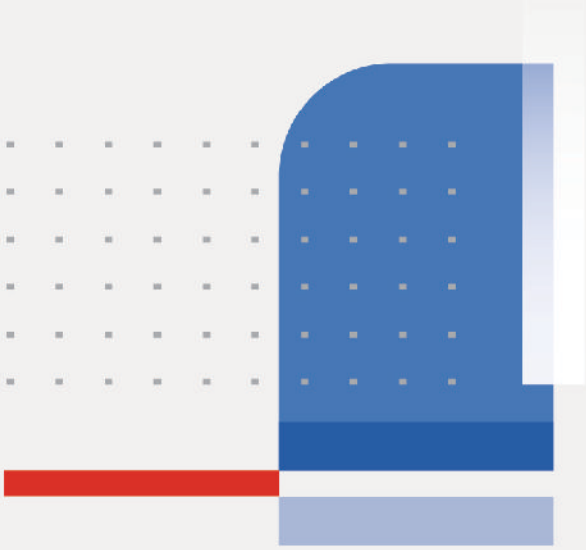
FortiAnalyzer Administrator Study Guide

FortiAnalyzer 7.6



FORTINET
Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

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

Fortinet Fuse User Community

https://community.fortinet.com/

Fortinet Forums

https://community.fortinet.com/t5/Support-Forum/bd-p/fortinet-discussion

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

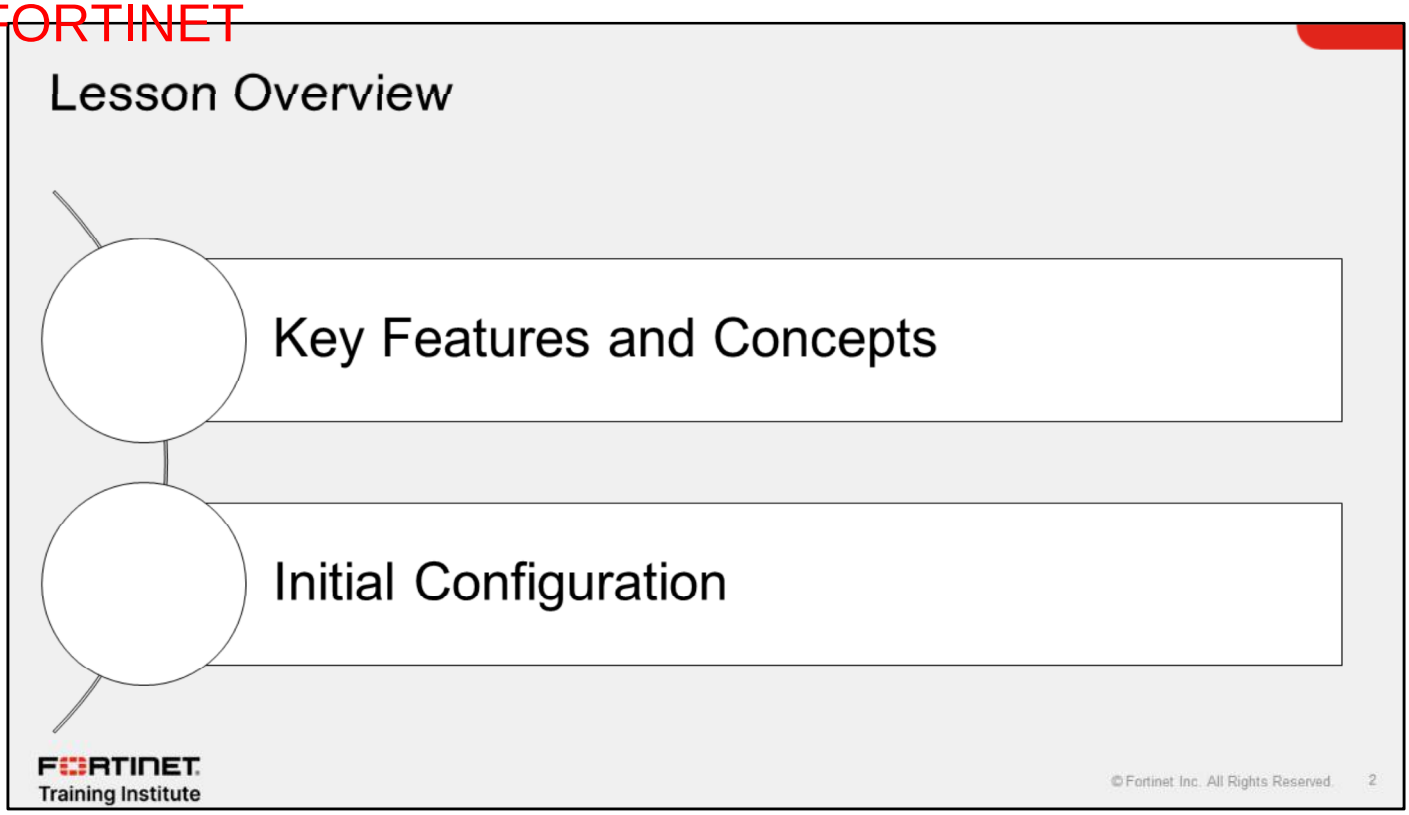
Fortinet Training Institute Helpdesk (training questions, comments, feedback)

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

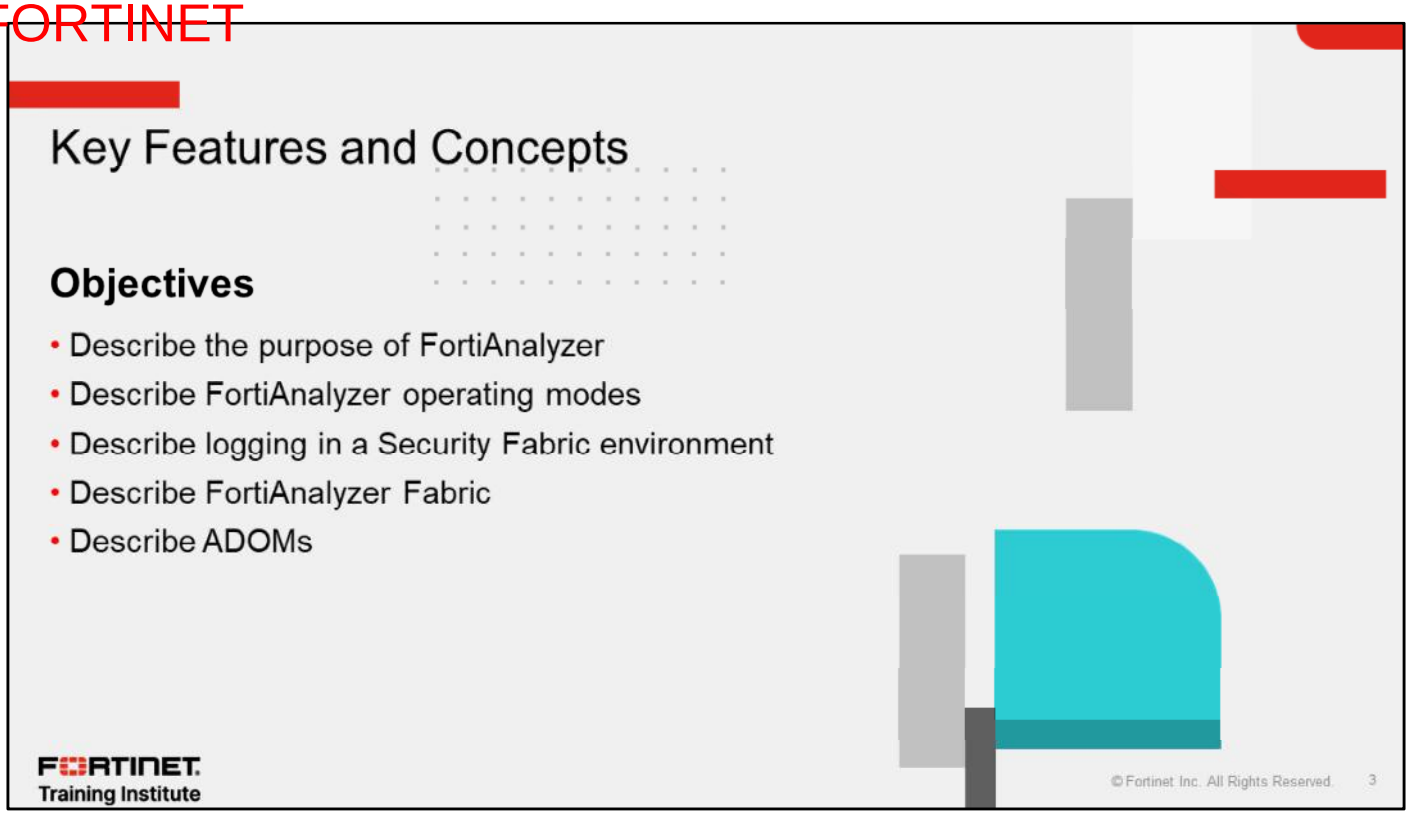
TABLE OF CONTENTS

In this lesson, you will learn about the key features and concepts of FortiAnalyzer and how to configure the initial settings.

FortiAnalyzer integrates logging, analytics, and reporting into one system, so you can quickly identify and react to network security threats.

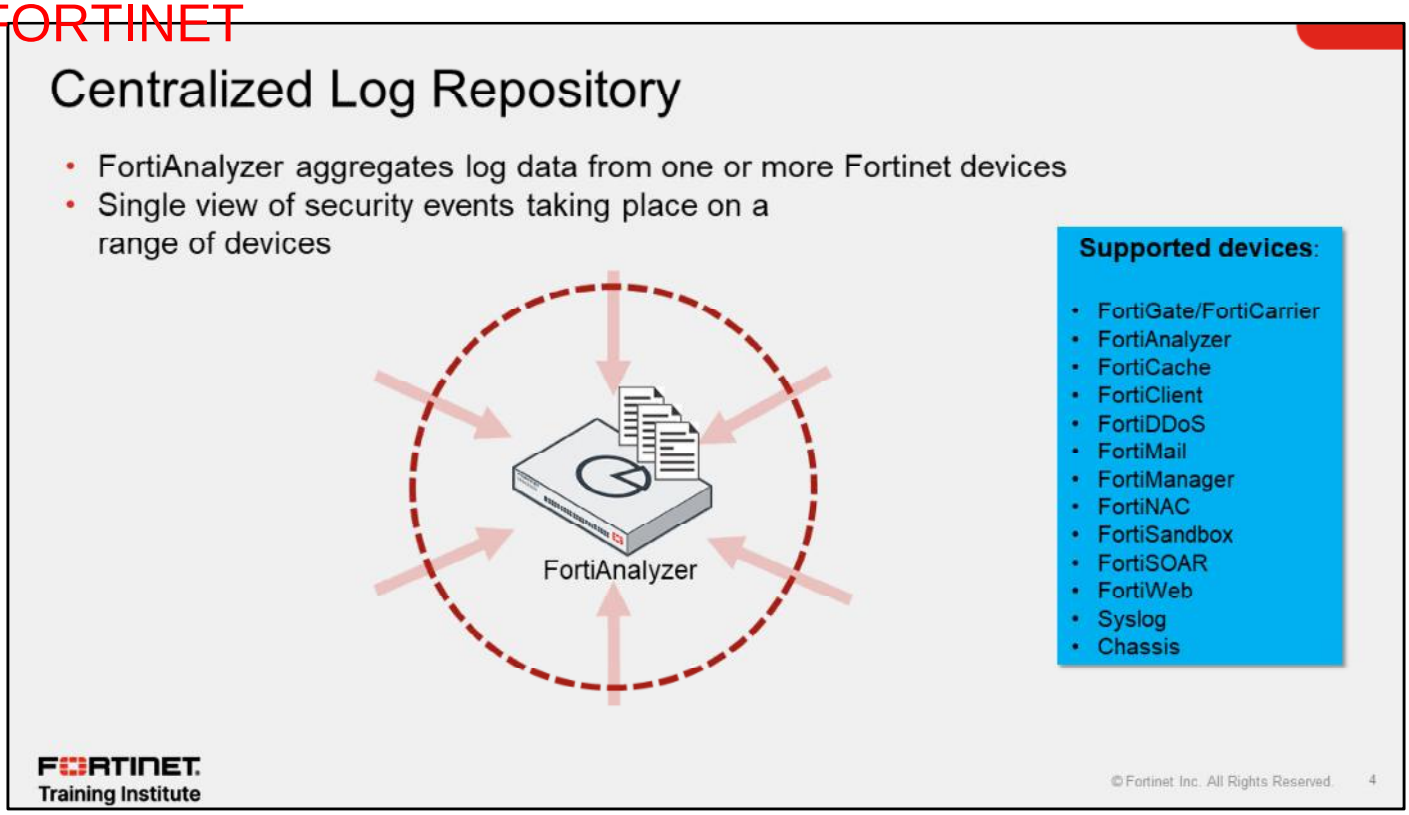


In this lesson, you will learn about the topics shown on this slide.



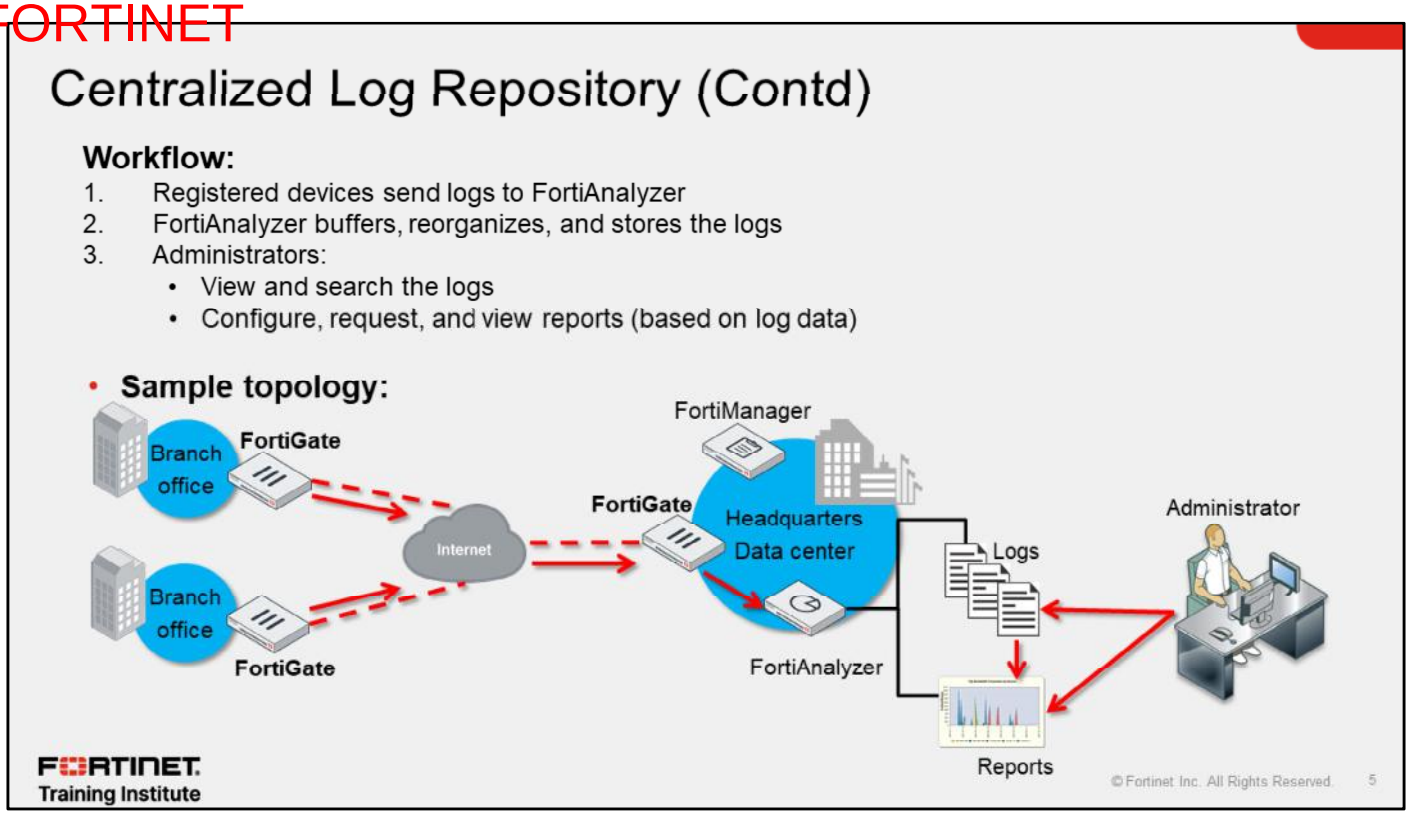
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiAnalyzer key features and concepts, you will be able to use the device effectively in your network.



FortiAnalyzer aggregates log data from one or more Fortinet devices, thereby acting as a centralized log repository. Log aggregation provides a single channel for accessing your complete network data, so you don't need to access multiple devices, several times a day.

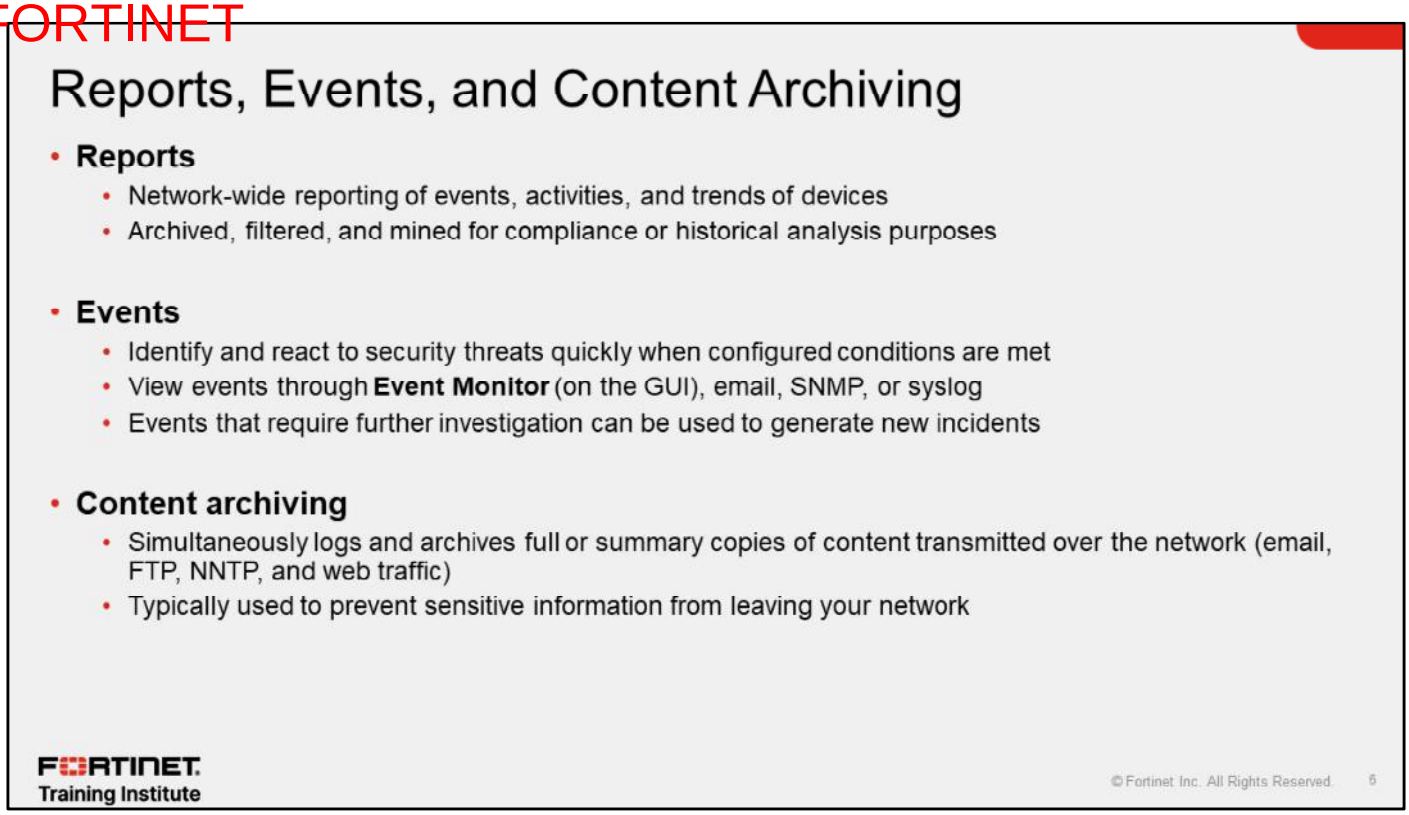
FortiAnalyzer can be integrated with many different Fortinet solutions. For a complete list, refer to the *Release Notes* at `docs.fortinet.com`.



The logging and reporting workflow operates as follows:

1. Registered devices send logs to FortiAnalyzer.
2. FortiAnalyzer collates and stores those logs in a way that makes it easy to search and run reports.
3. Administrators can connect to FortiAnalyzer using the GUI to view the logs manually or generate reports to analyze the data. Administrators can also use the CLI to perform administrative tasks.

FortiAnalyzer can be easily integrated into a network, even one with multiple sites. A sample topology can include various branches and headquarters. The location of each firewall is added to FortiAnalyzer, and the administrator can view logs and generate reports for the entire network under one interface.

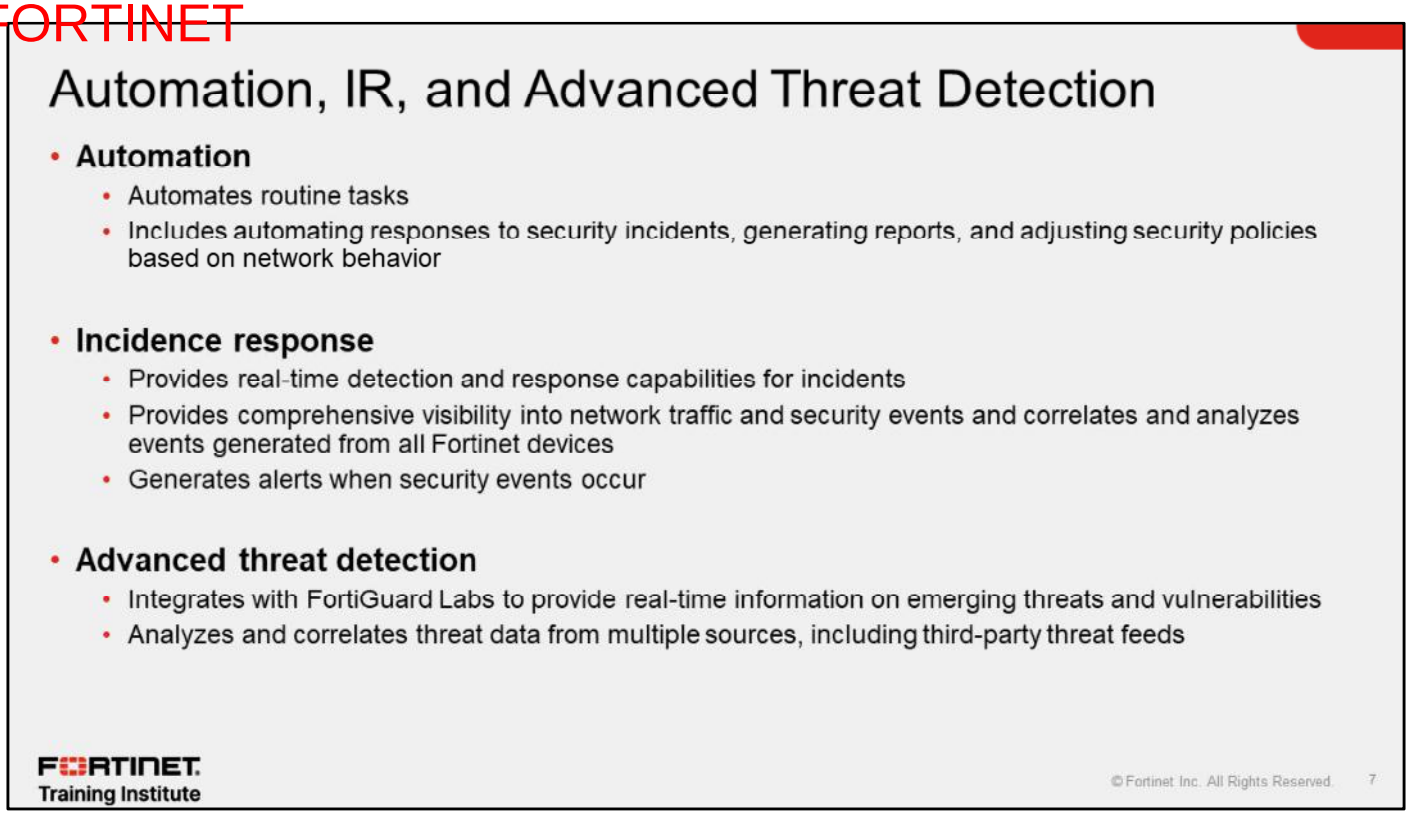


Some key features of FortiAnalyzer include reporting, alert generation, and content archiving.

Reports provide a clear picture of network events, activities, and trends occurring on supported devices. FortiAnalyzer reports collate the information in the logs so that you can interpret the data and, if necessary, take the required action. You can archive and filter the network knowledge you glean from these reports and mine it for compliance or historical analysis purposes.

FortiAnalyzer events allow you to react quickly to threats because it’s unrealistic to physically monitor your network around the clock. The system can generate events when the logs meet specific conditions—conditions you have configured FortiAnalyzer to monitor for registered devices. You can see events on the GUI and send them to multiple recipients by email, SNMP, or syslog. Additionally, you can use events that require further investigation to generate new incidents.

Content archiving provides a way to simultaneously log and archive full or summary copies of the content transmitted over the network. You typically use content archiving to prevent sensitive information from leaving your organization's network. You can also use it to record network use. The data loss prevention (DLP) engine can examine email, FTP, Network News Transfer Protocol (NNTP), and web traffic, but you must configure the archive setting for each rule in a DLP sensor on FortiGate, so you can specify what you want to archive.

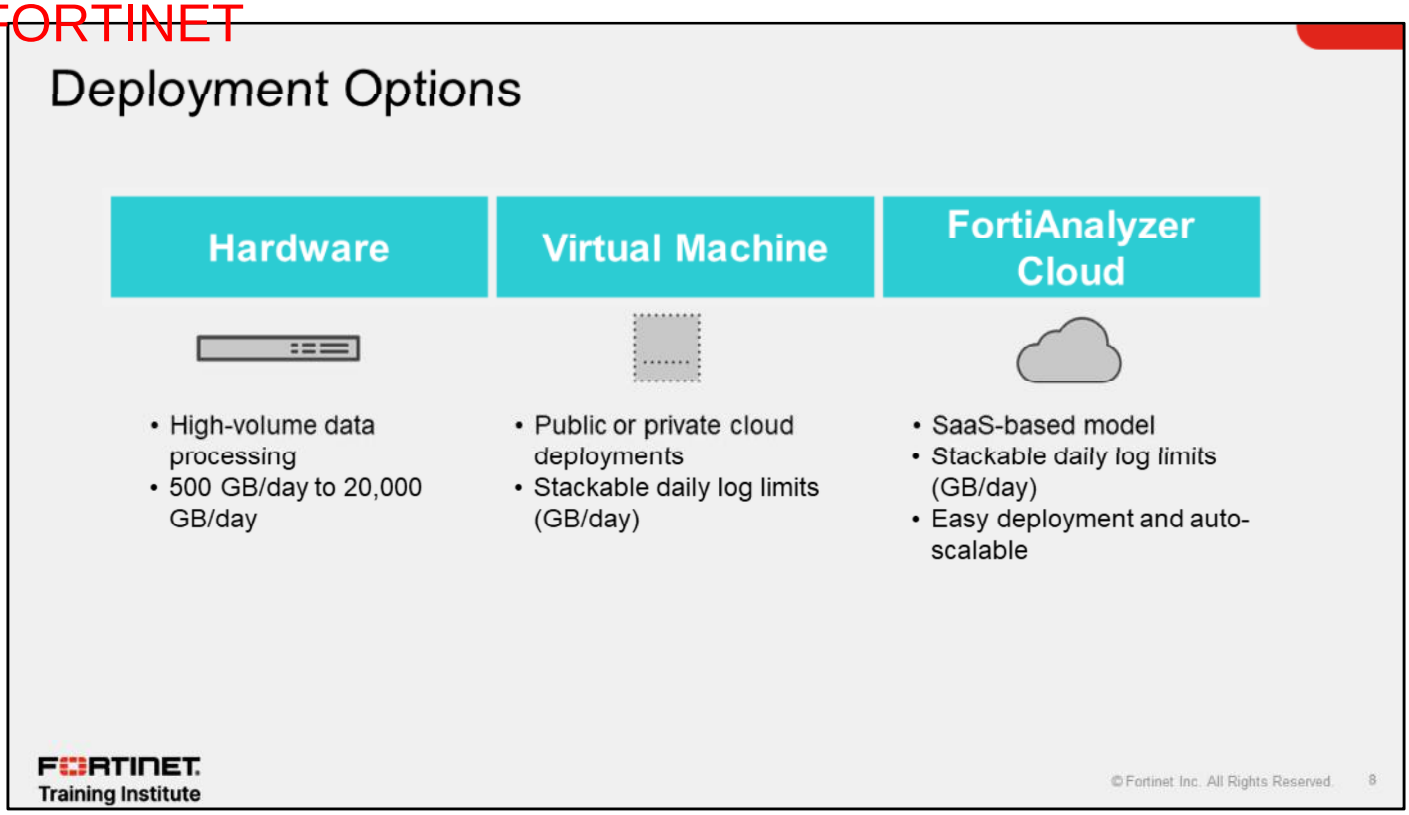


Additional key features of FortiAnalyzer include automation, incident response, and advanced threat detection.

The automation feature allows FortiAnalyzer to automate routine tasks. This includes automating responses to security incidents, generating reports, and adjusting security policies based on network behavior.

In incident response, FortiAnalyzer provides real-time detection and response capabilities. It provides comprehensive visibility into network traffic and security events and correlates and analyzes events generated from all Fortinet devices. This consolidates visibility to provide an accurate picture of security threats. FortiAnalyzer generates alerts when security events occur, such as when a user attempts to access a restricted website.

FortiAnalyzer is used for advanced threat detection. It integrates with FortiGuard Labs to provide real-time information on emerging threats and vulnerabilities. It also analyzes and correlates threat data from multiple sources, including third-party threat feeds.

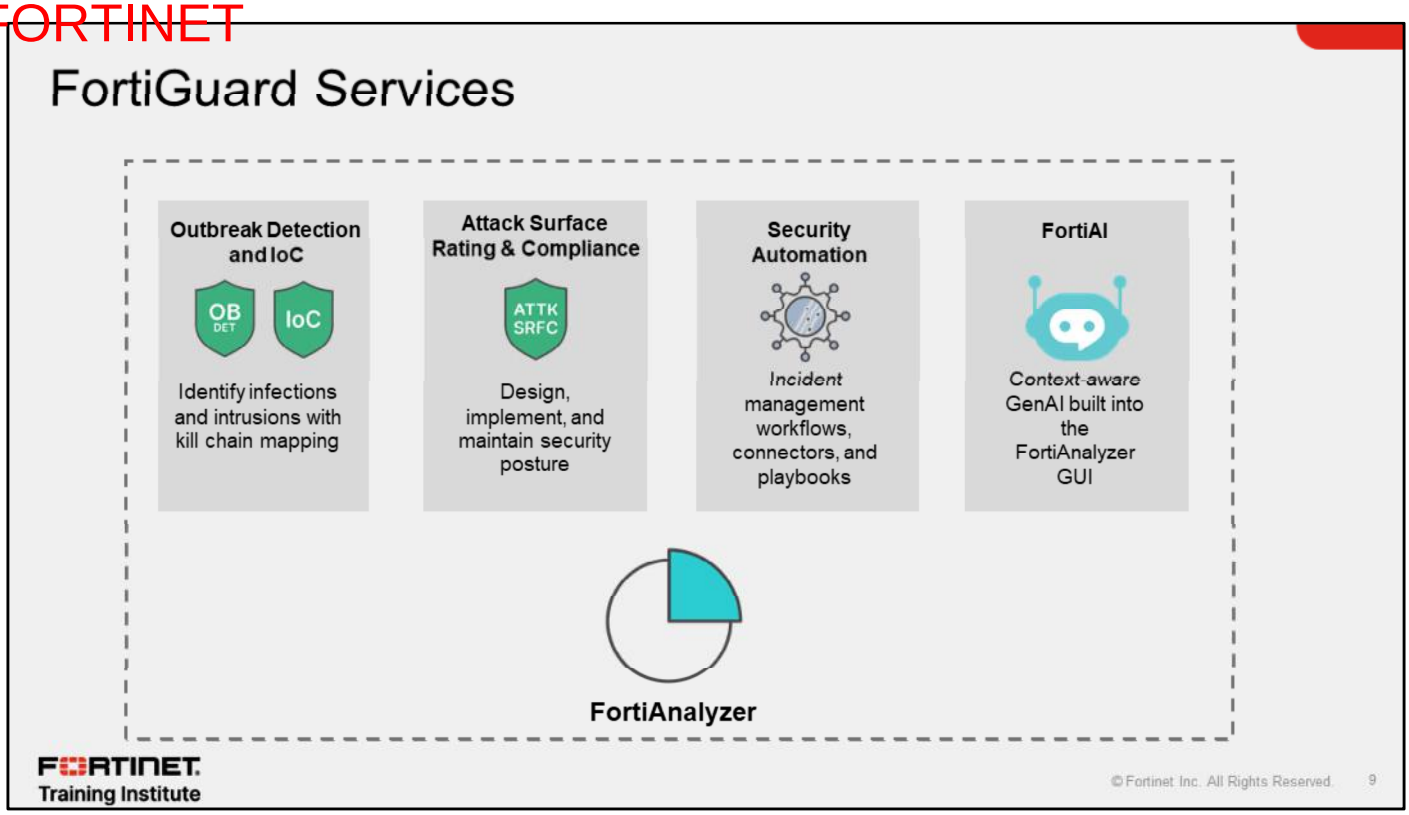


FortiAnalyzer offers various deployment options to suit various organizational needs.

