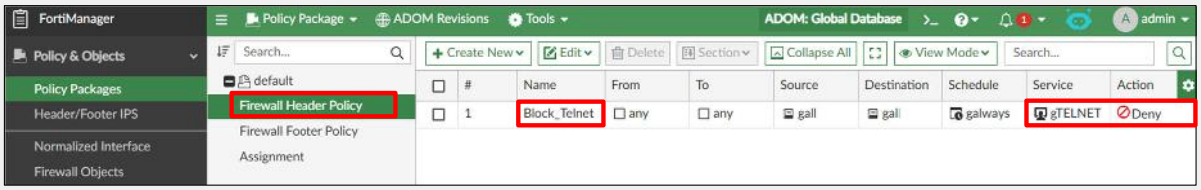
Enter the **Global Database** ADOM to access the global policy database.

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.

Example—Header Policy

- Create a firewall policy to block Telnet traffic



- 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

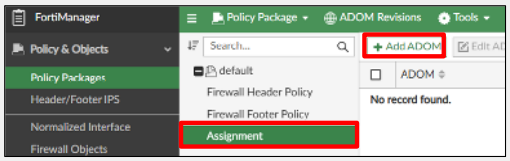
 7

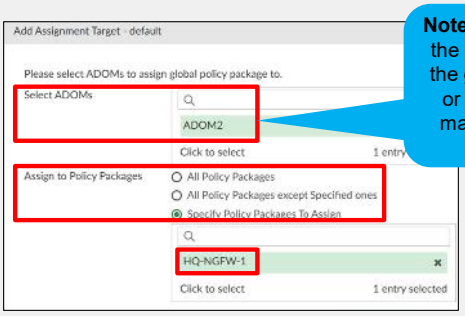
In the example shown on this slide, a header policy blocks Telnet traffic from passing through the managed firewalls.

The next step is to assign this policy to one policy package in an individual ADOM.

Assigning a Global Policy Package to an ADOM

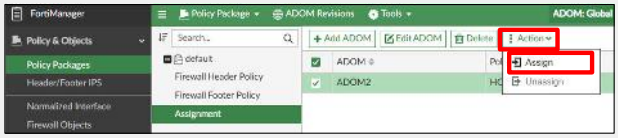
- First, add the required ADOMs as targets

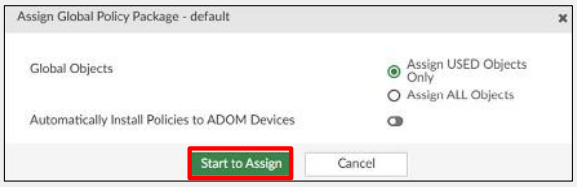




Note: Only ADOMs of the same version as the global database, or the next higher major release, are displayed.

- Second, assign the global policy package to the ADOMs





FORTINET Training Institute

 8

This slide shows the steps to assign a global policy package to an ADOM policy package.

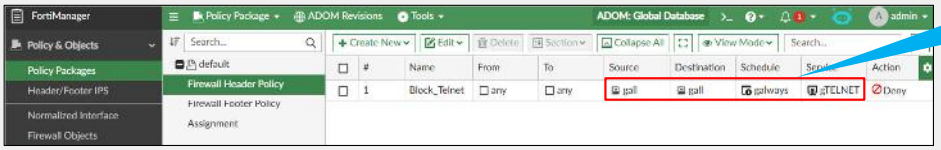
In this example, the **default** global policy package is added to the **HQ-NGFW-1** policy package in **ADOM2**. After installation, the status changes to **Up to date**.

Notice that there are several options available when assigning a global policy package, including:

- Assign used objects only
- Assign all objects
- Automatically install policies on ADOM devices

Viewing Assigned Global Policy

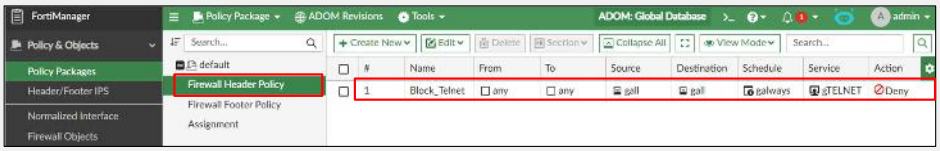
- Header policy created in global database ADOM



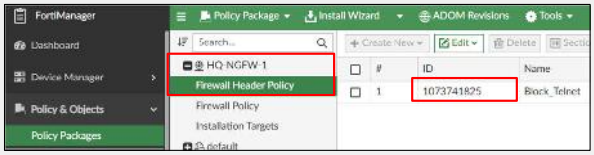
All global objects start with "g" and are edited or deleted in global ADOM only

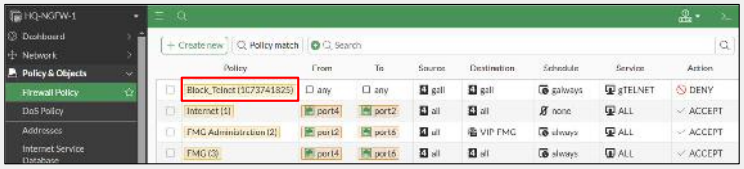
Caution: Never create address objects or profiles starting with letter “g” on the ADOMs or managed devices

- Local-FortiGate now includes the header policy created in global database ADOM



- After installation, the global policy shows at the top locally on FortiGate





FORTINET Training Institute

 9

After you assign the global database 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 database ADOM only.

A word of caution. Never create address objects or security profiles starting with letter “g” on an ADOM database or directly on the managed devices because this may create conflicts with global database ADOM objects and cause configuration failure issues.

In the example shown on this slide, the header policy is added to the HQ-NGFW-1 device. 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 cannot 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. A header policy is installed at the top of the list of the firewall rules on the target device.

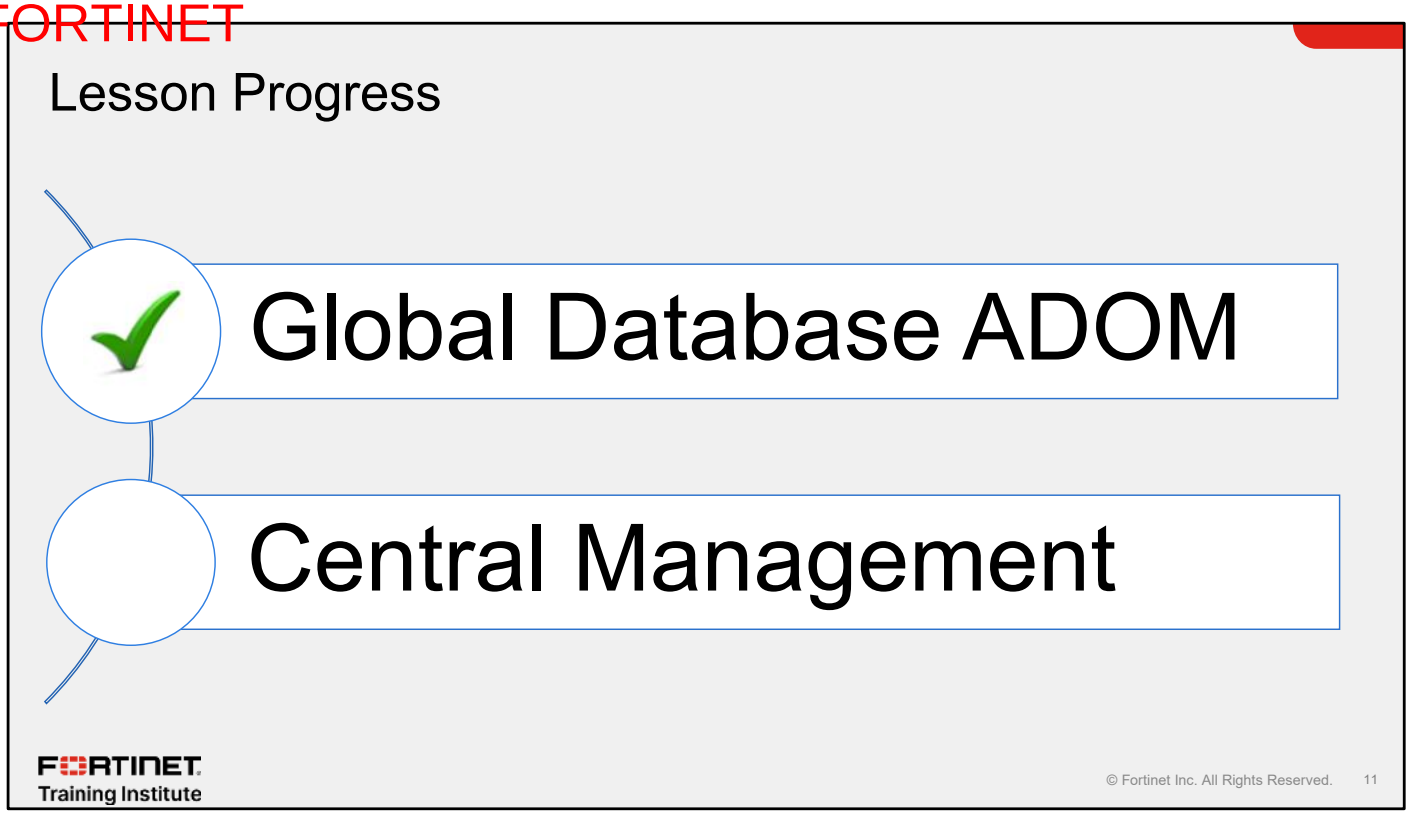
Knowledge Check

1. What is the purpose of the global database 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”.

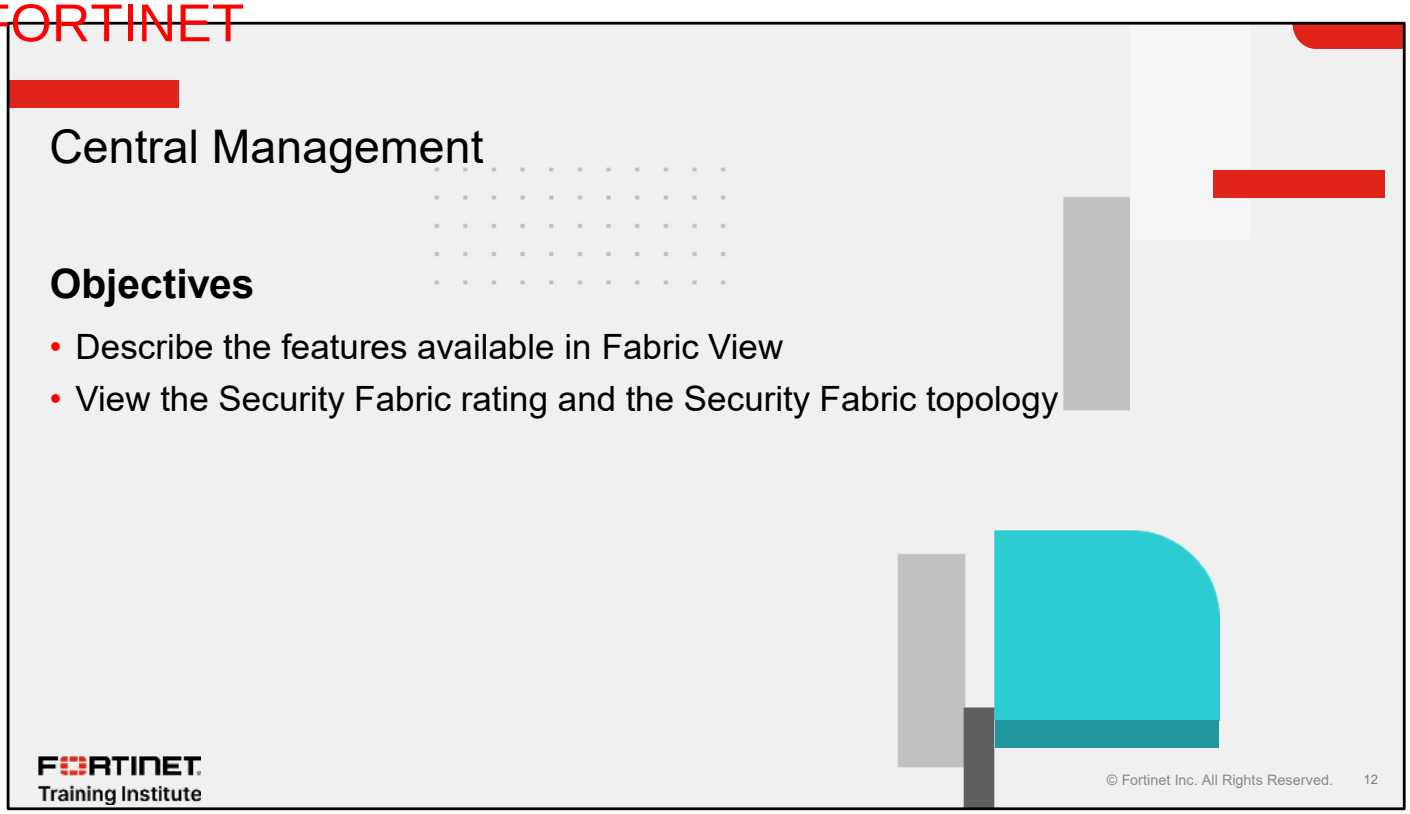
FORTINET Training Institute

 10



Good job! You now understand the global database ADOM.

Now, you will learn about other manager panes and the Security Fabric features available on FortiManager.

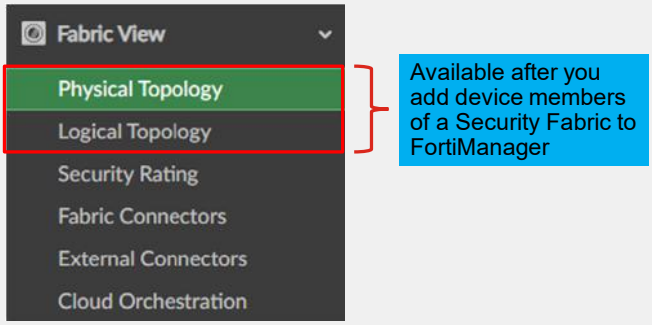


After completing this section, you should be able to achieve the objectives shown on this slide.

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.

Fabric View Pane

- You can view Security Fabric ratings of managed devices
- Physical and logical topologies available when managing FortiGate devices in a fabric
- Several connector types allow interaction with other products and platforms
- Ability to orchestrate the deployment of FortiGate autoscaling groups on AWS



Note: After adding the root FortiGate, all downstream devices in the fabric are automatically added as **Unauthorized** in the root ADOM.

Note: Refresh the fabric root after all the members of the group are added to FortiManager.

FORTINET Training Institute

 13

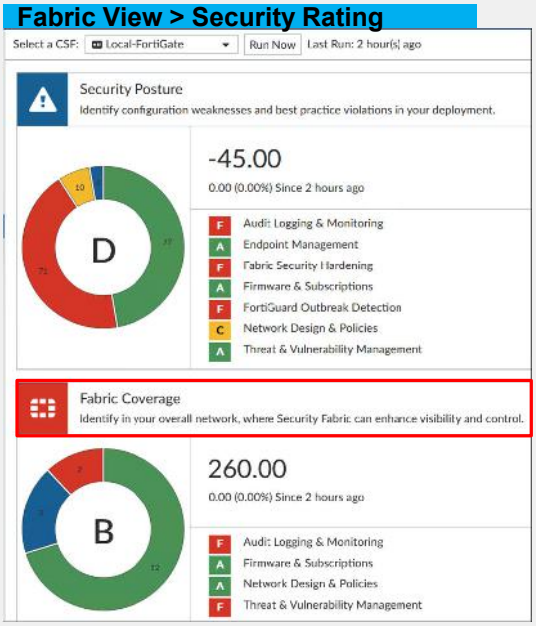
The **Fabric View** pane allows you to display the **Security Rating** reported by managed FortiGate devices. When FortiManager is managing FortiGate units that are part of a Security Fabric, the option to view the physical and logical topologies of the fabric becomes available.

From this pane you can also add several types of connectors that allow FortiManager to interact, and use objects created in other products and platforms, both in the local network and cloud based. Refer to the *FortiManager Administrator Guide* for the complete list of connectors available.

FortiManager supports the ability to orchestrate the deployment of FortiGate autoscaling groups (ASG) on Amazon Web Services (AWS). This allows administrators to use FortiManager as a single pane to deploy all resources required to implement FortiGate ASG in the public cloud.

Security Fabric Rating

- Displays the reported Security Fabric ratings
- Three major scorecards: **Security Posture**, **Fabric Coverage**, and **Optimization**
- Provides executive summary of the three largest areas of security focus



FORTINET Training Institute

 14

The **Security Rating** feature includes 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 for all FortiGate devices managed by FortiManager.

The **Security Rating** page includes the same three scorecards available on FortiGate:

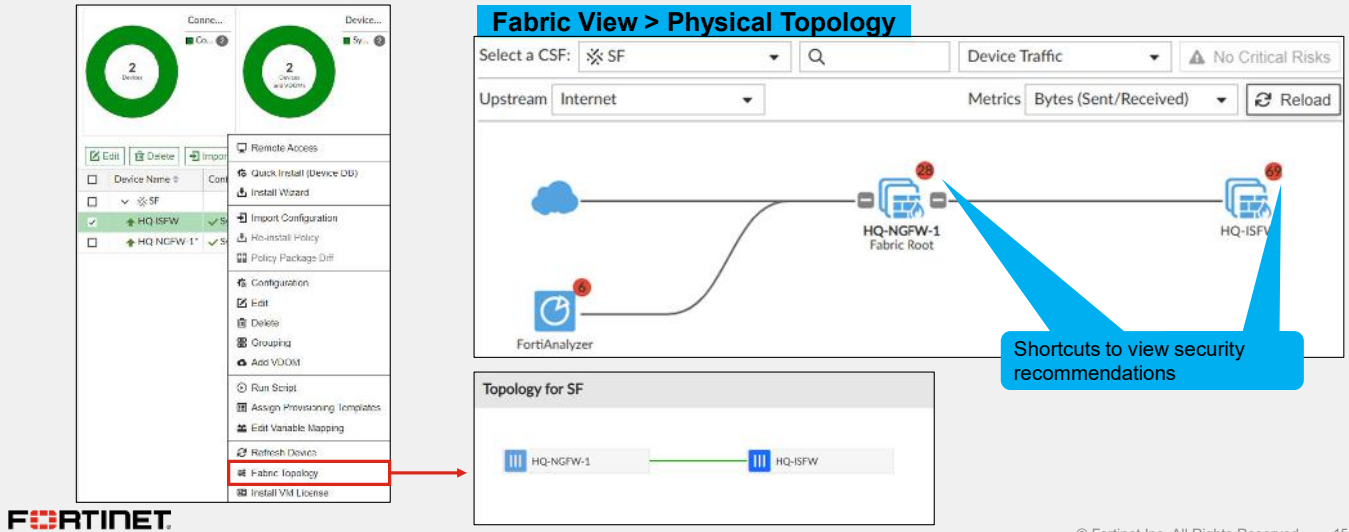
- **Security Posture**
- **Fabric Coverage**
- **Optimization**

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.

Fabric Topology View

- Full topology available at **Fabric View** > **Physical**, or **Fabric view** > **Logical Topology**
- Right-click a fabric member for FortiGate topology



FortiManager recognizes Security Fabric groups of devices and lets you display their fabric topology. You can click **Fabric View** > **Physical Topology**, or **Fabric View** > **Logical Topology** to view the full topology. This view includes shortcuts to any existing security recommendations that redirect you to the **Security Rating** pane.