The hardware-based appliances offer different capacities with various performance levels. They are suitable for organizations that prefer on-premises deployments and have specific storage and processing requirements. The higher-end model, especially FortiAnalyzer Big Data, can handle high log volumes.

The FortiAnalyzer VMs are supported on various public and private cloud infrastructures. VM deployments offer flexibility in resource allocation (CPU, memory, storage) and can leverage existing virtualized infrastructure.

FortiAnalyzer Cloud is a Software-as-a-Service (SaaS) offering from Fortinet. Organizations can leverage FortiAnalyzer capabilities without having to manage the underlying infrastructure. FortiAnalyzer Cloud offers easy deployment and management, as well as auto-scaling based on deployment needs.



FortiAnalyzer leverages various FortiGuard services to enhance its threat intelligence, analysis, and reporting capabilities.

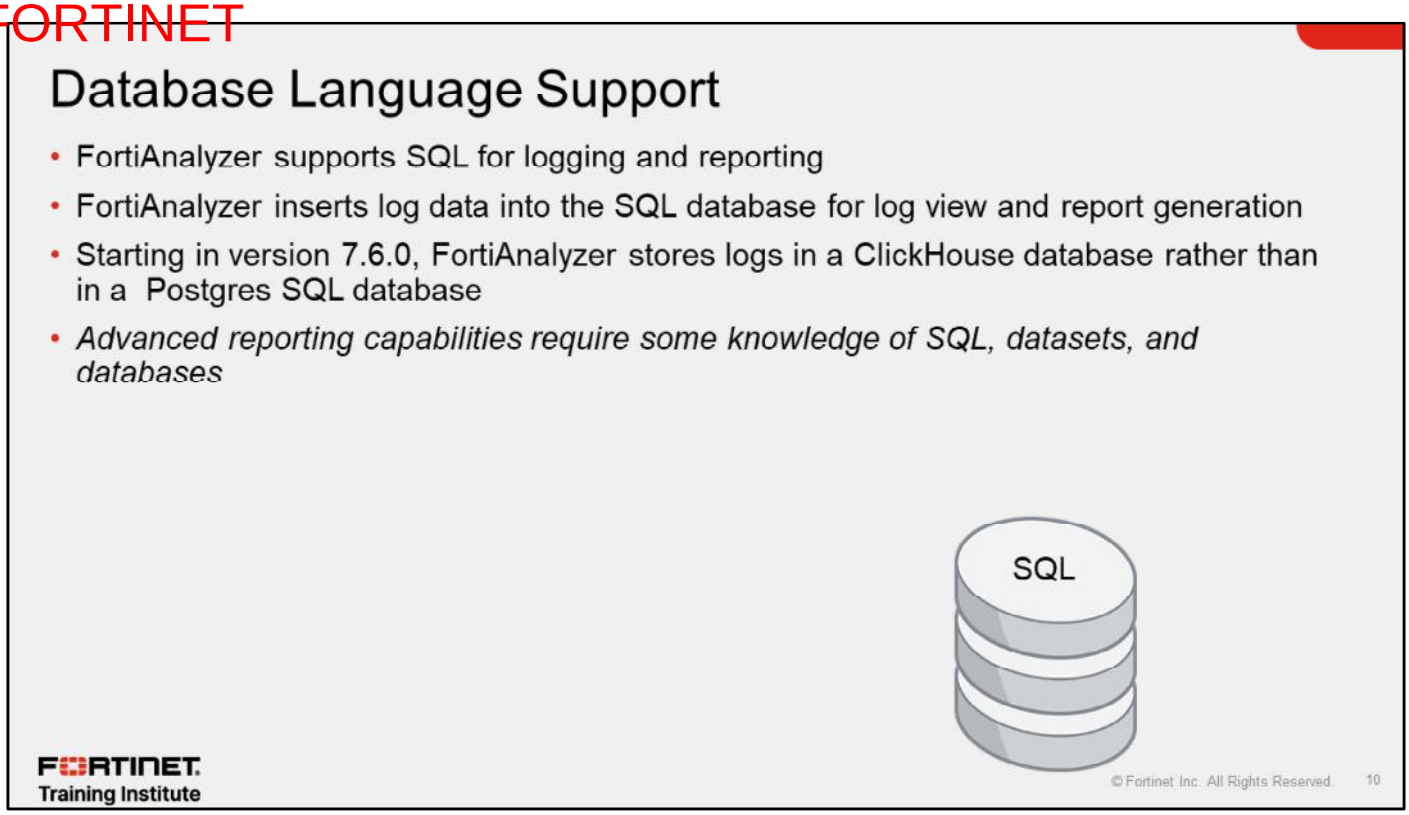
FortiGuard Labs analyzes global threat data to identify emerging attack campaigns, zero-day exploits, and rapidly spreading malware. With the Outbreak Detection service, FortiAnalyzer receives critical outbreak reports and corresponding event handlers. Administrators can use the event handlers to quickly identify systems affected by current outbreaks and take action.

The Indicators of Compromise (IoC) service provides FortiAnalyzer with a constantly updated feed of known malicious artifacts, such as IP addresses, domains, file hashes, and URLs associated with known cyberattacks. FortiAnalyzer can use these IoC feeds to enrich its historical and real-time logs to quickly identify compromised devices, users, or systems within your network.

The Attack Surface Rating and Compliance service offers a real-time security posture evaluation. This service continuously assesses your organization's security health, including unpatched vulnerabilities and critical security settings. Administrators can view a clear picture of network vulnerabilities, receive alerts for any changes, and receive best practice recommendations for improving their settings and configurations.

The Security Automation service provides content and updates for the automation and orchestration features. It includes predefined playbooks, event handlers, and connectors to streamline security operations.

FortiAI for FortiAnalyzer is a generative AI-powered security assistance designed to augment and accelerate analysts' work. Analysts can use natural language prompts to ask complex questions about their security events, logs, and network behavior. FortiAI can interpret security events, provide detailed summaries and potential impacts, and suggest remediation actions.



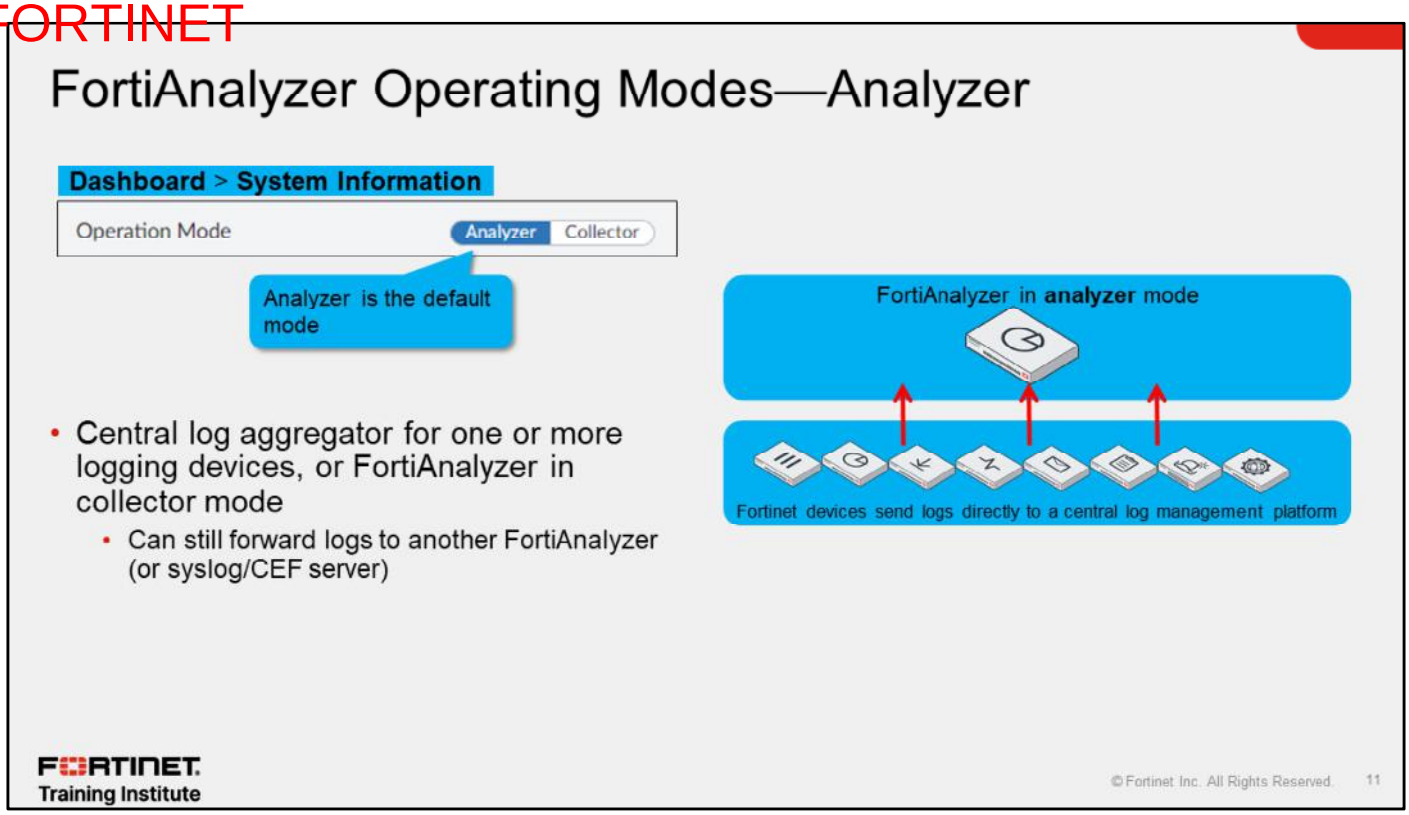
SQL is the database language that FortiAnalyzer uses for logging and reporting.

Starting in version 7.6.0, FortiAnalyzer stores logs in a ClickHouse database rather than PostgresSQL (PSQL) database. Prior to version 7.6.0, FortiAnalyzer used a PSQL database to store the log table. FortiAnalyzer 7.6.0 migrates the historical logs from PSQL to ClickHouse, inserting real-time logs into ClickHouse. All **FortiView** data and **Reports** are based on the new data table in ClickHouse.

When upgrading from an earlier version to FortiAnalyzer 7.6.0 or later, the log database will automatically begin migrating. During this migration process, all historical logs will be transferred from the PostgreSQL database to the ClickHouse database.

After the upgrade, you can monitor the migration progress on the GUI banner or by using the following command in the CLI: `diagnose sql status migrate-db`.

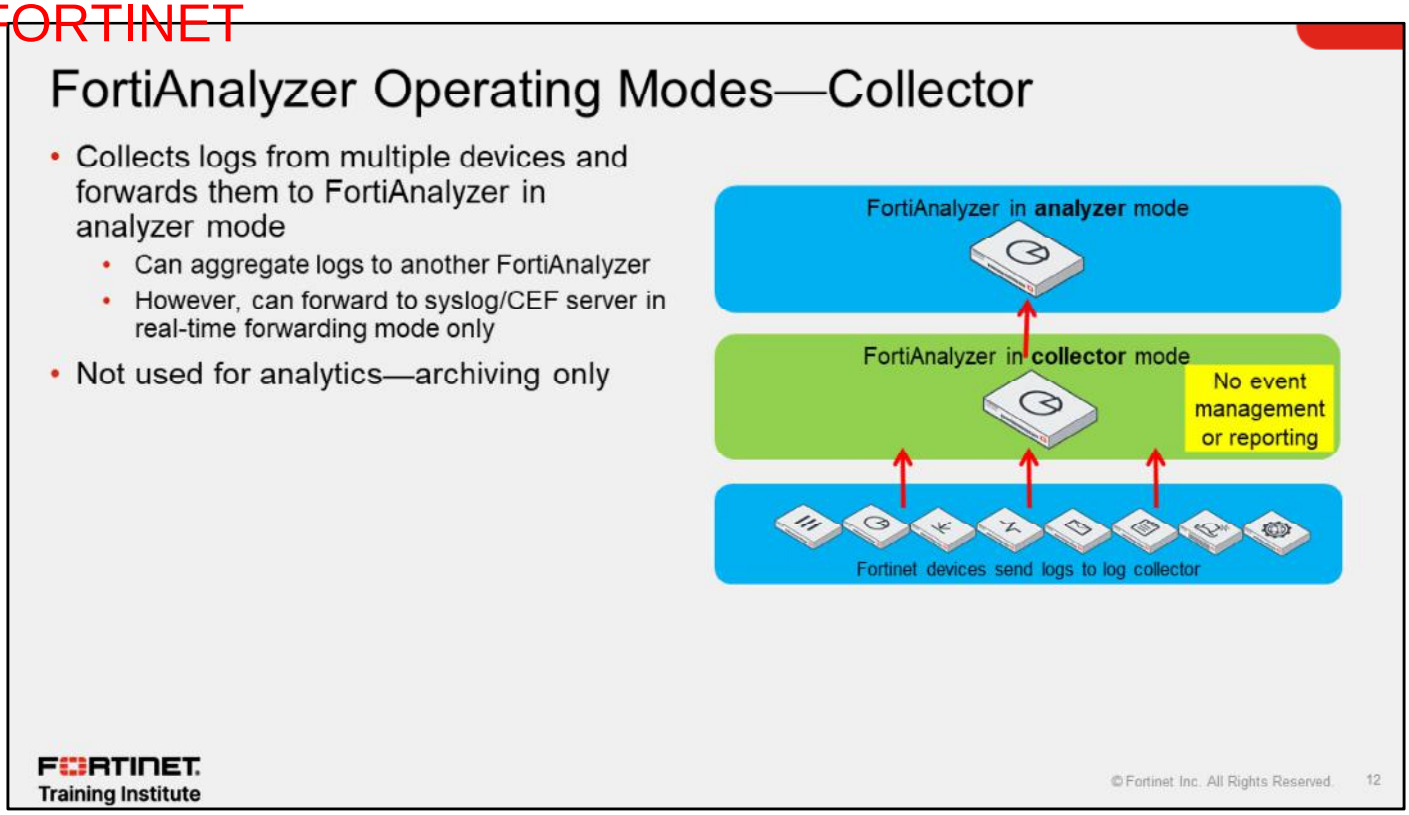
To take full advantage of advanced reporting features, you must have some familiarity with SQL and databases. You may need to create custom SQL queries, referred to as datasets, to extract the data you need from the database. For more information on SQL and FortiAnalyzer, please refer to the supplementary lesson *SQL and Datasets*.



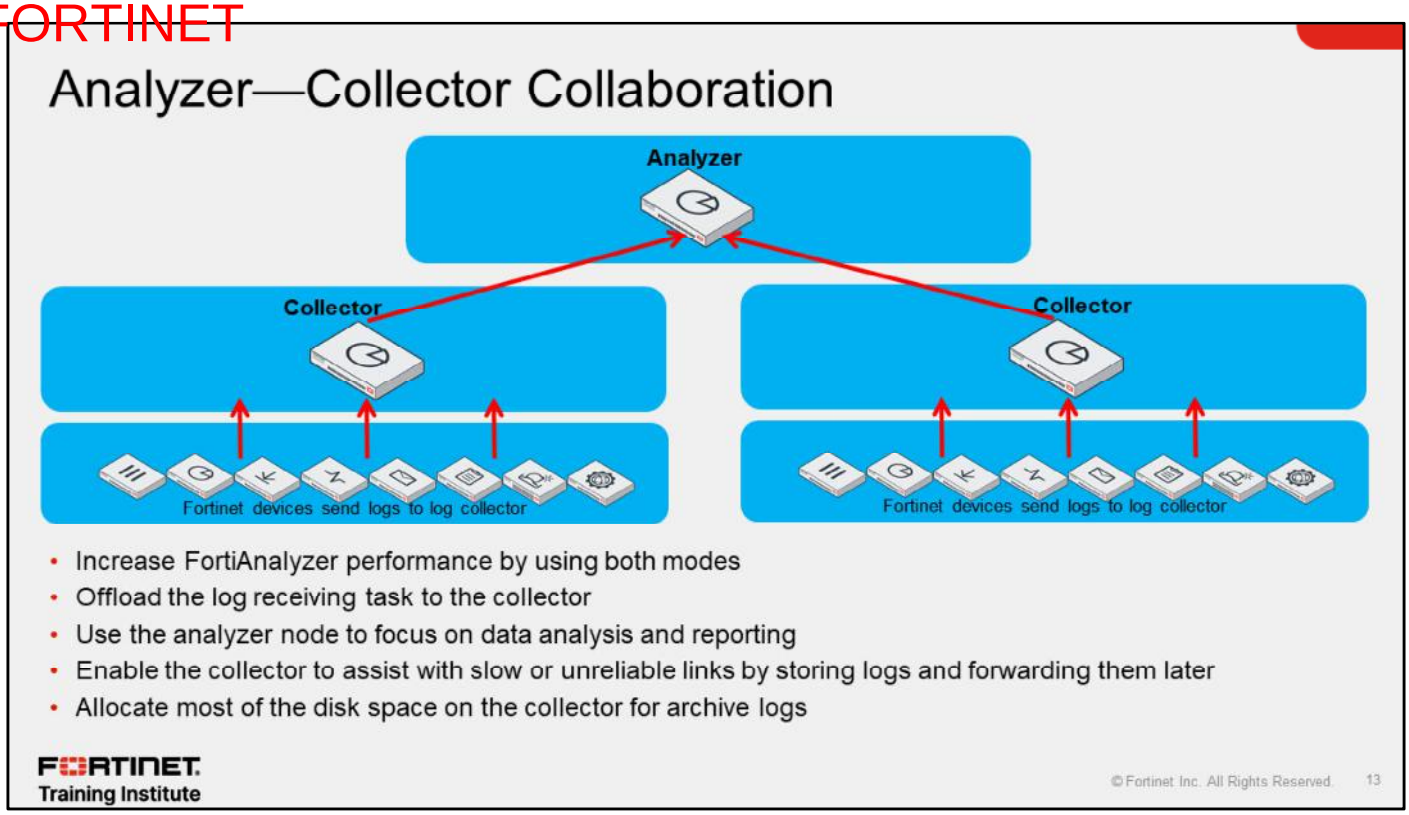
FortiAnalyzer has two modes of operation: analyzer and collector. The mode of operation you choose depends on your network topology and individual requirements.

You can change the operating mode in the **System Information** widget on the dashboard.

When operating in analyzer mode, FortiAnalyzer acts as a central log aggregator for one or more log collectors, such as a FortiAnalyzer operating in collector mode or any other supported device sending logs. Analyzer is the default operating mode.



When operating in collector mode, the device collects logs from multiple devices. Then, it forwards those logs, in their original binary format, to another device, such as FortiAnalyzer operating in analyzer mode. Depending on the forwarding mode, it can also send them to a syslog server or a Common Event Format (CEF) server. A collector does not have the same feature-rich options as an analyzer because its only purpose is to collect and forward logs. It does not allow event management or reporting.



By using both analyzer and collector modes, you increase FortiAnalyzer performance. Collectors offload the task of receiving logs from multiple devices from the analyzer, allowing the analyzer to focus on data analysis and reporting tasks.

Furthermore, because a collector is strictly dedicated to log collection, its log receiving rate and speed are maximized. If bandwidth is an issue, like in the case of slow WAN links, you can use the store and upload option to send logs only during low-bandwidth periods.

Since the collector performs no analytics tasks, you should allocate most of the disk space for archive logs.

Security Fabric Logging

- Store and analyze logs from devices in a Security Fabric group as if the logs are from a single device
- The Security Fabric logs each session once
  - The first FortiGate that handles a session
  - No duplicate traffic logs for sessions coming from another Fabric member's MAC address with the following exceptions:
    - An upstream FortiGate performs network address translation (NAT)
    - Upstream FortiGate devices still log unified threat management (UTM) events
- UTM and traffic logs are correlated so that session details, UTM events, reporting, and automation in the Security Fabric work correctly

FORTINET Training Institute

 14

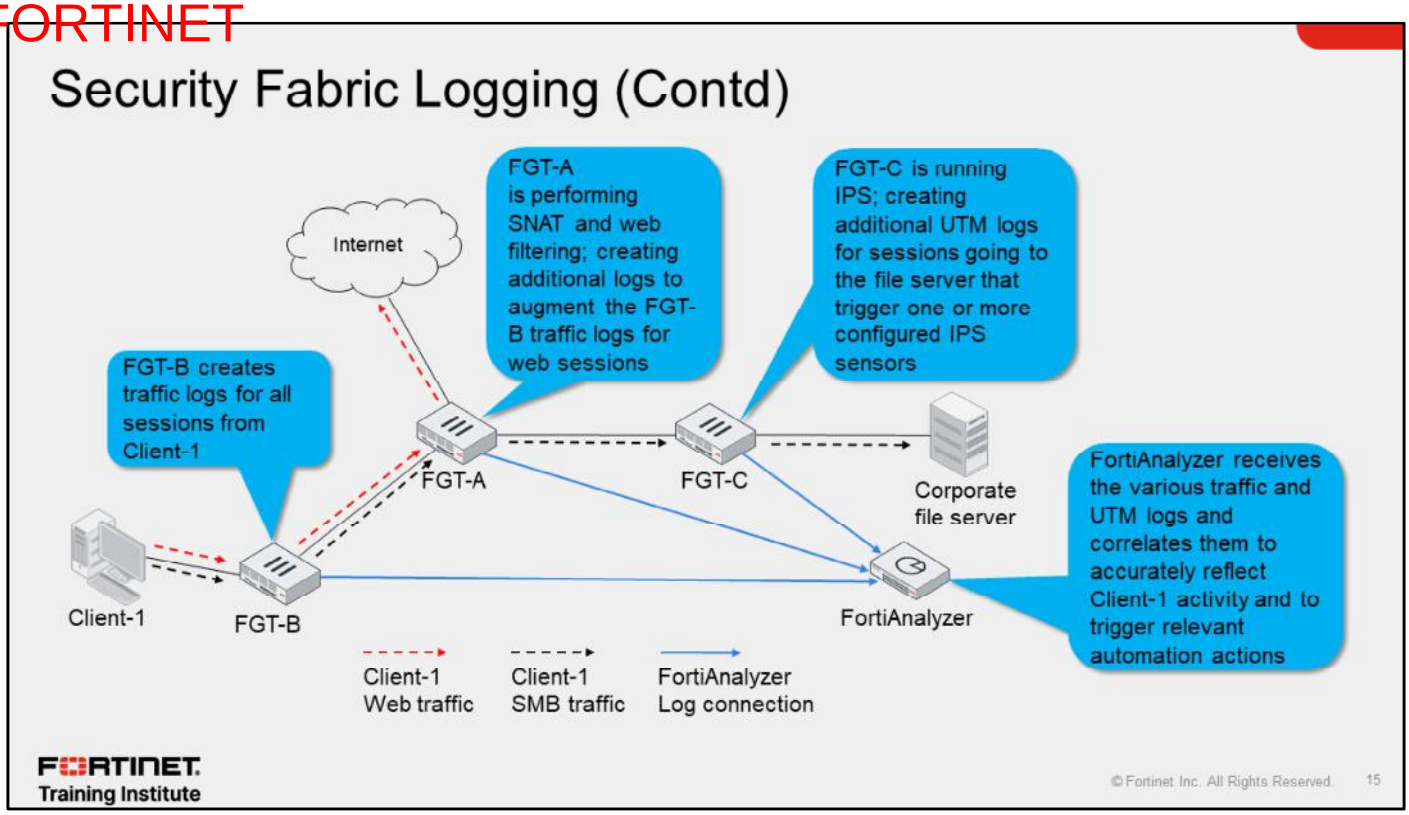
FortiAnalyzer supports the Security Fabric by storing and analyzing the logs from devices in a Fabric group as if they were from a single device. FortiAnalyzer correlates traffic logs to corresponding UTM logs to report sessions and bandwidth, together with its UTM threats.

A session's traffic is always logged by the first FortiGate that handled it in the Fabric. FortiGate devices in the Security Fabric know the MAC addresses of their upstream and downstream peers. If FortiGate receives a packet from a MAC address that belongs to another FortiGate in the Fabric, it does not generate a new traffic log for that session. This helps prevent multiple FortiGate devices from repeatedly logging the same session.

One exception to this behavior occurs when the upstream FortiGate device performs NAT. In this situation, FortiGate generates an additional log to capture NAT details, such as the translated ports and addresses.

If configured, upstream devices generate UTM logs, and FortiAnalyzer performs UTM and traffic log correlation for the Fabric to provide a concise and accurate record of any UTM events in the network. No additional configuration is required because FortiAnalyzer performs this function automatically.

Note that each FortiGate in the Fabric logs traffic to FortiAnalyzer independent of the root or other leaf devices. If the root FortiGate is down, logging from leaf FortiGate devices to FortiAnalyzer continues to function.



This slide illustrates how logging operates in the Security Fabric, providing complete visibility while eliminating duplicate logs throughout the environment. It shows three FortiGate devices configured in the Security Fabric along with a FortiAnalyzer device:

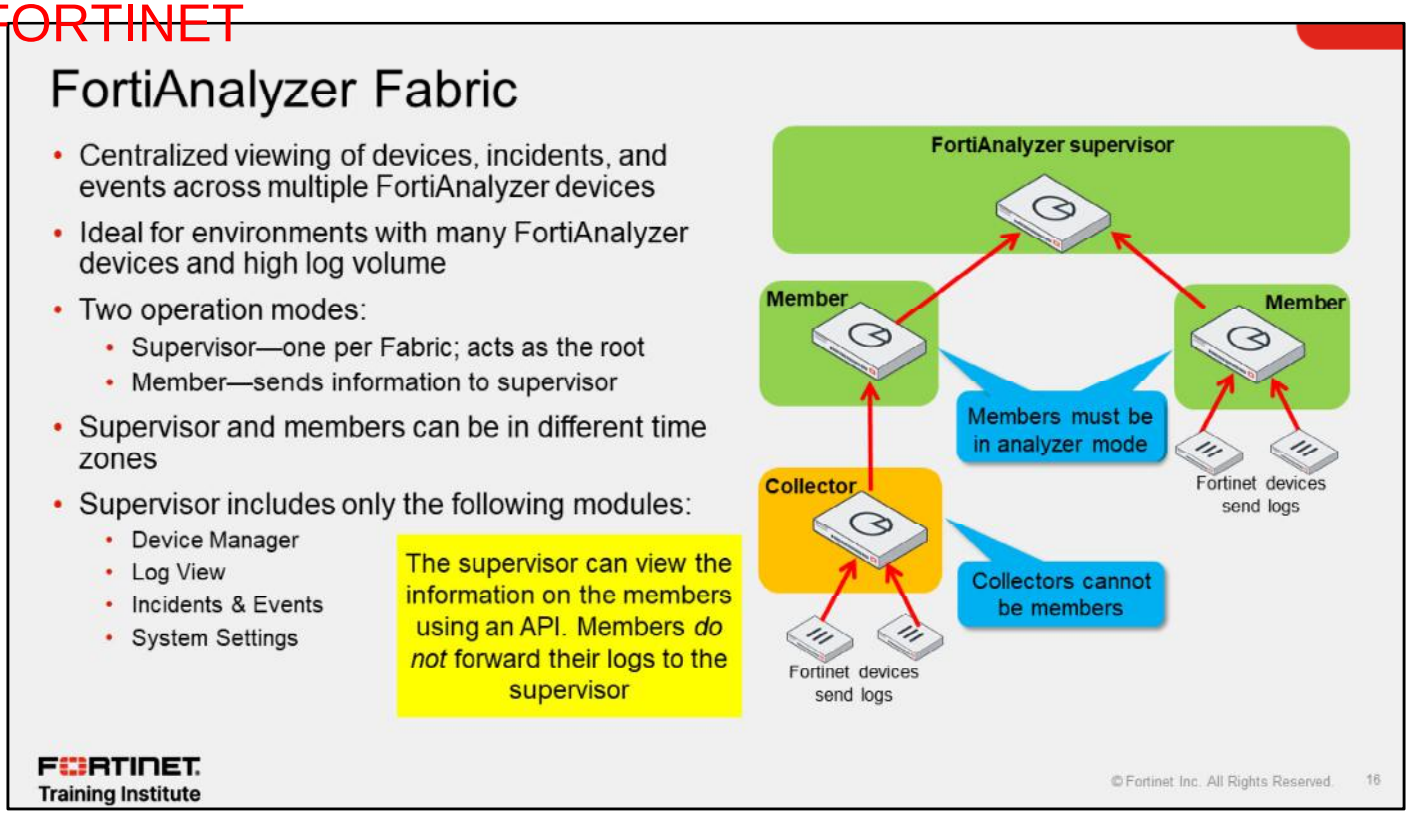
- FGT-A is installed between the corporate network and its ISP. It performs source network address translation (SNAT) on outbound communications for RFC-1918 hosts and web filtering for HTTP/HTTPS sessions.
- FGT-B is installed in the access layer, providing device detection, breach isolation, and basic denial-of-service (DoS) protection from the attached end-user LANs.
- FGT-C is installed in the data center, where it runs an intrusion prevention system (IPS) for all inbound communications to the servers behind it.

FGT-B receives all traffic from Client-1, which creates traffic logs for the initial session.

FGT-B forwards the web session to FGT-A, which doesn't duplicate the initial traffic log but generates a new traffic log because SNAT is applied to the session. Additionally, FGT-A applies a web filtering policy to this session and generates the relevant UTM logs, if appropriate.

FGT-B forwards the server message block (SMB) session to FGT-A, which does not duplicate the initial traffic log. FGT-A doesn't need to perform NAT or apply web filtering, so it forwards the traffic to FGT-C. FGT-C also does not generate a duplicate traffic log, but it performs IPS inspection based on its configuration. If a signature match triggers, it generates a log for that event.

FortiAnalyzer receives the various traffic and UTM logs and correlates them automatically to be linked for proper viewing, reporting, and automation actions.



The FortiAnalyzer Fabric enables centralized viewing of devices, incidents, and events across multiple FortiAnalyzer devices.

The FortiAnalyzer Fabric has two operation modes: supervisor and member.

Supervisors act as the root device in the FortiAnalyzer Fabric. SOC administrators can use the supervisor to view member devices and their ADOMs, authorized logging devices, and incidents and events created on members: the API syncs incident and event information from members to the supervisor.

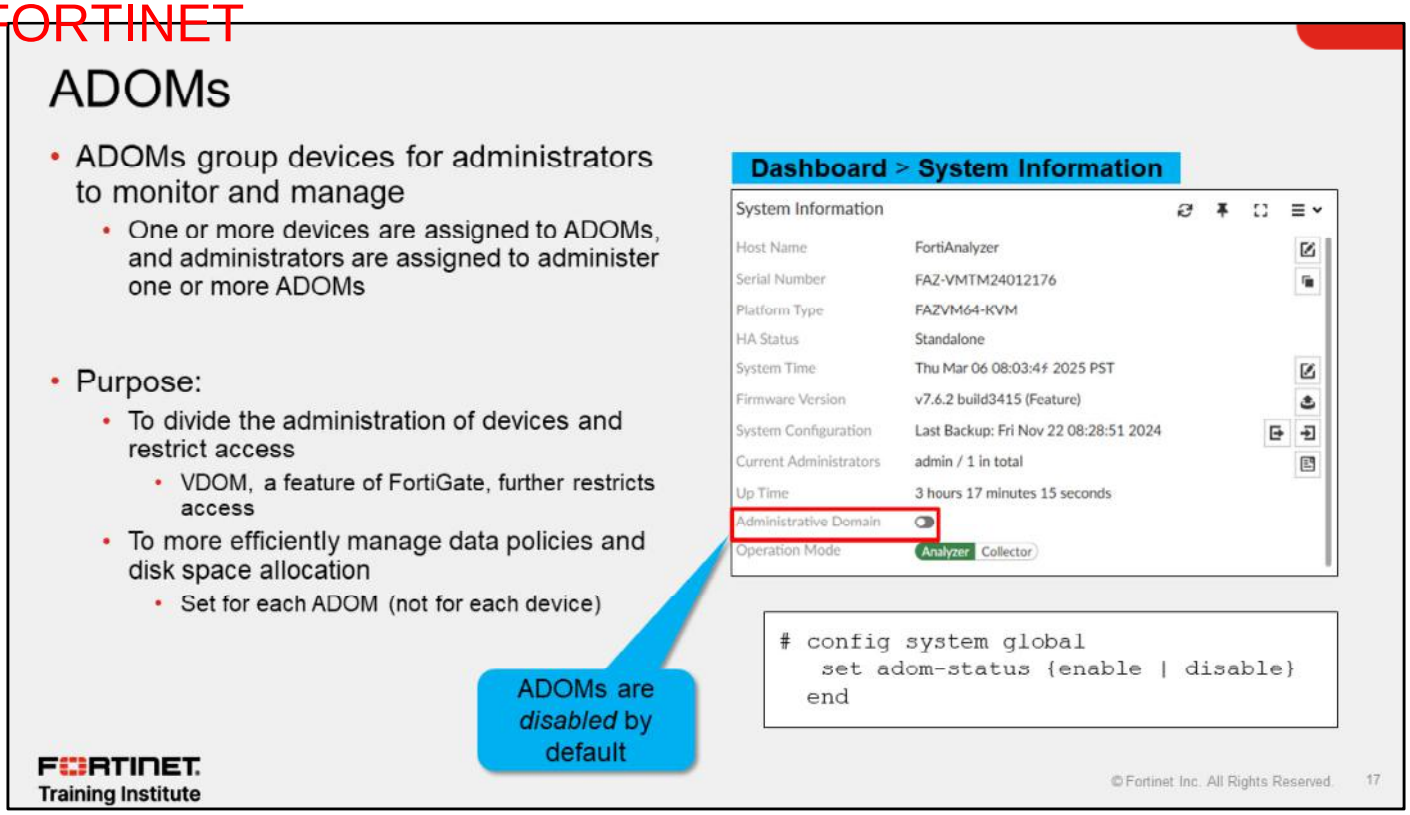
Members are devices in the FortiAnalyzer Fabric that send information to the supervisor for centralized viewing. When configured as members, FortiAnalyzer devices continue to have access to the FortiAnalyzer features identified in the *FortiAnalyzer Administration Guide*. Each member creates or raises incidents and events.

FortiAnalyzers configured with high availability (HA) can become members. However, HA is not supported by FortiAnalyzers acting as the Fabric supervisor.

All FortiAnalyzer Fabric members must be configured with the same time zone settings as the supervisor.

FortiAnalyzer can also join a FortiAnalyzer Fabric, which enables centralized viewing of devices, incidents, and events across multiple FortiAnalyzer devices acting as members.

The FortiAnalyzer Fabric is ideal for use in high-volume environments that consist of multiple FortiAnalyzer devices.



ADOMs allow you to group devices for monitoring and management. For example, administrators can manage devices grouped by geographical location or business division.

The purpose of ADOMs is to:
- Divide the administration of devices by ADOM and control (restrict) administrator access. If your network uses VDOMs, ADOMs can further limit access to data from the VDOM of a specific device.
- More efficiently manage data policies and disk space allocation, which are set for each ADOM.

ADOMs are disabled by default. You can configure ADOMs only using the default `administrator` account or any other administrator account with the superuser access profile. All Fortinet devices in a Fabric can be placed into an ADOM of the *Fabric* type, allowing for fast data processing and log correlation.

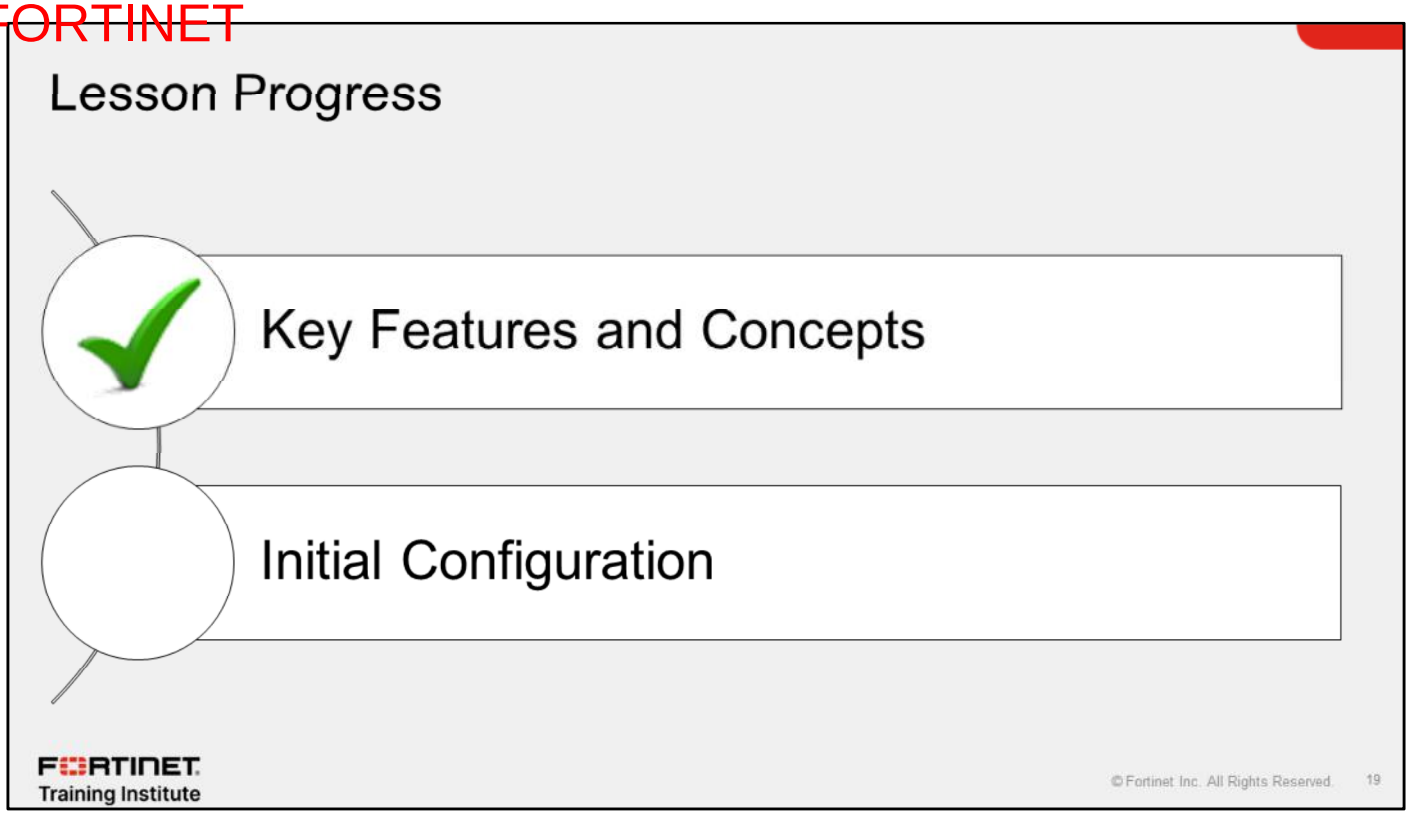
Knowledge Check

1. What is the default FortiAnalyzer operation mode?
   - ✓ A. Analyzer
   - B. Collector

2. Which FortiAnalyzer operating mode is used solely for the purpose of collecting logs from multiple devices and forwarding them to another device?
   - A. Analyzer
   - ✓ B. Collector

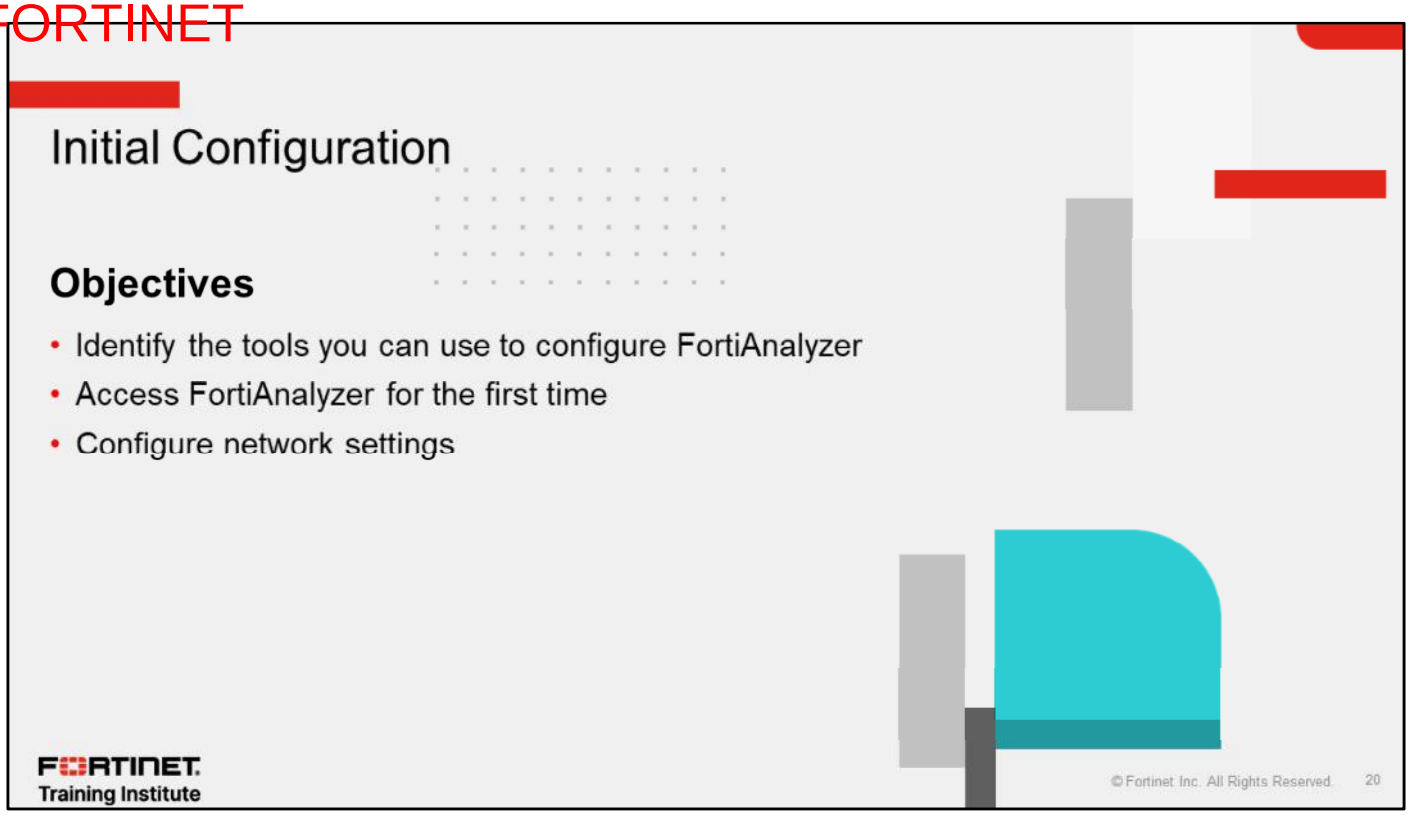
FORTINET Training Institute

 18



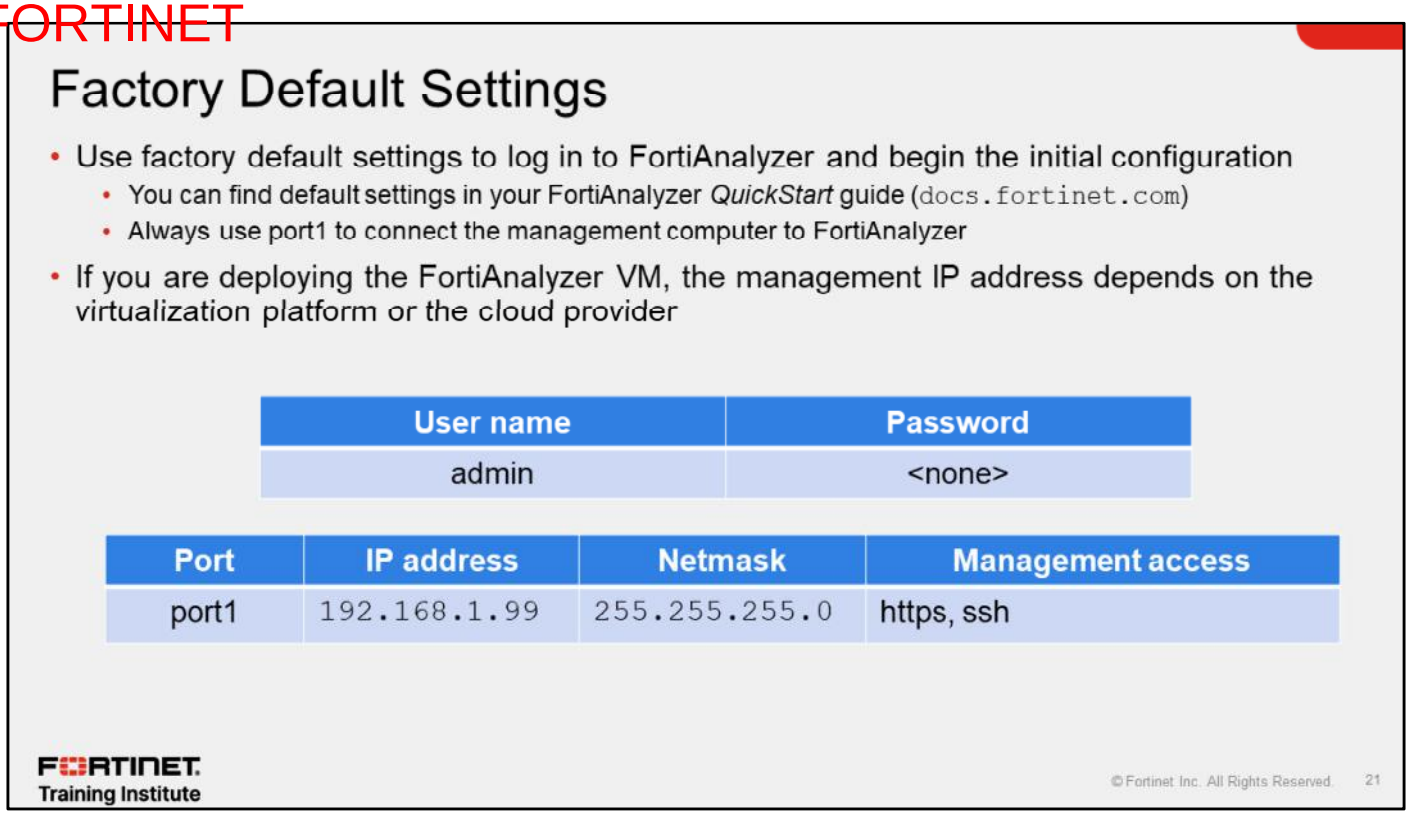
Good job! You now understand FortiAnalyzer key features and concepts.

Now, you will learn to perform the most common initial configurations on FortiAnalyzer.



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

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

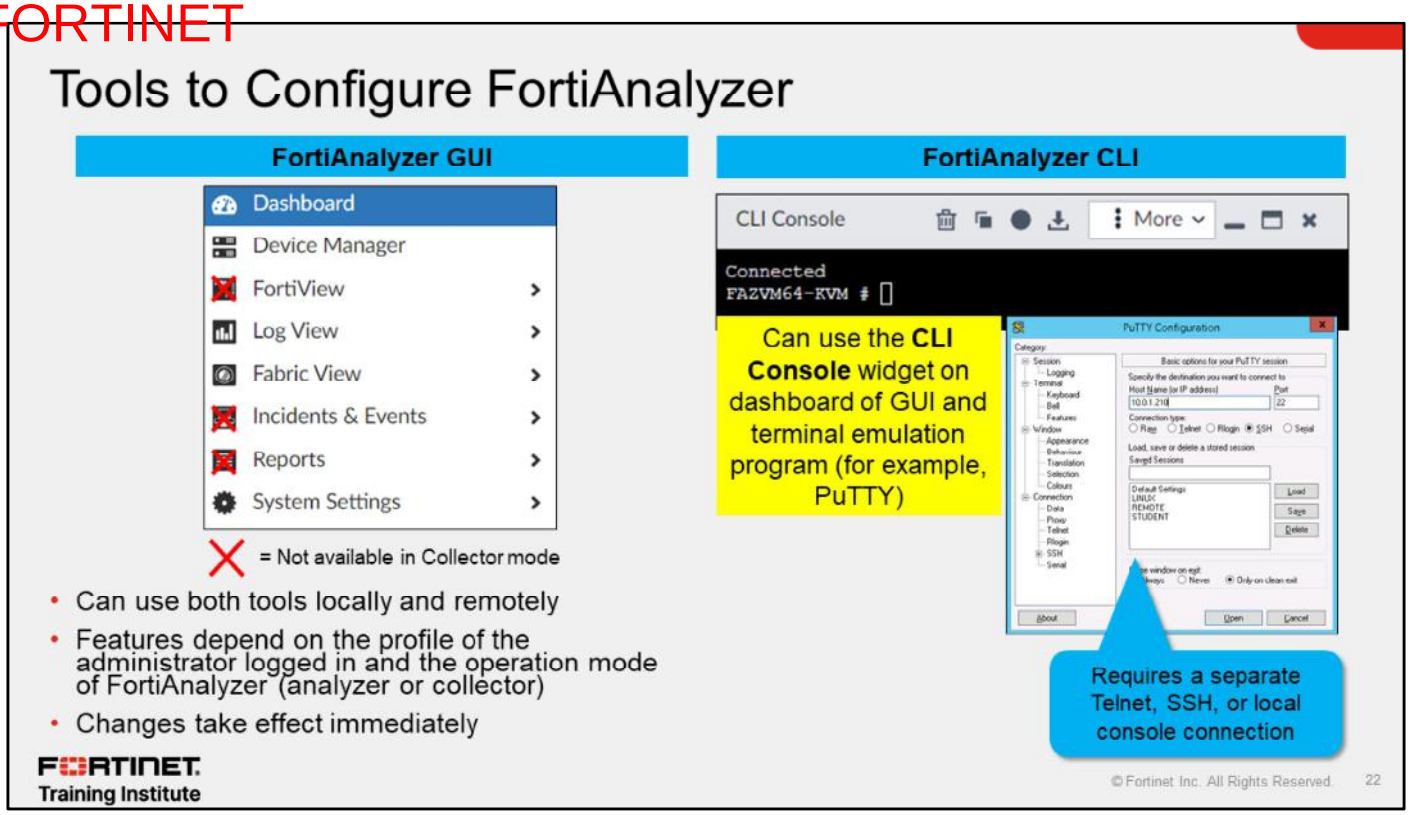


It is important to know the factory default settings, such as the default username and password, the port1 IP address, the netmask, and the default supported management access protocols, so you can initially connect to the management interface and configure FortiAnalyzer for your network.

The default settings are in the *FortiAnalyzer QuickStart Guide*, which is specific to your FortiAnalyzer model. Different FortiAnalyzer models have different port numbers, but port1 is the management port and always has the same default IP address.

If you deploy the FortiAnalyzer VM, the management IP address and its assignment depend on the virtualization platform. Visit `docs.fortinet.com` for more details.

To configure your management IP address on the CLI, use the `config system interface` command.



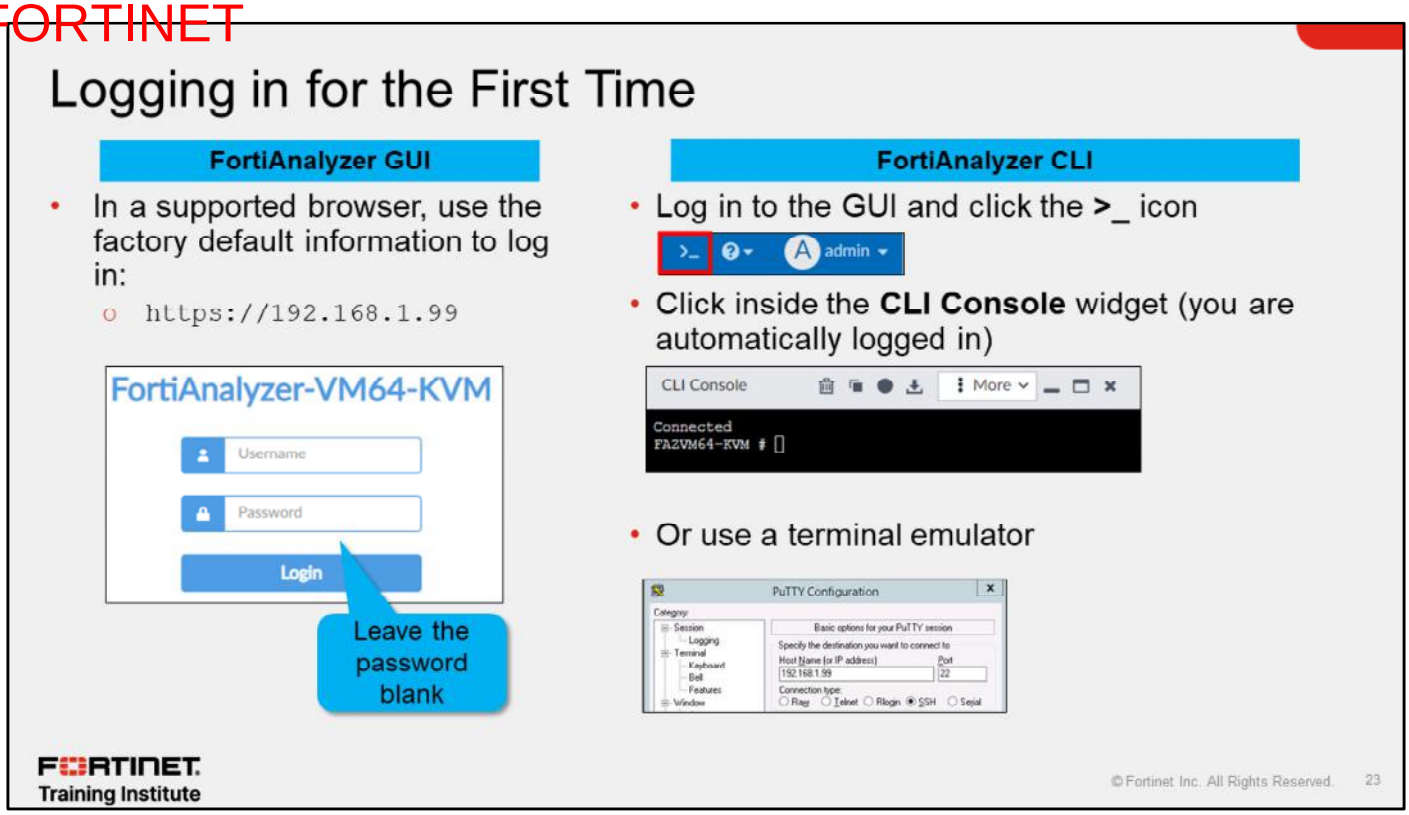
The GUI and CLI are the two tools you can use to configure and manage FortiAnalyzer. You can use both tools locally by connecting directly to FortiAnalyzer, or remotely, depending on your configuration settings. You can deny or permit access based on IP address.

When you use the CLI, you can execute commands through the **CLI Console** widget, available on the GUI dashboard, and through a terminal emulation application, such as PuTTY. Using PuTTY requires a separate Telnet, SSH, or local console (DB-9) connection.

The features accessible through the GUI and CLI depend on the administrator profile you are logged in with and the operational mode of FortiAnalyzer. For example, when in collector mode, the GUI does not offer access to **FortiView**, **Reports**, or **Incidents & Events**. Additionally, if you are logged in with the Standard_User or Restricted_User profiles, you will not have the same full access privileges that are available to the Super_User profile. The CLI also includes some settings that are not accessible through the GUI.

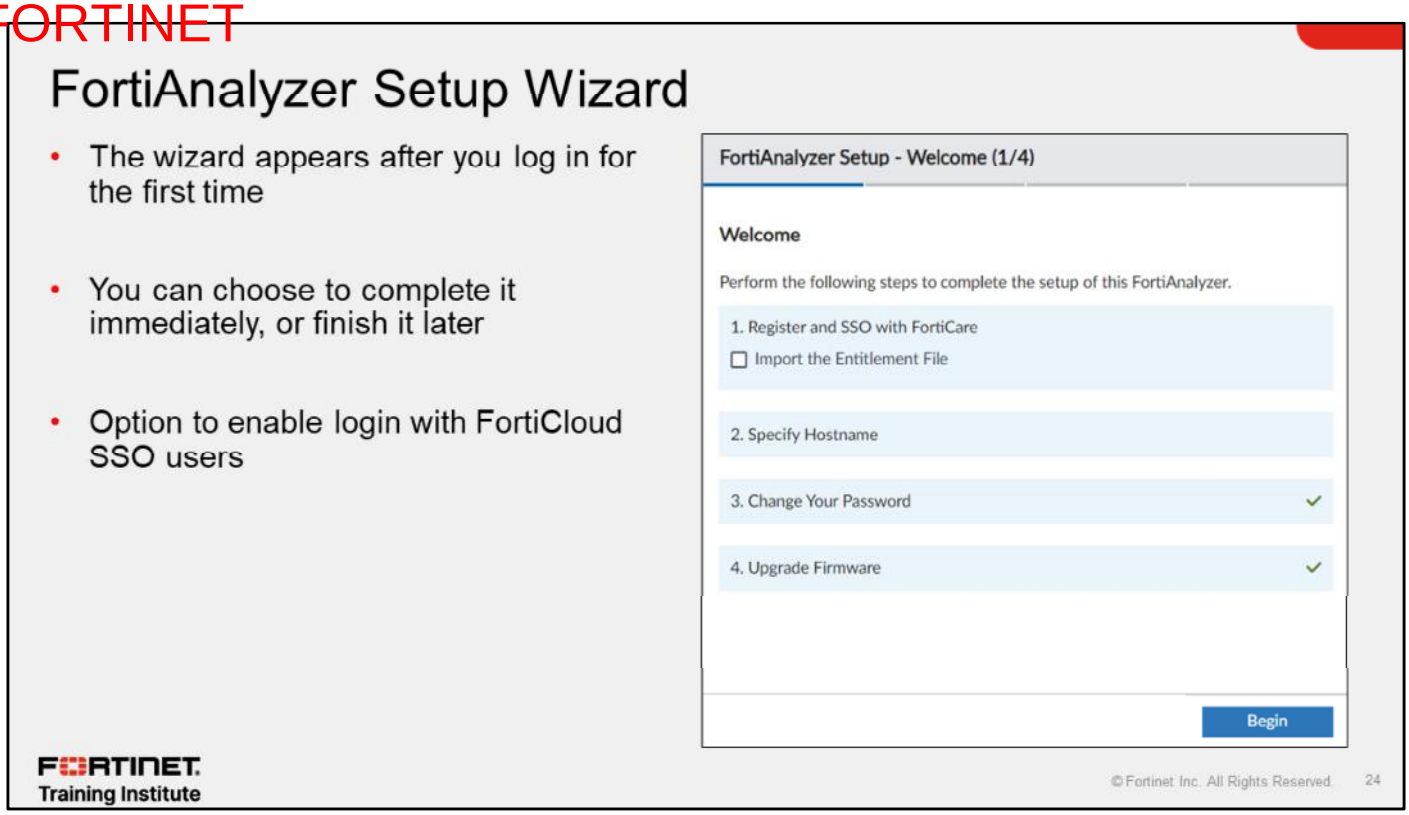
Any configuration changes you make using the GUI or CLI take effect immediately upon applying the settings, without the need to reset the FortiAnalyzer system or interrupt services.

Note that the SQL database is disabled, by default, when FortiAnalyzer is in collector mode, so logs that require the SQL database are not available in collector mode unless the SQL database is enabled through the CLI.



To log in to the FortiAnalyzer GUI for the first time, open a browser and enter the URL `https://` followed by <`the management IP address`>. After the login screen opens, use the factory default administrator credentials to log in: Type the username `admin` (in lowercase) and leave the password field empty.

To log in to the CLI for the first time, you can use one of two methods:
- Integrated CLI console: Log in to the GUI and click the CLI icon in the upper-right corner. You are automatically logged in to the console.
- Terminal emulation application (such as PuTTY): Enter the FortiAnalyzer port1 IP address and select a supported management access protocol, such as SSH. When connected and prompted to log in, use the factory default administrator credentials.

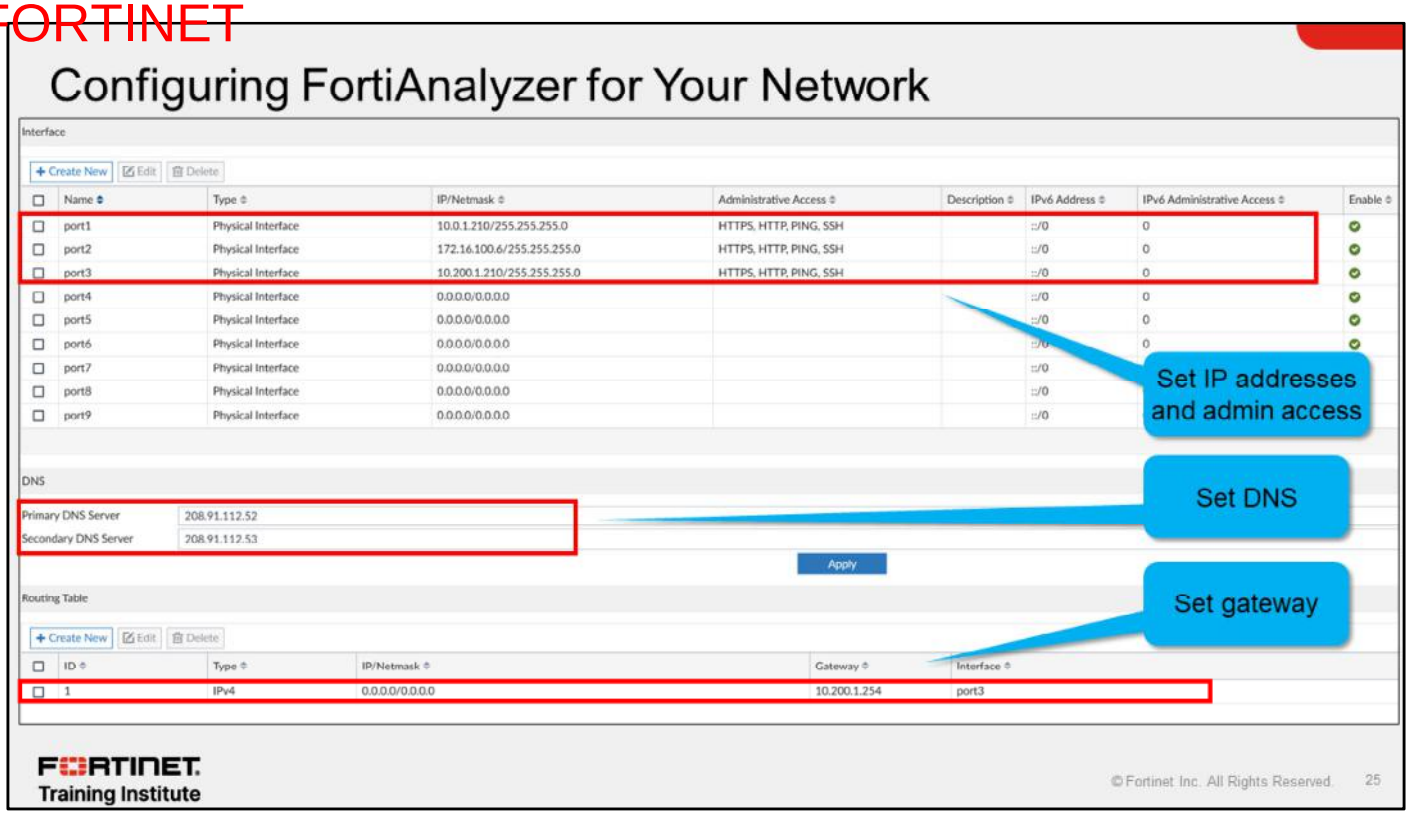


The **FortiAnalyzer Setup** wizard appears after you log in for the first time.

You can use it to register your FortiAnalyzer device with FortiCare, enable SSO with FortiCloud, change the default password, set the correct time zone, and set the device hostname.