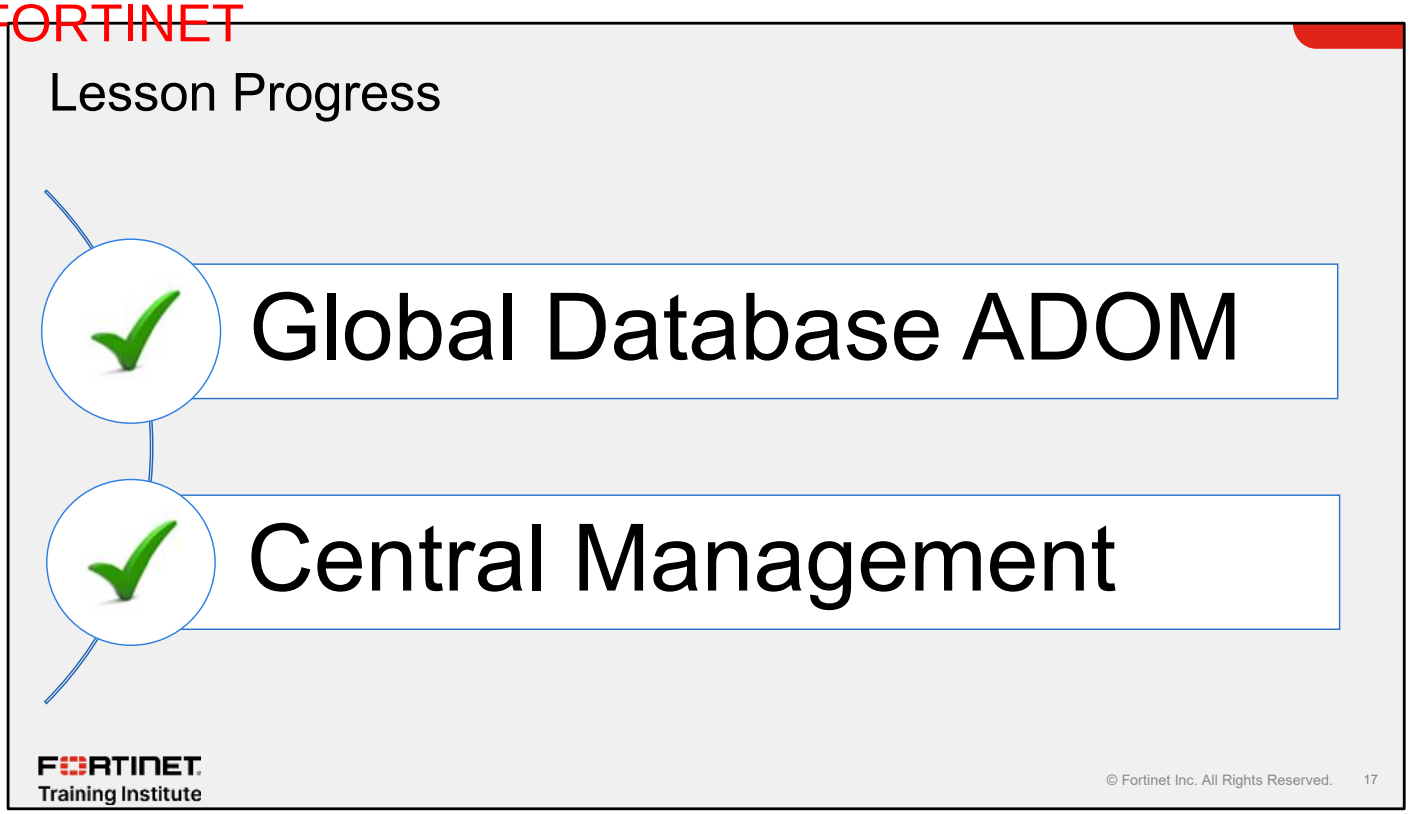
You can also can right-click any device in the fabric, and then select **Fabric Topology** to view its location relative to other fabric members. This is illustrated on the slide for the HQ-NGFW-1 device.

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. Modify the topology of the Security Fabric.

FORTINET Training Institute

 16



Congratulations! You have completed this lesson.

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

Review

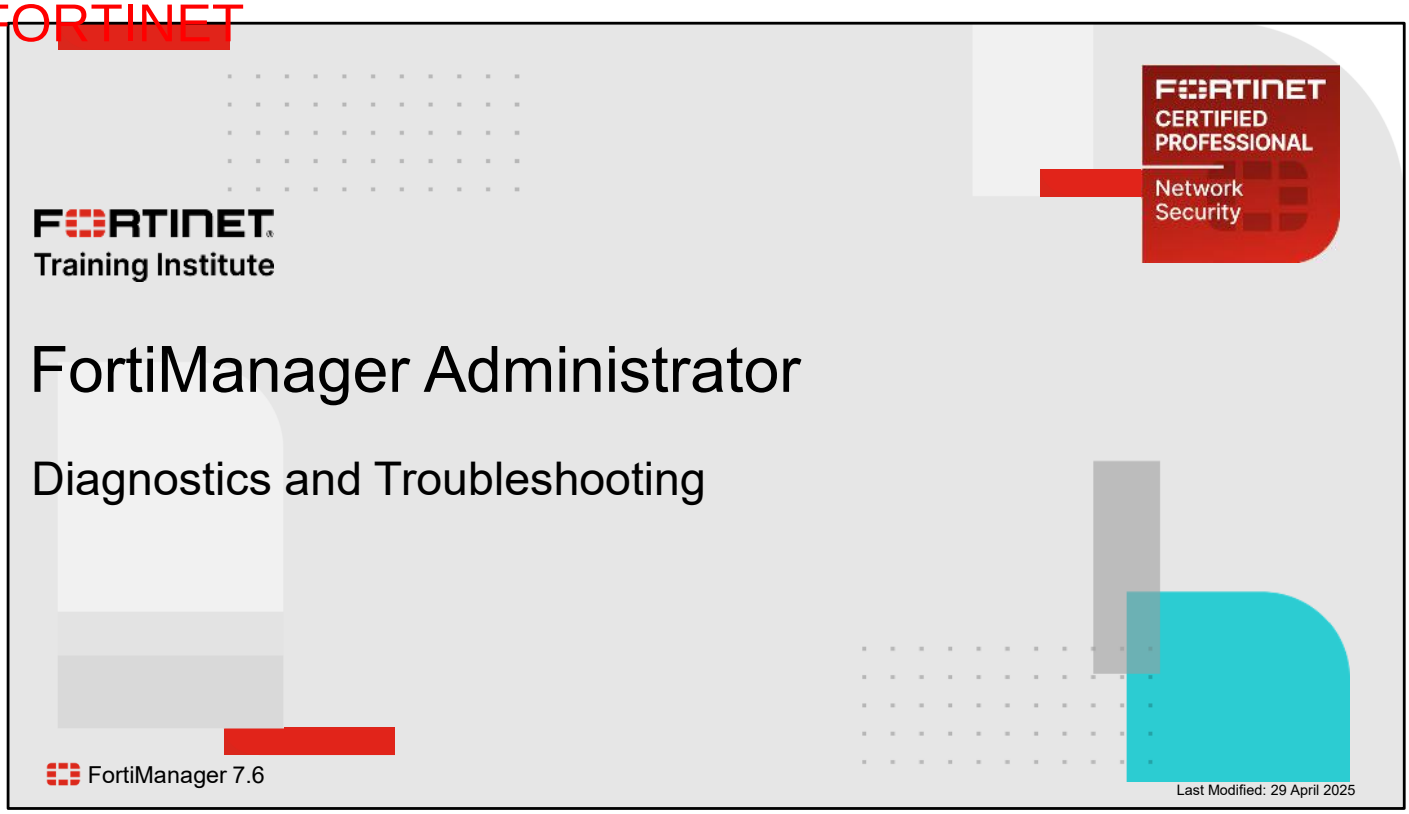
- ✓ Explain global policies and objects
- ✓ Describe how to use the global database ADOM
- ✓ Configure a global policy
- ✓ Describe the features available in Fabric View
- ✓ View the Security Fabric rating and the Security Fabric topology

FORTINET Training Institute

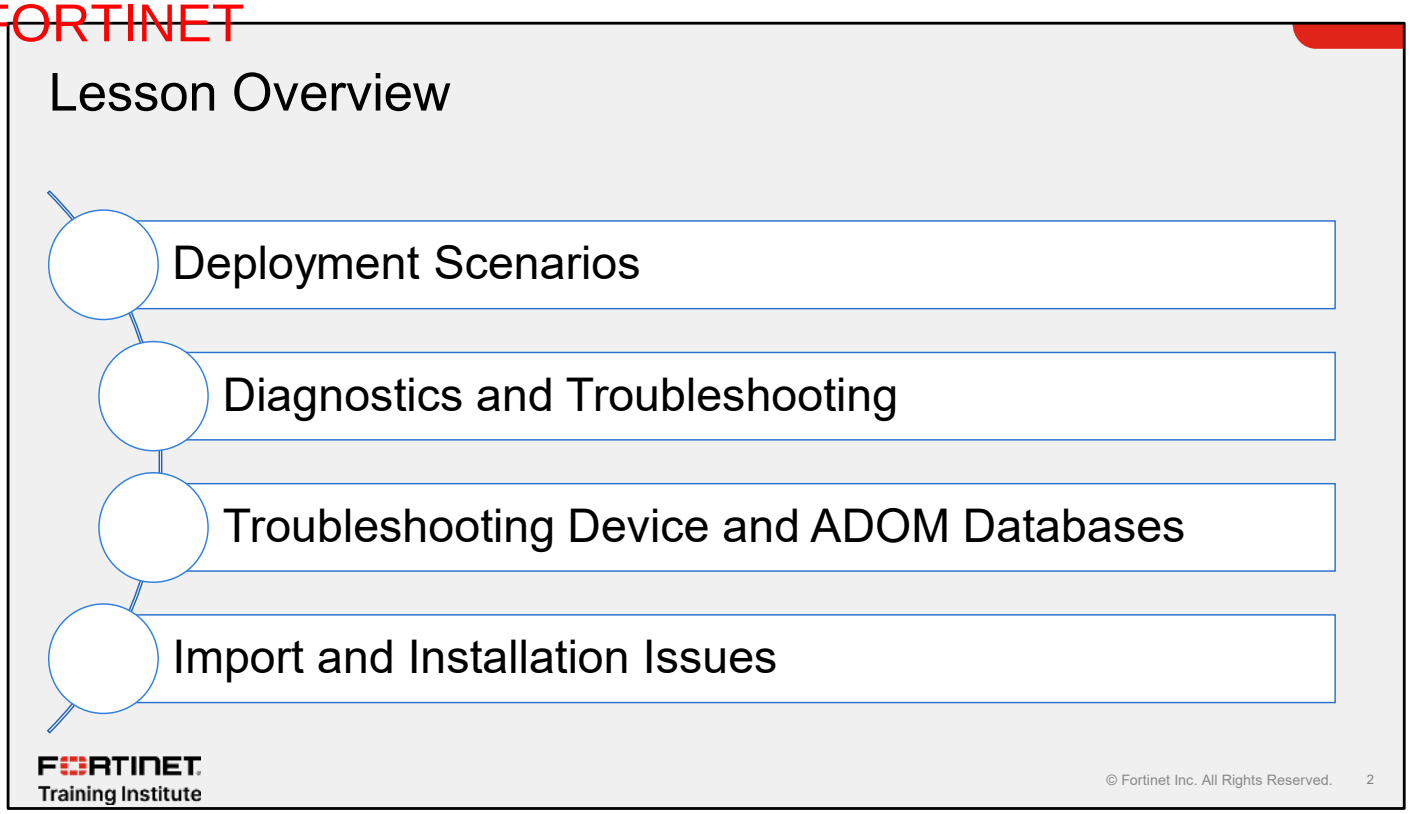
 18

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

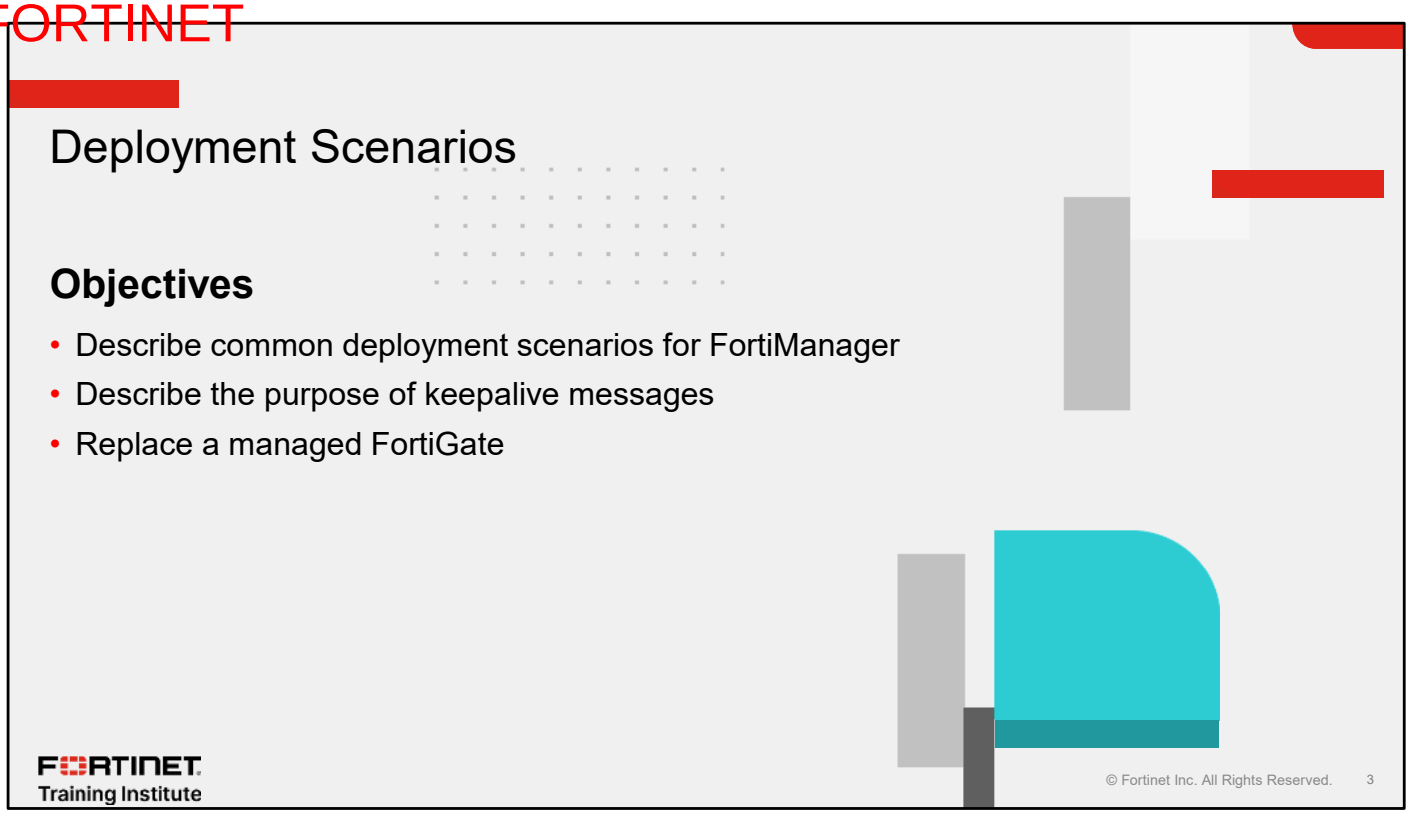
By mastering the objectives covered in this lesson, you learned about the global database ADOM, and the Security Fabric.



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



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

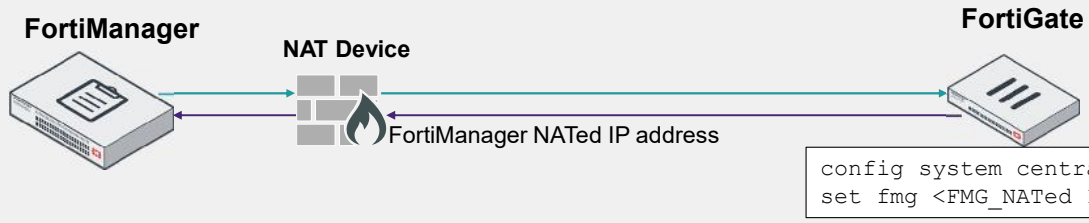


After completing this section, you should be able to achieve the objectives shown on this slide.

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.

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 reestablish the FGFM tunnel, if torn down

If FortiManager is behind a NAT device, it is recommended that you configure the FortiManager NATed IP address using `system admin settings` on FortiManager. You can also configure the FortiManager FQDN if it has one associated.

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

FORTINET Training Institute

 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 FortiGate-FortiManager communication protocol (FGFM) tunnel is torn down, *only* FortiManager tries to reestablish the FGFM tunnel. This is because, by default, the network address translated (NATed) FortiManager IP address is not configured on FortiGate central management.

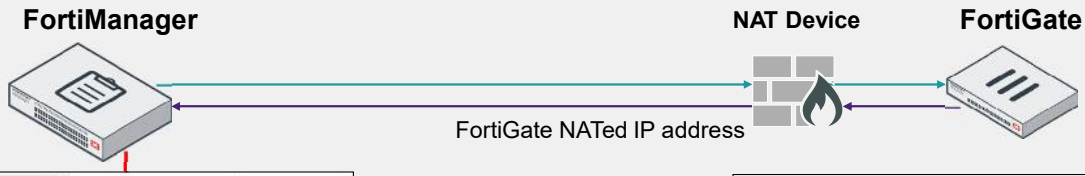
How can FortiGate announce itself to the NATed FortiManager, or try to re-establish the FGFM tunnel if it is torn down?

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 reestablish 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.

Additionally, if your FortiManager has an FQDN associated, you can also configure it so FortiGate devices can use it to announce themselves and reconnect to FortiManager if needed.

FortiGate Behind a NAT Device

- FortiManager can discover FortiGate through the FortiGate NATed IP address
- FortiManager doesn't automatically attempt to reestablish the FGFM tunnel, if it is torn down
  - Clicking the **Refresh Device** icon in the **Managed FortiGate** forces a one-time connection attempt




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

- FortiGate can announce itself to FortiManager
- Only FortiGate tries to reestablish the FGFM tunnel, if torn down

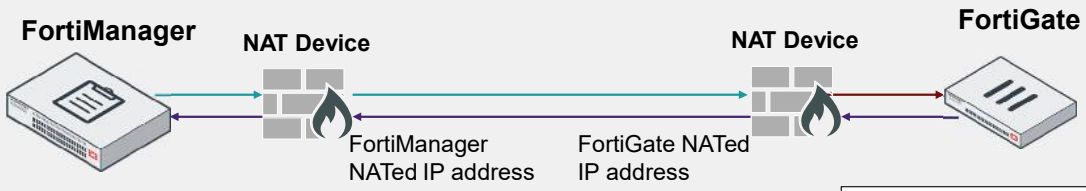
FORTINET Training Institute

 5

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 re-establish 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 **Refresh Device** icon in the **Managed FortiGate** for the managed device in Device Manager.

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

 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.

FGFM Keepalive Messages

- Configured on FortiManager

```
config system dm
set fgfm-sock-timeout 360
set fgfm_keepalive_itvl 120
```

- If FortiManager does not receive a keepalive message for the duration of the `fgfm-sock-timeout` value, the tunnel is torn down

```
# FGFMs: Timeout[360] for sock.
FGFMs(FGVM..-10.0.11.254):
Cleanup devid=307 tunnel_ip from
DVM (ret=0)
```

FortiManager didn't receive a keepalive and the tunnel is torn down

FORTINET Training Institute

 7

Keepalive messages are sent from FortiGate at configured intervals. 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.

You can configure the timeout and interval by setting the following parameters:

- `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

FGFM Keepalive Messages (Contd)

- Only FortiGate sends a keepalive message to FortiManager, regardless of which device established the FGFM tunnel
  - FortiGate also sends a configuration checksum to confirm synchronization as a part of the message

From FortiGate

```
FortiGate # diagnose  debug application fgfmd 255
FortiGate # diagnose debug enable
FGFMs: client:send:
keepalive
checksum=56 06 ae ab ea 15 72 ..
ipsversion=18.00132(2021-07-31 01:29)….
```

FortiGate sends keepalive, which includes checksum and IPS version

From FortiManager

```
FMG # diagnose debug application fgfmsd 255
FMG # diagnose debug enable
FGFMs(FGVM01…-265-100.65.1.111): fgfm_keepalive_handler: old chksum: 56 06 ae ab ea 15 72 …
FGFMs(FGVM01…-265-100.65.1.111): fgfm_keepalive_handler: new chksum: 56 06 ae ab ea 15 72 …
FGFMs(FGVM01…-265-100.65.1.111): server:send:
reply 200
request=keepalive
cur_tun_serial=
```

FortiManager receives keepalives and compares checksums to see if there are configuration changes

FORTINET Training Institute

 8

Only the FortiGate devices send keepalive messages to FortiManager, regardless of which device established the FGFM tunnel. FortiGate includes a configuration checksum in the keepalive messages to confirm synchronization as a part of the keepalive message. The intrusion prevention system (IPS) version is also included in the messages.

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

 9

When you perform an installation 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 and nothing is 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.

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

 10

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.