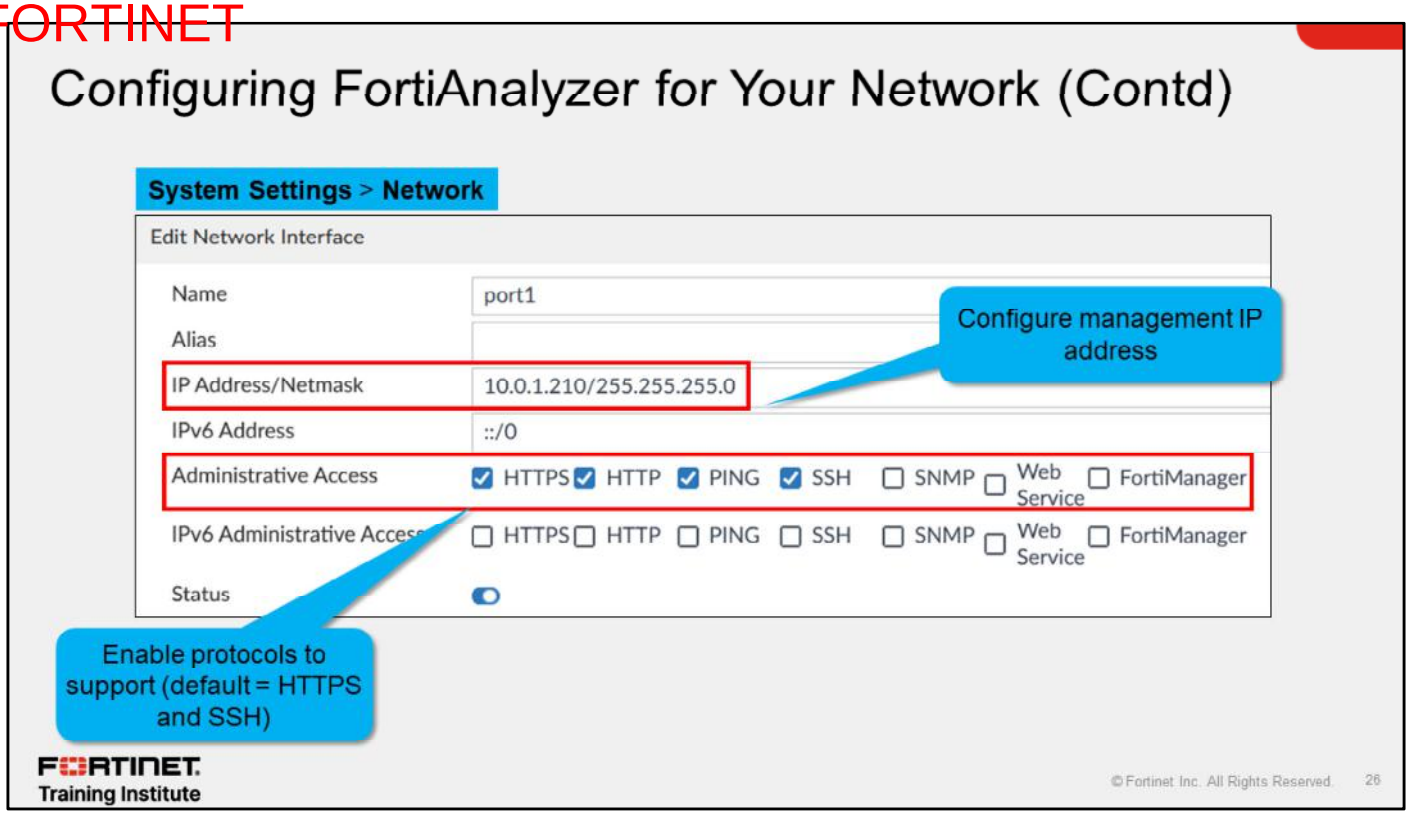
For air-gap environments where the FortiAnalyzer has no direct internet access to contact FortiGuard, you can obtain an entitlement file by contacting Fortinet Customer Service.

You can choose to complete all or some of the steps now or later. A green check mark is displayed beside each completed step.



The initial configuration of FortiAnalyzer is very similar to the initial configuration of FortiGate.

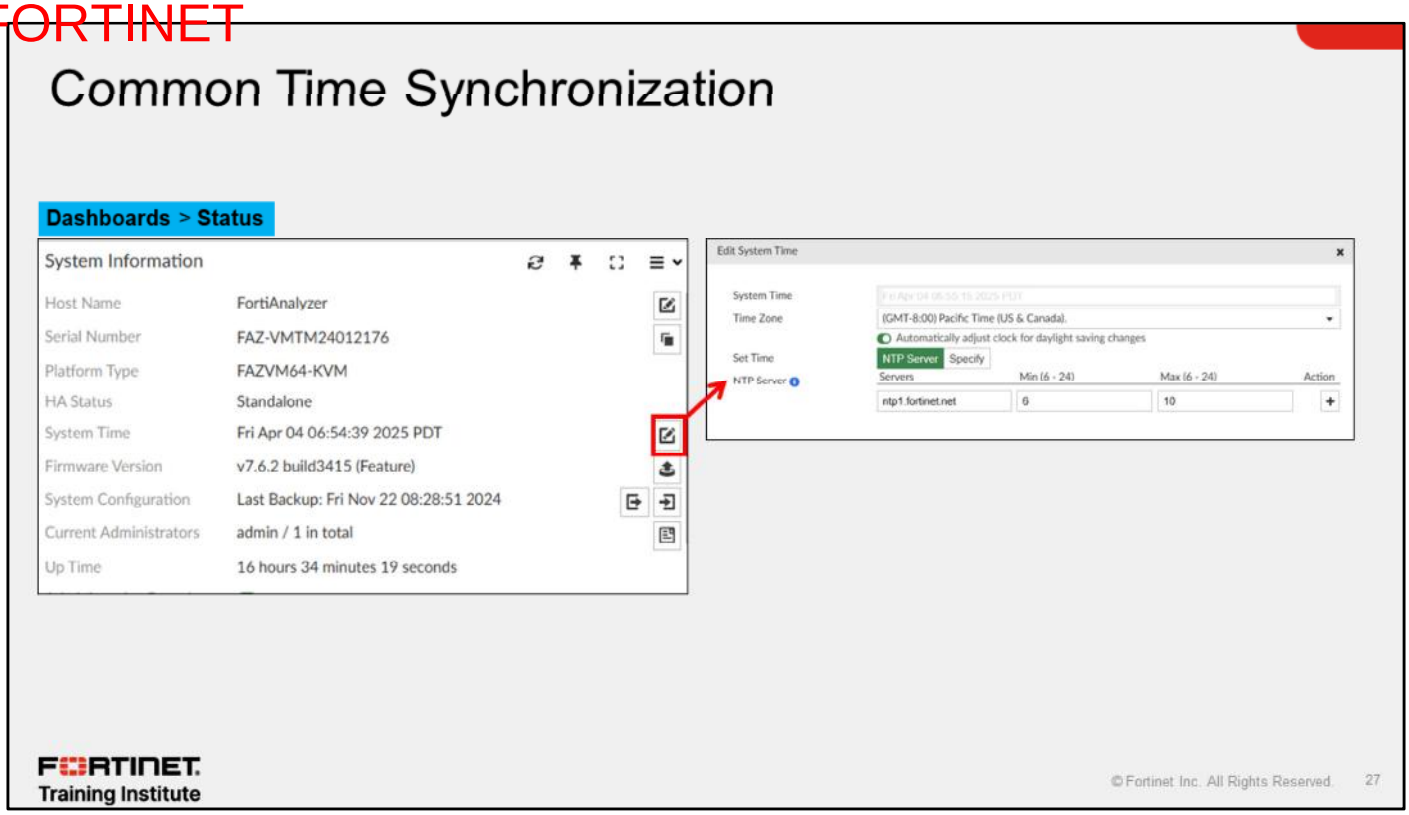
To configure FortiAnalyzer for your network, you must set the IP address and netmask, select supported administrative access protocols, and specify a default gateway for routing packets. You can also specify a primary and a secondary DNS server. You can do all this on the **Network** page.



Setting your own IP address and netmask provides more security than using the default address. If more than one FortiAnalyzer device is in the same network, different network settings are mandatory. The management interface must have a dedicated (unique) address. You should be careful if you need to change the management IP address because you will lose access to FortiAnalyzer unless you have another interface with administrative access enabled.

There are a few nonstandard administrative access protocols that are worth mentioning as well:

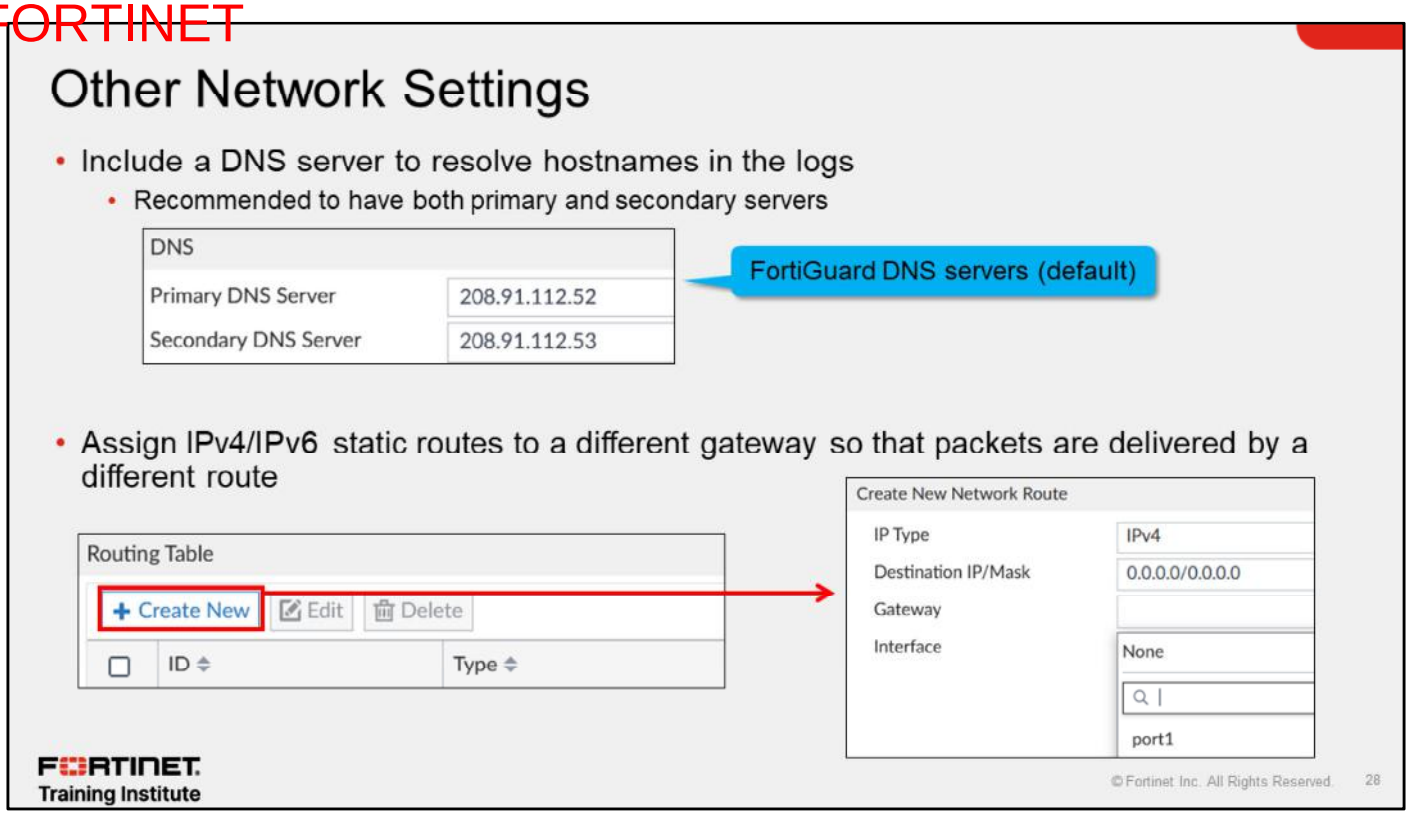
- Web Service: Allows access to the FortiAnalyzer API using Simple Object Access Protocol (SOAP) on port 8080
- FortiManager: Allows FortiManager central-management access



Accurate time information is crucial, especially when investigating security incidents. Any investigation into new incidents must be traced back to when that incident was first seen by the device and when the log was received by FortiAnalyzer. To make sure this information is determined precisely, the clock must be accurate; otherwise, it will be difficult to determine how far this malware has spread.

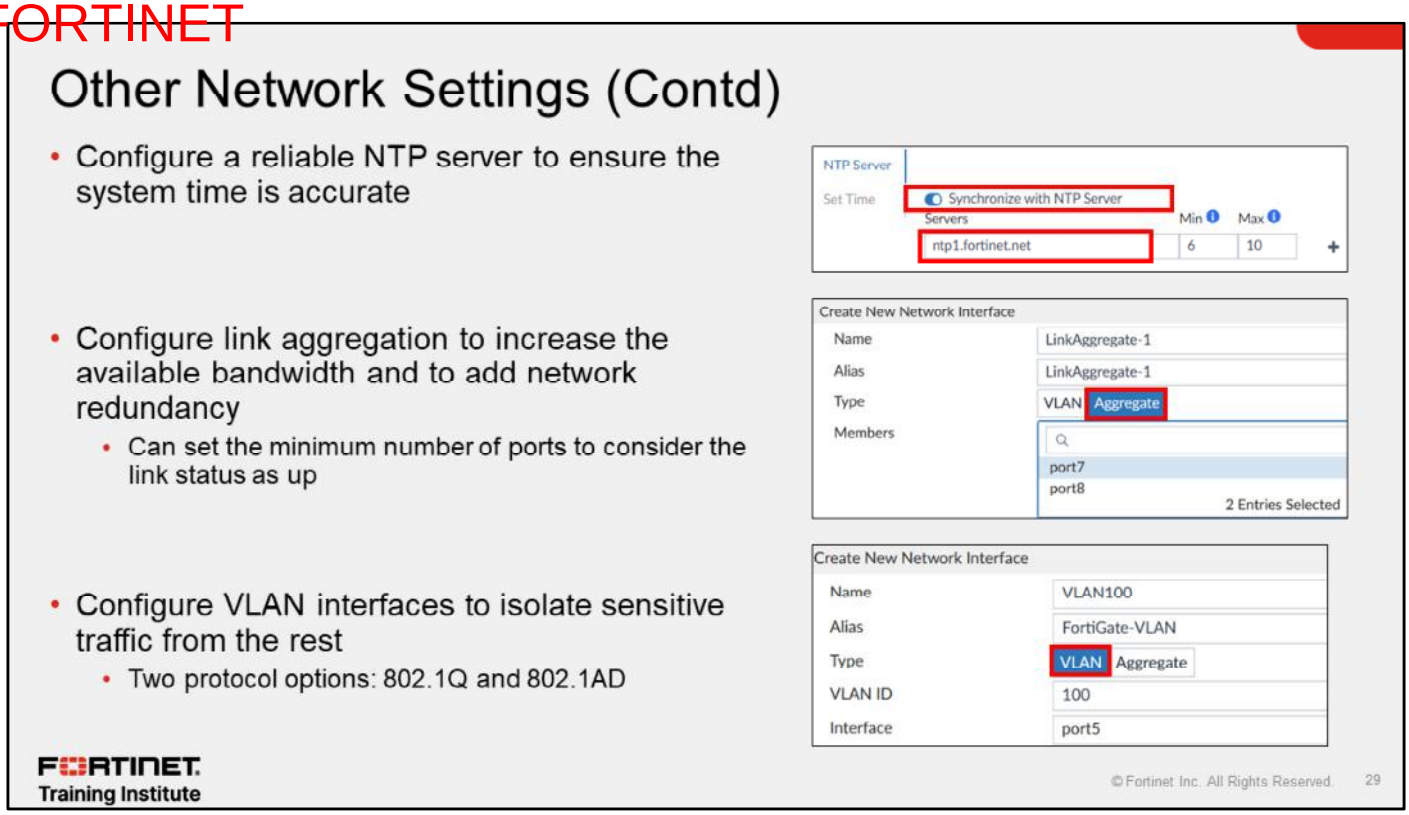
Many FortiAnalyzer features require an accurate system time to work correctly. It is highly recommended that the system time be synchronized with a reliable NTP server. This can be done under the **System Information** widget included on the default dashboard.

To make incident response easier (or perhaps even possible), it is important to ensure that all network devices have their clocks set accurately. For best results, synchronize your devices to the same NTP server.



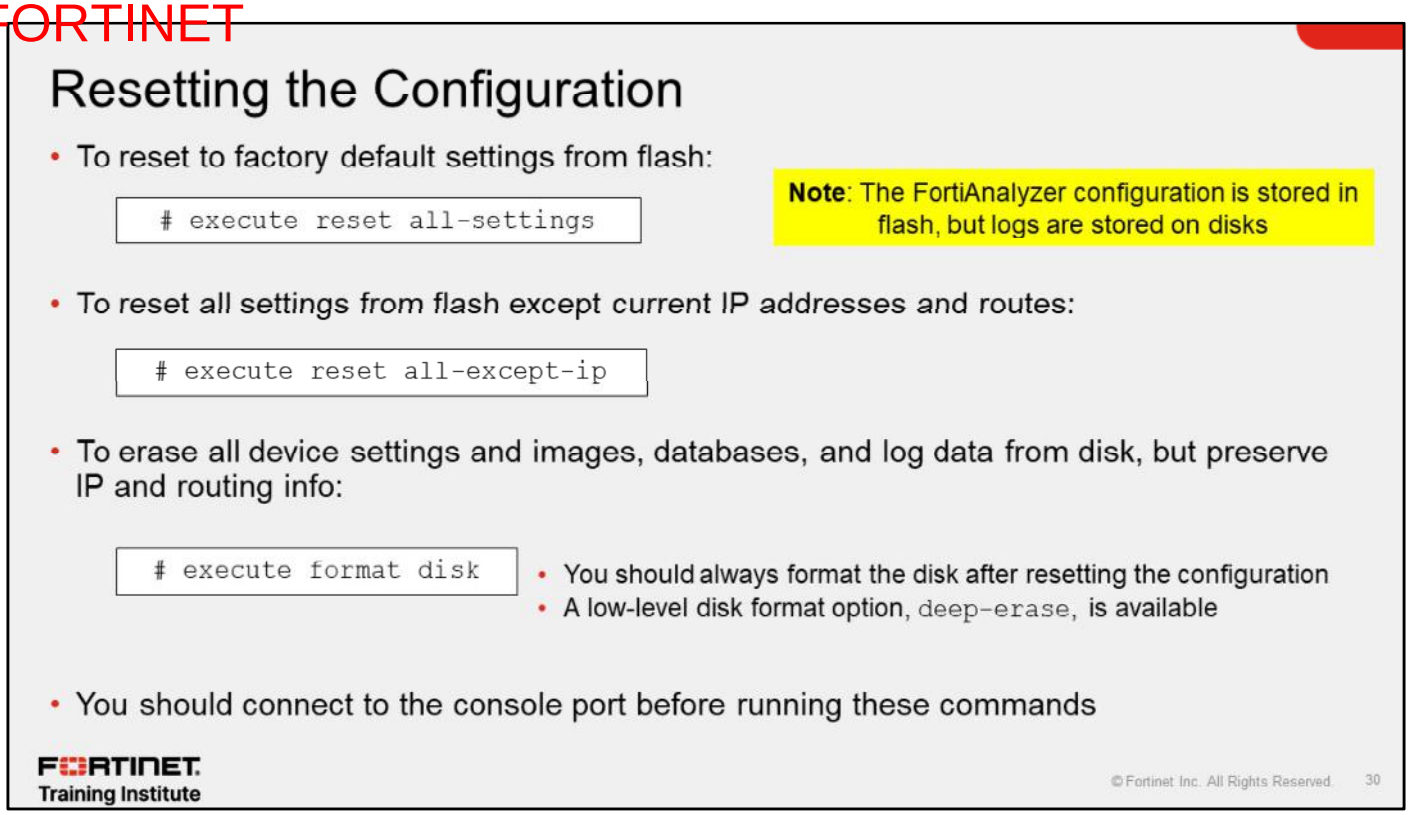
If you want to resolve host names in the logs, you need a DNS server. The default primary and secondary DNS server addresses are the FortiGuard DNS servers. You can use these addresses or change them to other servers, including your internal DNS servers. It is a best practice to have both a primary and a secondary server. Furthermore, response times are a consideration for DNS, so choose DNS servers that are as close as possible to your network.

If you want to configure another port on FortiAnalyzer, you can assign specific IPv4 or IPv6 static routes to a different gateway so that a different route delivers packets.



You can configure one or more aggregate links to increase the bandwidth available to receive logs and add network redundancy to FortiAnalyzer. These logical links combine two or more physical interfaces, effectively combining their bandwidth. Additionally, these links will remain active if there is at least one working physical interface, adding network redundancy to your device.

VLANs isolate different types of traffic in your network. This adds security and, if needed, allows the application of different policies or priorities to that traffic. You can configure VLAN interfaces on FortiAnalyzer to use the existing VLANs in your environment. FortiAnalyzer supports both IEEE 802.1Q and 802.1AD protocols.



If you need to reset your configuration, you can use these commands:

- The `execute reset all-settings` command erases the show configuration on flash, which contains the IP addresses and routes, while the `execute reset all-except-ip` command leaves the settings for IP addresses and routes.
- The `execute format disk` command erases all device settings, images, databases, and log data while preserving the IP addresses and routing info. You should always run this command after resetting the configuration.
- If your environment requires it, you can use the `execute format disk deep-erase` command to perform a low-level format of the disk one or more times. FortiAnalyzer will overwrite the hard disk with random data to ensure that data cannot be recovered. Remember that this process can take a very long time, even days, depending on the size of the disk and the number of rounds you specify.

It is a best practice to run these commands while connected directly using the console port to avoid losing access after resetting the configuration.

Basic CLI Commands for System and Network Settings

- Use the following FortiAnalyzer CLI commands to examine or troubleshoot system and network settings:

Command	Information displayed
`get system status`	General status of your FortiAnalyzer device
`get system interface`	Network interfaces configuration, such as port status, speed, and associated IP address
`show system dns`	Configured DNS server addresses
`show system ntp`	Time setting using a network time protocol (NTP) server
`show system route`	Configured static routes entries
`execute ping <remote>`	Tests connectivity between FortiAnalyzer and another network device

- Example:

```
FAZVM64-KVM # get system interface
== [ port1 ]
name: port1    status: disable   ip: 10.0.1.210   255.255.255.0   speed: auto
== [ port2 ]
name: port2    status: enable    ip: 172.16.100.6 255.255.255.0   speed: auto
```

FORTINET Training Institute

 31

You can use the CLI commands shown on this slide to examine or troubleshoot system and network settings on FortiAnalyzer.

In general, the first word of a command indicates what you are trying to achieve in the CLI:
- The `get` commands allow you to view information in a more readable format.
- The `show` commands allow you to view the exact CLI configuration for that section, including the correct indentation.
- The `execute` commands allow you to perform a function in FortiAnalyzer.

You can type a question mark (`?`) to view available syntax options. You can also use the `Tab` key to autocomplete your command or cycle through possible commands.

Viewing Server Information

- Use these commands to view system information:

Command	Information displayed
`diagnose system ntp status`	NTP server information, such as IP address, stratum, poll time, latency, and so on
`diagnose system print cpuinfo`	CPU information, such as vendor ID, CPU family, model, stepping, CPU MHz, cache size, physical ID, cores, and many more
`diagnose system print df`	File system disk space details, such as file system, 1K-blocks, used and available space, percent used, mount directories
`diagnose system print hosts`	Static table lookup for host names
`diagnose system print netstat`	Network statistics for active connections including protocol, local address, foreign address, and state
`diagnose system print route`	Complete routing table, including directly connected routes

- Example:

```
FAZVM64-KVM # diagnose system print route
Destination     Gateway         Genmask         Flags Metric Ref Use   Iface
10.0.1.0        0.0.0.0         255.255.255.0   U     0      0   0     port1
10.200.1.0      0.0.0.0         255.255.255.0   U     0      0   0     port3
10.200.3.0      10.200.1.254    255.255.255.0   UG    1      0   0     port3
172.16.100.0    0.0.0.0         255.255.255.0   U     0      0   0     port2
```

FORTINET Training Institute

 32

To access and view detailed system-related information, use the `diagnose system` commands.

For a complete list of arguments, refer to the *FortiAnalyzer CLI Reference*, which you can obtain from `docs.fortinet.com`.

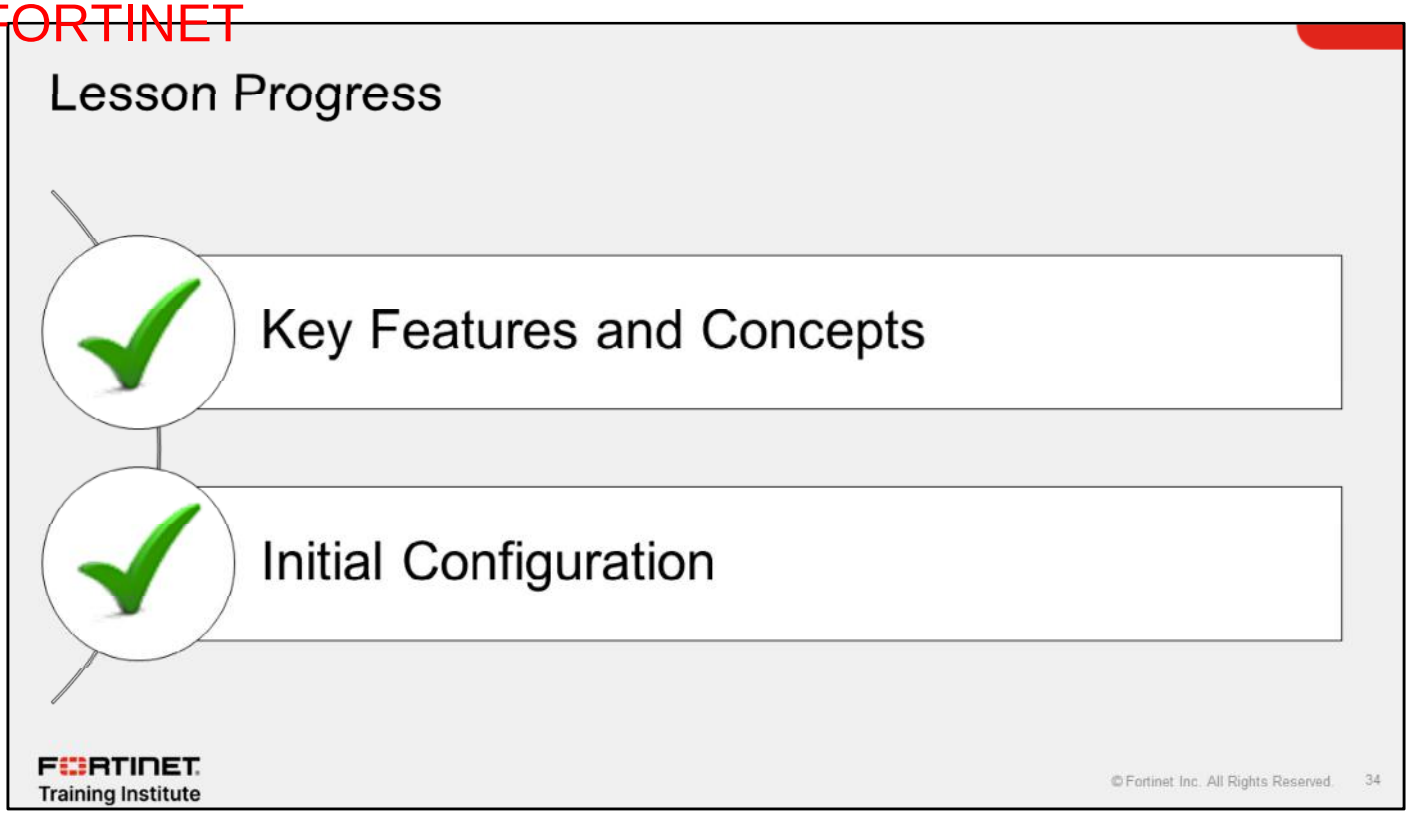
Knowledge Check

1. What is the purpose of configuring NTP on FortiAnalyzer?
   - A. To increase the available bandwidth
   - ✓ B. To have a reliable system time

2. What should you always do after erasing the configuration from flash memory?
   - ✓ A. Run the `execute format disk` command.
   - B. Run the `execute reset all-settings` command.

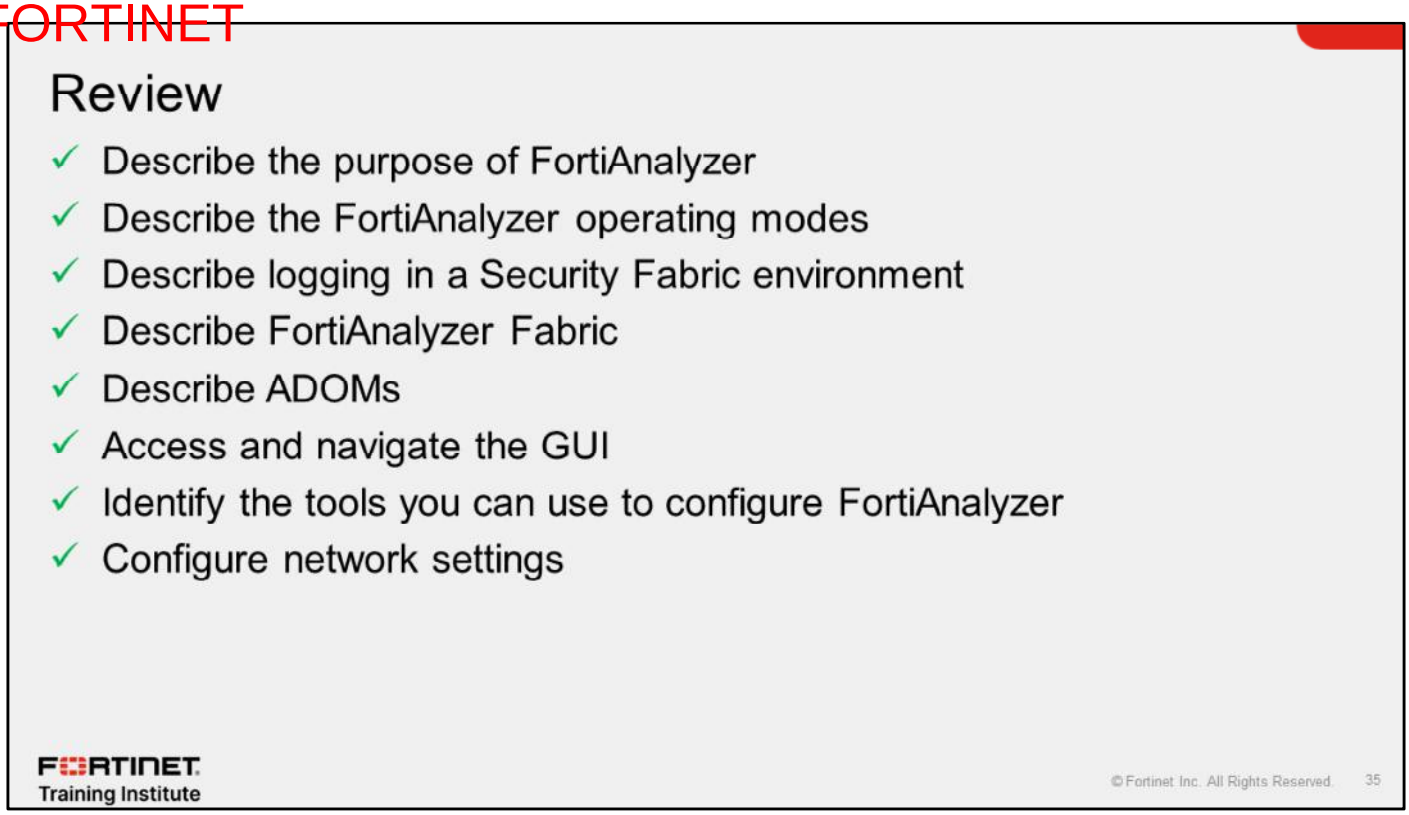
FORTINET Training Institute

 33



Congratulations! You have completed this lesson.