Replace a Managed Standalone Device (Contd)

1. Note the original FortiGate device name

```
diagnose dvm device list
```

devname = Original FortiGate device name
serial_number = Serial number of replacement FortiGate

2. Update the serial number of the replacement FortiGate

```
execute device replace sn <devname> <serial_number>
```

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

```
diagnose dvm device list
```

Replacement FortiGate should not contact FortiManager before `execute device replace sn <devname> <serial_number>` is run. *If it does, you must delete the unregistered device entry prior to rerunning the command !*

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>
```

FORTINET Training Institute

 11

Note that the replacement FortiGate should not contact FortiManager before the `execute device replace sn <devname> <serial_number>` 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 you execute the `replace` command, 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 **System Information** widget on 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.

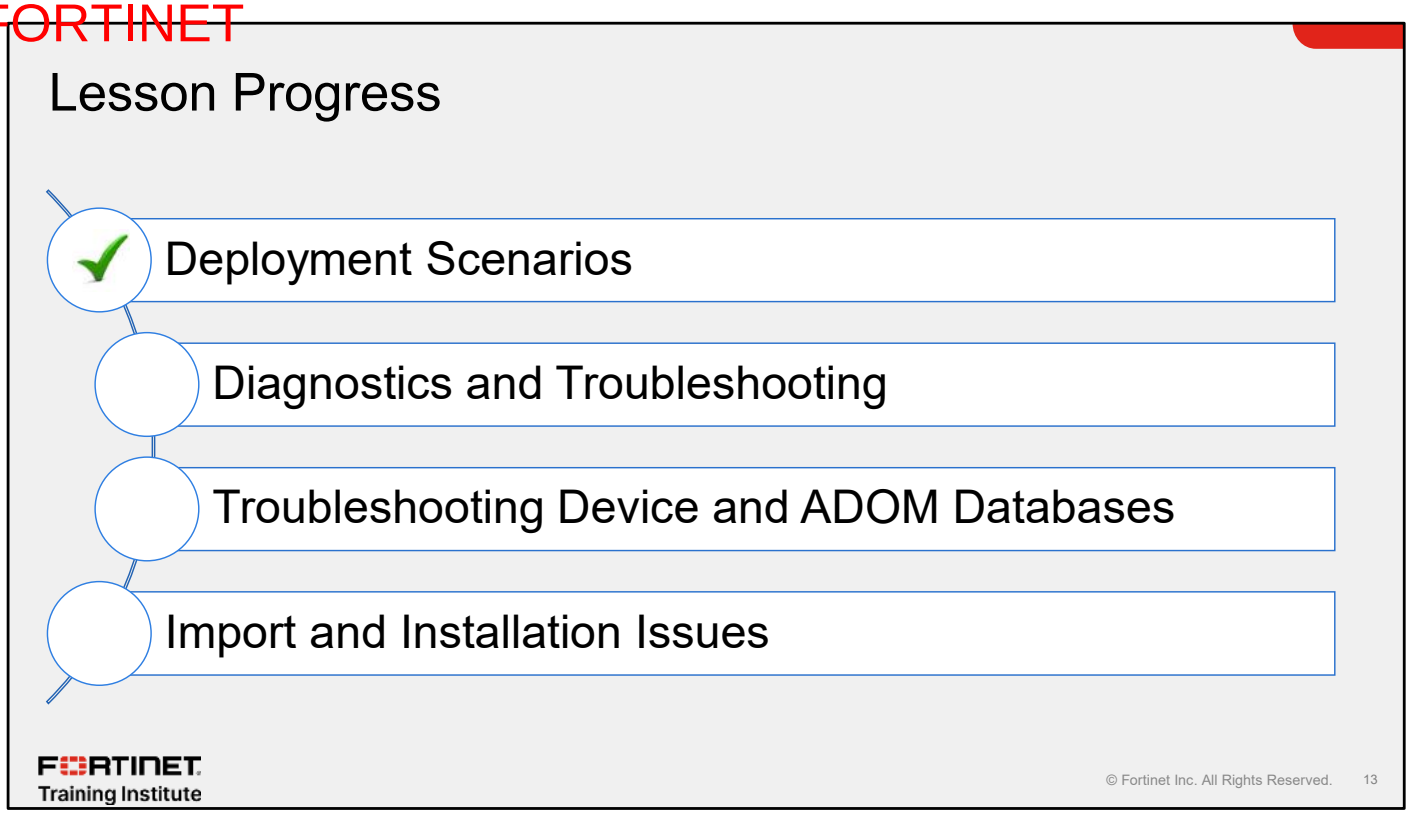
Knowledge Check

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.

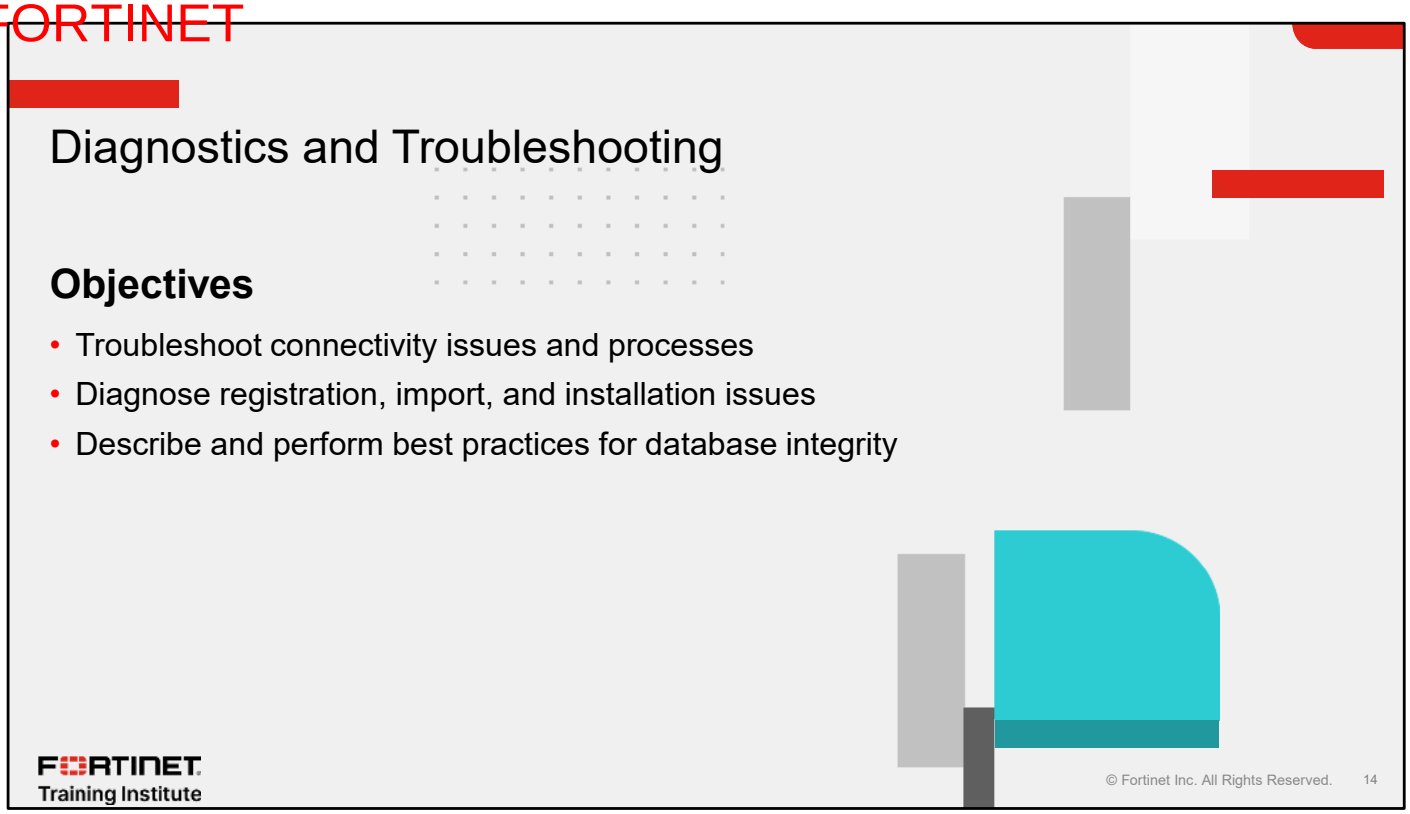
FORTINET Training Institute

 12



Good job! You now understand deployment scenarios.

Now, you will learn how to use some diagnostic commands to troubleshoot issues with FortiManager connectivity and performance.



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.

Basic Troubleshooting 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
`# diagnose debug crashlog read`	Crash logs
`# diagnose sniffer packet <interface> <filter> <verbose> <count> <timestamp>`	Packet sniffer
`# diagnose fgfm session-list` `# diagnose dvm device list`	Confirming FGFM tunnel is up
`# diagnose system print df` `# diagnose system print partitions`	Disk partition layout and status
`# diagnose debug klog read`	Lists all kernel logs. Useful to identify if FortiManager is running out of memory.

FORTINET Training Institute

 15

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.

System Resources Usage

- `get system performance` displays information about system resources, such as CPU, memory, hard disk, and flash disk usage

```
FortiManager # 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

 16

The `get system performance` command provides summarized information about system resource usage. The output includes the following resource types:

- `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` row 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.

High CPU and Memory Troubleshooting

- The `execute top` command displays real-time system monitoring
  - Type `h` or `Shift+?` to display the help

```
FortiManager # execute top
top - 13:08:23 up 1 day,  1:01,  0 users,  load average: 2.40, 3.19, 3.34

Tasks: 188 total,   2 running, 186 sleeping,   0 stopped,   0 zombie

%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

MiB Mem : 2010.164 total,   41.250 free,  974.086 used,  994.828 buff/cache

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
 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]
...
```

1 2 3 4 5 6

Process IDs

CPU and RAM

FORTINET Training Institute

 17

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, 5 minutes and 15 minutes)
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: physical and virtual memory usage, respectively
Row 6: details for each process, including the process ID, user, priority, nice value, virtual memory used, percent of memory (RAM) used, percent of CPU used, 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.

This is an interactive command, and you can change the format used in its output. For example, you can change the sorting order, or change the number of tasks displayed. This command includes a help page you can access by pressing `h` or `Shift+?`.

High Disk Usage Troubleshooting

- `execute iotop` displays the processes that are responsible for high I/O usage
- By default, processes are sorted by highest percentage under the `IO>` column
  - Press < or > to change the sort by column

```
FortiManager # execute iotop

Total DISK READ :       0.00 B/s | Total DISK WRITE :       3.83 K/s
Actual DISK READ:       0.00 B/s | Actual DISK WRITE:      24.50 K/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]
...
```

Sorted by I/O % by default

FORTINET Training Institute

 18

You can use the `execute iotop` command to identify the specific processes that may be causing high disk I/O read/writes.

By default, processes are sorted by the highest percentage under the `IO>` column, but you can change which column is used to sort them. Press < to move the sorting column to the column on the left of the current one, and press > to move the sorting column to the right of the current one. The current sorting column is indicated by the > sign.

FortiManager File System

- `diagnose system print df` displays information of mounted file systems
  - Add `-h` for human readable output
- Useful for troubleshooting incorrect disk partitioning and insufficient disk size issues

```
FortiManager # diagnose system print df -h
Filesystem                Size      Used  Available  Use%  Mounted on
rootfs                    1.9G   938.0M    1000.5M   48%  /
none                      1.9G         0       1.9G    0%  /dev
none                      3.2G    16.0K       3.2G    0%  /dev/shm
none                     64.0M    44.0K      64.0M    0%  /tmp
/dev/vda1               983.9M   294.9M     689.0M   30%  /data
/dev/mdvg/mdlv           49.0G    22.9G      26.0G   47%  /var
/dev/mdvg/mdlv           49.0G    22.9G      26.0G   47%  /drive0
/dev/mdvg/mdlv           49.0G    22.9G      26.0G   47%  /Storage
/dev/loop0                8.7M    97.0K       8.1M    1%  /var/dm/tcl-root
```

FORTINET Training Institute

 19

The `diagnose system print df` command displays the file system information on FortiManager. It shows the file systems currently mounted, as well as their sizes, usage, available space, usage in percentage, and mount point.

This command can be useful when troubleshooting issues related to disk space utilization.

Some of the common file systems used by FortiManager include:

- `/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.

Processes Status

- A stuck task blocks other tasks from running
- On an idle system, there should not be any
- Find slow tasks with the command:

```
# 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
```

```
# diagnose dvm proc list
...
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 February 19 14:45:12 2025
```

- Cancel or delete stuck or pending tasks from the task monitor
- When you cannot cancel or delete stuck tasks from the GUI, run these CLI commands:

```
# diagnose dvm task repair
```

```
# diagnose dvm task reset
```

FORTINET Training Institute

 20

On FortiManager, a stuck task blocks other tasks from running. On an idle system, there should not be any stuck task.

If FortiManager is taking longer than expected to complete a task, you can use the `diagnose dvm proc list` command to identify any process or task that is stuck. A stuck task may prevent subsequent tasks from being processed.

You can cancel or delete a pending or stuck task from the task monitor. If you cannot cancel or delete the stuck or pending tasks from the GUI, you can run the following CLI commands to repair or delete:

- `diagnose dvm task repair` keeps existing data, where possible, while repairing the task database.
- `diagnose dvm task reset` removes the logs from the FortiManager task database. All existing tasks and task history are erased.

Note that when you use either of these CLI commands, FortiManager restarts after fixing the task database.

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: registration, deletion, 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 and install processes, including CLI scripts run directly on devices, retrievals, 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`

```
FortiManager # 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
Application
        ddmd debug filter:              disable
        depmanager debug level:         255
        fgfmsd debug filter:            HQ-NGFW-1
        fgfmsd debug level:             255
        oftpd debug filter:             disable
```

FORTINET Training Institute

 21

You can use the debug commands shown on this slide to troubleshoot issues between FortiManager and FortiGate. These issues could be related to actions such as adding, deleting, refreshing, auto-updating, and installing.

Running a debug command shows the output from all other enabled debugs if they are not disabled or reset. As a general best practice, and before you run any debug commands, you should always check if any other debugs are enabled. Always reset the debug level setting before enabling any new debugs.

Example—Debug Adding a Device

```
FortiManager # diagnose debug application depmanager 255
FortiManager # diagnose debug enable
FortiManager # Request:
{ "client": "dvm\/cmd:dvm\/cmd\/discover\/device ...:5907", "id": 2, "method": "
exec", "params": [{ "data": { "host": "100.65.1.111", "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

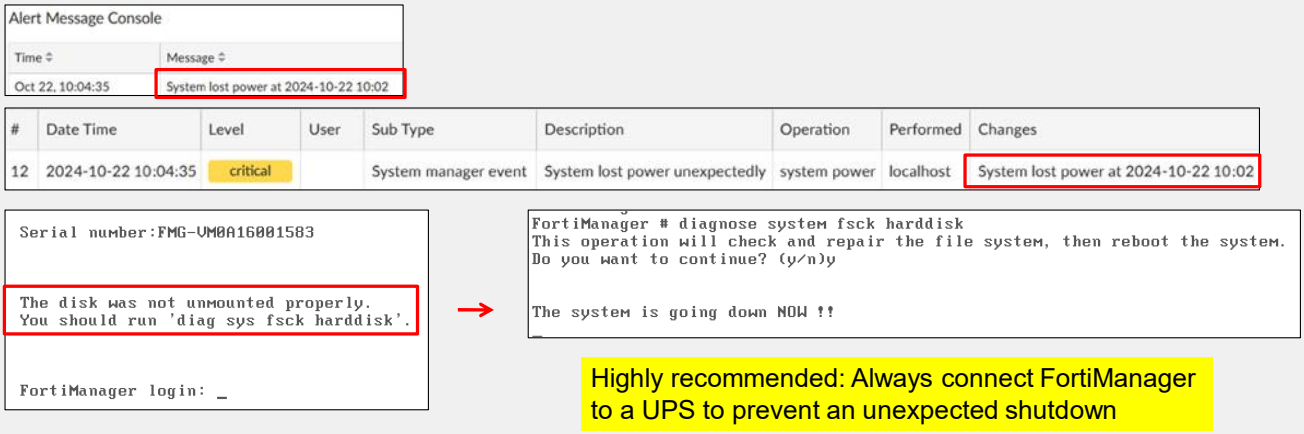
 22

The example on this slide shows a partial output of the `diagnose debug application depmanager 255` command. This command allows you to obtain the real-time status of the FortiGate device being added.

Note that the output of this command is verbose and includes the output from all managed devices.

Check File System Integrity After Power Failure

- An abnormal shutdown can cause corruption to the file system and database
  - Check the **Alert Message Console** widget and **Event Logs** for related messages
  - Shows message on console connection during boot up
    - You should back up FortiManager before repairing the file system



Highly recommended: Always connect FortiManager to a UPS to prevent an unexpected shutdown

FORTINET Training Institute

 23

An ungraceful shutdown on FortiManager can cause corruption to the file system and the internal databases. This applies to both hardware and virtual machines.

If FortiManager loses power, a message on the console connection advises you to repair the file system. Information about this and other unexpected events is also found in the **Alert Message Console** widget and **Event Logs**.

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 shutdown.

Best Practices—Database Integrity

- Always perform a graceful shutdown using the GUI or the `execute shutdown` command
  - A hard shutdown (power off) can damage the internal database
- Always follow the proper upgrade path
- Enable ADOM locking to avoid configuration conflicts
- Before performing a firmware upgrade, make sure all administrators are logged off, and perform database integrity checks
  - If you upgrade an inconsistent database, it might end up in a worse condition

If you cannot resolve a data integrity problem, you can factory reset FortiManager and restore its configuration from a good backup!

FORTINET Training Institute

 24

To ensure database integrity on FortiManager, you should follow these best practices:

- Always gracefully shut down FortiManager. Using a hard 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.

Database Integrity

- Before executing database integrity commands, you should:
  - Back up the FortiManager database,
  - Have all the administrators log off
  - Have all the ADOMs unlocked
- Integrity checks modify the FortiManager database if errors are found
- Configure scheduled backups of FortiManager, which:
  - Create new entries in **Event Logs** and the **Alert Message Console** widget
  - Automatically executes database integrity commands
    - Does not automatically make corrections
    - Must be run again to correct the problems

Device database

```
diagnose dvm check-integrity
```

```
diagnose cdb check adom-integrity
diagnose cdb check adom-revision
diagnose cdb check policy-packages
diagnose cdb check update-devinfo
```

Configuration database

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

 25

If you are experiencing unusual behavior on FortiManager, check for issues with the databases integrity.

Database integrity commands modify any database errors that are found. It is recommended that you perform a backup before executing database integrity commands. Additionally, it is recommended to have all the administrators log out and all the ADOMs unlocked, if workspace 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 scheduled backup and creates logs. If there are any issues with database integrity, you must rerun the commands to fix the problem since scheduled backups do not make the necessary corrections.

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`	Upgrade existing ADOMs to the same ADOM version in order to clean up and correct the ADOM syntax
`# diagnose cdb check policy-packages`	Verify and check dynamic mappings, and remove invalid dynamic mappings

FORTINET Training Institute

Not all integrity issues are found or fixed! After running a database integrity command, run it again to confirm the fixes.

 26

This slide lists several commands that you can use to verify and maintain database integrity.

After executing a database integrity command that performs corrections to the database, you should rerun the command to verify the proper implementation of those corrections.

Example—Database Integrity

```
FortiManager # 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 errors found in device database

Checking My_ADOM integrity and found no errors

```
FortiManager # diagnose cdb check adom-integrity My_ADOM
        General updating - adom My_ADOM                    ... ..100%    No errors
```

If any issues are found, the system recommends you perform a backup before applying any fixes to the affected database

FORTINET Training Institute

 27

In the example on this slide, FortiManager does not find any integrity errors in the device manager databases or the My_ADOM ADOM database.

If any errors are found, the system displays a message recommending you to perform a backup before applying any changes to the database.

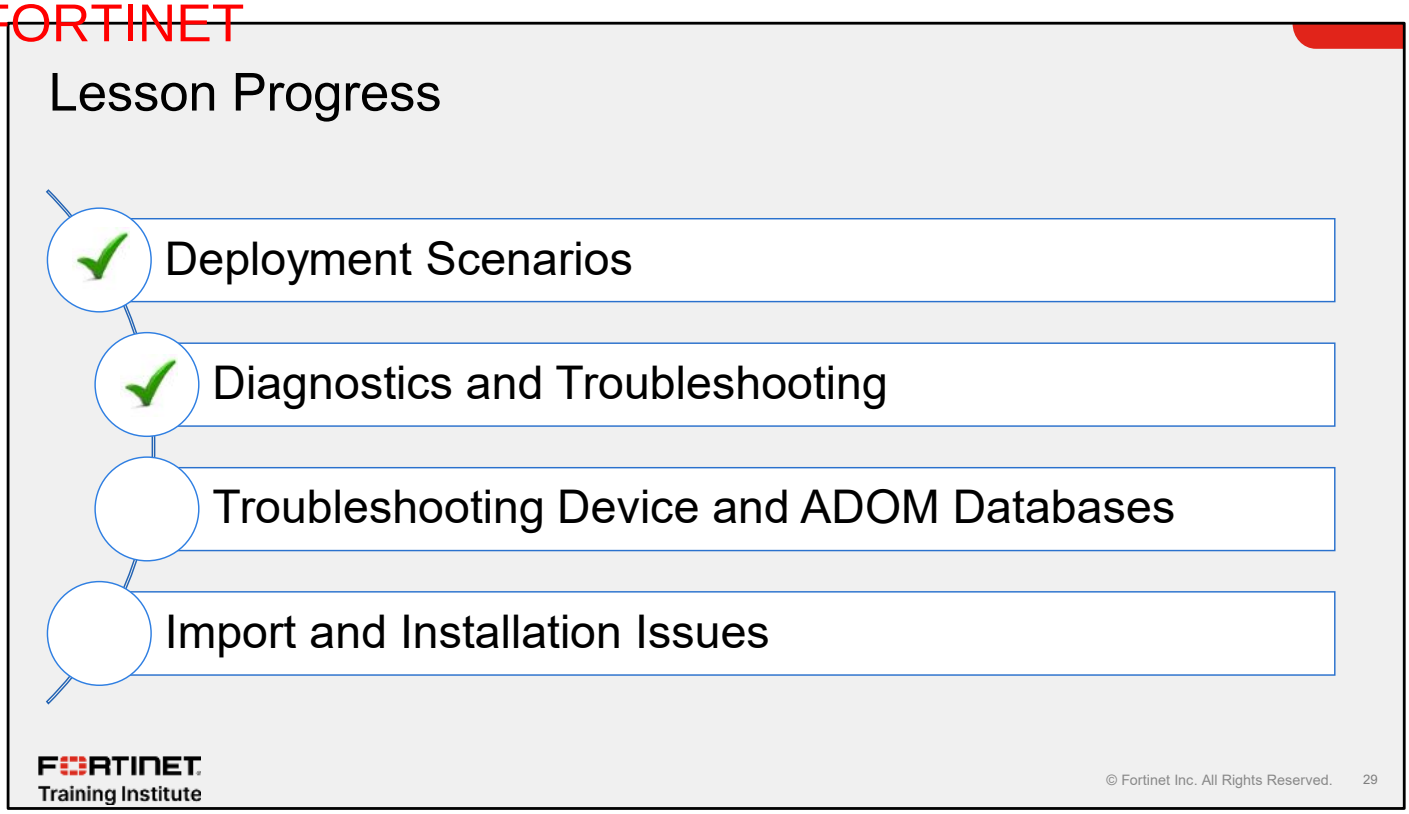
Knowledge Check

1. Which command can you use to check and repair the filesystem in FortiManager?
   - A. `diagnose dvm check-integrity`
   - ✓ B. `diagnose sys fsck harddisk`

2. Which statement about FortiManager best practices is true?
   - ✓ A. When you need to turn off FortiManager, always perform a graceful shutdown using the `execute shutdown` command.
   - B. When you need to turn off FortiManager, always make a backup of the device database.

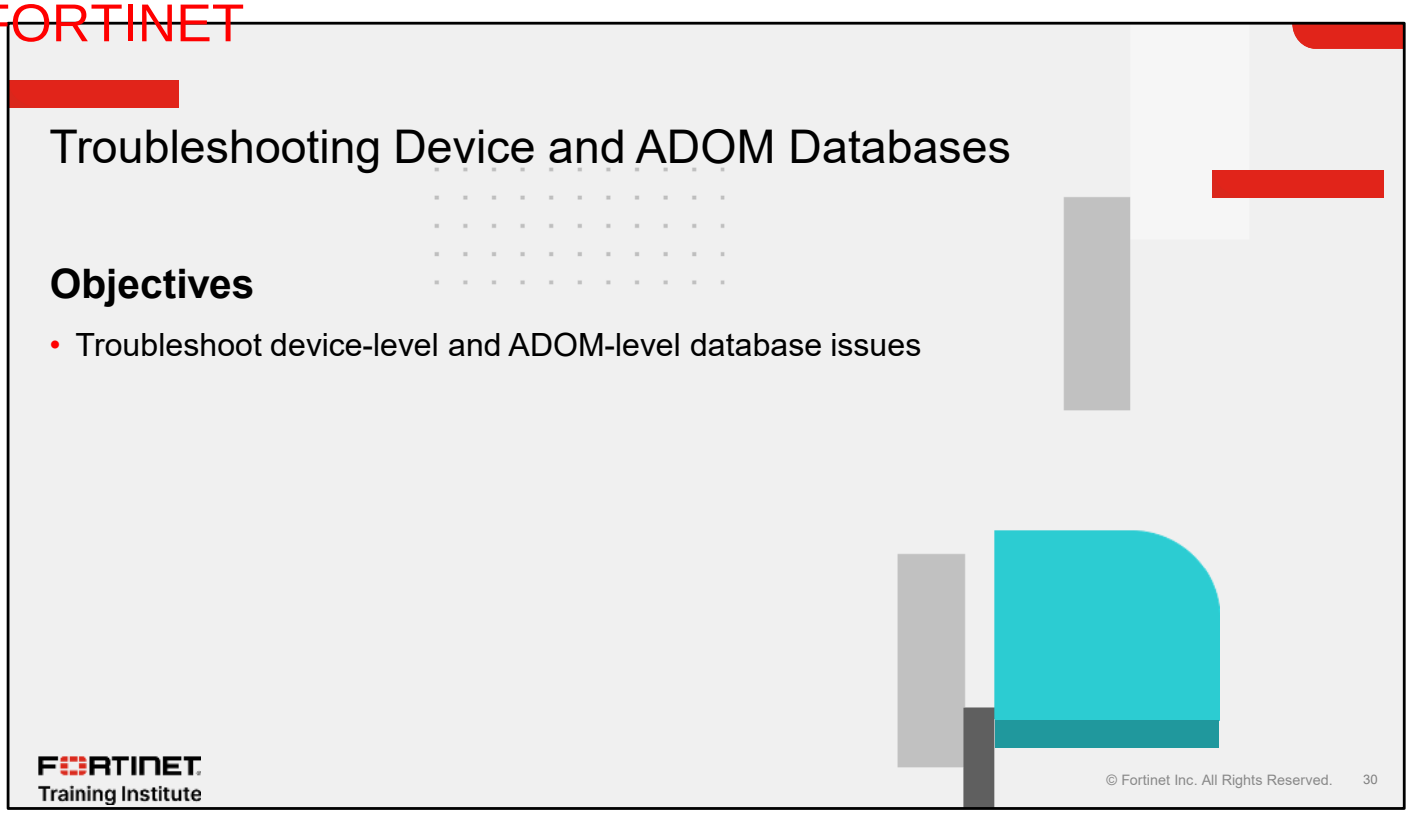
FORTINET Training Institute

 28



Good job! You now understand how to diagnose and troubleshoot various issues with FortiManager.

Now, you will learn about troubleshooting device and ADOM databases.

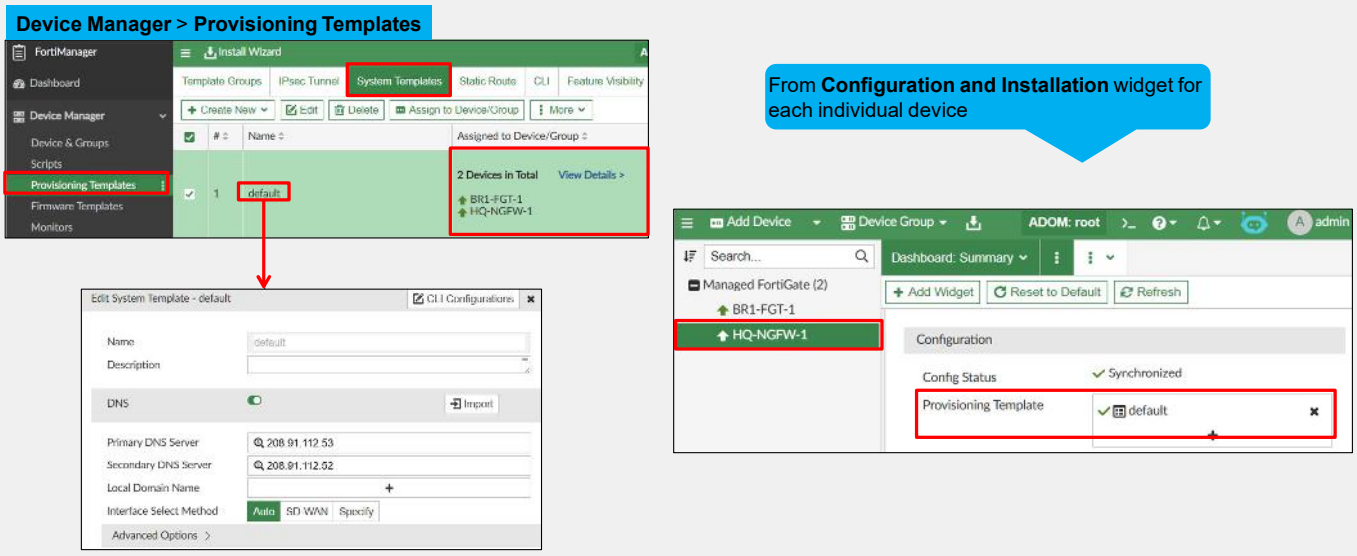


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding how to use CLI commands related to device-level and ADOM-level databases, you will be able to troubleshoot device-level and ADOM-level issues.

Provisioning Templates

- Multiple ways to verify which template is assigned to which managed device



FORTINET Training Institute

 31

You can verify which templates are applied to which FortiGate device from the **Provisioning Templates** pane, or from the individual device **Configuration and Installation** widget.

In the example on this slide, the default system template is applied to HQ-NGFW-1 and BR1-FGT-1 for DNS settings.

View FortiGate Full Configuration on FortiManager

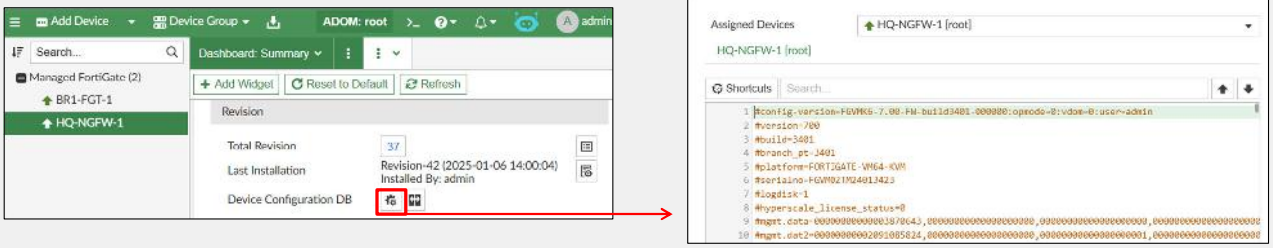
- Use the `execute fmpolicy print-device-database` command to export the entire device configuration to a file
  - File can be uploaded using the `execute fmpolicy upload-print-log` command to an FTP, SFTP, or SCP server
  - You can display the information on screen, but the output is extremely verbose (15,000+ lines)

- Example: Display HQ-NGFW-1 configuration

```
execute fmpolicy print-device-database ADOM1 HQ-NGFW-1
```

You can also use the ADOM and device IDs instead of their names

- The same information is available on the GUI



FORTINET Training Institute

 32

You can use the `execute fmpolicy print-device-database` command to export the entire device configuration to a file, which you can then upload to an FTP, SFTP, or SCP server.

Optionally, you can display the output directly on a CLI session, but the information is extremely verbose, and you will have to increase the buffer size of your terminal session considerably to make it fit.

The same information is available by clicking the **View Full Config** button in the **Configuration and Installation** widget.

Commands for ADOM Databases

Command	Information
`execute fmpolicy print-adom-database <adom> <output>`	Exports the entire ADOM database to a file You can display the information on screen but the output is extremely verbose
`execute fmpolicy print-adom-package <adom> <policy package/template name> <package name> <category name> <object name>`	Firewall policies contained in a specific policy package in the ADOM
`execute fmpolicy print-adom-object <adom> <category name>`	Individual objects in an ADOM

After exporting the entire ADOM database, you can use the `execute fmpolicy upload-print-log` command to upload the resulting file to an FTP, SFTP, or SCP server

FORTINET Training Institute

 33

You can also view the policies and objects at the ADOM level, using the commands shown on this slide.

Comparing the Device Database With the ADOM Database

- Device database information:

```
FortiManager # FortiManager # execute fmpolicy print-device-object 3 247 3 181 1
Dump object [1] of category [firewall policy] in device [HQ-NGFW-1] vdom[root]:
---------------
config firewall policy
edit "1"
set name "Internet"
set uuid 5476b1d8-8be7-51ef-d3c8-3e0539bb2ec0
set action accept
set srcintf "port4"
set dstintf "port2"
set nat enable
set srcaddr "all"
set dstaddr "all"
set schedule "none"
set service "ALL_ICMP" "FTP" "HTTP" "HTTPS"
next
```

Current device database includes FTP in the policy

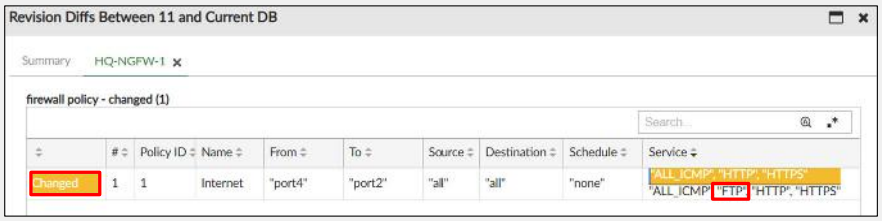
- ADOM database information

```
FortiManager # execute fmpolicy print-adom-package 3 1 5514 181 1
Dump object [1] of category [firewall policy] in adom [root] package [HQ-NGFW-1]
---------------
config firewall policy
edit "1"
set name "Internet"
set uuid 5476b1d8-8be7-51ef-d3c8-3e0539bb2ec0
set action accept
set srcintf "port4"
set dstintf "port2"
set nat enable
set srcaddr "all"
set dstaddr "all"
set schedule "none"
set service "ALL_ICMP" "HTTP" "HTTPS"
next
```

Current ADOM database doesn't include FTP in the policy

Note: In this example, **166** is the ADOM ID, and **181 1** refers to the firewall policy with ID 1

- From the GUI:



FORTINET Training Institute

 34

This slide shows an example of how you can use the CLI to compare the configuration in the device database with the configuration in the ADOM database.

On the left side, at the device level, the firewall policy named **Internet** includes FTP in the list of services allowed.

On the right side, the ADOM database does not include FTP in the list of services allowed in this policy. This discrepancy indicates that the most recent version of the policy needs to be installed on HQ-NGFW-1.

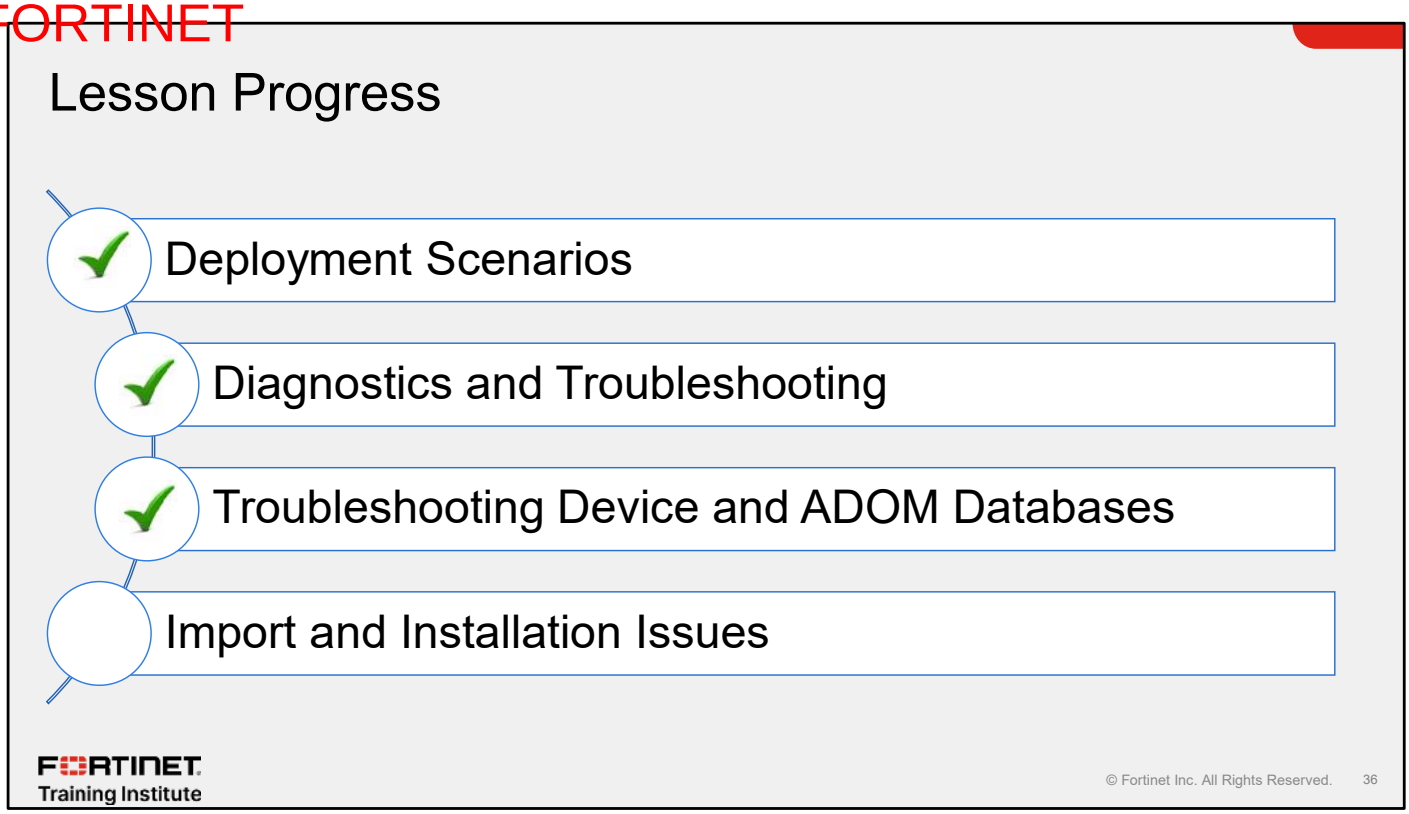
Alternatively, for the example on this slide, you can obtain the same information in the GUI by right clicking the HQ-NGFW-1 device, and then selecting the **Policy Package Diff** option. The differences between both versions of the policy can be examined in the **Policy Package Diff** window as shown in the image**.**

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. Where can you upload the resulting file after you export the entire ADOM database?
   - A. HTTP server
   - ✓B. SFTP server

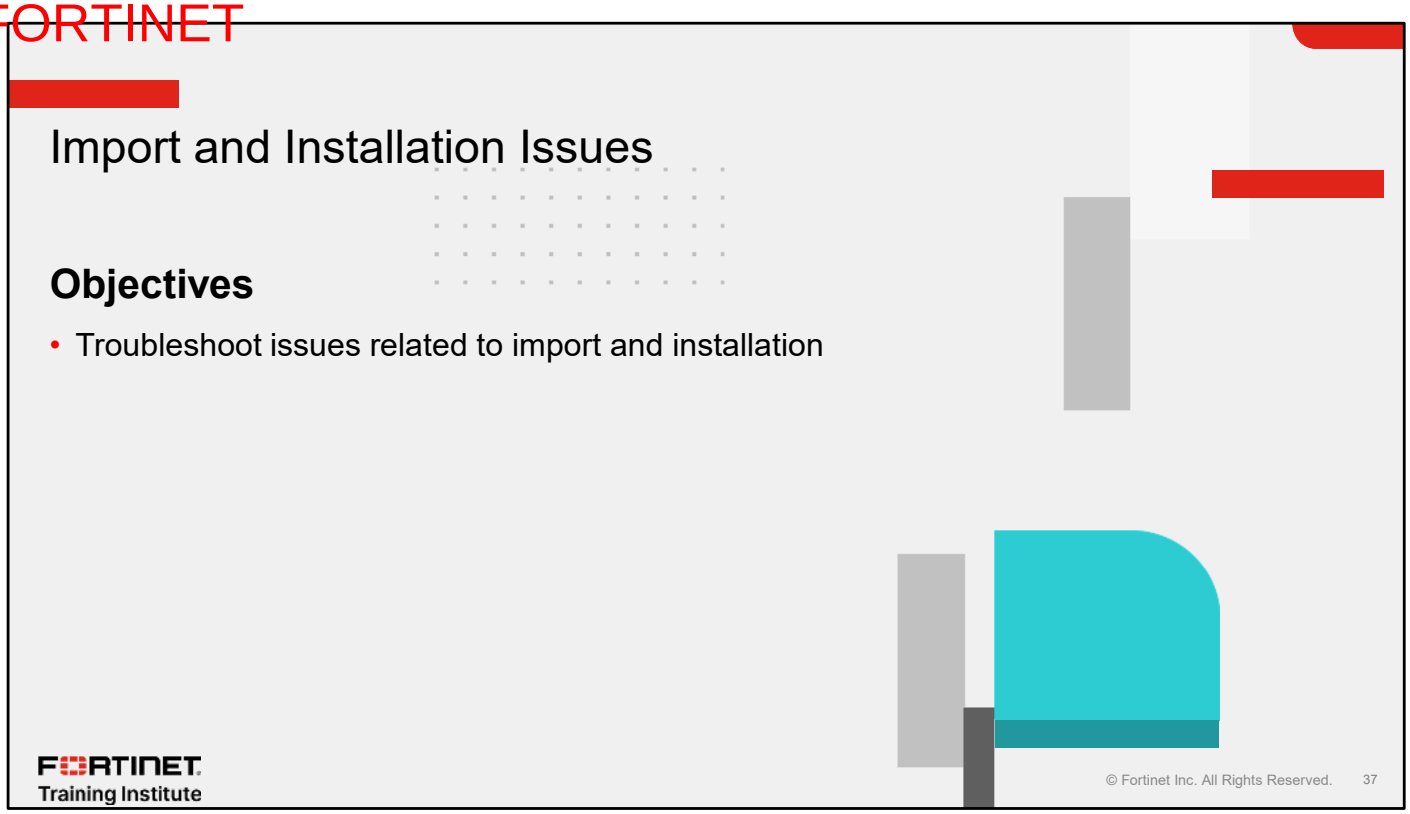
FORTINET Training Institute

 35



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.