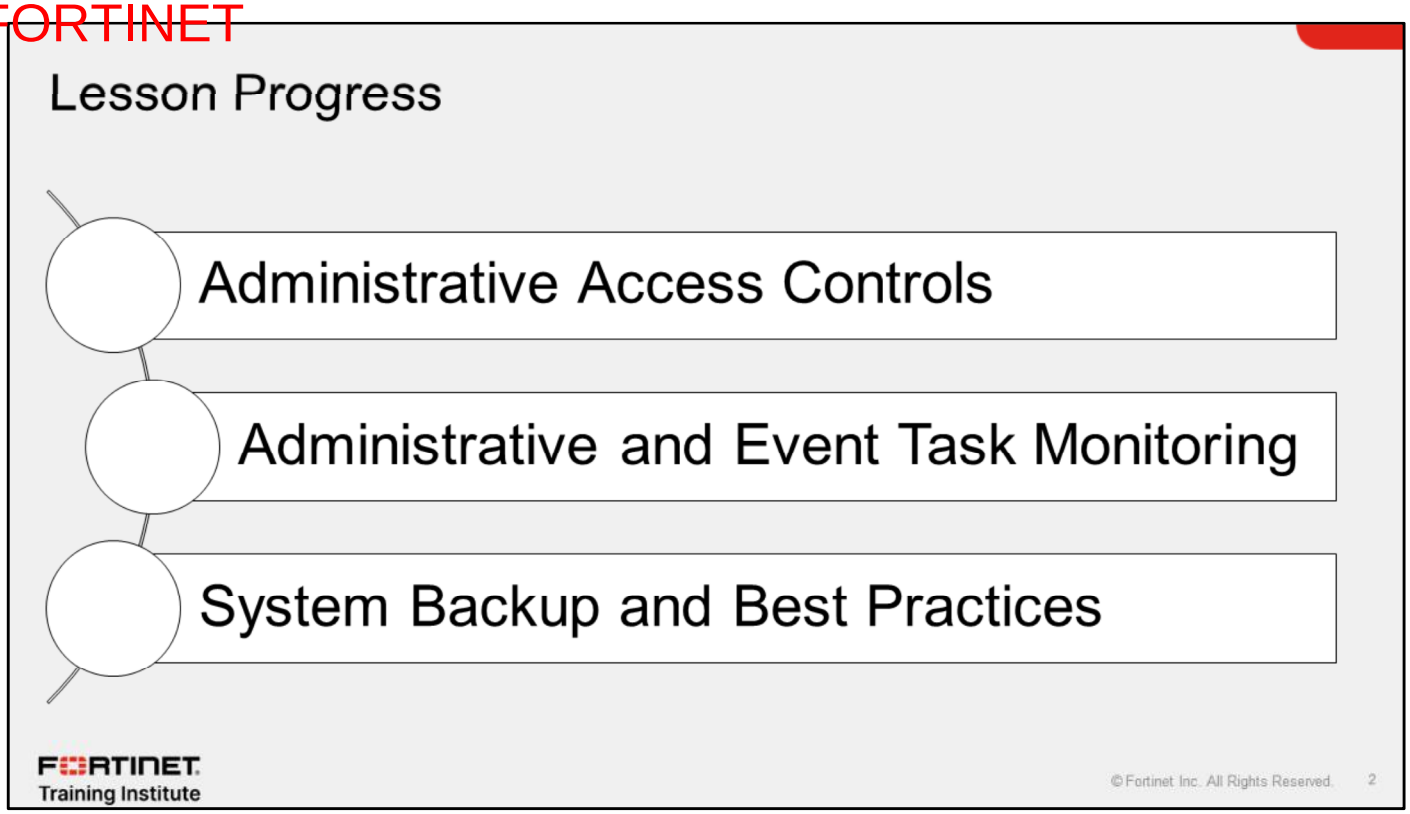
Now, you will review the objectives that you covered in this lesson.



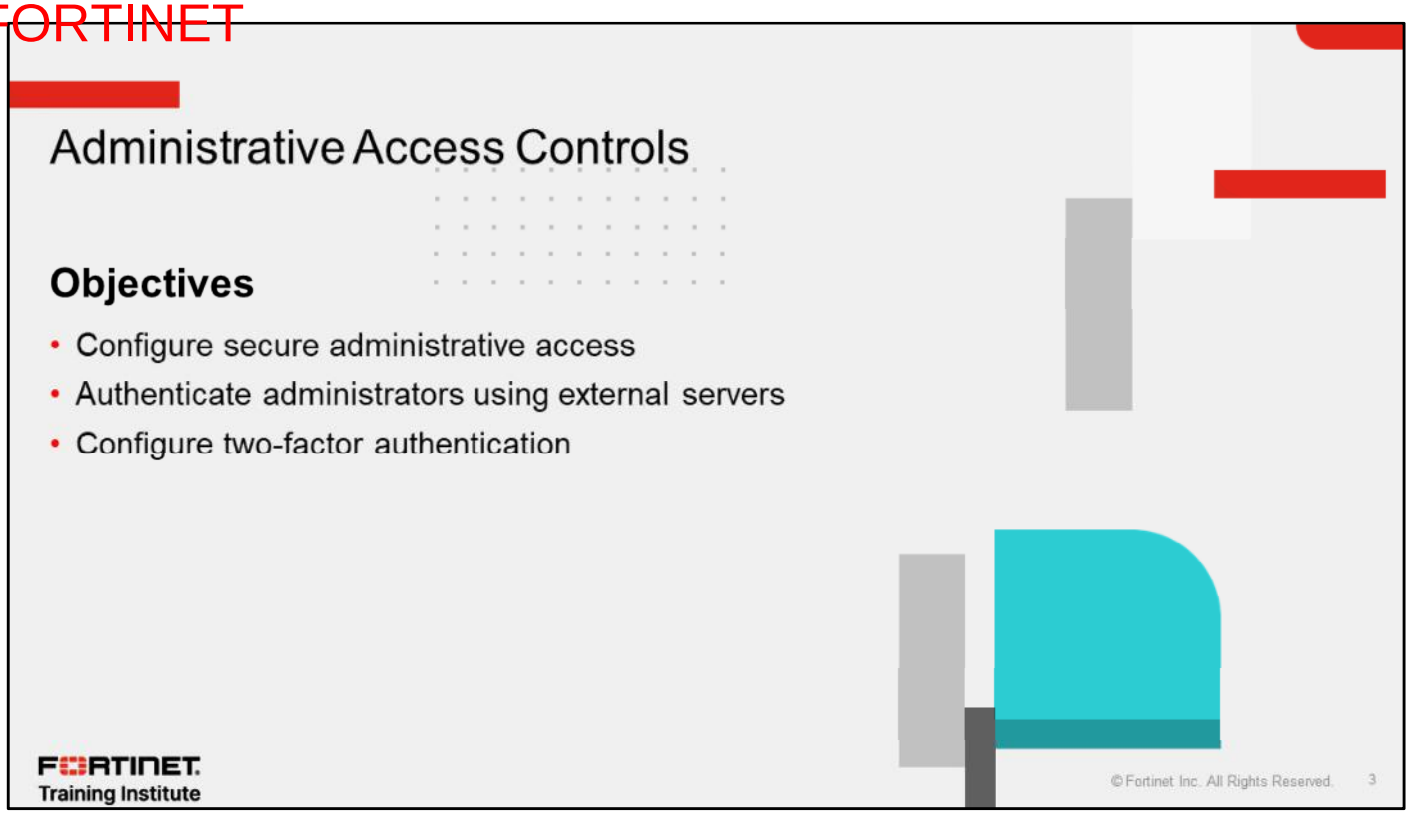
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about FortiAnalyzer key features and concepts and how to configure FortiAnalyzer.

In this lesson, you will learn administration and management functions you can use to protect FortiAnalyzer—and the sensitive log data it stores—from external or internal threats.

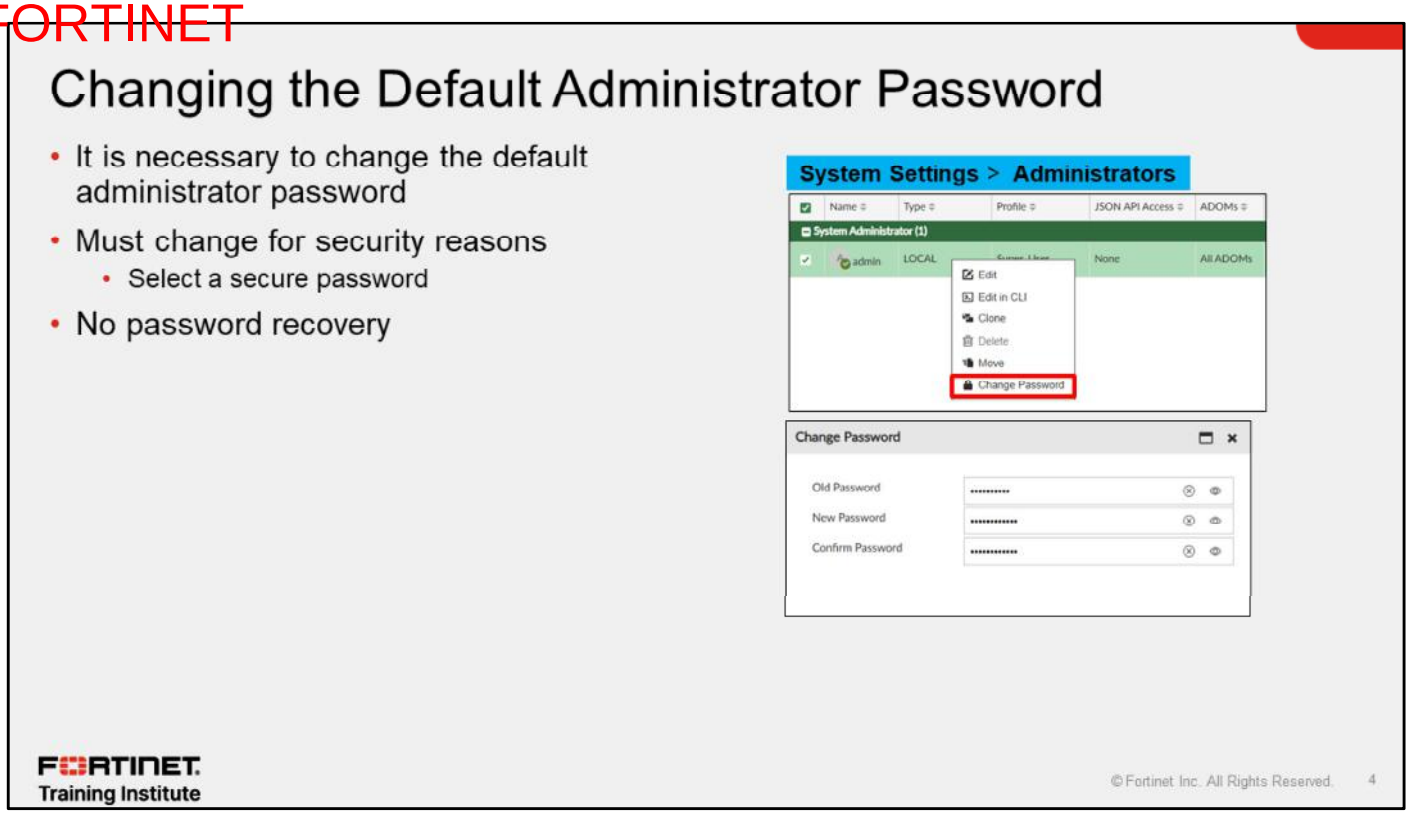


In this lesson, you will learn about the topics shown on this slide.



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

By demonstrating competence in using administrative access controls, you will be able to better safeguard the administration of your FortiAnalyzer device and the sensitive data it collects.

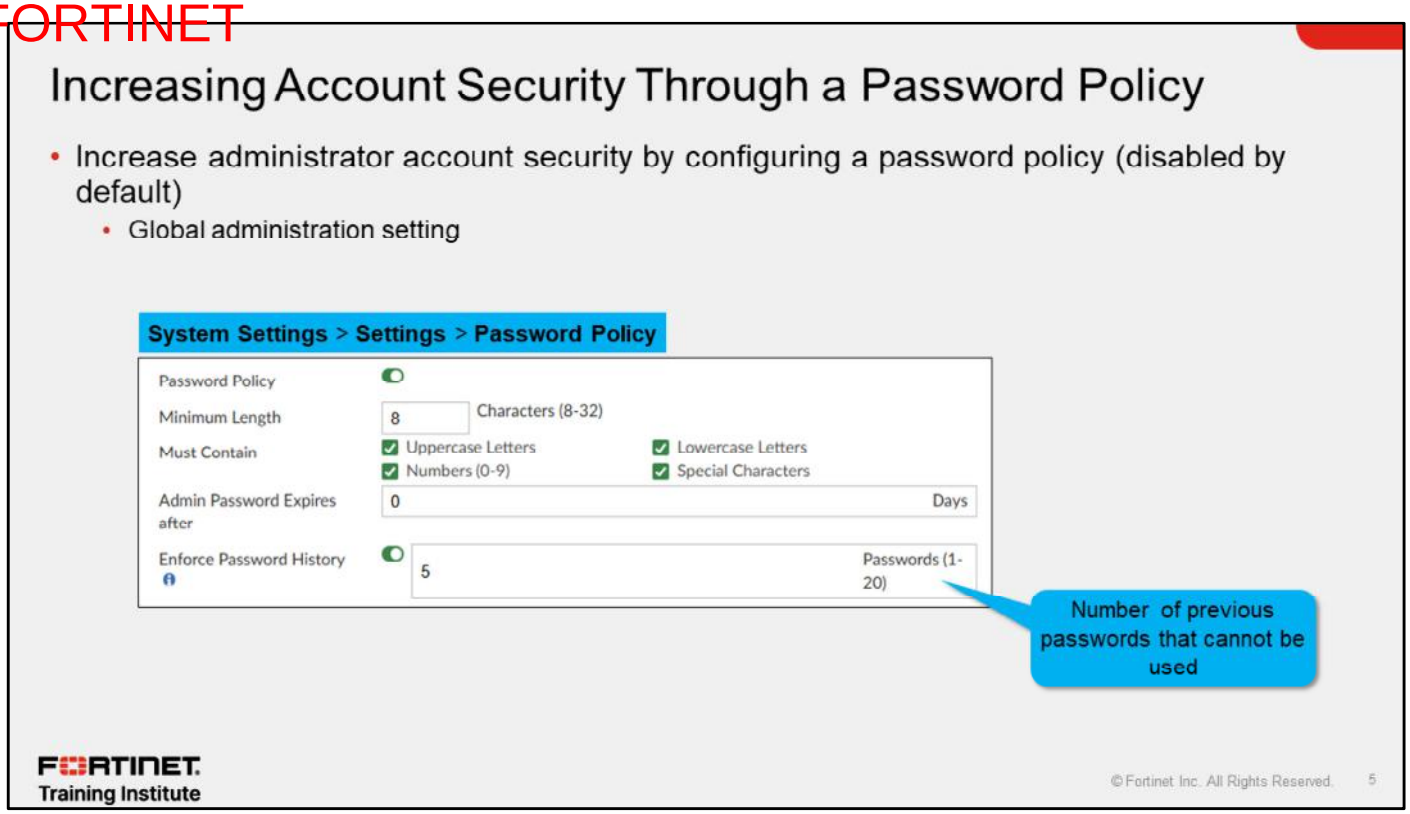


For security reasons, one of the first tasks you should perform is to change the default `administrator` password. Fortinet recommends that you make this change through the Setup Wizard. You can change it anytime on the **Administrators** page, as shown on this slide. Always use a secure, strong password.

Be aware that there is no password recovery option for FortiAnalyzer! If you forget your password and lose access to FortiAnalyzer, one option is to use the `execute migrate` command, which allows you to load a backup of the configuration. Follow these steps:

1. Perform a factory reset on the VM or device.
2. Run the `execute migrate` command.
3. Use the default `administrator` account and password. System settings are not restored.

The other option is to format the flash drive and reload the image from the BIOS configuration menu. This erases the system settings, including the administrative accounts. So, make sure you remember your password or store it in a secure location.

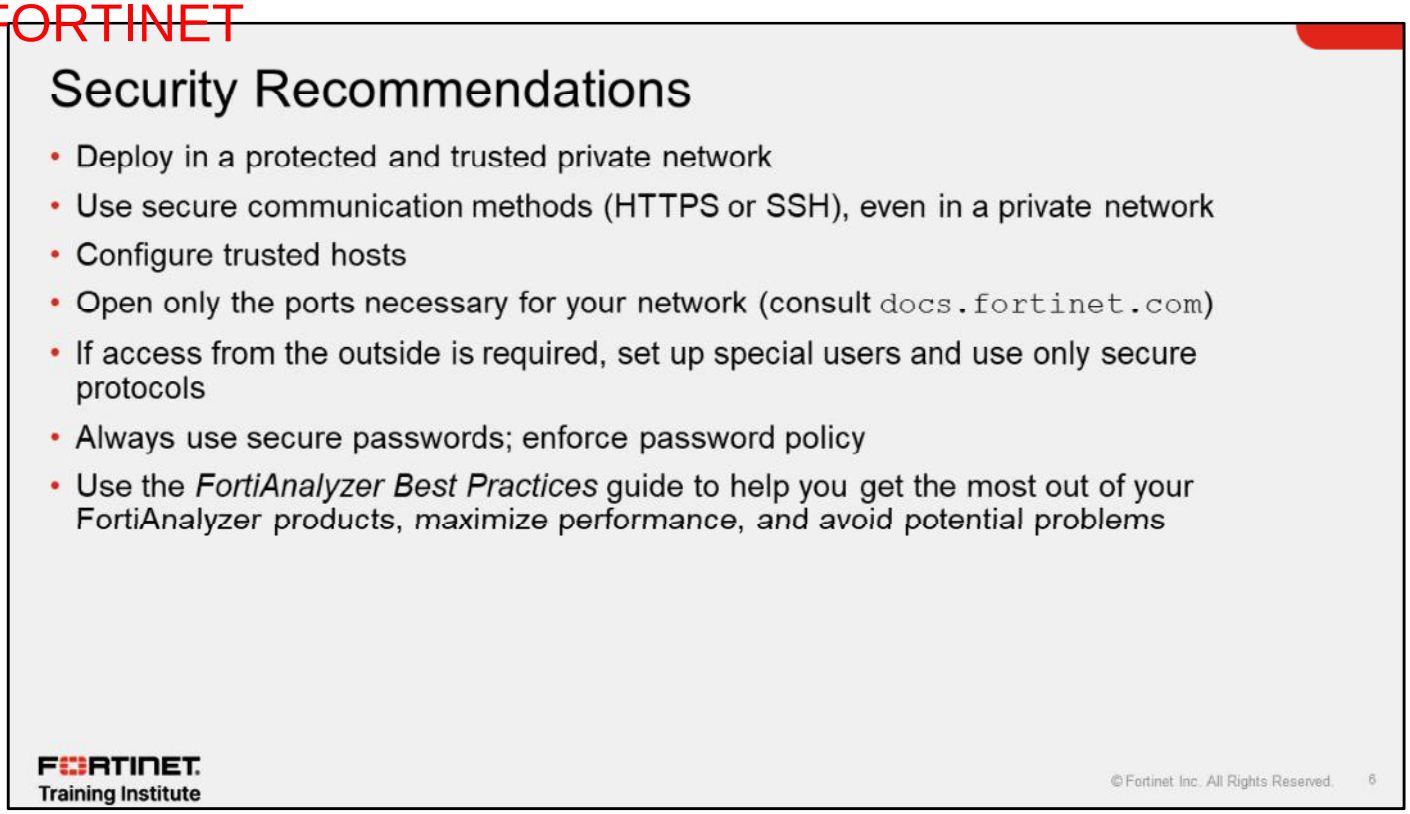


You can increase the security of your administrator accounts by configuring a global password policy for all administrators on the **Admin Settings** page. By default, the password policy is disabled.

A password policy allows you to set a minimum password length, specify if characters or numbers must be included, and specify the number of days a password remains valid.

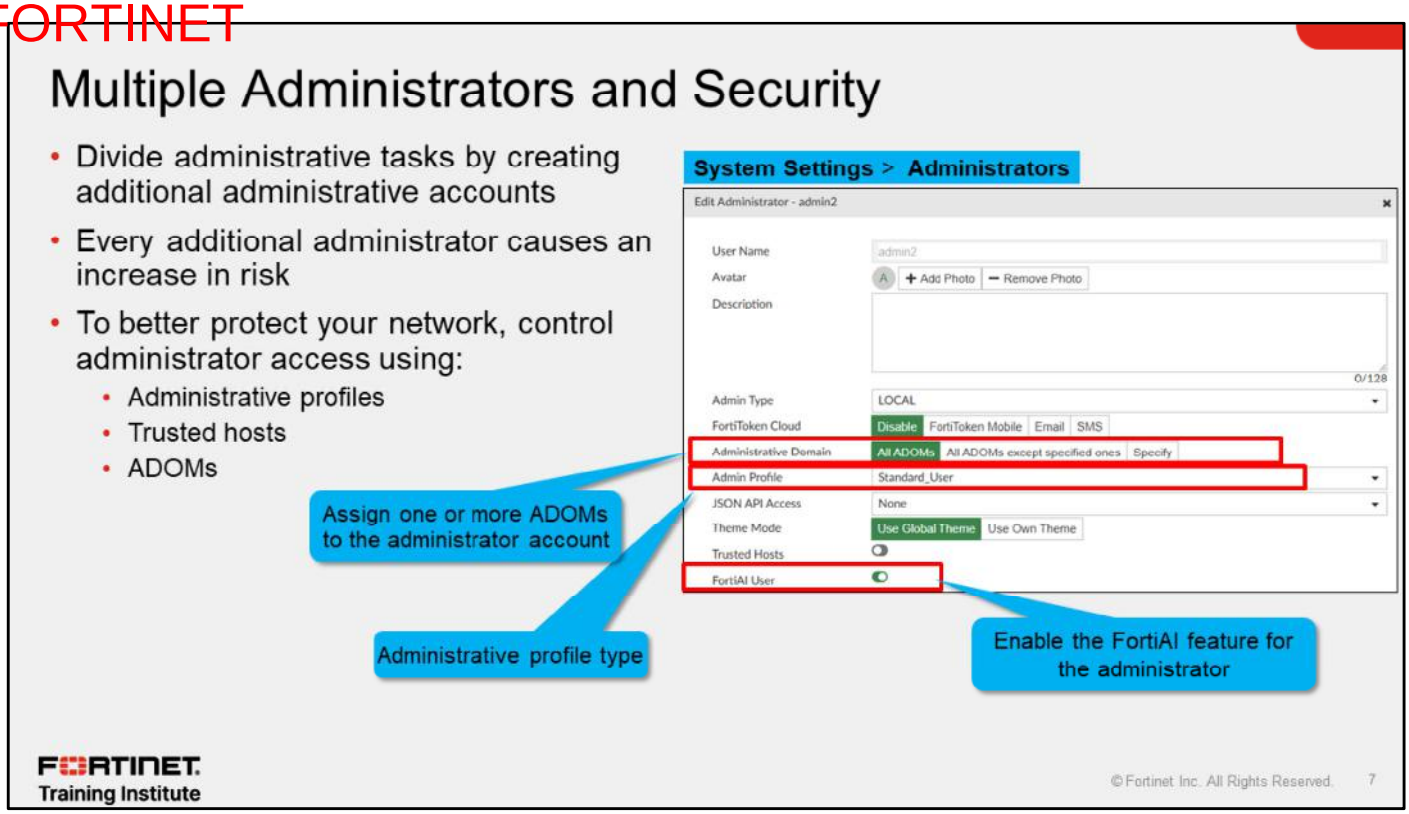
If you set a password expiry date, ensure you adhere to the policy and change the password before it expires, because there is no password recovery option.

Enable **Enforce Password History** to set the number of unique new passwords that must be used before a previous password can be reused.



Before you review the configuration settings, you must understand the importance of security. FortiAnalyzer stores your network log information, so it is *vital* that you protect your data correctly. This slide lists some security recommendations:

- Deploy FortiAnalyzer in a protected and trusted private network. You should never deploy FortiAnalyzer outside the network.
- Always use secure connection methods for administration: HTTPS for the GUI or SSH for the CLI. Methods like HTTP and Telnet use plaintext, and are not secure, so an attacker can use packet-sniffing tools to obtain information that they can use to breach your network.
- Use trusted hosts to allow logins from only specific locations. If you do need to open outside access to the device so that remote FortiGate devices can connect, open only the ports necessary for this. Consult *FortiAnalyzer Ports and Protocols* documentation at `docs.fortinet.com`. Unnecessary open ports increase your security risk. If you need to open direct login access from the outside, be sure to set up special user accounts for this purpose, and open only protocols that are secure. Use a secure password because they are important if you start transmitting traffic over connections that anyone (that is, the internet) could be listening to.
- Store your administrator password in a secure location because FortiAnalyzer password recovery requires erasing system settings.
- Use the *FortiAnalyzer Best Practices* guide found at `docs.fortinet.com` to help you get the most out of your FortiAnalyzer products, maximize performance, and avoid potential problems.

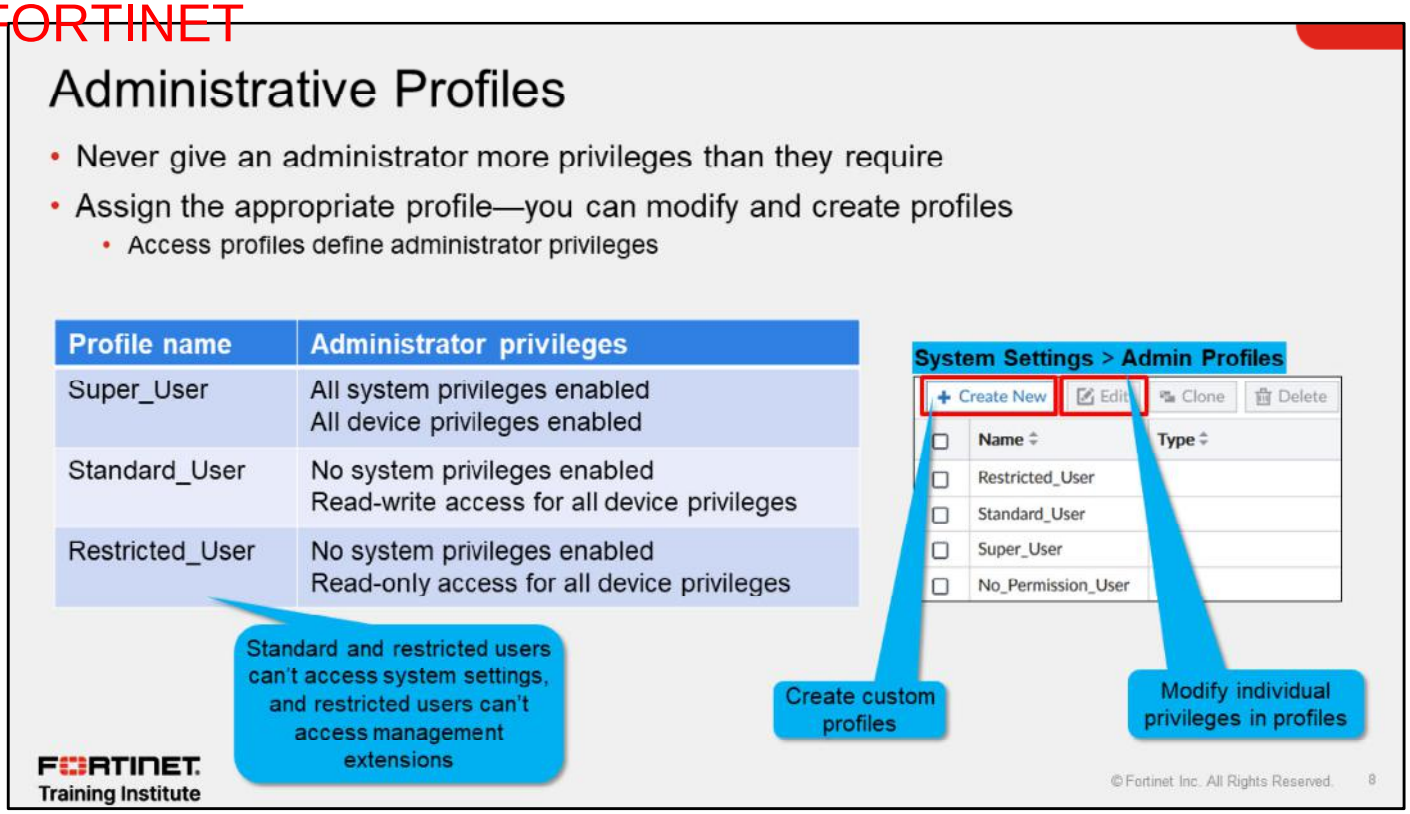


Depending on your deployment, you may decide to divide FortiAnalyzer administrative tasks among multiple employees by creating additional administrative accounts. However, every additional individual to which you give administrator access causes a potential growth in risk.

To protect your network, you can control and restrict administrative access using the following methods:
- Administrative profiles: Determine the level of access, or privileges, granted.
- Trusted hosts: Determine from where a connection can be established.
- ADOMs: Determine to which devices the administrator will have access to view and manage logs.

By dividing administrative access among multiple people and employing control methods, you can better protect your network.

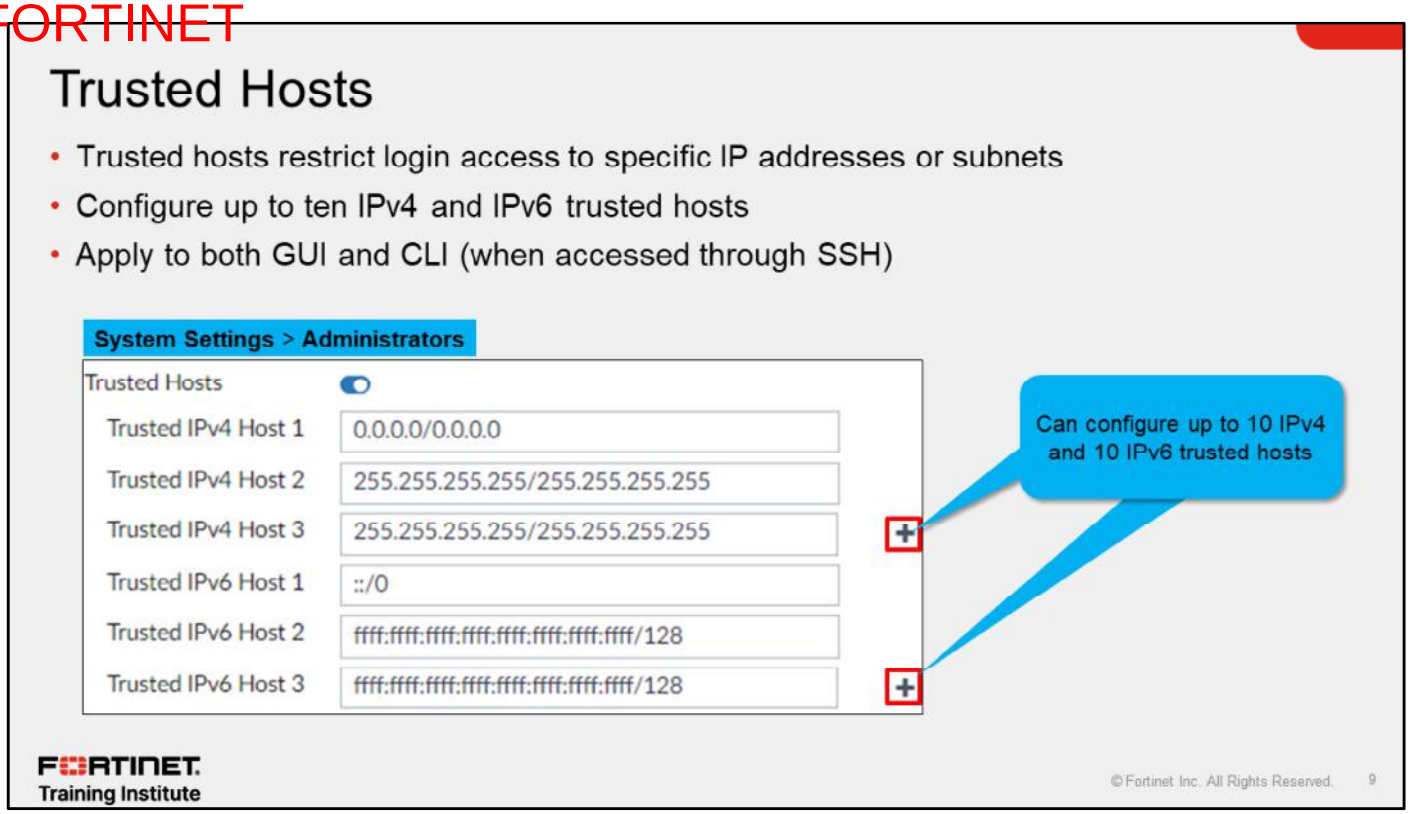
You can allow the administrator to use the FortiAI feature by enabling FortiAI on the administrator profile. FortiAI can be applied only to local users and not single sign-on (SSO) users. You need a valid FortiAI license for this feature to be available on the administrator profile.