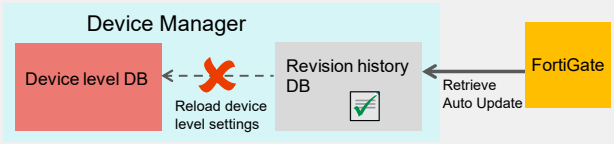


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding import and installation issues, you will be able to troubleshoot them if they occur in your network.

Failed Reload

- An operation that fails to update the device-level database from the revision history database
- Caused by inconsistent or corrupt FortiGate configuration
  - Can be due to not following proper upgrade path
- Troubleshooting reload failure




```
# diagnose test deploymanager reloadconf <devid>
```

Device ID from `diagnose dvm device list`

- Shows the stage at which the configuration is failing to update the device-level database
- If successful, the device-level database is updated with the FortiGate configuration
  - No new revision history is created

```
# diagnose test deploymanager reloadconf 183
Retrieving configuration file from FGT...
Configuration file import succeeded.
Reloading configuration file...
Configuration reload succeeded.
```

FORTINET Training Institute

 38

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.

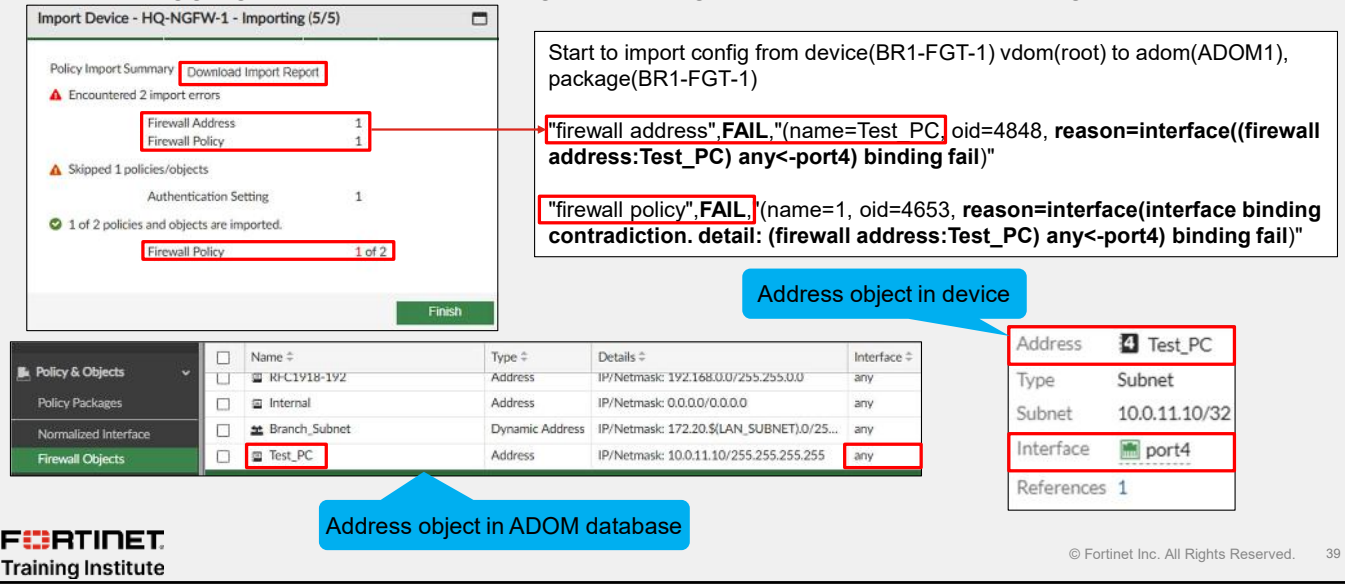
There are two possible outcomes:

- 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.

Import Issues—Understanding Failed Import

- Check the download report to find a reason for a failed import
- If local logging level is set to debug, event logs include failed import logs



When you add a FortiGate device using the **Add Device** wizard, or import policies using the **Import Configuration** wizard, always make sure that the policies and objects are successfully imported.

In the example on this slide, the FortiManager ADOM database has a firewall address object named **Test_PC** that is associated with the interface **any**. However, HQ-NGFW-1 also has a firewall address object named **Test_PC,** but that is associated with the interface **port4**. This firewall address object is referenced in a firewall policy on the HQ-NGFW-1.

When a policy package was added or imported to HQ-NGFW-1, the operation failed to import the firewall address object **Test_PC**, as well as the associated firewall policy. The partial output of the import report shown in the image provides the reason for the failed import.

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.

Examining the event logs in FortiManager can also provide details about the objects that caused the import failure issue.

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

 40

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:

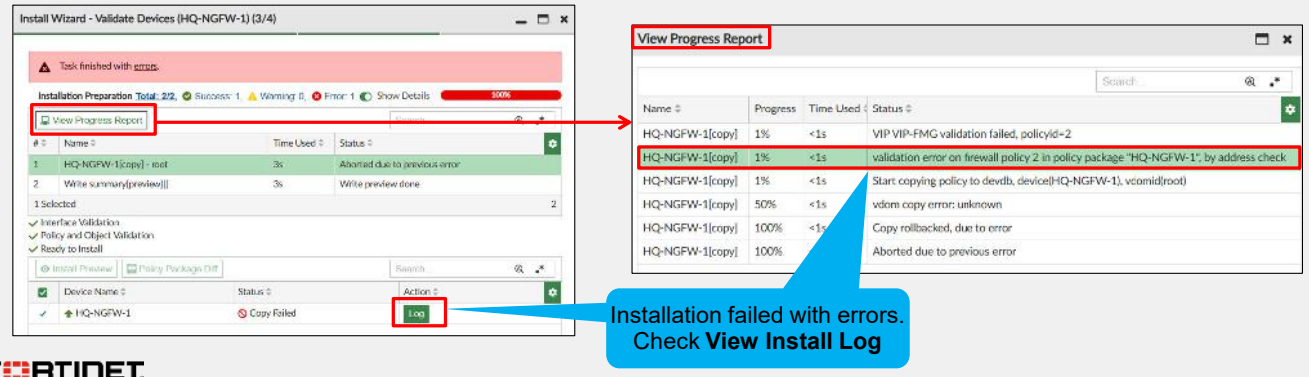
- You can remove the interface binding to make it the same as the FortiManager ADOM object.
- If there is a need to keep the interface binding for FortiGate that is having issues with a partial policy import, you can rename the address object to a unique name that is not part of the ADOM database.

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 FortiManager allows you to choose the object either from FortiManager or FortiGate if both have the same object name without **Per-device Mapping**.

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
- Can be due to missing or incorrect object dependency, or the use of invalid parameters when copying from ADOM database to device database
- When performing the installation, **View Progress Report** shows the failing message



FORTINET Training Institute

 41

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, or invalid parameters being used when copying from the ADOM database to the device database. The incorrect or missing object dependencies can be caused by corruption or inconsistencies in the FortiManager database. Invalid parameters are usually caused by human error.

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.

Always check **View Install Log** to see which CLI commands were not executed or accepted by FortiGate.

The following are among the most common reasons for installation failures:

- 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

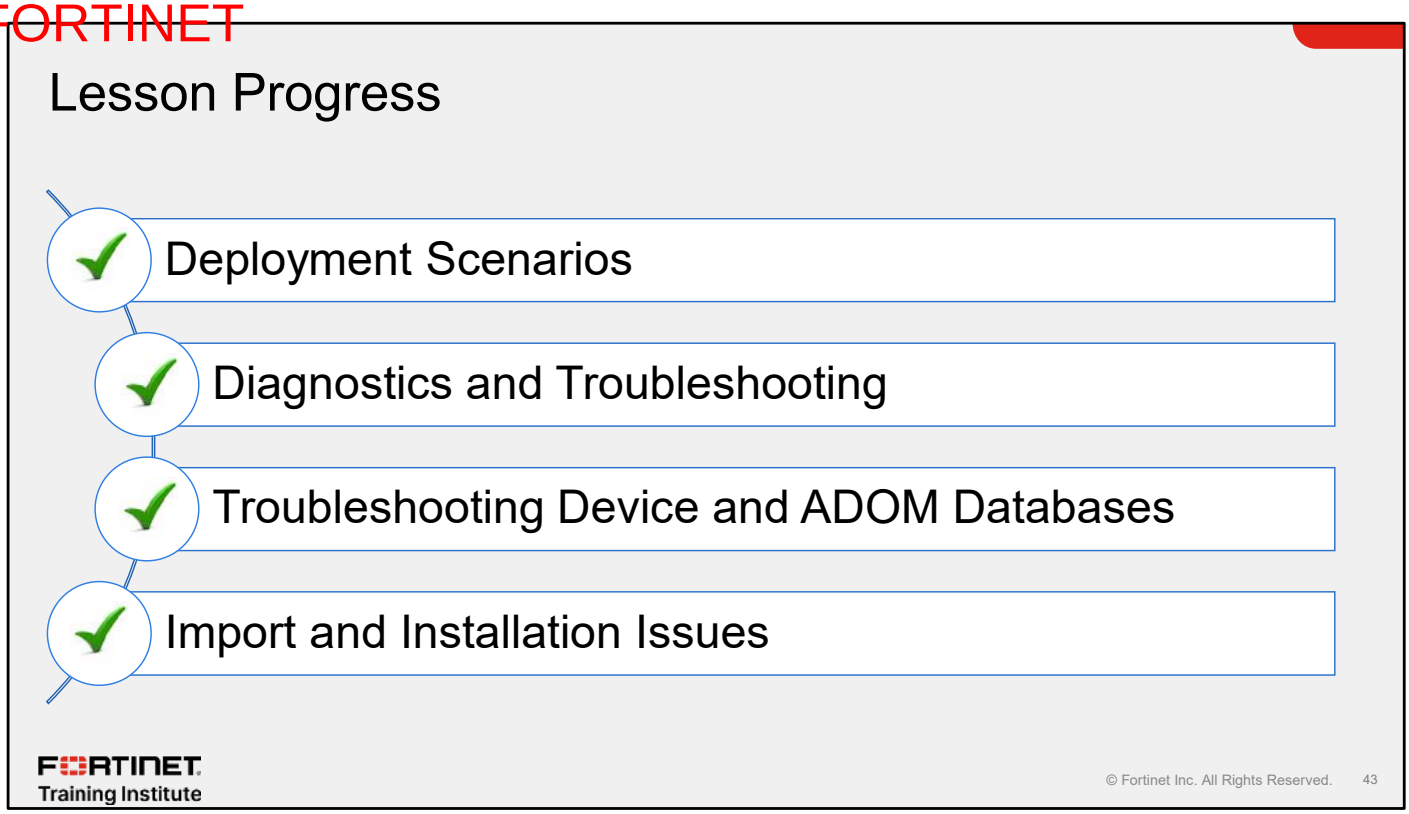
Knowledge Check

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

 42



Congratulations! You have completed this lesson.

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

Review

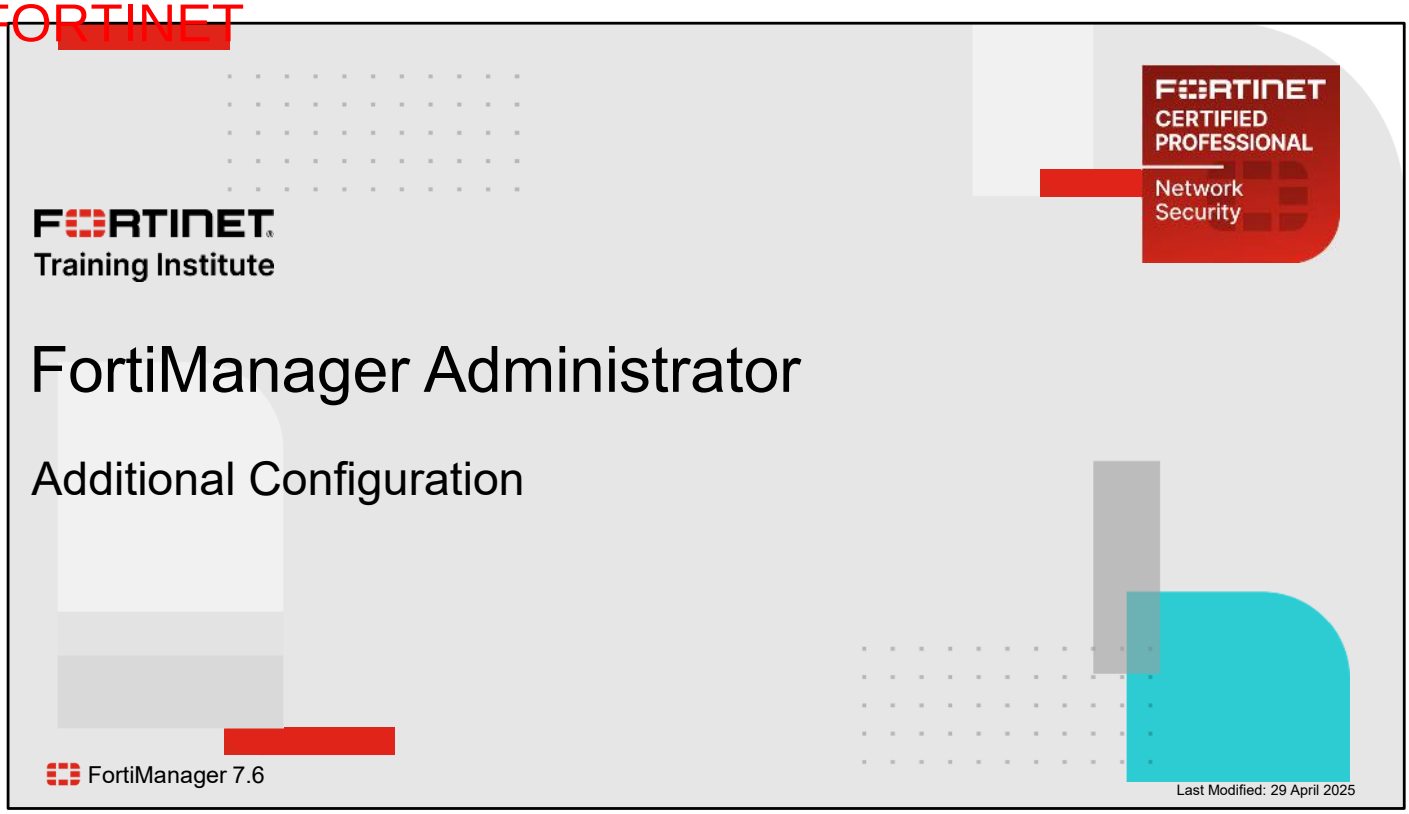
- ✓ Describe common deployment scenarios for FortiManager
- ✓ Describe the purpose of keepalive messages
- ✓ Replace a managed FortiGate
- ✓ Troubleshoot connectivity issues and processes
- ✓ Diagnose registration, import, and installation issues
- ✓ Describe and perform best practices for database integrity
- ✓ Troubleshoot device-level and ADOM-level database issues
- ✓ Troubleshoot issues related to import and installation

FORTINET Training Institute

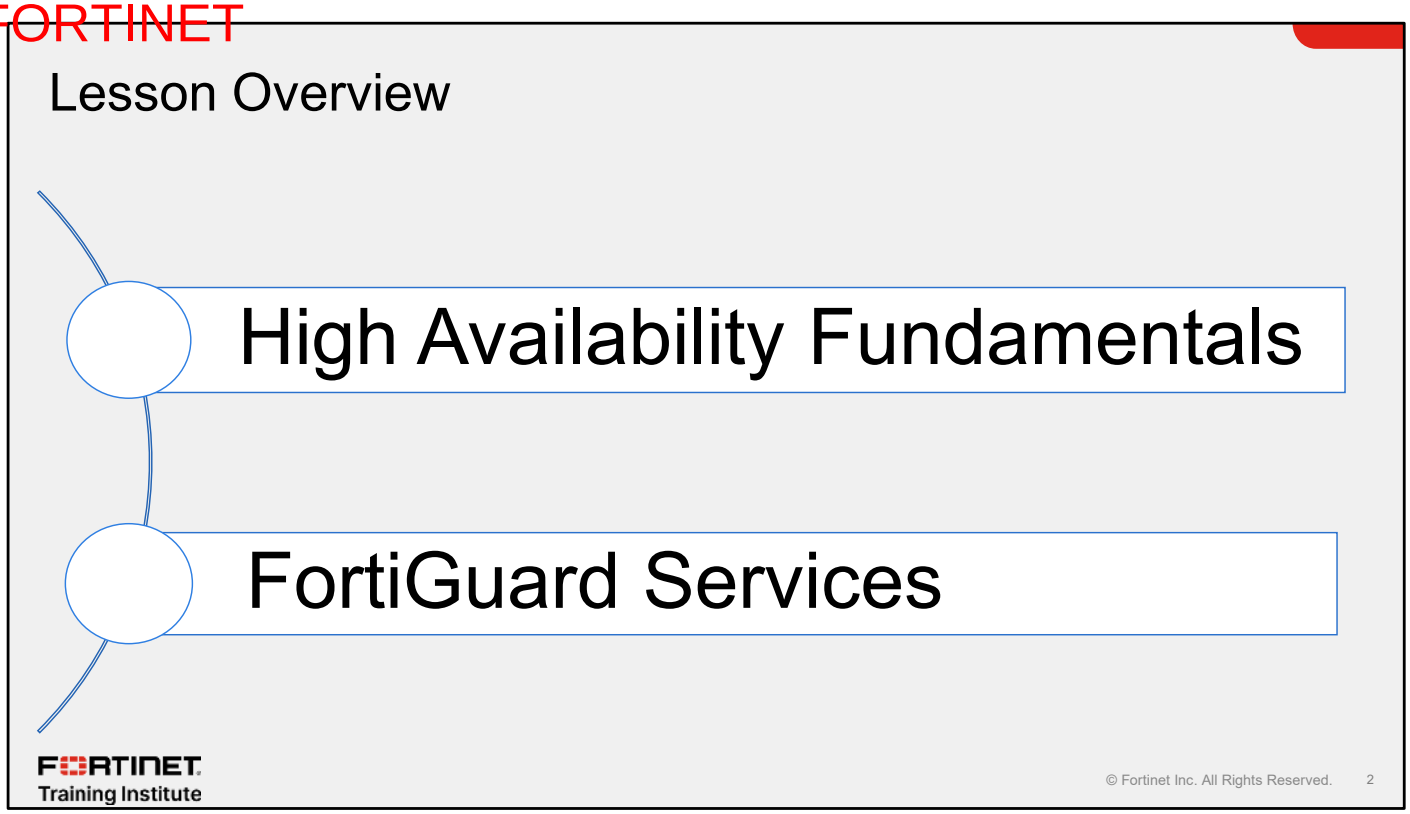
 44

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

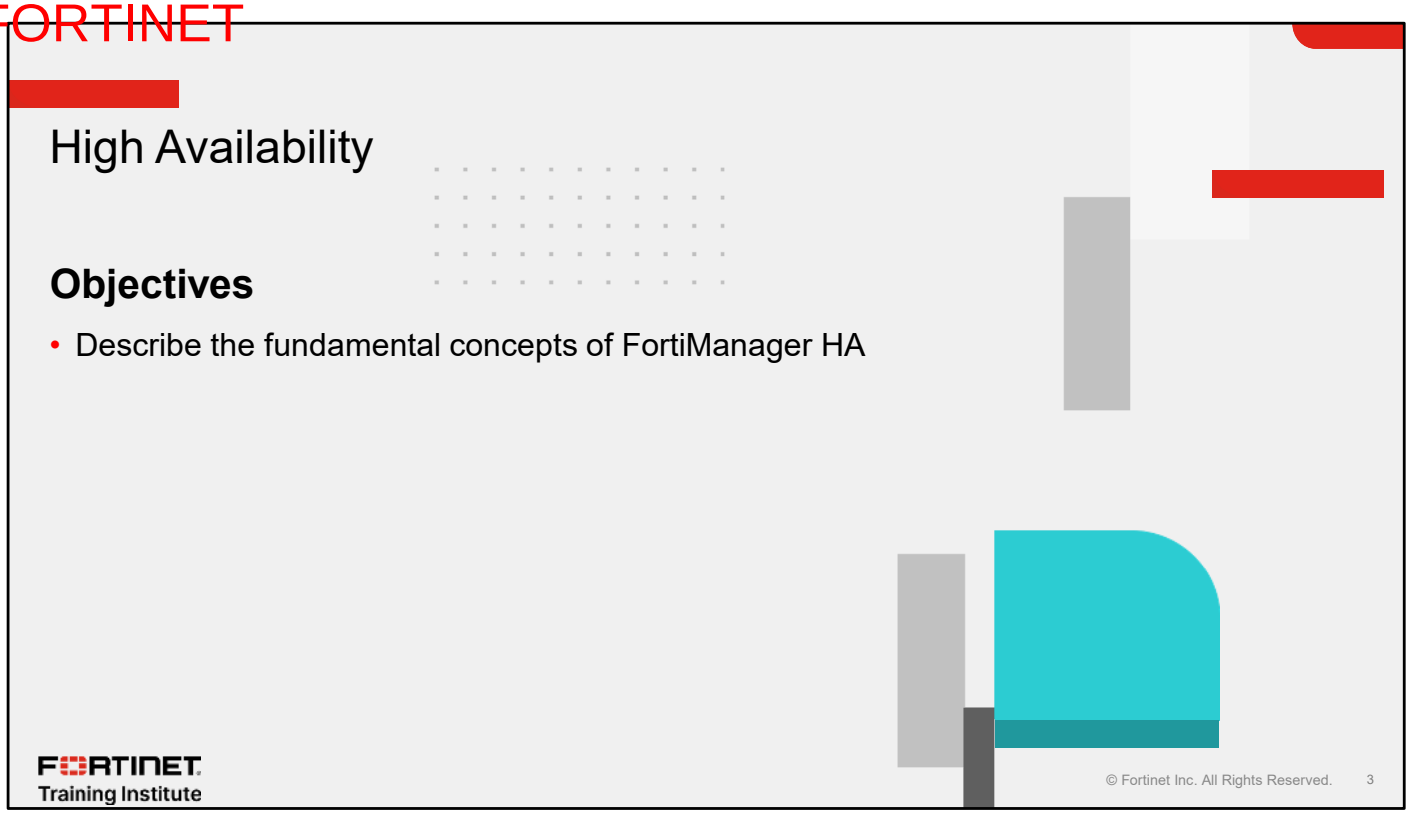
By mastering the objectives covered in this lesson, you learned how to diagnose and troubleshoot issues related to FortiManager and managed devices.



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.



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

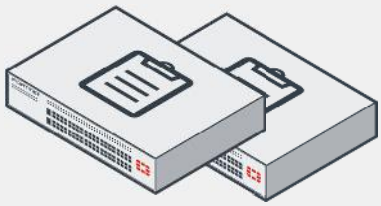


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in FortiManager HA cluster fundamentals, you will be able to explain how this FortiManager solution enhances reliability in your network.

High Availability (HA)

- A FortiManager HA cluster includes up to five devices (one primary, up to four secondary)
- All devices must be the same model and firmware
- HA heartbeat uses TCP port 5199
- Supports geographic redundancy if communication is possible
- Firmware upgrades affect all devices, causing reboots
- Schedule a maintenance window for upgrades
- GUI access may be unavailable until synchronization is complete
- SSH and telnet may be slow during upgrades, but the console can still be used



FortiManager HA cluster

FORTINET Training Institute

 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 supports geographic redundancy so the primary unit and secondary units can be in different locations attached to different networks as long as communication is possible between them (for example, on the internet, on a WAN, or in a private network).

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. Administrators may not be able to connect to the GUI until the upgrade synchronization process is completed. During the upgrade, SSH or telnet connections to the CLI may also be slow. You can still use the console to connect to the CLI of the primary device.

HA Synchronization

- Changes are made to the primary FortiManager, which are automatically synchronized with one or more secondary devices
  - Database is replicated
  - A secondary device can be promoted in case of primary device failure
- What is synchronized?
  - Global database
  - All device configurations
  - All configuration revisions
- What is **not** synchronized?
  - Interfaces and routes
  - HA, SNMP, and log settings
  - FortiAnalyzer features (if enabled), FortiGate logs
  - Antivirus/IPS packages, web filter/antispam databases
  - Local logs and alerts

FORTINET Training Institute

 5

All changes to the FortiManager database are saved on the primary FortiManager. These changes are then 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 servers.

Failover Modes

- Manual
  - When the primary device fails, you must manually reconfigure one of the secondary devices to become the new 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
- VRRP (Automatic failover)
  - Must configure VIP, VRRP interface, priority, and monitored IP
  - 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

 6

There are two HA failover modes:
1. Manual
2. VRRP (Automatic)

In manual mode, when the primary unit fails, you must manually configure one of the secondary units to become the primary unit. The new primary unit will keep its IP address. The FortiManager IP address registered on FortiGate will be automatically changed when the new primary unit is selected.

You don't need to reboot devices that you promote from secondary to primary.

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 with the highest priority automatically becomes the primary. This mode requires the configuration of a virtual IP (VIP) for the cluster, a VRRP interface, priorities for each member, and a monitored IP.

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                 : 10.0.13.120
```

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

 7

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.

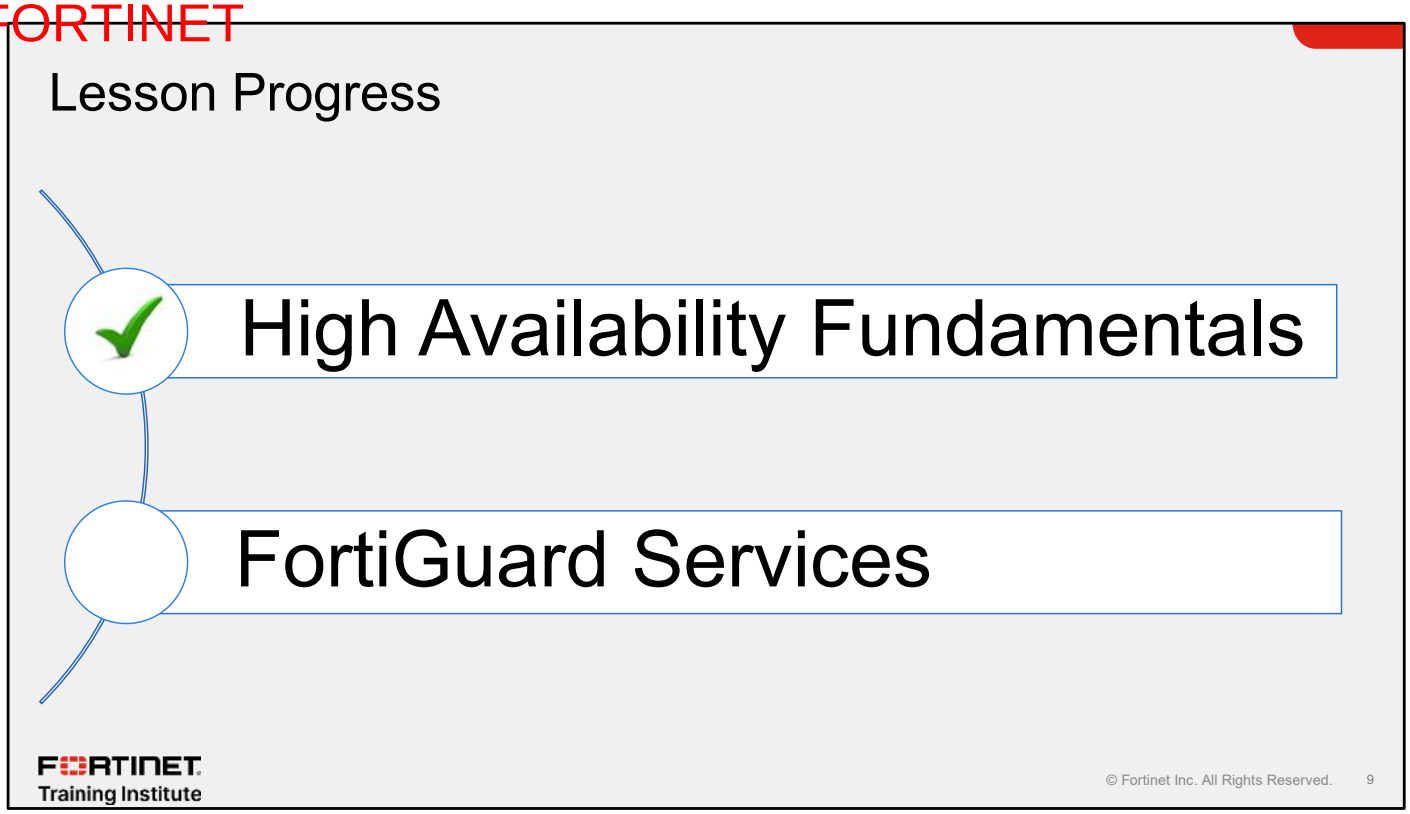
Knowledge Check

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. Cluster members can be in different locations.
   - B. A FortiManager HA cluster supports an active-active configuration.

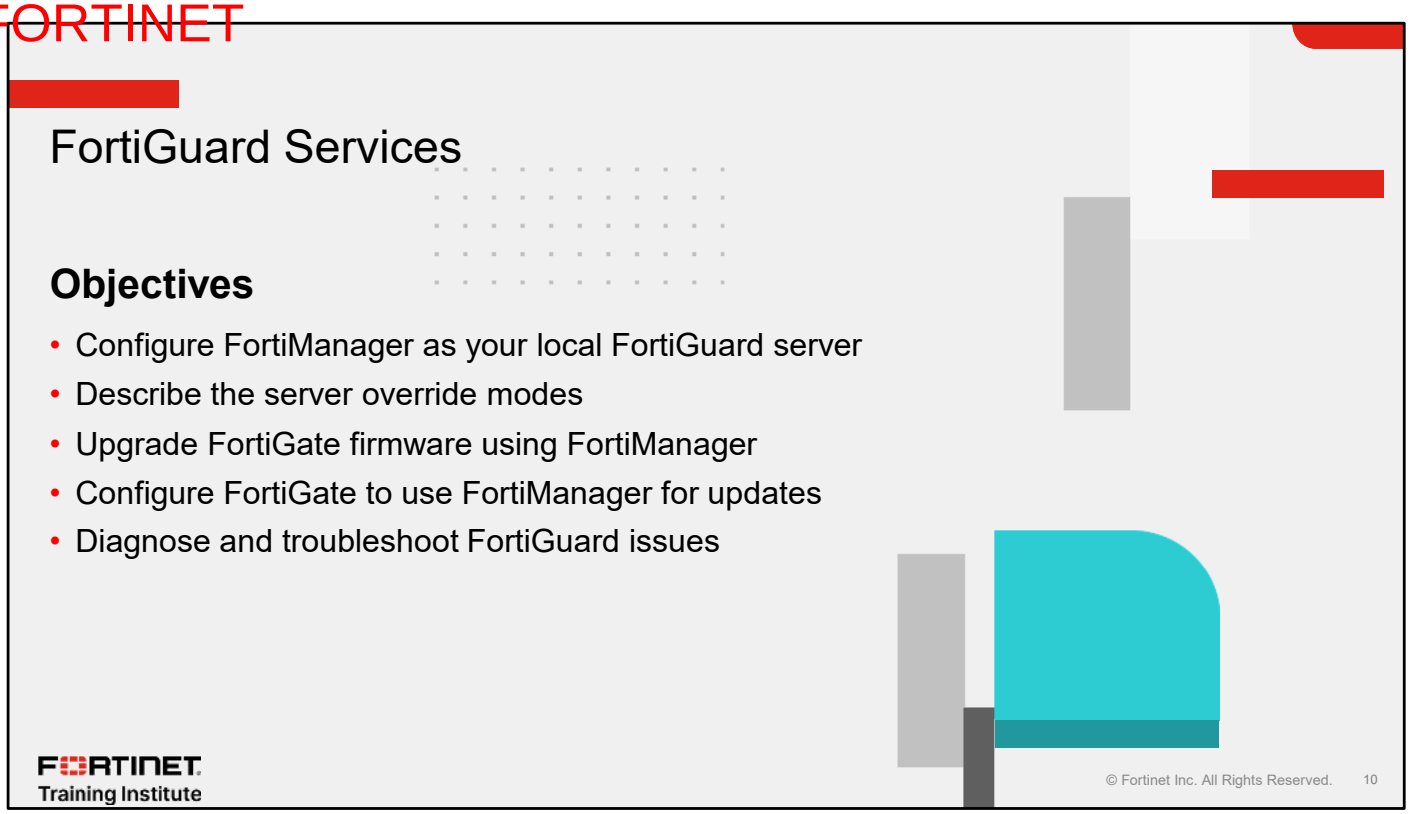
FORTINET Training Institute

 8



Good job! You now understand how to implement, configure, and troubleshoot an HA cluster.

Now, you will learn about FortiGuard services.



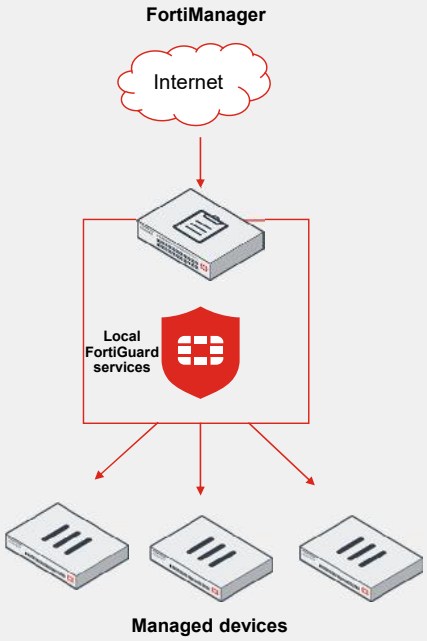
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiGuard services on FortiManager, you will be able to use your FortiManager effectively as a local FDS.

FortiManager as a Local FortiGuard

Configuring FortiManager to act as a local FortiGuard server allows you to:

- Download all antivirus and IPS packages, and web filter and email filter databases on FortiManager
- Reduce internet connection load
- Provide devices a faster connection to updates
- Redistribute the packages to many devices
  - In some high-security environments, internet access internal FortiGate devices is restricted



FORTINET Training Institute

 11

A FortiManager device that is acting as a local FortiGuard, synchronizes the FortiGuard updates and packages with the public FortiGuard Distribution Network (FDN), and then provides the updates to the supported devices in your network. The local FortiGuard reduces the internet connection load and provides a faster connection, which minimizes the time required to apply updates, such as IPS signatures, to many devices.

FortiManager as a Local FortiGuard Cache

- Periodically connects to FortiGuard servers (unless configured for closed network operation)
  - Downloads license statuses for managed devices
  - Syncs FortiGuard packages
- Can cache available firmware updates for managed devices
- Each FortiManager in an HA cluster acts as an individual FortiGuard server
  - Each cluster member independently downloads and provides these services to FortiGate devices
- The use of FortiGuard services on FortiManager may be resource intensive

FortiGate devices *must* have valid and active service contracts to obtain updates!

FORTINET Training Institute

 12

FortiManager can function as a local FortiGuard cache unless it is configured for closed-network operations. It continuously connects to the public FortiGuard servers to obtain managed device license information and check for firmware available updates.

In a FortiManager cluster, the FortiGuard information is not synchronized, and each cluster member individually downloads and is able to provide these services independently.

FortiManager supports requests from registered (managed) and unregistered (unmanaged) devices.

The use of FortiGuard services on FortiManager may be resource intensive and you may need to consider using a dedicated FortiManager for this task.

FortiGuard Terminology

- FortiGuard services include all updates to services that Fortinet provides to its clients:
  - Intrusion prevention service (IPS)
  - Antivirus
  - Web filter and email filter
- Historically, the terms in the table below have been used:
  - Currently, the term FortiGuard covers all services

Terminology used	Service type
Fortinet Distribution Servers (FDS)	Antivirus and IPS
FortiGuard service (FGD)	Web filter and email filter
FortiGuard Distribution Network(FDN)	Public FortiGuard Distribution Network

FORTINET Training Institute

 13

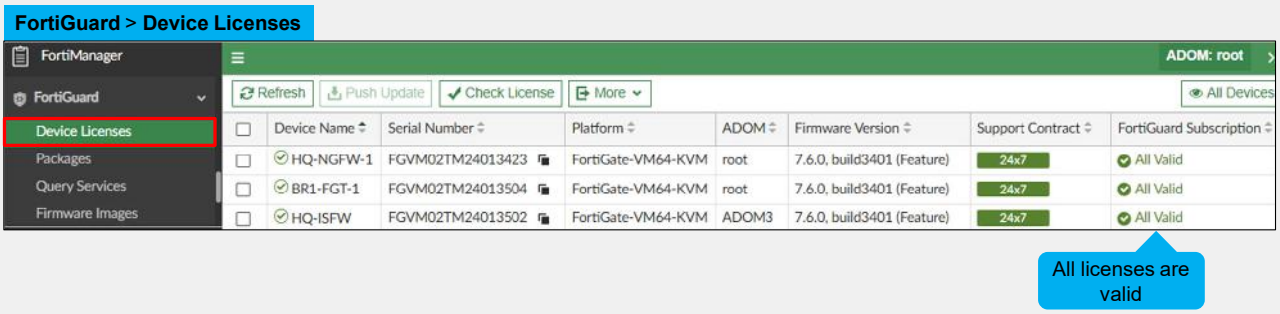
FortiGuard services represent the antivirus, IPS, web-filtering, and antispam update services that Fortinet provides to its clients.

Historically, the antivirus and IPS services have been referred to as the FortiGuard Distribution Servers (FDS), and the web filter and email filter services as the FortiGuard service.

Currently, the term FortiGuard covers all services; however, specific FortiManager GUI or CLI configuration sections continue to refer to them using the terminology shown on this slide.

FortiGuard License Status

- View license information for FortiGate devices



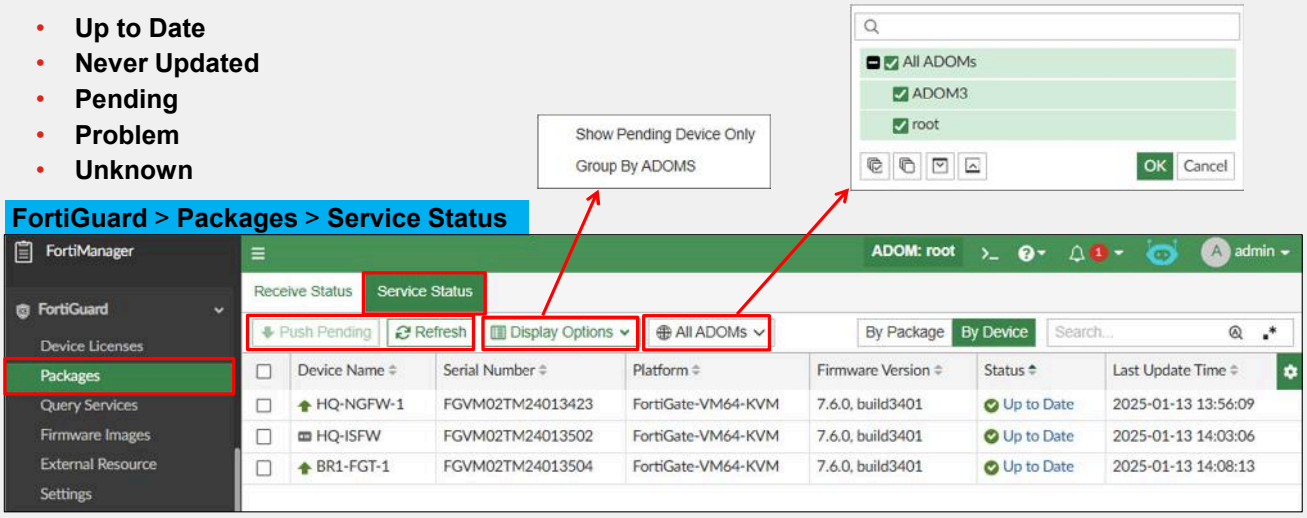
FORTINET Training Institute

 14

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.

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**



FORTINET Training Institute

 15

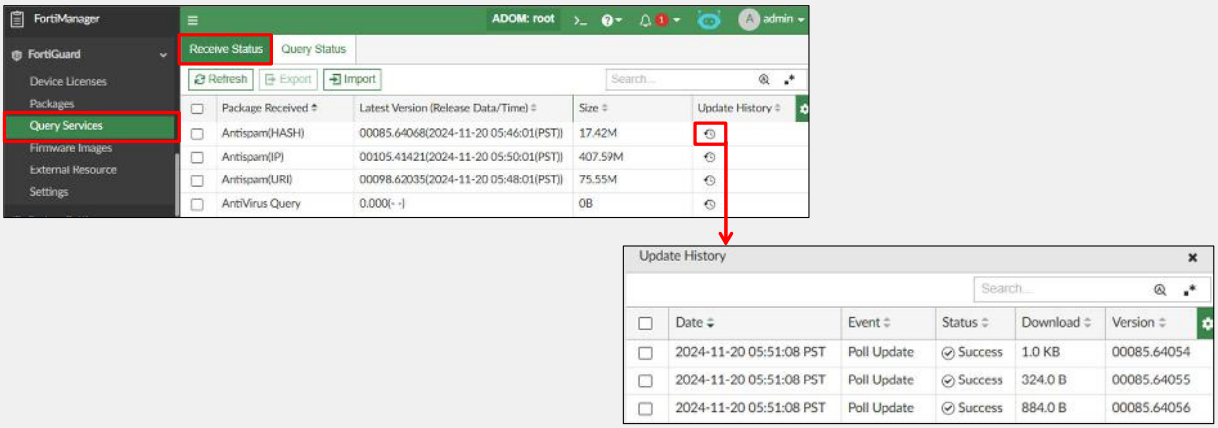
There are five main statuses for FortiGate devices configured to receive updates from the FortiManager:

- **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.

Query Server Management

- You can find information about the packages received from FortiGuard at **FortiGuard** > **Query Services** > **Receive Status**



- Under **Query Status** you can see the number of queries made from all devices to FortiManager

FORTINET Training Institute

 16

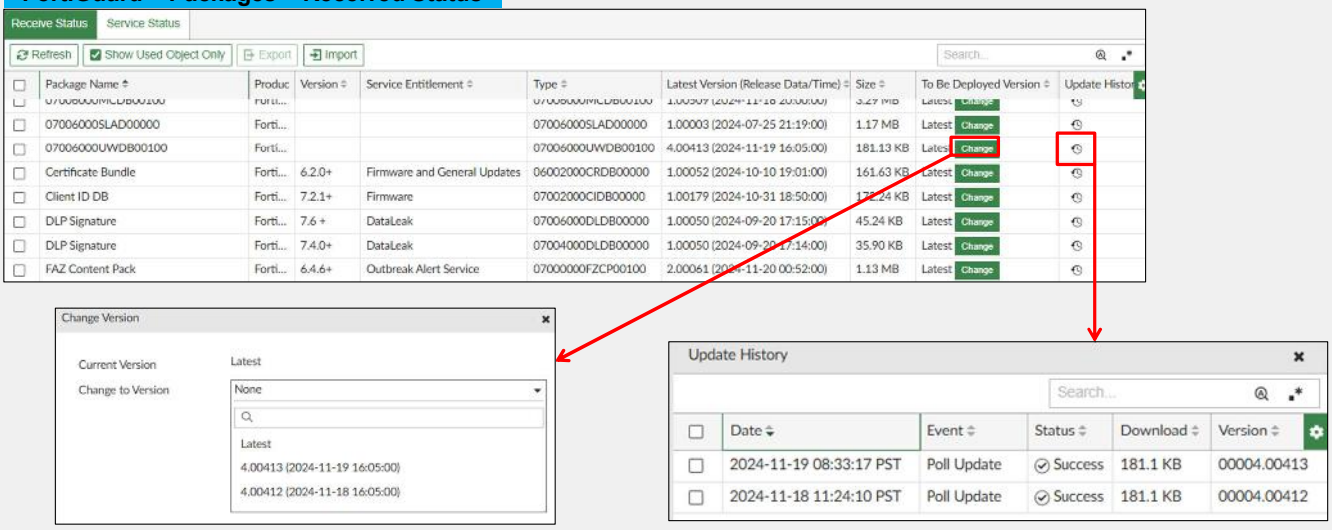
The web and antispam databases received from FortiGuard are listed under **Receive Status**. The date and time updates are received from the server, the update version, the size of the update, and the update history are also shown. You can click **Update History** to see more information about individual 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.

Package Management—Receive Status

- Shows information about a package received from FortiGuard

FortiGuard > Packages > Received Status



FORTINET Training Institute

 17

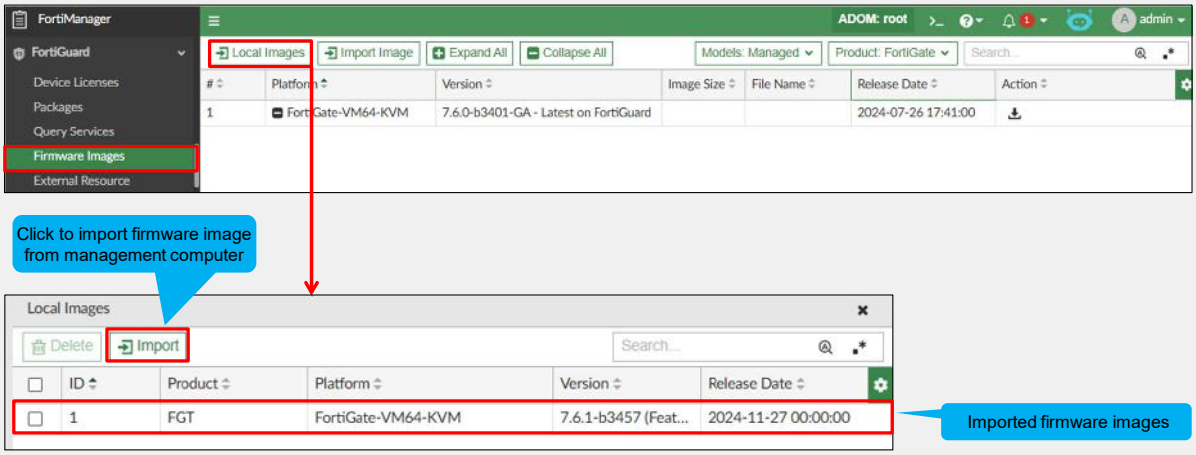
The **Receive Status** displays the package received, latest version, size, to be deployed version, and update history for the antivirus and IPS signature packages received from FortiGuard.

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.

Firmware Cache

- **FortiGuard > Firmware Images**
  - Download firmware images for managed devices
  - Import images from management computer



FORTINET Training Institute

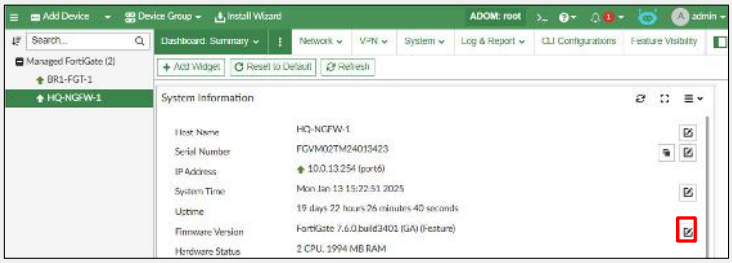
 18

FortiManager can download images from the FDN, or you can upload firmware images from your management computer that you can then use to change the device firmware using your FortiManager device.

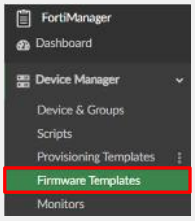
You can view the available firmware based on the supported product type, and filter for all devices or only managed devices.

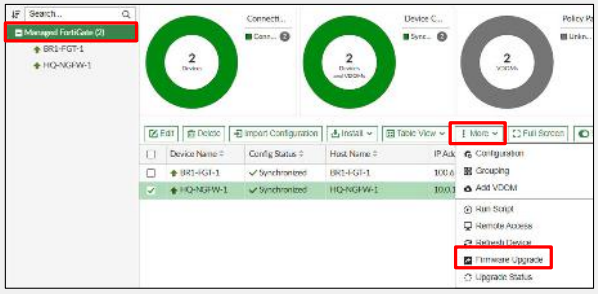
FortiGate Firmware Update From FortiManager

- You can upgrade the firmware in the following ways:
  - For individual devices
    - From the System Information widget
  - For multiple devices in an ADOM
    - From the Device Manager pane
    - You can also upgrade firmware on a group



- You can schedule firmware upgrades using Firmware Templates





FORTINET Training Institute

 19

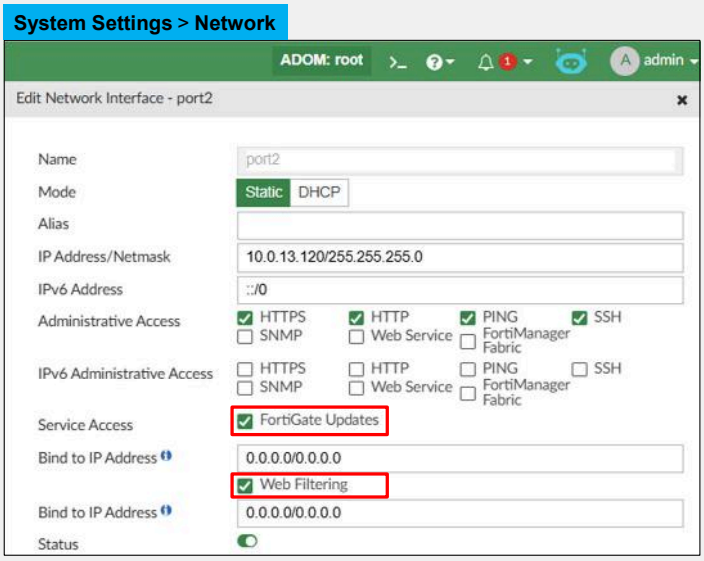
You can upgrade the FortiGate firmware in the following ways:

- 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 for later using the **Firmware Templates** option.

Enabling Built-In FDS—Step 1

- Enable service access settings for each interface used to communicate with FortiGate devices
- **Bind to IP Address** use a unique IP address in the same subnet and default setting uses the interface's IP address.



FORTINET Training Institute

 20

In order to enable the built-in FortiGuard service, you must enable the service access setting on the FortiManager interface and the FortiGuard services.

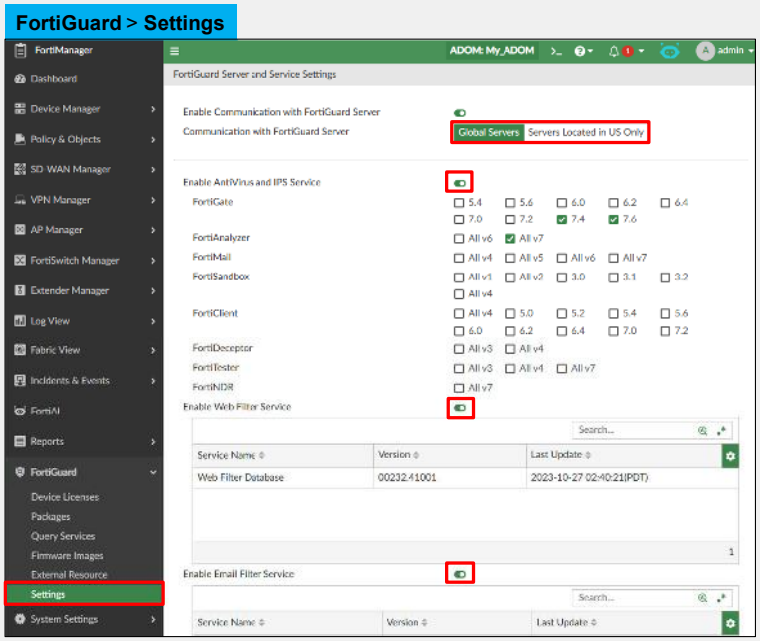
You must configure the **Service Access** settings on FortiManager per interface. This is useful when different FortiGate devices are communicating with FortiManager on different interfaces. FortiGate devices use FortiGuard services to query and obtain updates from FortiManager. The **FortiGate Updates** service is for antivirus, IPS, and license validation. The **Web Filtering** service is for web filter and antispam.

The IP address entered in **Bind to IP Address** should be a unique address within the same subnet as the interface's IP address. This IP address is used for sending update and rating requests to FortiManager over TCP port 443.

If **Bind to IP Address** is set to 0.0.0.0/0.0.0.0 (the default value), the interface's IP address will be used (10.0.13.120, as shown in the screenshot above).

Enabling Built-In FDS—Step 2

- By default, communication with public FDN is enabled on FortiManager
- Can change FortiGuard communication between **Global Servers** or **Servers Located in US Only**
- Enable the following services as needed:
  - Antivirus and IPS
  - Web filter
  - Email filter



FORTINET Training Institute

 21

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 servers.

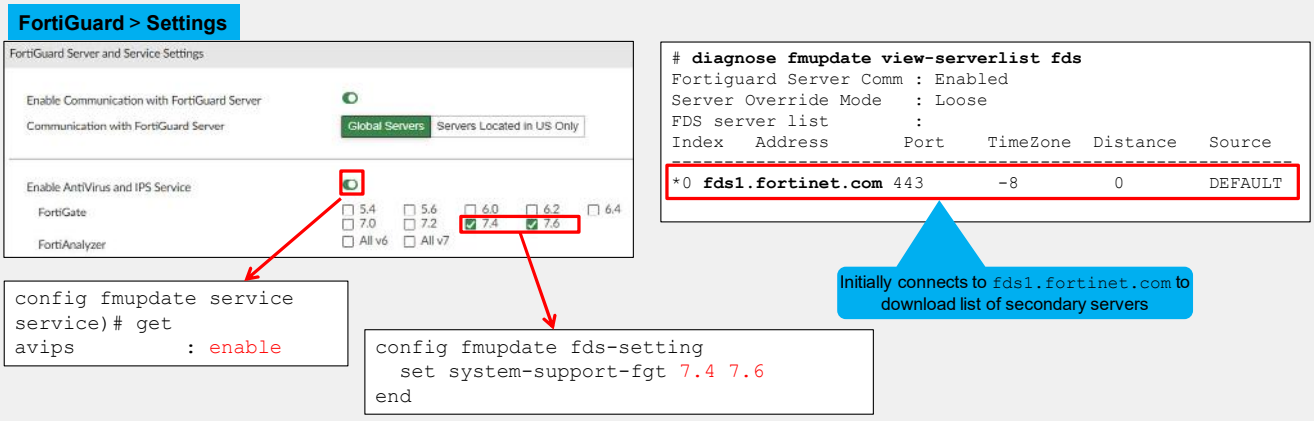
You can select **Servers Located in the US Only** to limit communication to FortiGuard servers located in the USA. Select **Global Servers** to communicate with servers anywhere.

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 FortiGuard servers.

During 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.

Antivirus and IPS Service

- Antivirus and IPS update services are enabled together
- Must enable supported FortiGate firmware versions to download packages based on that firmware
- Updates available for FortiGate, FortiClient, FortiAnalyzer, and FortiMail, among others

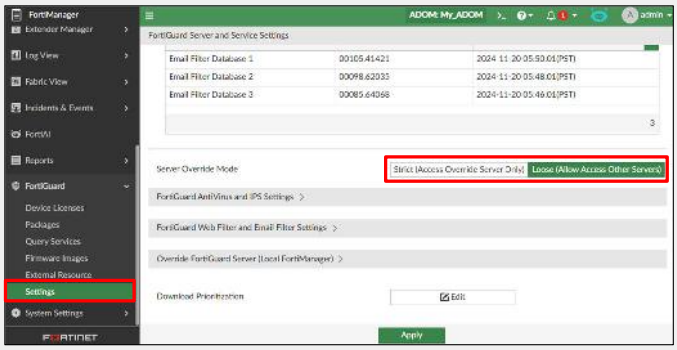


The antivirus and IPS services are enabled together and use TCP port 443 to obtain the updates from the public FortiGuard servers. You can enable updates for the supported products by enabling the firmware version that you want to download the updates for.

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.

Server Override Mode

- Server overrides allow FortiManager to fall back to other FDN servers if needed
- Two modes are available:
  - Loose: Default mode. Allows fallback to the other FDN servers
  - Strict: FortiManager can access only the configured override server