You should never give administrators more privileges than they need to fulfill their role. FortiAnalyzer comes with four preinstalled default profiles that you can assign to other administrative users. Administrator profiles define administrator privileges and are required for each administrative account.

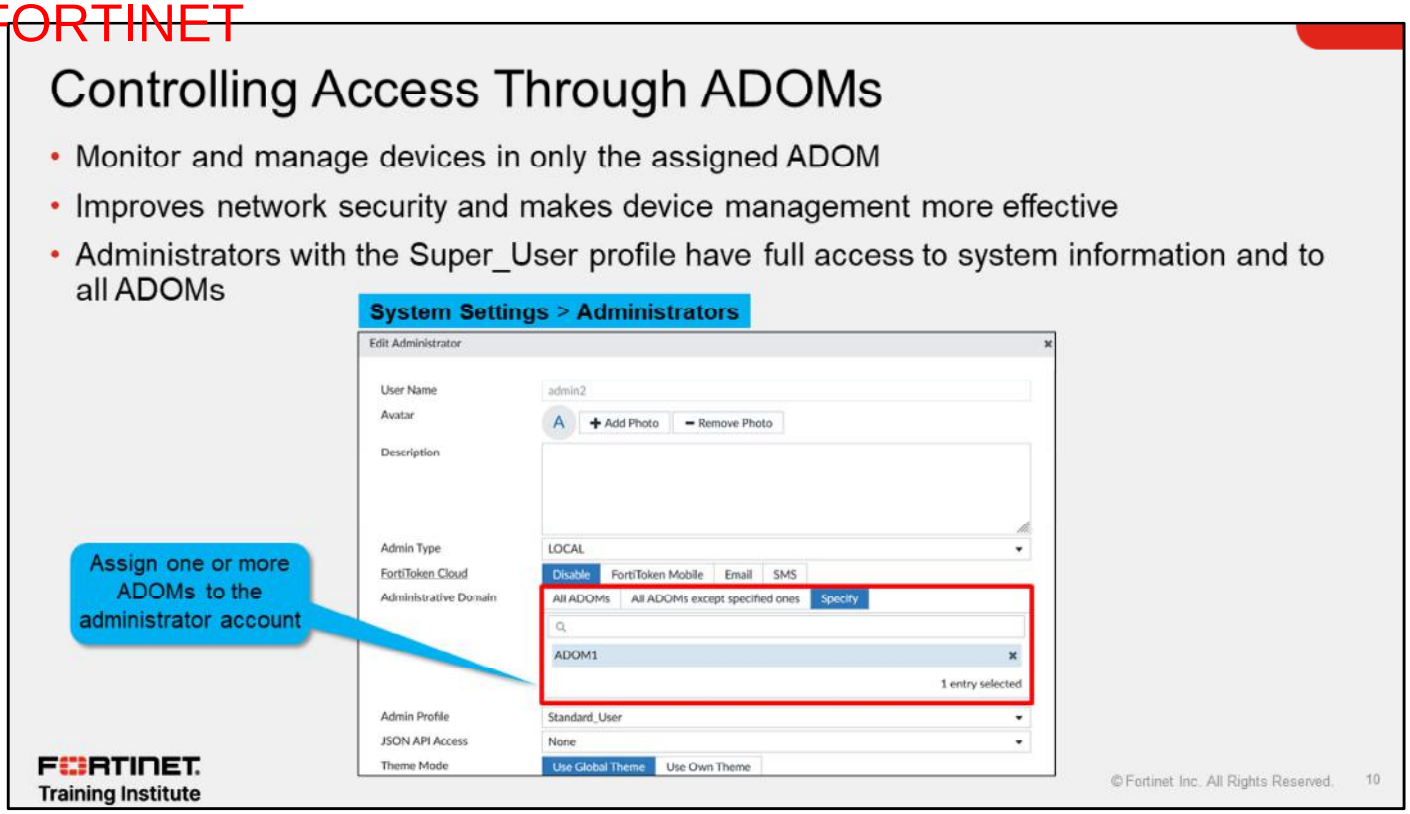
The four default profiles are:
- Super_User, which provides access to all device and system privileges.
- Standard_User, which provides read and write access to device privileges, but not system privileges.
- Restricted_User, which provides read access to only device privileges but not to system privileges, and removes all access to the management extensions.
- No_Permission_User, which provides no system or device privileges, and can be used for example, to temporarily remove access granted to existing admins.

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



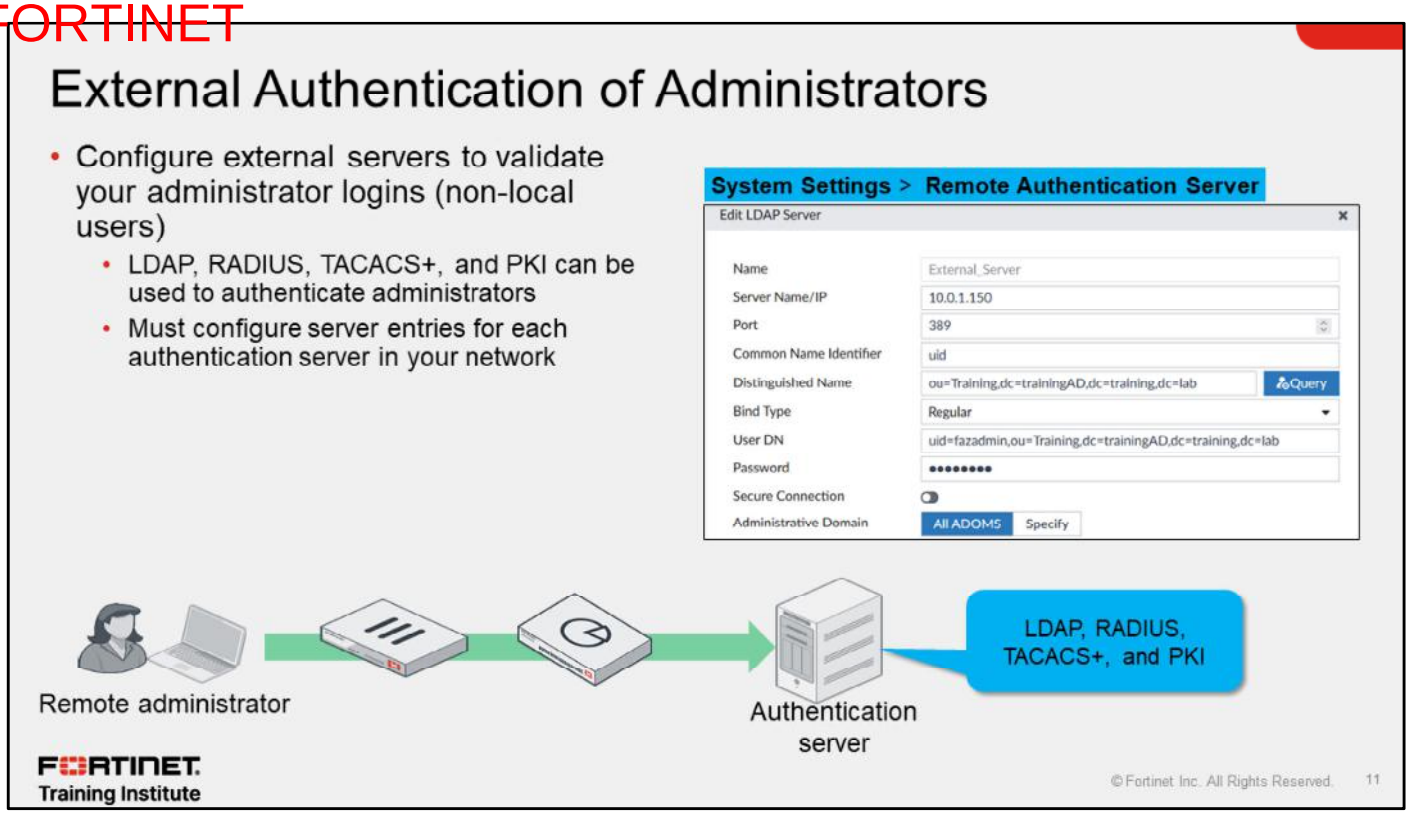
In addition to controlling administrative access through administrator profiles, you can further control access using trusted hosts for each administrative user. This restricts administrators to logging in from only specific IP addresses or subnets. If you define only one trusted host IP address, you can limit that administrator to a single source IP address.

The trusted hosts you define apply to the GUI and the CLI when accessed through SSH.



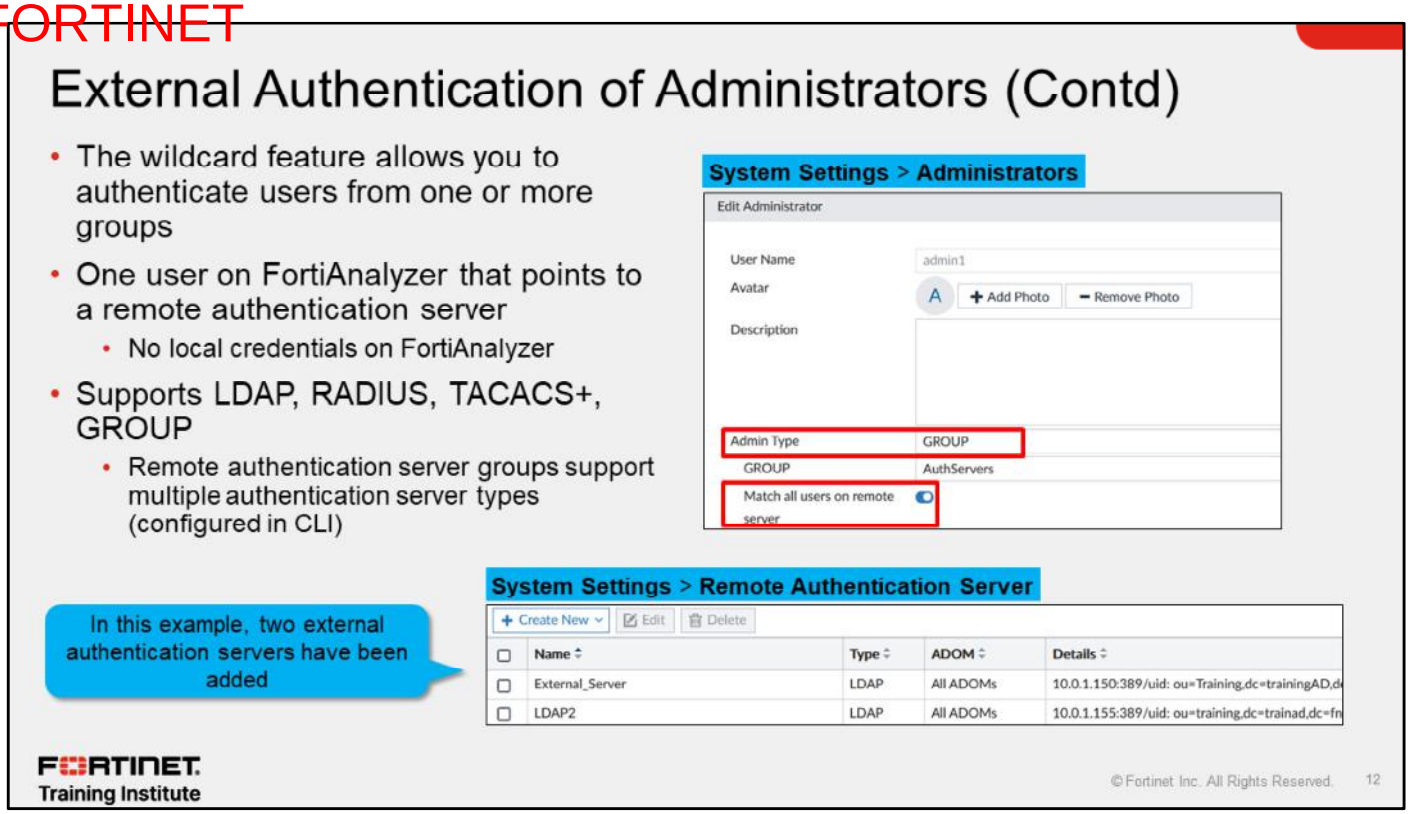
Another way you can control administrative access is through ADOMs. Using ADOMs makes device management more effective because administrators need to monitor and manage only devices in their assigned ADOMs. It also makes the network more secure because administrators are restricted to only those devices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

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



Instead of creating local administrators, where FortiAnalyzer validates logins, you can configure external servers to validate your administrator logins. RADIUS, LDAP, TACACS+, and PKI can all be used to authenticate administrators.

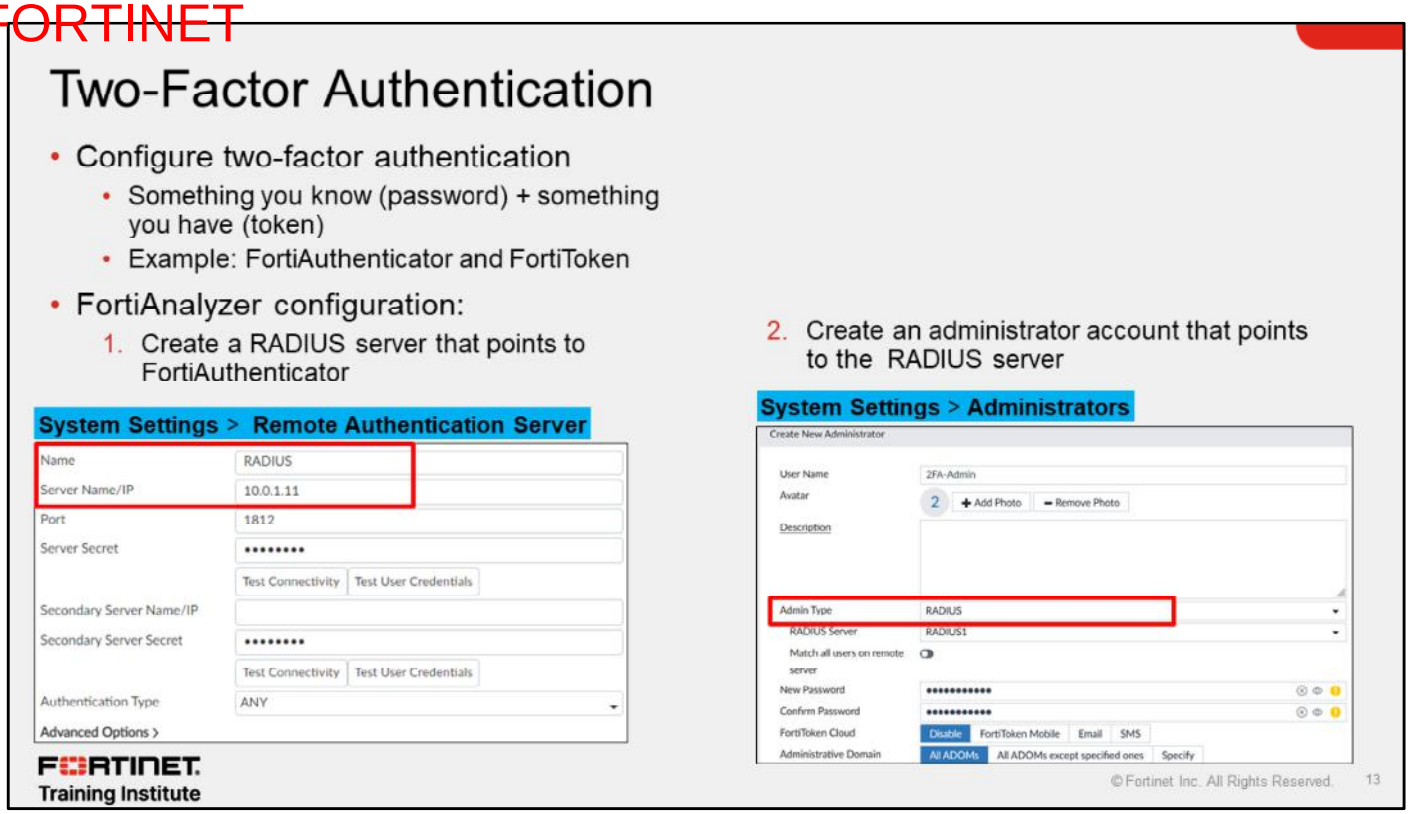
The image on this slide shows an example of an LDAP server configuration.



You can enable the **Match all users on remote server** option to allow administrators to log in to FortiAnalyzer using their credentials on a remote authentication server, such as RADIUS, TACACS+, and LDAP. This option is useful for creating wildcard administrators and removes the need for FortiAnalyzer to store local credentials, because a remote authentication server is being used. This simplifies administration. For example, if an employee leaves the company, their account does not exist on FortiAnalyzer—they exist only as a user on a remote authentication server. If you do not select this option, you must provide a password that is used only if FortiAnalyzer is unable to connect to the authentication server.

You can set remote authentication server groups, which are listed as **GROUP** in the **Admin Type** field, to extend administrator access. Usually, you create a wildcard administrator for only a single server. However, if you group multiple servers, you can apply a wildcard administrator to all the servers in the group. If you added an LDAP and RADIUS server to your authentication group, and the administrator has login credentials on both servers, then the administrator can authenticate on FortiAnalyzer using either their LDAP or RADIUS credentials.

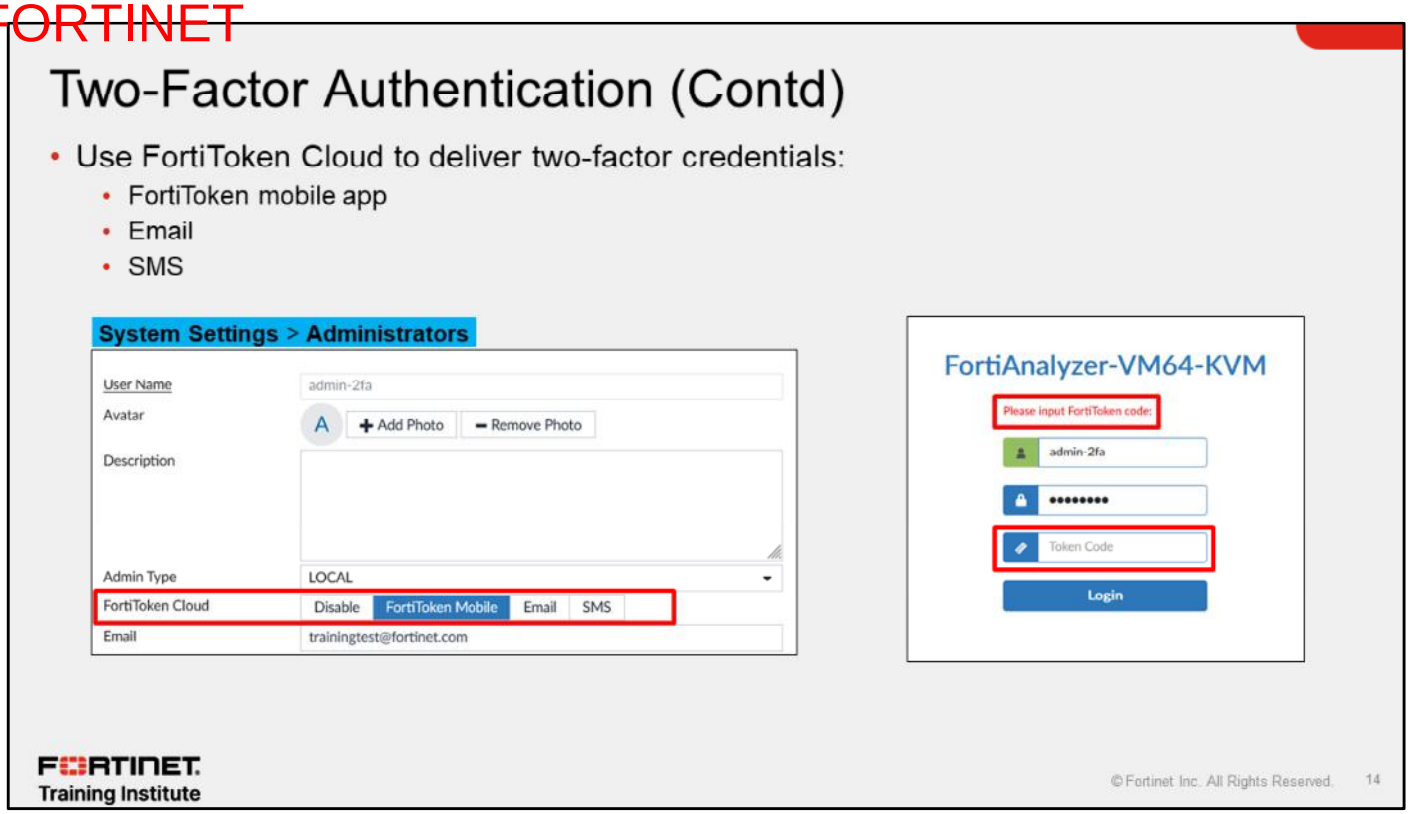
You can group multiple servers of the same type to act as backup—if one server fails, the administrator can still be authenticated by another server in the group. You can add remote authentication server groups using the CLI only. In the example shown on the slide, two existing LDAP servers were added. On the CLI, under `config system admin group`, an authentication server group was added and named `AuthServers`, and the servers were added to this group.



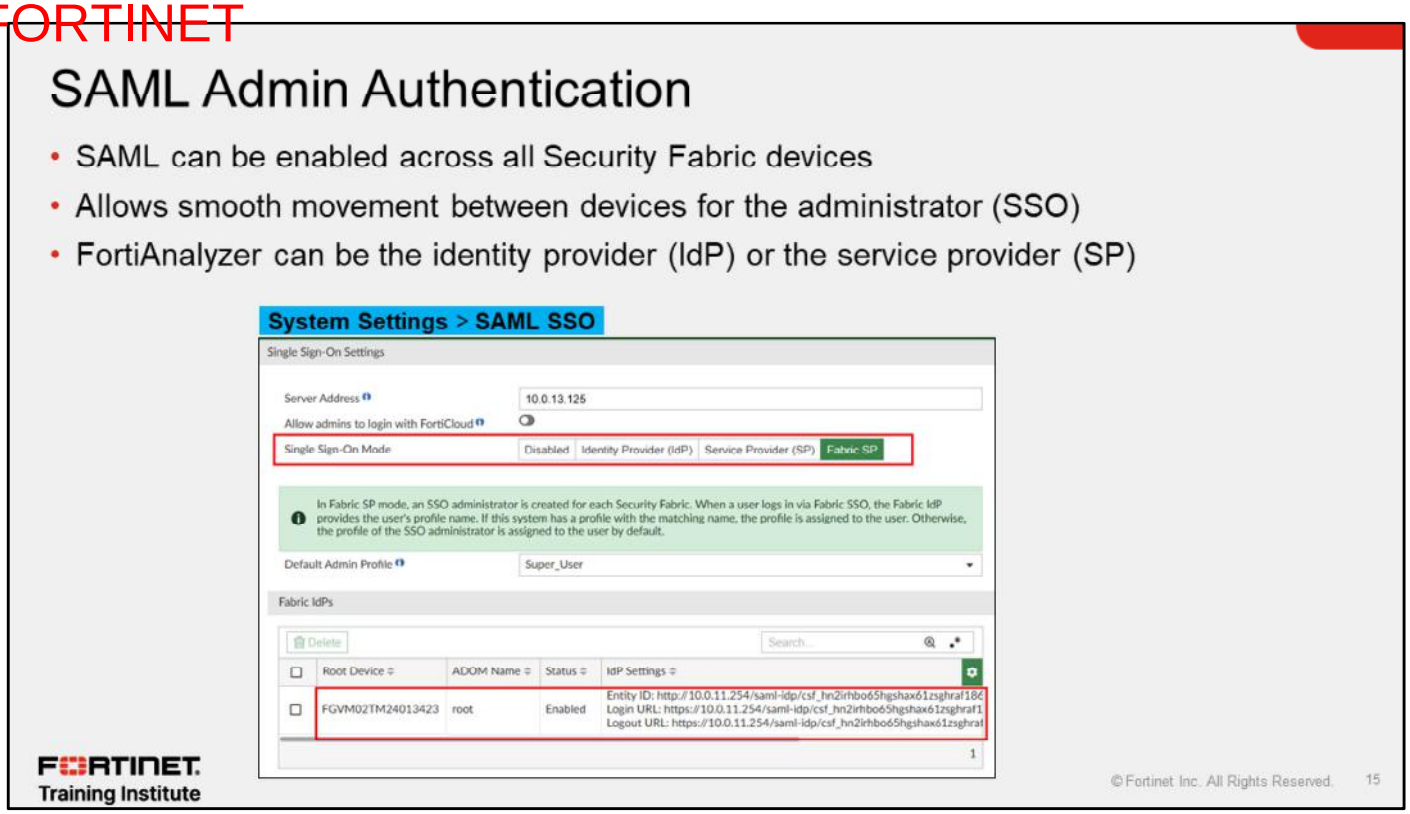
To add additional security to external administrators, you can configure two-factor authentication. To do this, you can use FortiAuthenticator and FortiToken.

On the FortiAnalyzer side, you need to create a RADIUS server that points to FortiAuthenticator and then create an administrator account that points to the RADIUS server.

For more information about configuring external servers and two-factor authentication, refer to the *FortiAnalyzer Administration Guide*.



FortiAnalyzer also supports two-factor authentication with FortiToken Cloud. With an active FortiToken Cloud license, you have three options for delivering two-factor credentials. You can install the FortiToken Mobile application on your smartphone and receive the verification code by email or SMS.



FortiAnalyzer supports SSO in multiple ways. It can act as the IdP, SP, or Fabric SP.

When FortiAnalyzer is configured as a Fabric SP, it automatically registers itself to the Fabric root FortiGate as an SP, allowing for simplified configuration. A default SSO administrator is automatically created for each Security Fabric. The IdP certificate is also automatically uploaded to FortiAnalyzer.

You can also create a wildcard SSO administrator that will match multiple users with an IdP. Configuration requirements are drastically reduced if the IdP leverages a remote authentication server, such as LDAP. If you don't enable the **Match all users on the remote server** wildcard option, then you must create all those users on FortiAnalyzer.

There is also an option to use SSO with a FortiCloud account or its identity and access management (IAM) users. However, FortiAnalyzer must be registered under that account.

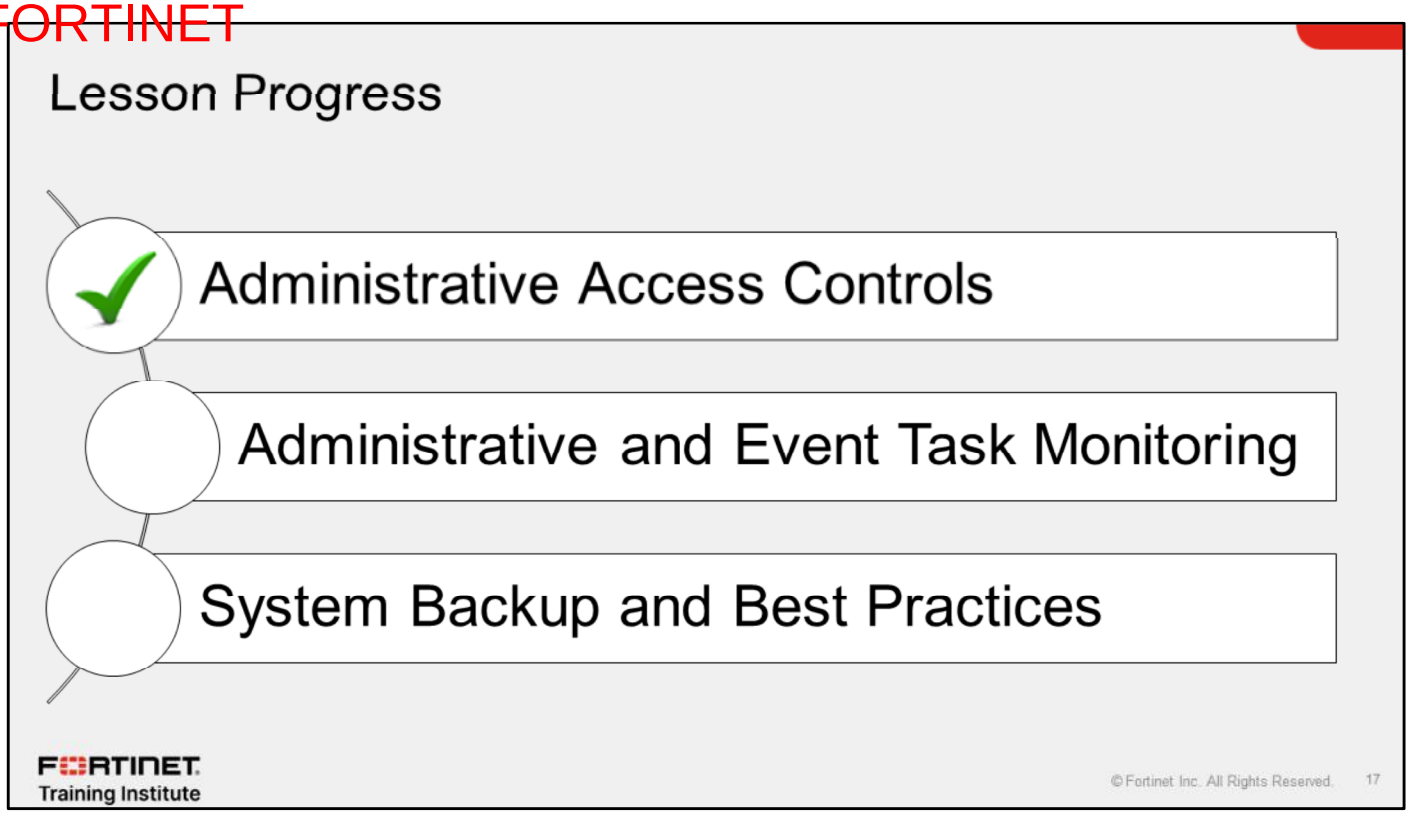
Knowledge Check

1. How do you restrict an administrator's access to a subset of your organization's ADOMs?
   - ✓A. Assign the ADOMs to the administrator's account.
   - B. Configure trusted hosts.

2. What is the function of a wildcard administrator?
   - A. It allows administrators to log in with credentials stored locally on FortiAnalyzer.
   - ✓B. It allows administrators to log in with credentials stored on a remote authentication server.

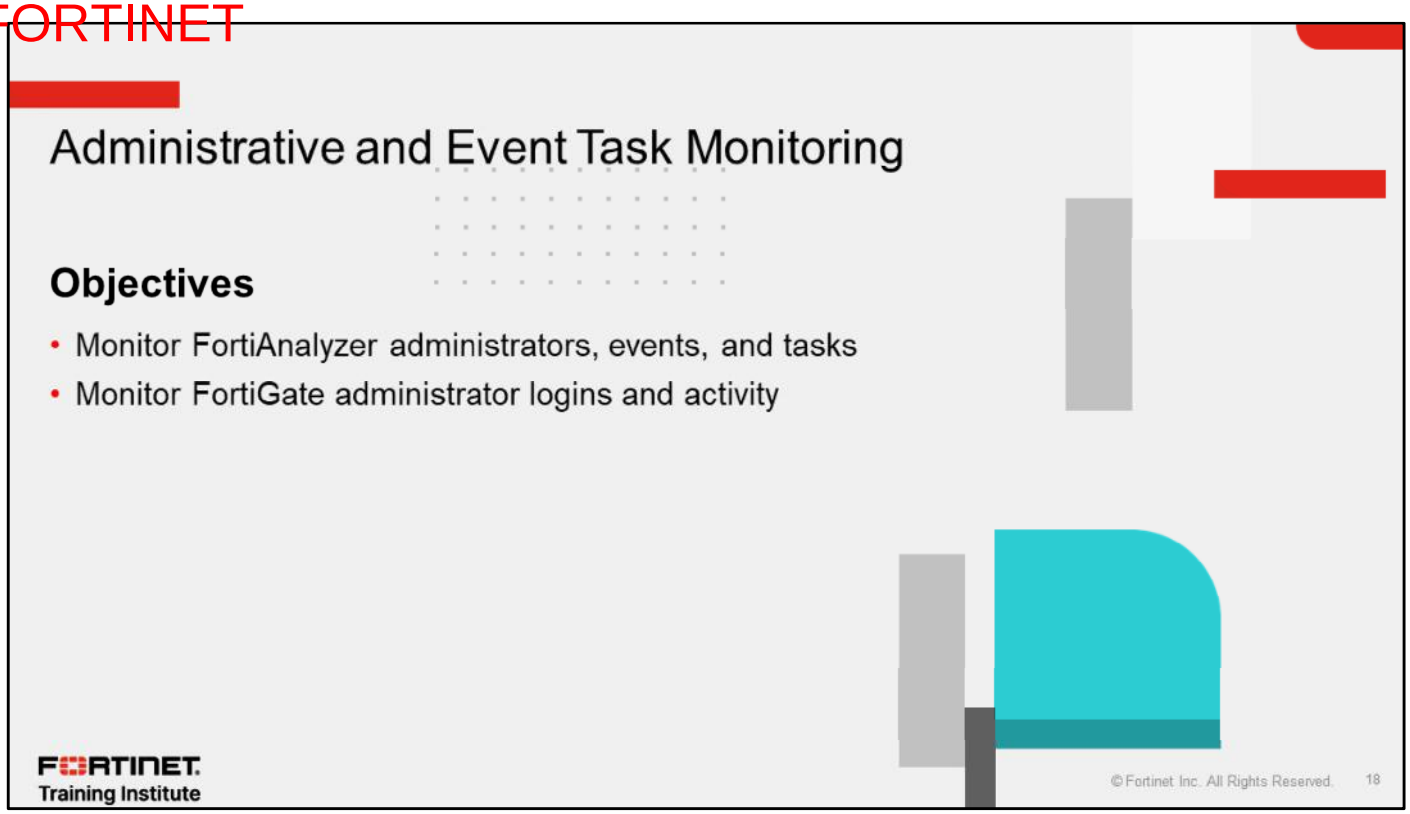
FORTINET Training Institute

 16



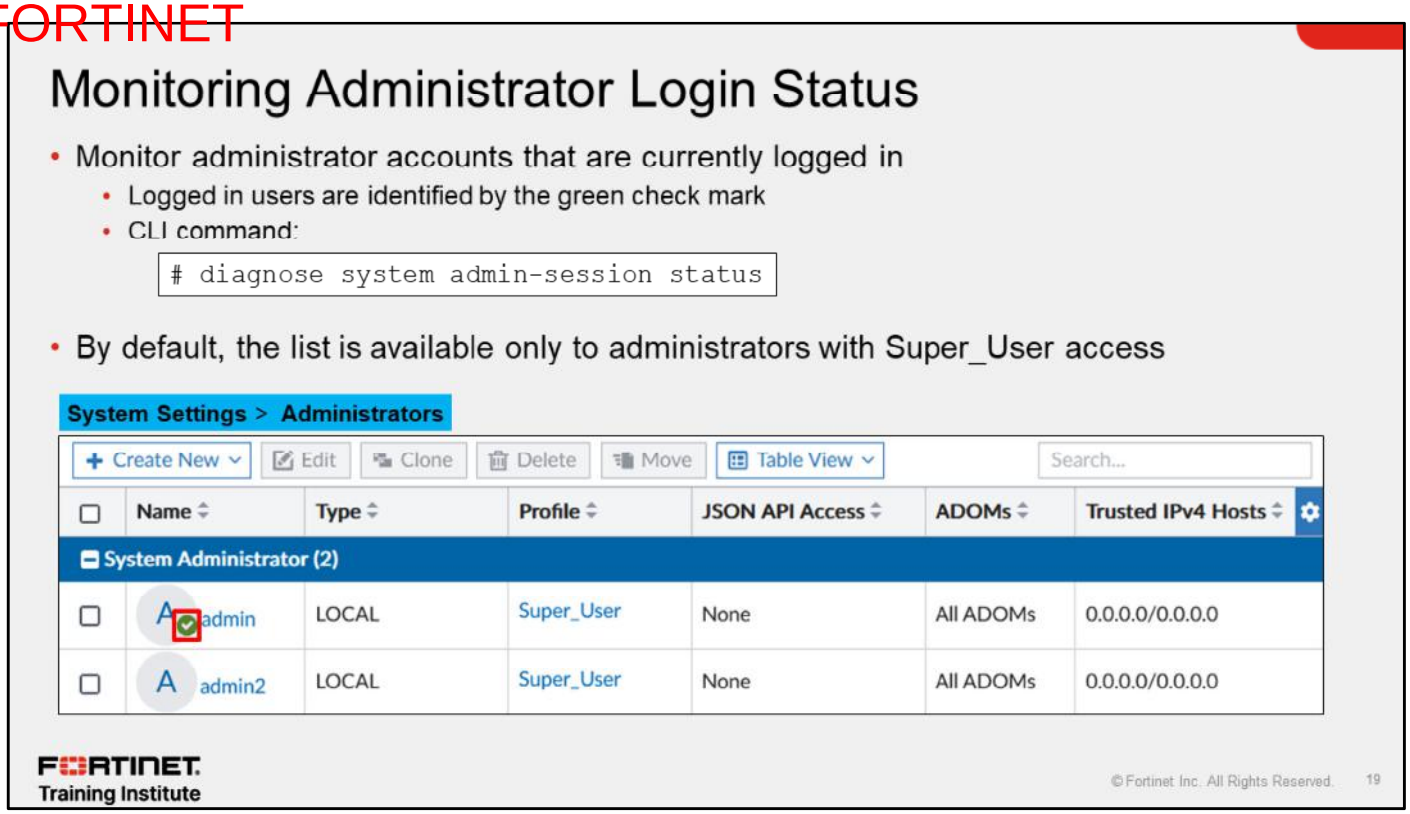
Good job! You now understand administrative access controls.

Now, you will learn how to monitor administrative events.



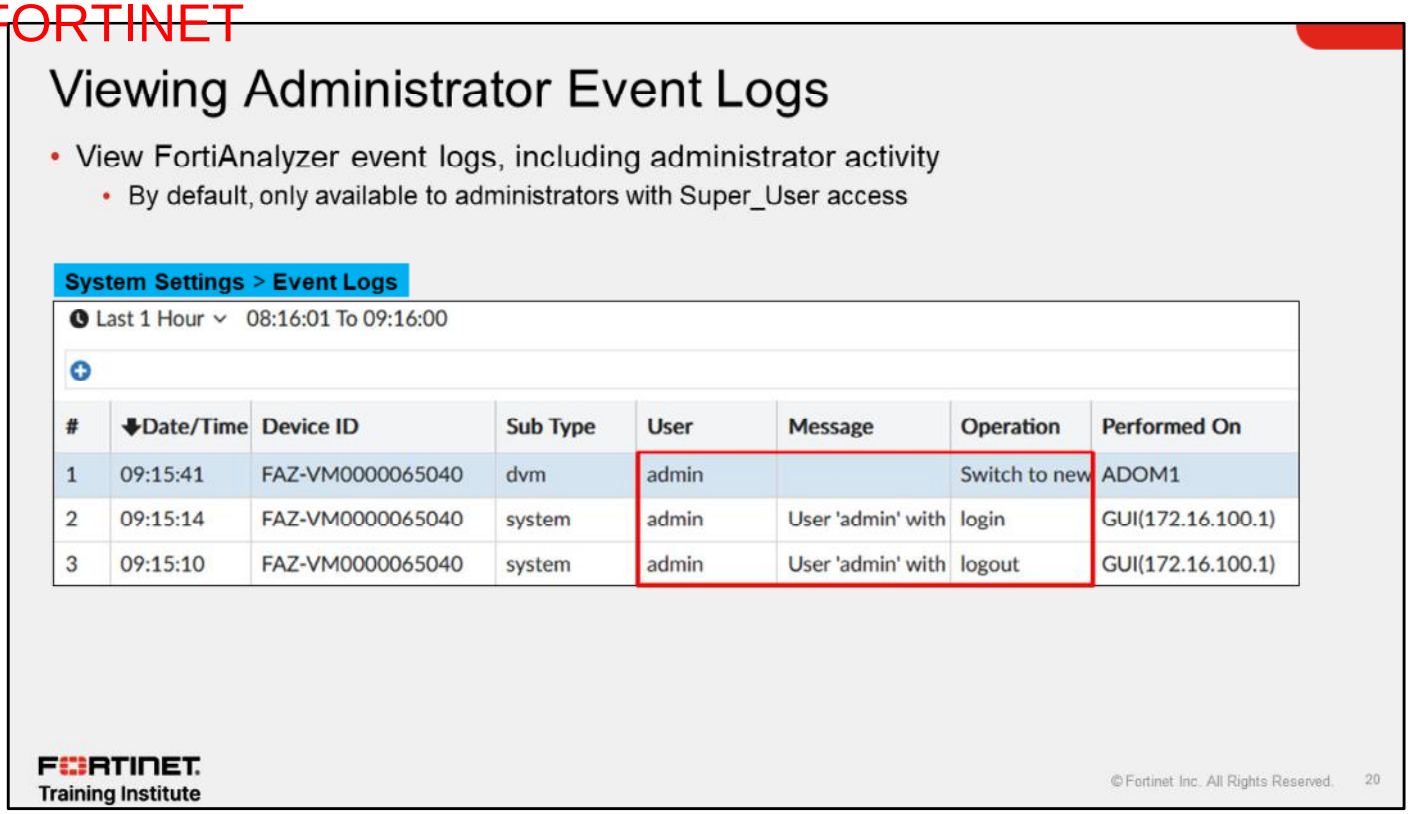
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in monitoring administrative events and tasks, you will be able to ensure administrators are operating within their assigned role, thereby mitigating risk to your organization.



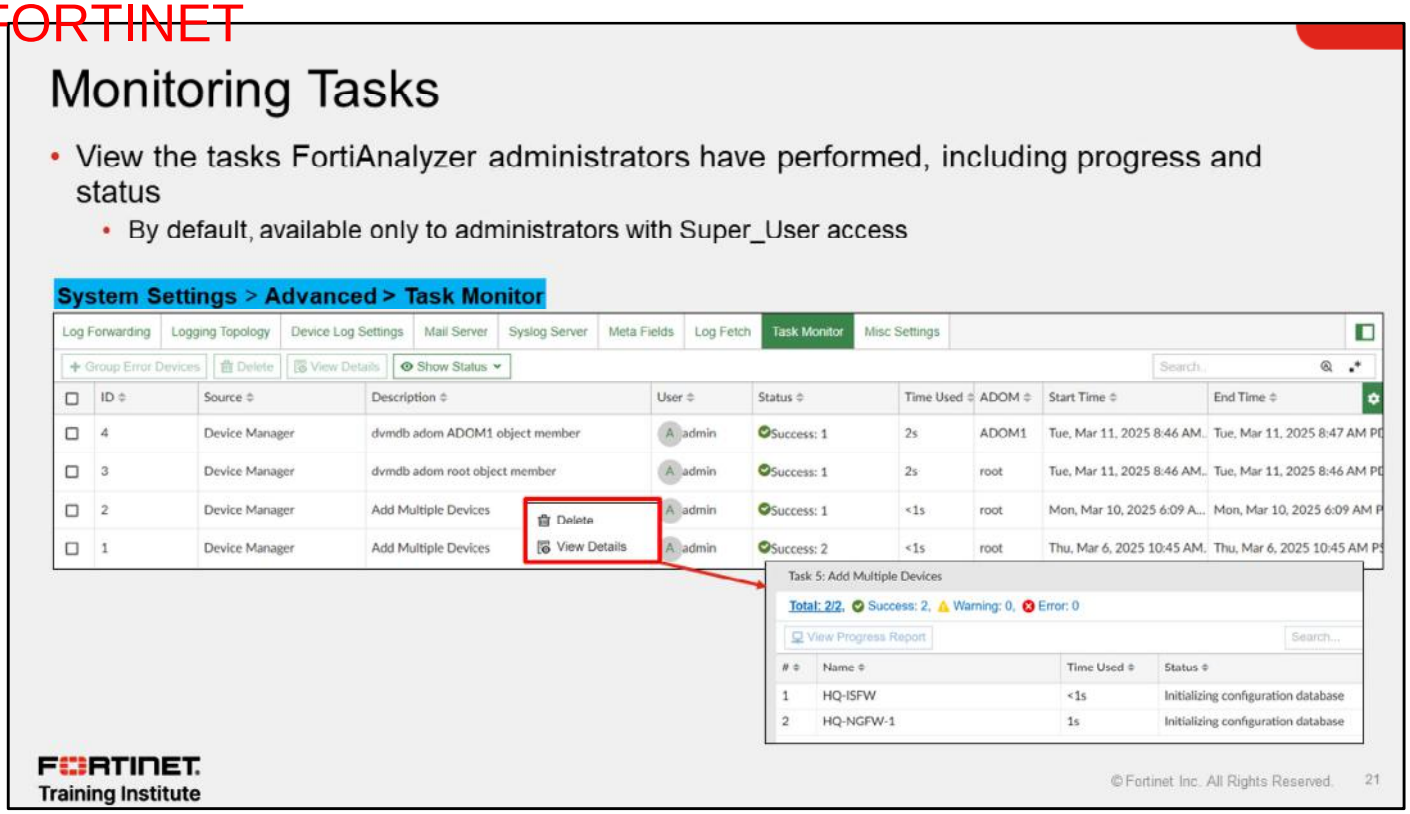
You can track administrator user sessions on the **Administrators** page, including who is currently logged in and on which trusted host. By default, only administrators with Super_User access can see the complete list of administrators.

Administrators who are logged in are indicated by a green check mark.



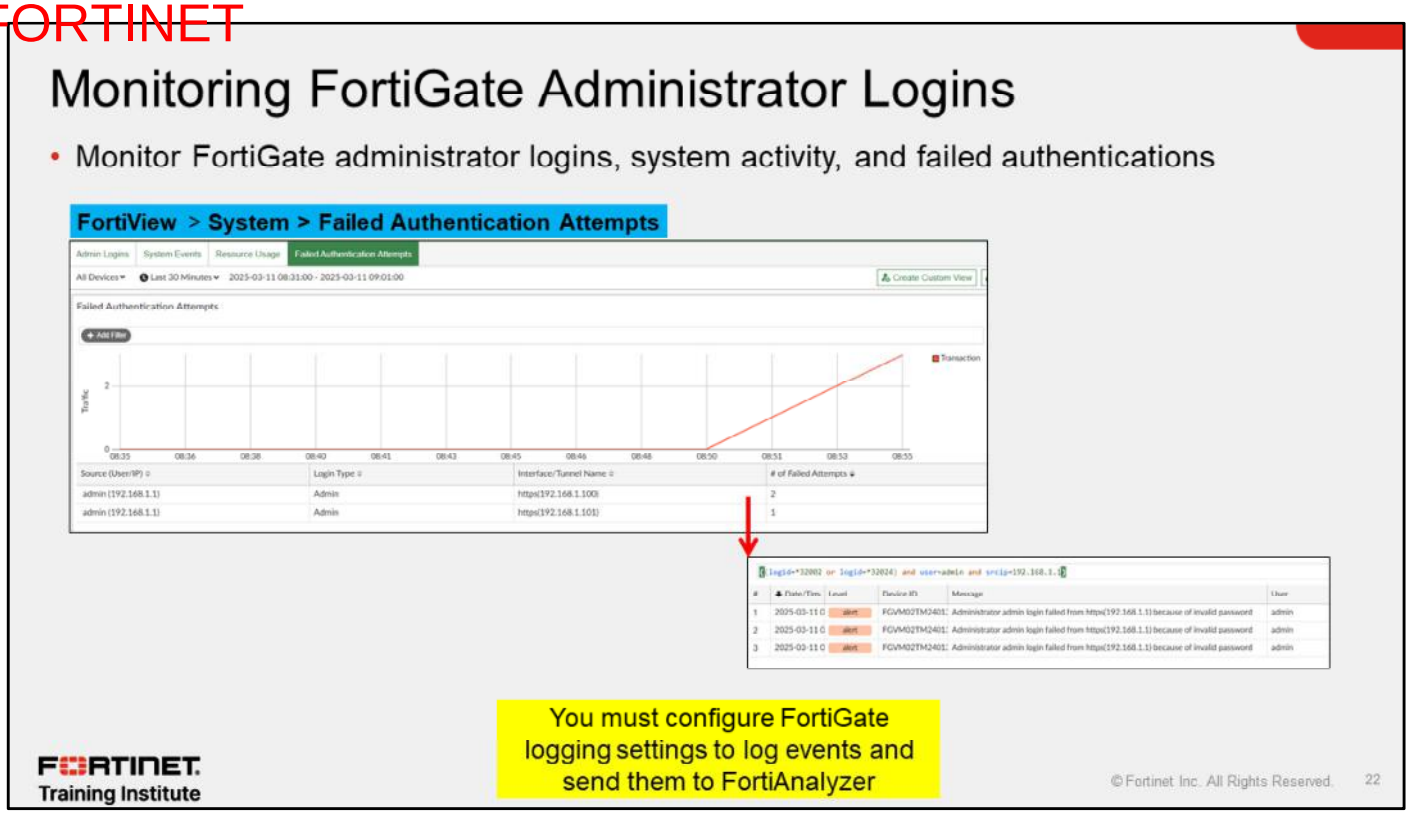
FortiAnalyzer audits administrator activity so you can source changes to an individual.

You can view the local event log messages, such as configuration changes and logins, on the **Event Log** page. To fine-tune the results, you can add filters. For example, to view local events performed by a specific administrative user, filter by username.



The **Task Monitor** page lets you view the progress and status of administrator tasks..

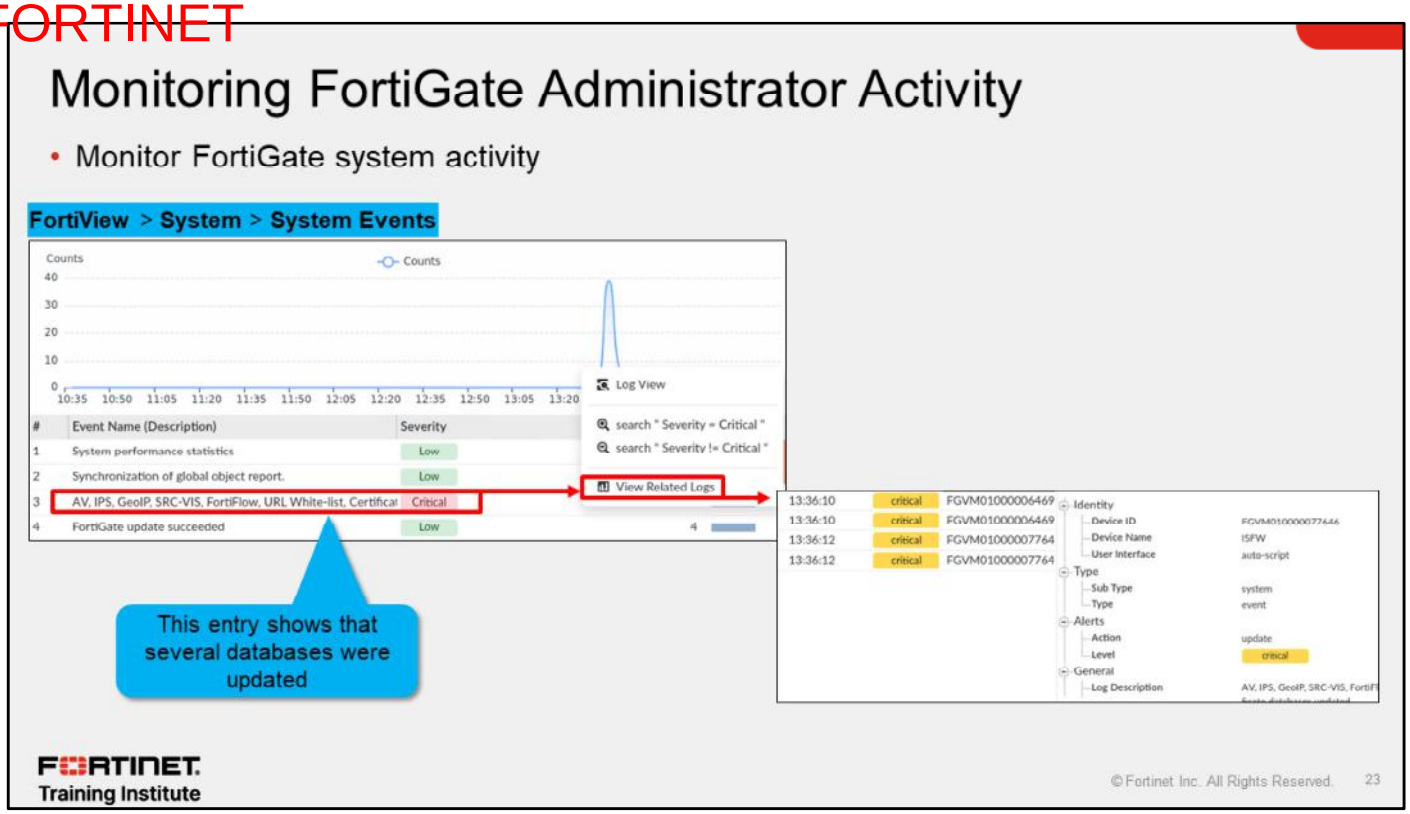
You can right-click on a task to view more details, including a progress report for each subtask inside the main task.



FortiAnalyzer also allows you to monitor FortiGate administrative login activity through FortiView.

The **Failed Authentication Attempts** page shows failed login attempts and includes the source IP address of the login, the login type, the interface, the protocol used, and the number of failed login attempts.

The **Admin Logins** page (not shown on this slide) shows logins, failed logins, login duration, and configuration changes.



On FortiAnalyzer, you can monitor FortiGate administrative activity using FortiView.

The **System Events** page displays all system and administrator-invoked events. To see more details about an event type, right-click on it and select **View Related Logs** to go to the corresponding section in **Log View**, where more information is available.

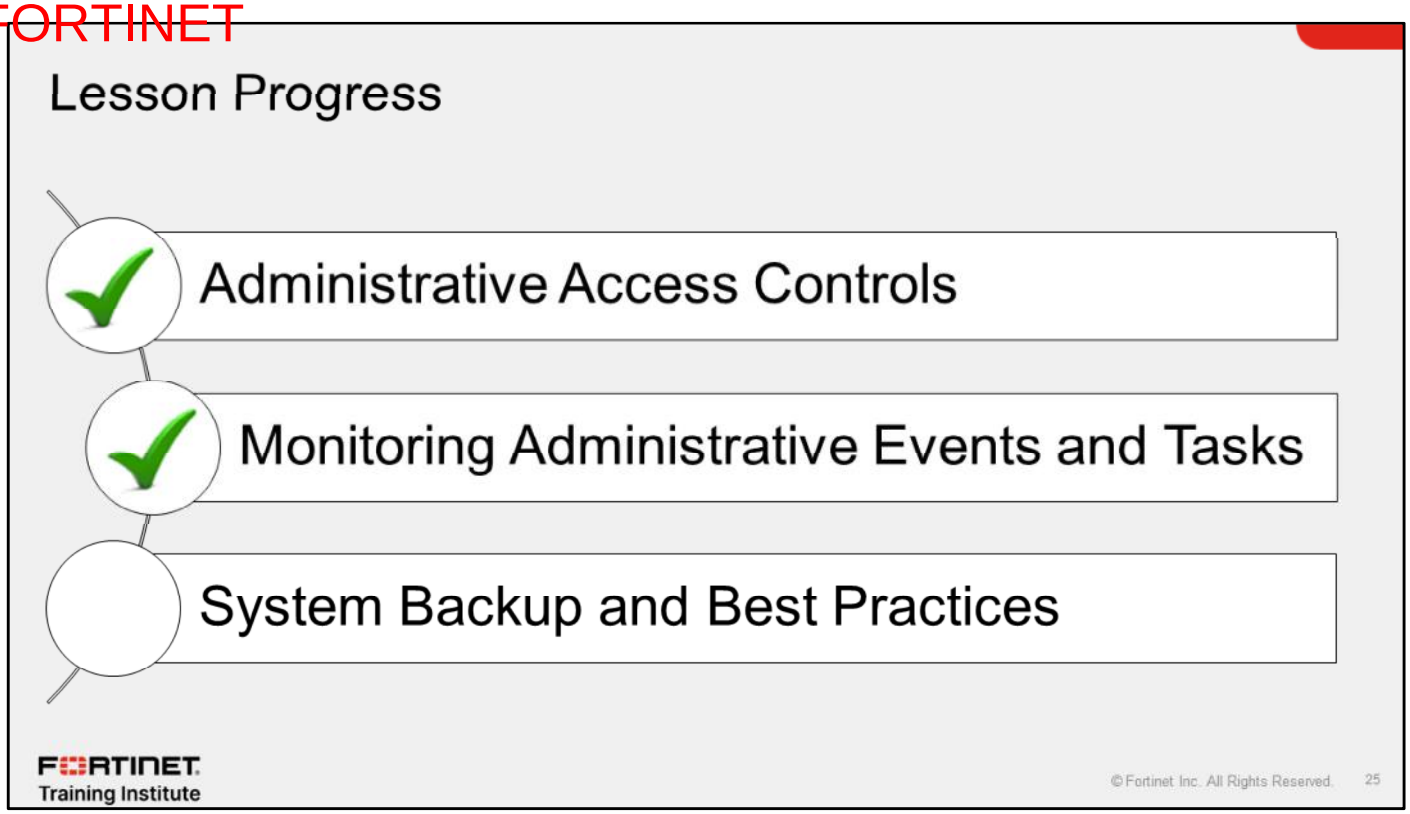
Knowledge Check

1. Which configuration is required to view FortiGate event logs on FortiAnalyzer?
   - A. FortiGate must be registered to the root ADOM.
   - ✓ B. FortiGate logging settings must have event logging enabled.

2. Which administrative profile should you assign to an administrative user who needs to manage devices but not system settings?
   - A. Super_User
   - ✓ B. Standard_User

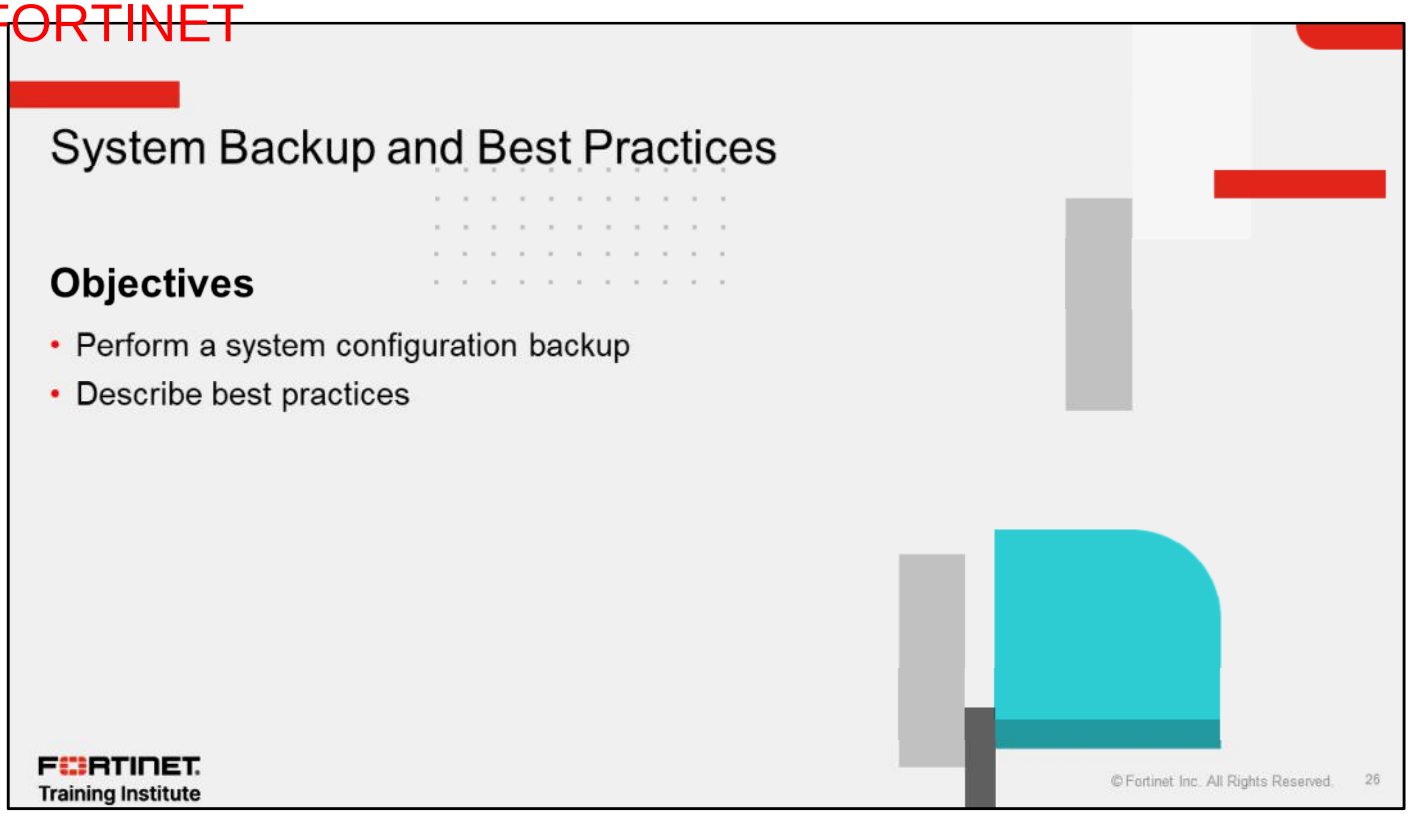
FORTINET Training Institute

 24



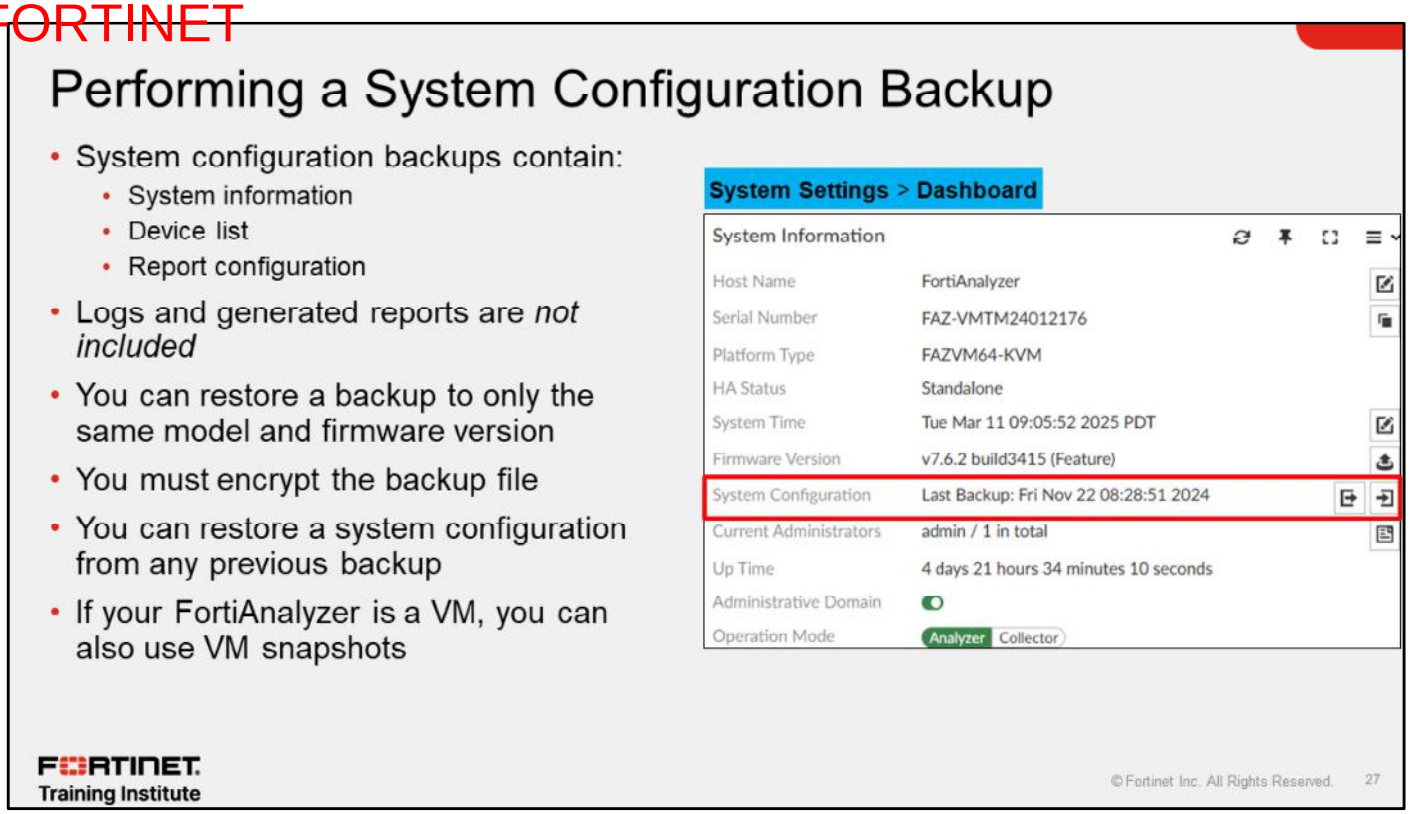
Good job! You now understand how to monitor administrative events and tasks.

Now, you will learn how to back up your FortiAnalyzer and some best practices.