```
# diagnose fmupdate view-serverlist fds
Fortiguard Server Comm : Enabled
Server Override Mode   : Loose
FDS server list        :
Index  Address            Port   TimeZone  Distance   Source
-------------------------------------------------------------
*0     10.2.1.1           443    -8          0        CLI
 1   fds1.fortinet.com    443    -8          0        DEFAULT
```

```
# diagnose fmupdate view-serverlist fds
Fortiguard Server Comm : Enabled
Server Override Mode   : Strict
FDS server list        :
Index  Address          Port   TimeZone  Distance  Source
-------------------------------------------------------------
*0     10.20.1.1        443    -8          0       CLI
```

FORTINET Training Institute

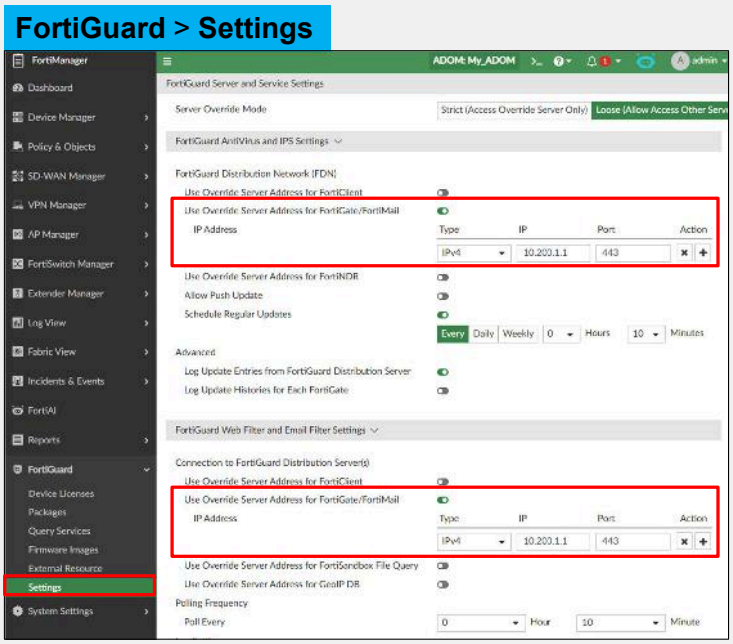
 23

The server override 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. By default, **Server Override Mode** is set to **Loose**, which is the recommended mode.

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.

Override Server Address

- You can configure specific FDS server addresses for FortiManager to connect to and get updates from
- This option is useful when:
  - It is necessary to connect FortiManager to a specific FDN server on the internet
  - You need to connect a downstream FortiManager to an upstream FortiManager to download updates
- Can configure override server address for
  - Antivirus, IPS
  - Web filter and email filter
  - Other private FortiGuard servers



FORTINET Training Institute

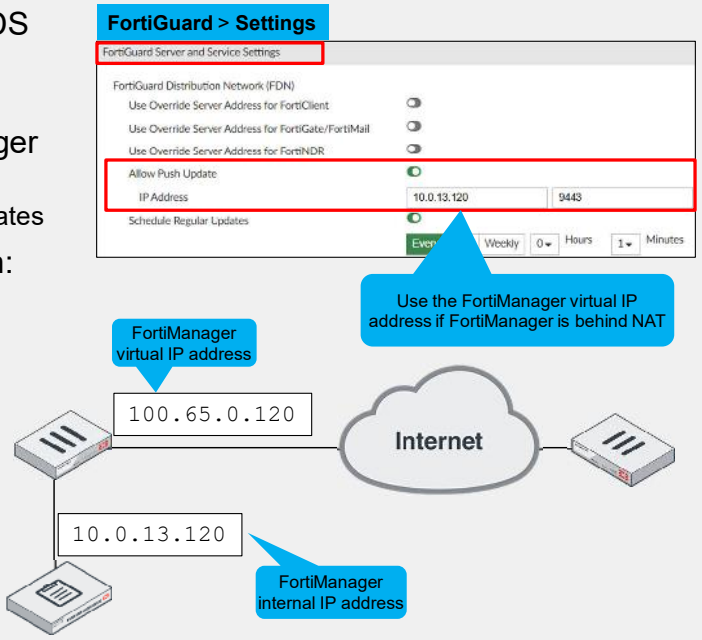
 24

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.

Push Updates

- By default, FortiManager contacts public FDS on a configured schedule
- Push updates allow for 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
  - Push updates
- Push updates fail if FortiManager is behind NAT device
  - Use the NAT device IP address instead
  - Allow traffic from NAT device to FortiManager to receive updates



FORTINET Training Institute

 25

What if there are important IPS updates available on the public FortiGuard? How can you ensure that FortiManager always receives new updates?

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?

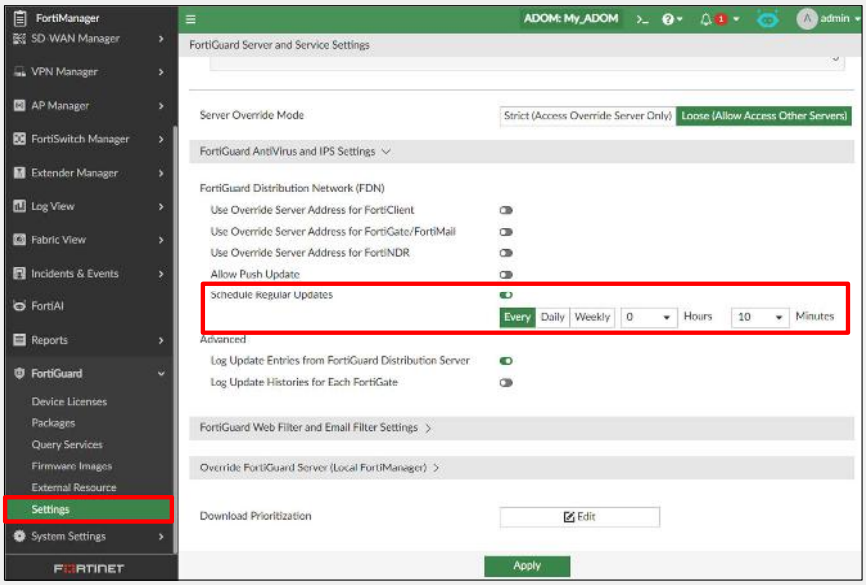
If FortiManager is behind a NAT device, sending its IP address for push updates causes push updates to fail because this is a nonroutable IP address from the FDN. You must configure the following:

- 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.

Schedule Updates for Antivirus and IPS

- By default, FortiManager schedules updates every ten minutes
  - You can select a different interval



FORTINET Training Institute

 26

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:

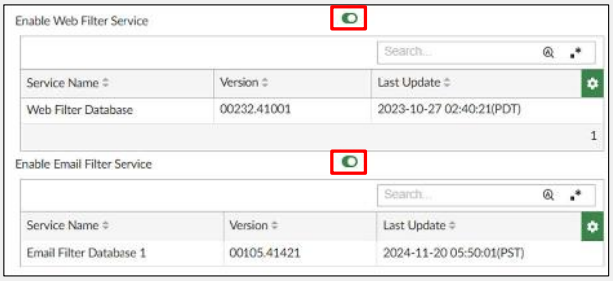
- FortiManager is scheduled to poll or update its local copies of update packages
- Push updates are enabled (it receives an update notification from the FDN)

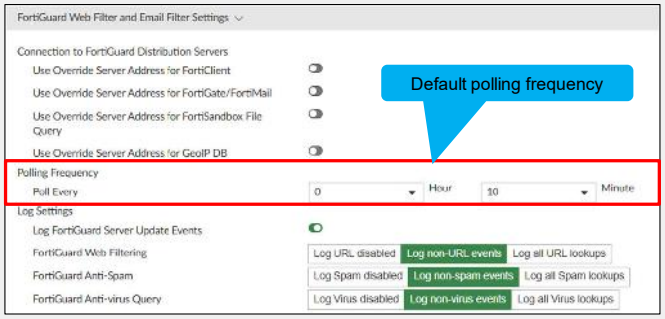
If the network is interrupted when FortiManager is downloading a large file, FortiManager downloads all files again when the network resumes. You can configure scheduled updates on an hourly, daily, or weekly schedule.

By default, FortiManager schedules updates every ten minutes because antivirus updates occur frequently.

Configuring Web Filter and Email Filter

- Through FortiGuard settings






```
# diagnose fmupdate view-serverlist fgd
Fortiguard Server Comm : Enabled
Server Override Mode   : Loose
FGD   server list      :
Index   Address              Port      TimeZone     Distance
------------------------------------------------------------
 0      208.184.237.64        443       -8           0
 1      208.184.237.63        443       -8           0
*30     guard.fortinet.net    443       -8           0
```

Initially connects to guard.fortinet.net to download a list of secondary servers

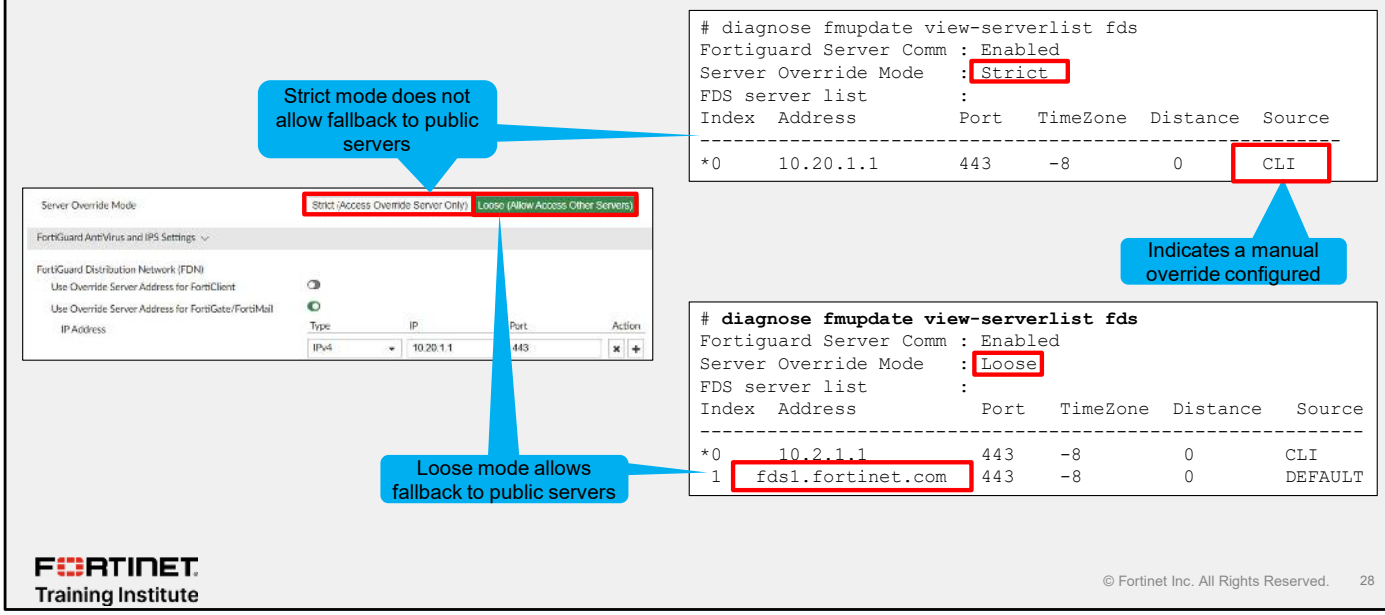
FORTINET Training Institute

 27

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 then it downloads web and antispam packages. By default, FortiManager is scheduled to check for updates every ten minutes.

FortiGate/FortiMail Server Override—Antivirus and IPS

- Override server address configuration depends upon server override mode



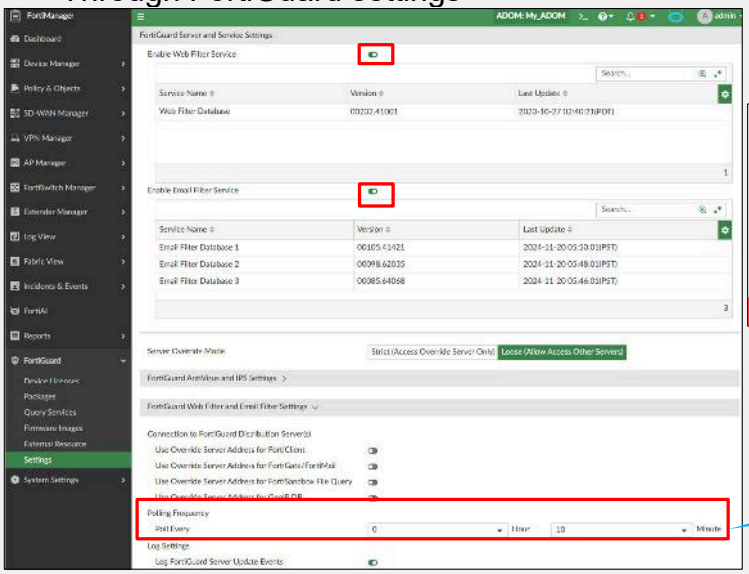
FortiManager tries to obtain updates from the servers configured in the **Use Override Server Address for FortiGate/FortiMail** section. Depending on the **Server Override Mode** configuration, you can restrict FortiManager to receiving updates from the configured override servers list, or allowing fallback 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, one override server address is configured. The image illustrates how, when **Server Override Mode** is set to **Strict**, FortiManager gets updates *only* from the server in the list. There is no fallback to other public servers, even if this configured server is not available.

However, if you set **Server Override Mode** to **Loose**, FortiManager first tries to get updates from the configured server list and; if that server becomes unavailable, FortiManager falls back to other public FDS servers to get updates.

Configuring Web Filter and Email Filter

- Through FortiGuard settings




```
# diagnose fmupdate view-serverlist fgd
Fortiguard Server Comm : Enabled
Server Override Mode   : Loose
FGD   server list      :
Index   Address               Port      TimeZone     Distance
------------------------------------------------------------
 0      208.184.237.64         443       -8           0
 1      208.184.237.63         443       -8           0
..
*30     guard.fortinet.net     443       -8           0
```

Initially connects to guard.fortinet.net to download a list of secondary servers

Default polling frequency

FORTINET Training Institute

 29

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 then it downloads web and antispam packages. By default, FortiManager is scheduled to check for updates every ten minutes.

Troubleshooting FortiGuard Connectivity

- Use the `diagnose fmupdate view-serverlist [fds|fgd]` command to list all upstream FDN servers FortiManager is communicating with
  - The following outputs can occur when FortiManager is unable to connect to the FDN servers

```
# 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     -8          0       DEFAULT
```

```
# diagnose fmupdate view-serverlist fgd
Fortiguard Server Comm : Enabled
Server Override Mode   : Loose
FGD server list        :
Index   Address          Port   TimeZone   Distance  Source
-------------------------------------------------------------
*0 guard.fortinet.net    443      -8          0       DEFAULT
```

Only one primary FDN server on list. FortiManager is unable to connect the public FDN servers because of unreachability.

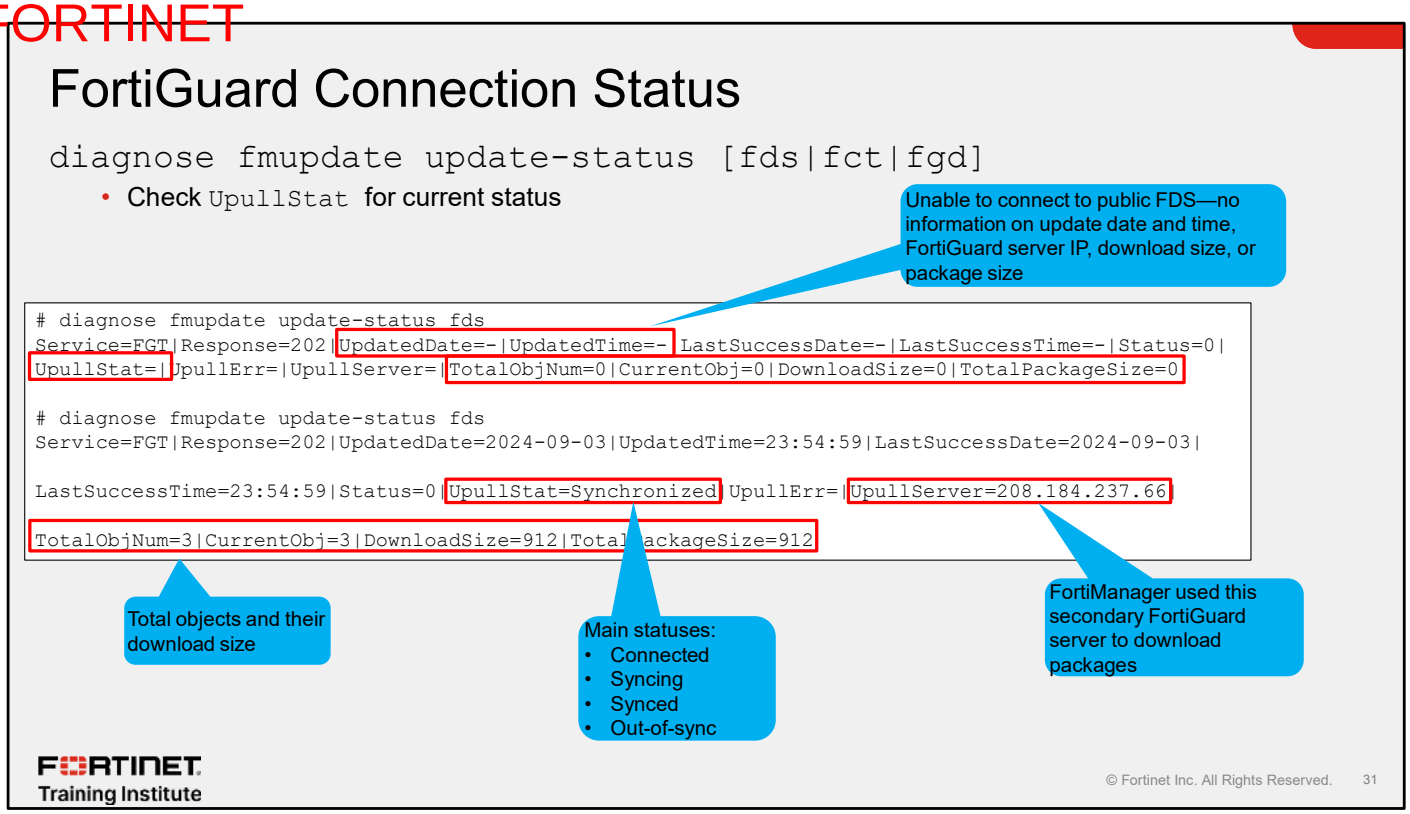
FORTINET Training Institute

 30

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 by 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.



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.

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
  - `fgdupd`
    - Responsible for database merging and consolidating smaller delta files into larger files
  - `fgdsvr`
    - Serves FortiGate and FortiClient for web filter and email filter requests

FORTINET Training Institute

 32

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.

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
  - This is an example configuration

```
config system central-management
        config server-list
            edit 1
                set server-type update rating
                set server-address 10.0.13.120
            next
        end
    set include-default-servers {enable/disable}
end
```

- Update includes antivirus, IPS, and license verification
- Rating includes– web filter, email filter

FortiManager IP address

Enable allows the use of public FDS, if FortiManager is unavailable
Disable uses only FortiManager for FDS updates

FORTINET Training Institute

 33

You can also configure unmanaged FortiGate devices to use FortiManager as a local FDS. For this, 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 can be one or both of the following:
  - `update` — used for antivirus, IPS updates, and FortiGate license verification
  - `rating` — used for web filter or anti-spam rating

By default, the `include-default-servers` option 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 the inclusion of public FortiGuard servers in the override server list.

Managed FortiGate to Use FortiManager as FDS

- By default, registered FortiGate uses public FDN, but you can configure them to use FortiManager for FDS updates by:
  - Configuring and installing a system template
  - Configuring, and then install, a script that sets central management with the default servers

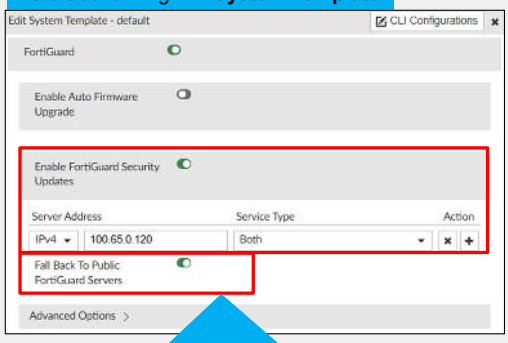
Managed FortiGate default settings

```
config system central-management
    set type fortimanager
    set fmg "10.0.13.120"
    set include-default-servers enable
end
```

By default, no `server-list` configured to use FortiManager as local FDS

Using public FDN

FortiGuard widget in **System Template**



Enable – use public FDS, if FortiManager is unavailable
Disable – use only FortiManager for FDS updates

FORTINET Training Institute

 34

By default, when FortiGate is managed by FortiManager, it uses public FortiGuard servers. This is because not every organization uses FortiManager for local FDS.

You can configure FortiGate to use FortiManager as a local FDS using one of the following procedures:

- Configure FortiGuard settings in a system template that 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 that includes the settings of the central management with the use inclusion of the default servers as shown on this slide.

Verifying Configuration to Troubleshoot FortiGuard Issues

- The following commands can be used to:
  - Verify the FortiGuard server address on FortiManager is resolved

```
execute ping <FortiGuard domain address>
```

  - Verify the communication to public network is enabled

```
# get fmupdate publicnetwork
status               : enable
```

  - Verify that the service is enabled

```
#get fmupdate service
avips                : enable
query-antispam       : enable
query-webfilter      : enable
...
```

FORTINET Training Institute

 35

The first step you should perform when troubleshooting FortiGuard issues is to verify the configuration on FortiManager. You should confirm that:

- You can resolve the public FDN servers by domain name. For example, check if you are able to ping `fds1.fortinet.com`.
- The communication to public network and services is enabled on FortiManager
- The services are enabled on FortiManager

Verifying FortiGate Contract Information on FortiManager

- Use the `diagnose fmupdate dbcontract` command to lists the contract information for all the devices

FortiGate devices *must* have valid and active service contracts to obtain updates!

```
FortiManager4 # diagnose fmupdate dbcontract
FGVM010000077646 [SERIAL_NO]
  AccountID:yyyy@Fortinet.com
  Industry: Technology
  Company:  Fortinet
  Contract: 14
        AVDB-1-06-20251111
        AVEN-1-99-20180531
        NIDS-1-99-20190611
  Contract Raw Data:
    Contract=AVDB-1-06-20250531:0:1:1:0*AVEN-1-99-
20180531:0:..

FGVM010000064692 [SERIAL_NO]
  AccountID: yyyyy@fortinet.com
  Industry: Technology
  Company:  Fortinet
  Contract: 14
        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..
```

99 are trial or expired licenses

AV service contract

FORTINET Training Institute

 36

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.

FortiGate Troubleshooting Commands

- To show version, last update, and contract expiration date:

```
 # get system fortiguard-service status
NAME                VERSION LAST UPDATE          METHOD    EXPIRE
AV Engine            7.018  2024-05-18 01:46:00  manual    2027-01-19 23:59:59
Virus Definitions    91.1635  2024-04-25 20:04:46  scheduled 2027-01-19 23:59:59
Extended set         91.1635  2024-04-25 20:04:46  scheduled 2027-01-19 23:59:59
```

- To display real-time update information

```
# 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 10.0.1.120:8890
[782] ssl_new: SSL object is created pack_obj[183]-Packing pack_obj[196]-Packing
obj=Protocol=3.2|Command=Update|Firmware=FGVM64-FW-7.60-
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

 37

On the FortiGate CLI, you can check the latest update version, when it was last updated, and the 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).

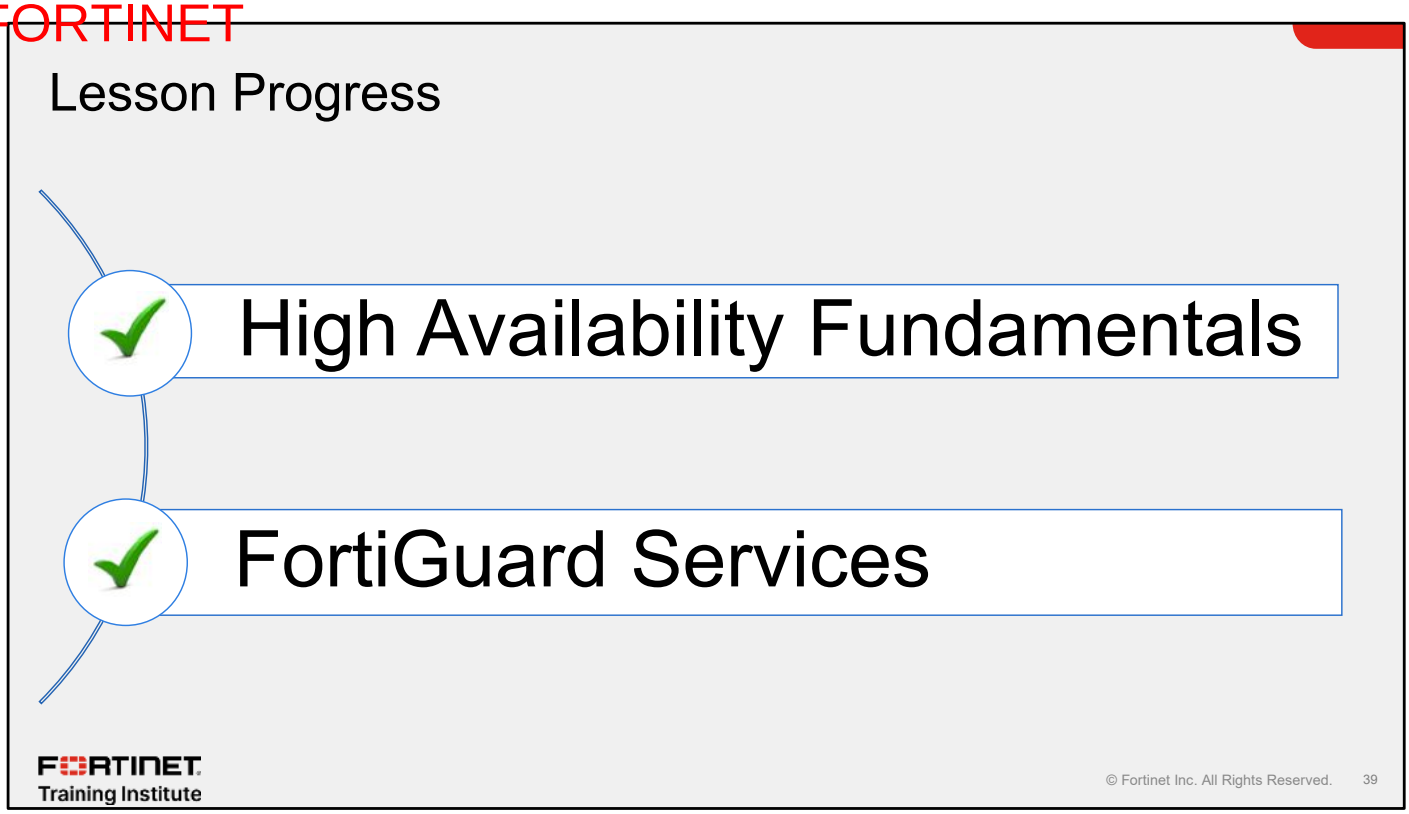
Knowledge Check

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 provides devices with a faster connection to updates.
   B. It provides updates for registered devices only.

FORTINET Training Institute

 38



Congratulations! You have completed this lesson.

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

Review

- ✓ Describe the fundamental concepts of FortiManager HA
- ✓ Configure FortiManager as your local FortiGuard server
- ✓ Describe the server override modes
- ✓ Upgrade FortiGate firmware using FortiManager
- ✓ Configure FortiGate to use FortiManager for updates
- ✓ Diagnose and troubleshoot FortiGuard issues

FORTINET Training Institute

 40

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

By mastering the objectives covered in this lesson, you learned about the fundamentals of FortiManager HA clusters, and how to use FortiManager as a local FortiGuard server for your devices.