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

By demonstrating competence in performing a system configuration backup and following best practices, you will be able to minimize the downtime experienced during a system failure or accidental misconfiguration.



As a best practice, you should back up your initial configuration after you complete it. You can perform a backup on the GUI using the **System Information** widget.

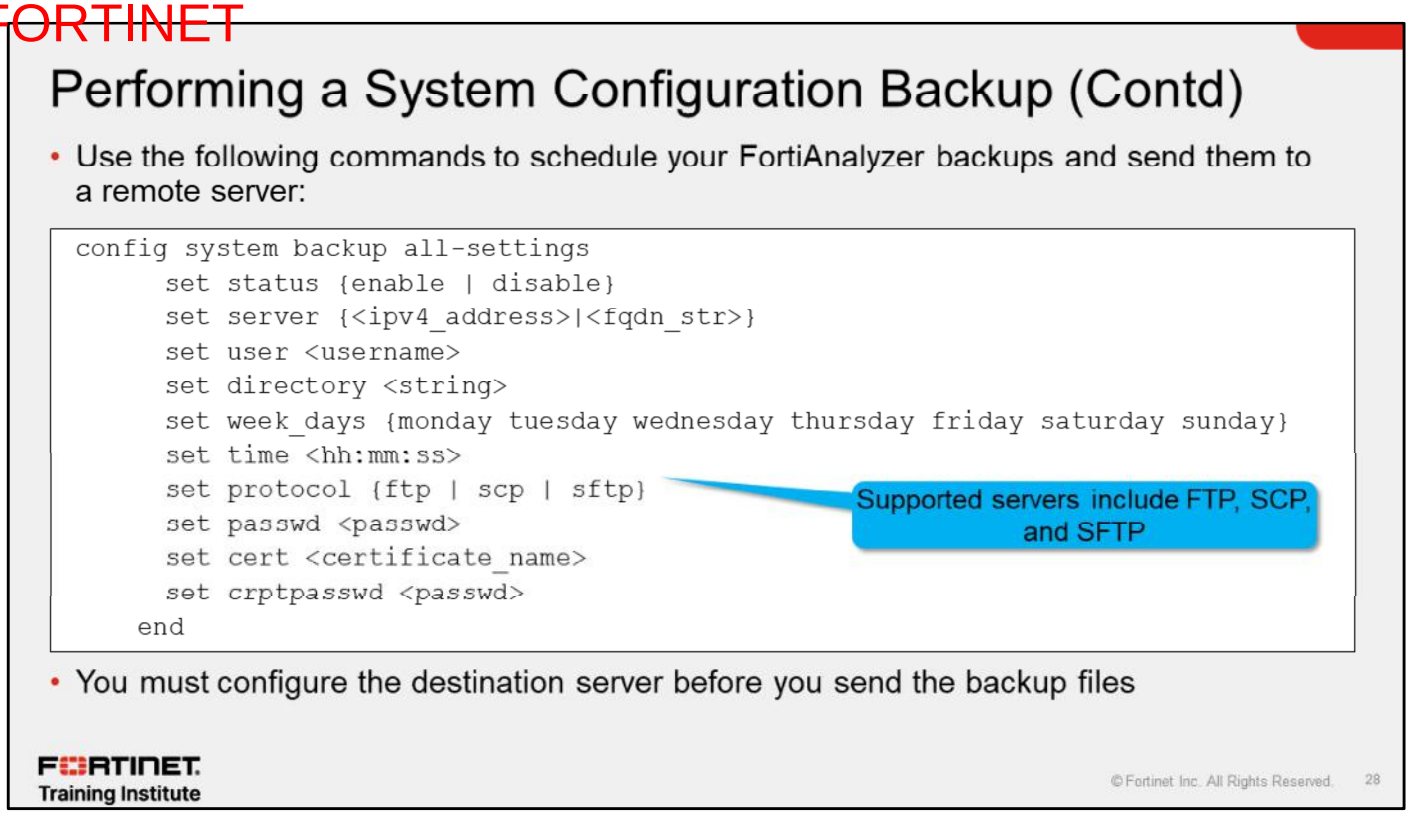
System configuration backups contain everything *except the actual logs and generated reports*. You can back up logs and reports using the GUI on the **Log View** and **Reports** pages or using the CLI with the command `execute backup`.

The system configuration backup includes the following:
- System information, such as the device IP address and administrative user information
- Device list, such as any devices you configured to allow log access
- Report information, such as configured report settings and all your custom report details. These details are not the actual reports.
- Automation and incident and events configurations, such as playbooks and event handlers

You must save the backup file as an encrypted file for additional security using a password. However, you can restore a backup to only the same model and firmware version. Furthermore, if you require assistance from Fortinet Support and your configuration is required to assist with troubleshooting, your backup should not be encrypted.

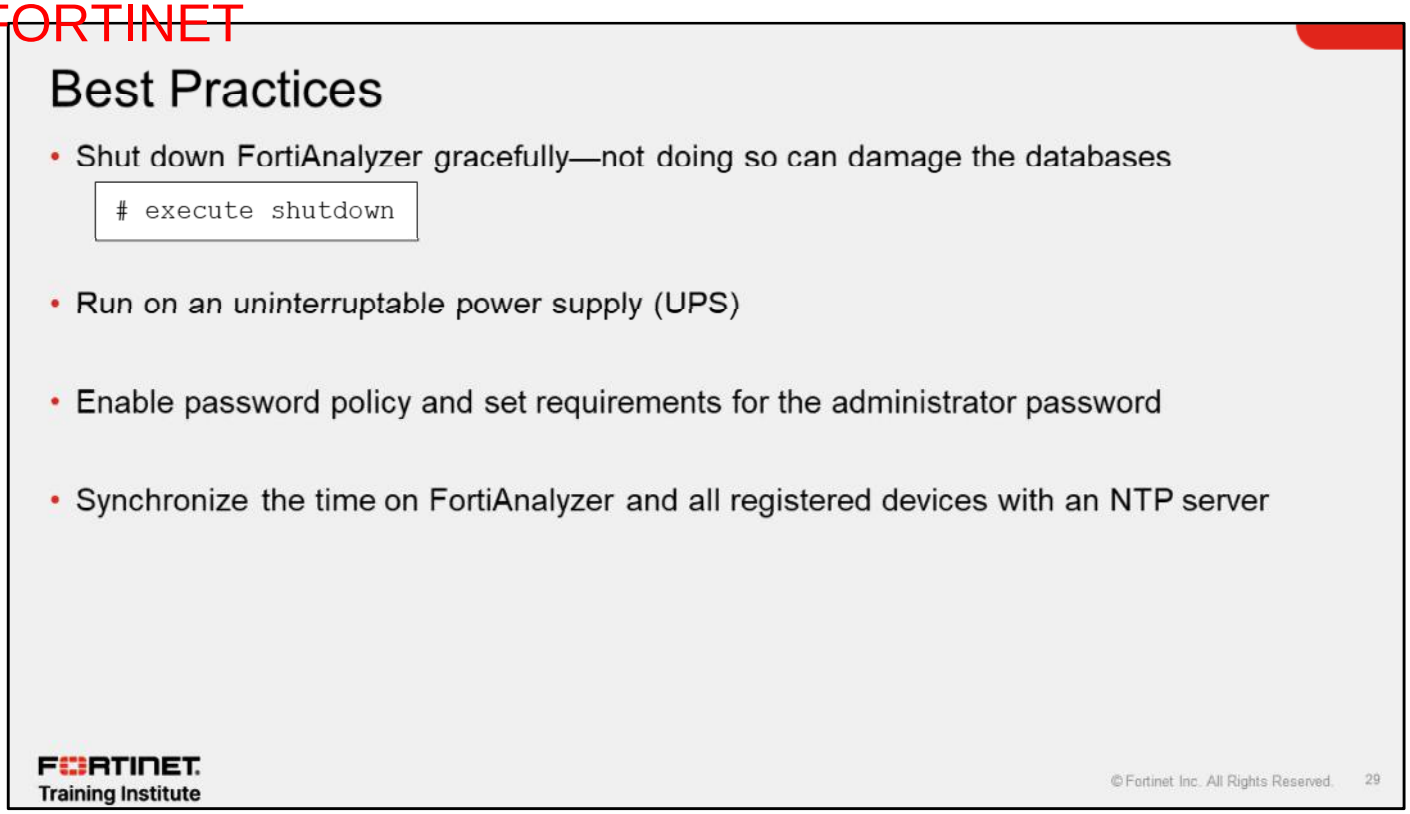
If you make changes to FortiAnalyzer that negatively affect your network, you can restore the configuration from any of your backups.

If your FortiAnalyzer is a VM, you can also use VM snapshots.



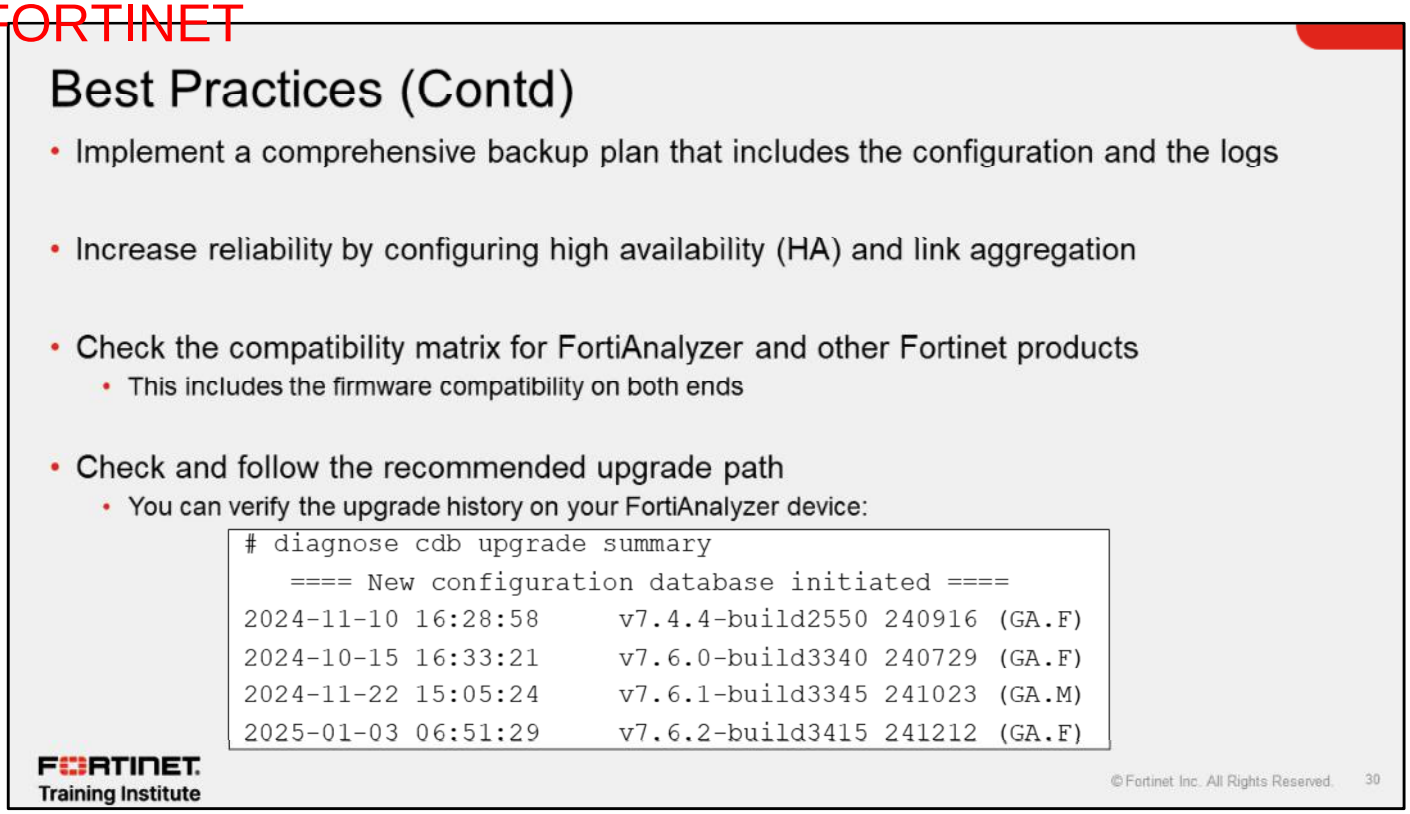
You can schedule your backups and store them on a remote server. FortiAnalyzer supports sending its backup files to FTP, SCP, and SFTP servers. You must configure the destination server to which you send the backup files. You must have valid credentials with read-write permissions in the destination folder.

This slide shows the commands you use to schedule the backup jobs.



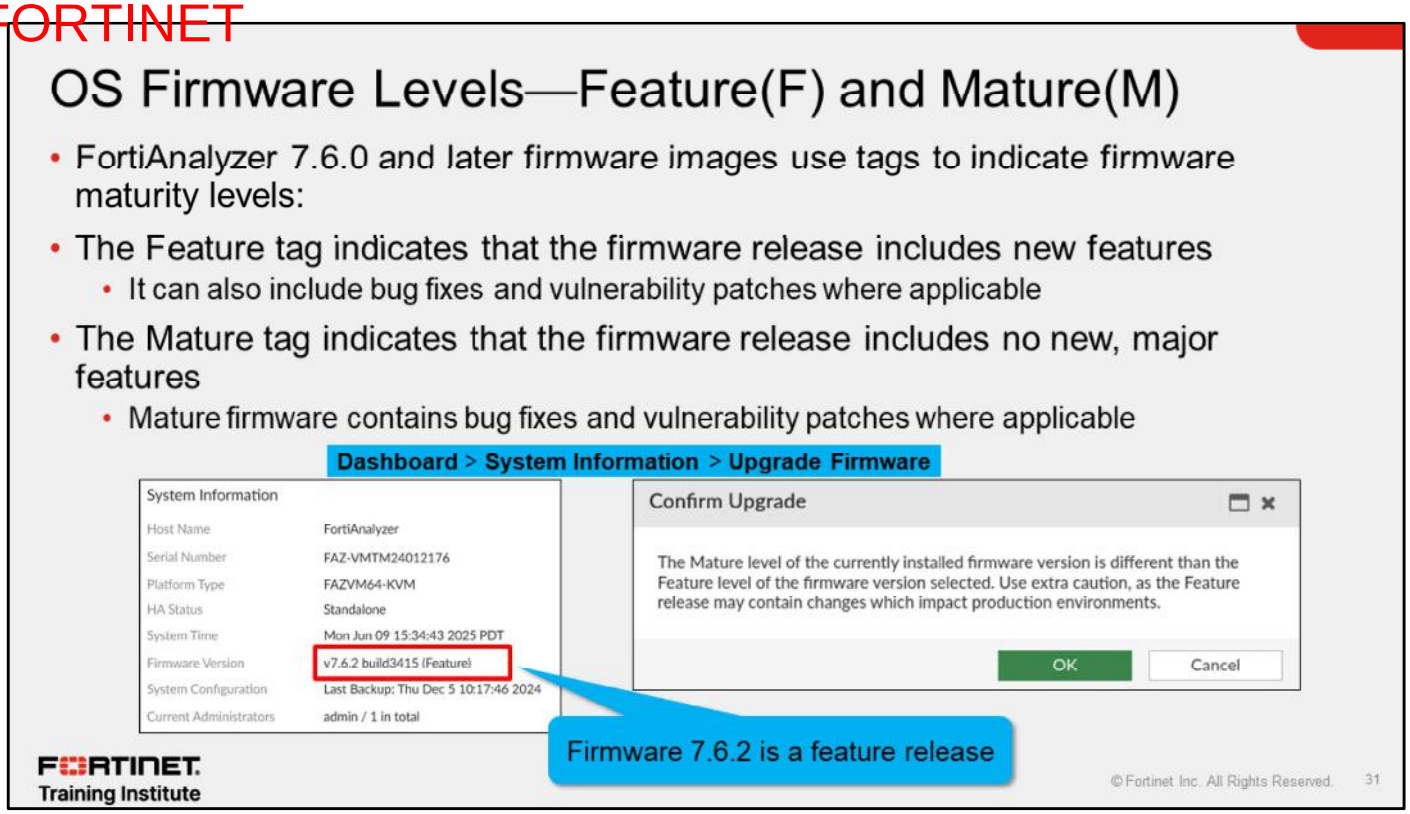
The following are some best practices for operating FortiAnalyzer:

- Always shut down FortiAnalyzer *gracefully* because not doing so can damage the databases.
- Run FortiAnalyzer on a UPS to prevent unexpected power-off events. Also, ensure your UPS is stable and has enough current to provide the expected behavior.
- Enable password policy and set requirements for the administrator password. The password policy lets you specify the administrator's password minimum length, type of characters it must contain, and the number of days to password expiry.
- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for correct log correlation.



In addition, there are a few more best practices that you should follow:

- Implement a comprehensive backup plan that includes the configuration and the logs. Log backups are covered in the *Logs and Reports Management* lesson.
- Increase reliability by configuring HA and link aggregation.
- Check the compatibility matrix for FortiAnalyzer and other Fortinet products. This includes firmware compatibility on both ends.
- Check and follow the recommended upgrade path. Consult `docs.fortinet.com` to find the appropriate upgrade path.



FortiAnalyzer 7.6.0 and later firmware images use tags to indicate the following maturity levels:

- The **Feature** tag indicates that the firmware release includes new features. It can also include bug fixes and vulnerability patches where applicable.
- The **Mature** tag indicates that the firmware release includes no new, major features. Mature firmware contains bug fixes and vulnerability patches where applicable.

Administrators can use the tags to identify the maturity level of the current firmware on the GUI or CLI.

When upgrading from mature firmware to feature firmware, FortiAnalyzer displays the warning message shown on the slide.

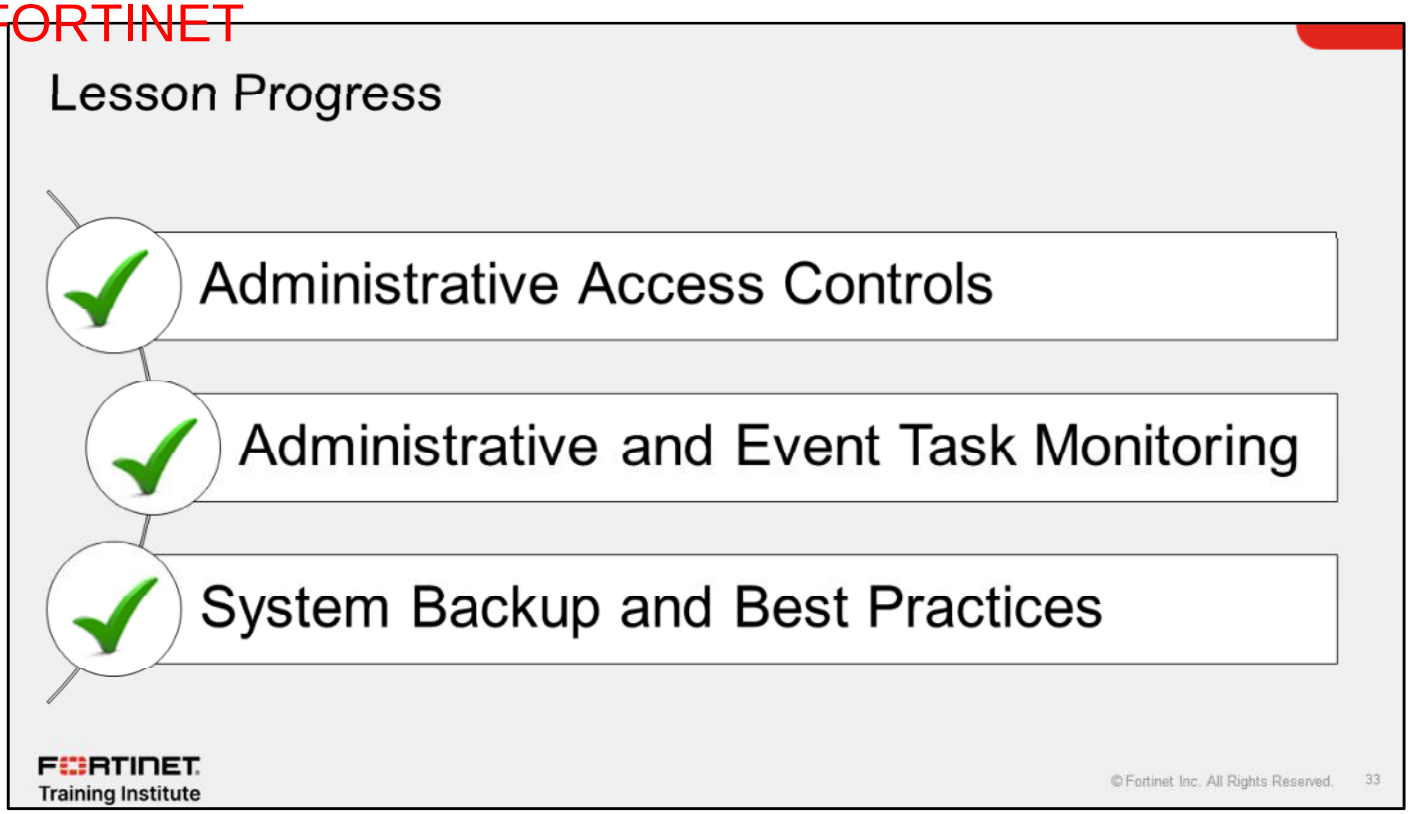
Knowledge Check

1. Which two types of data does the system backup configuration include? (Choose two.)

✓A. Registered device list
B. Reports
C. Events
✓D. System information

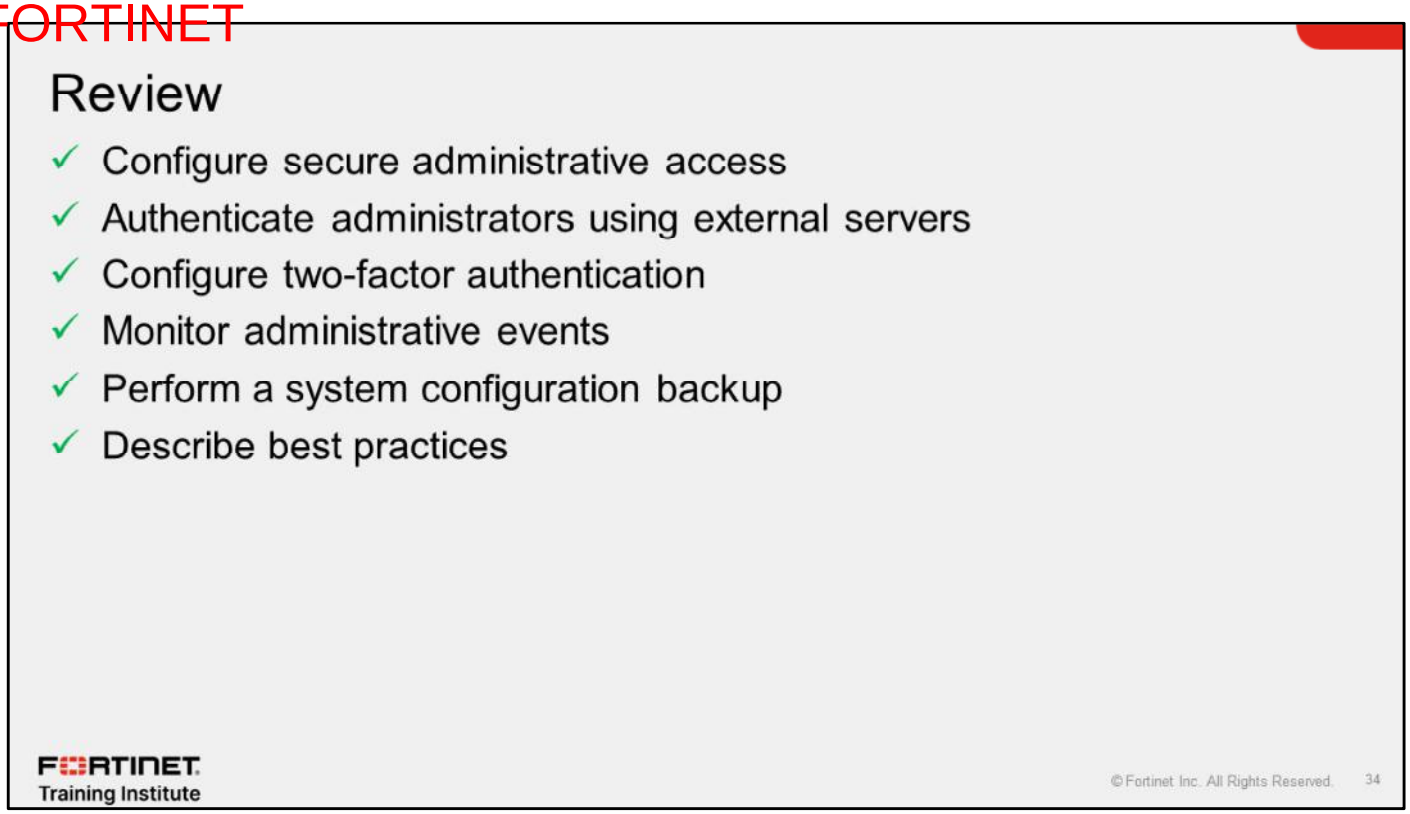
FORTINET Training Institute

 32



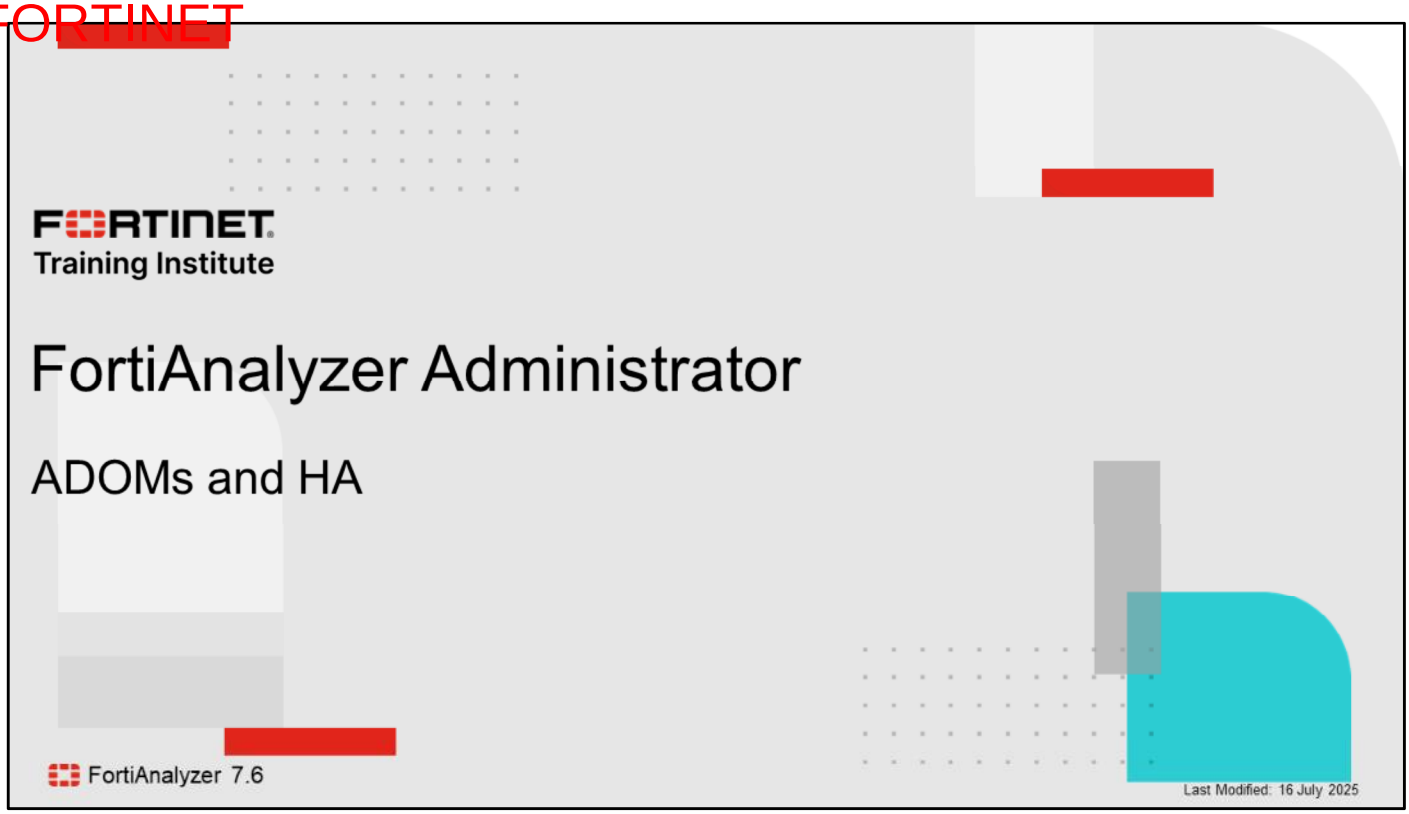
Congratulations! You have completed this lesson.

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

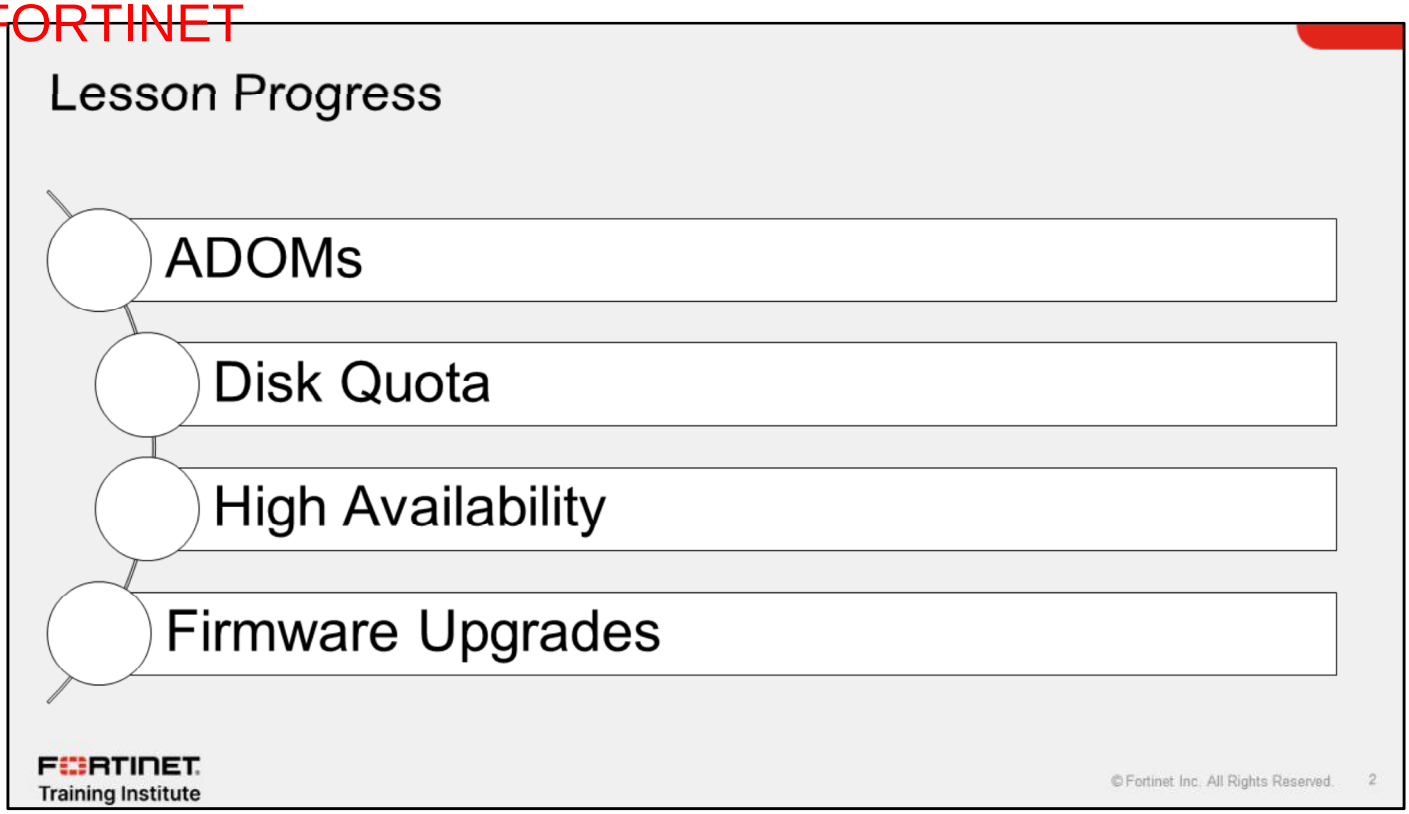


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use administration and management functions to better defend FortiAnalyzer—and the sensitive log data it stores—against external and internal threats.



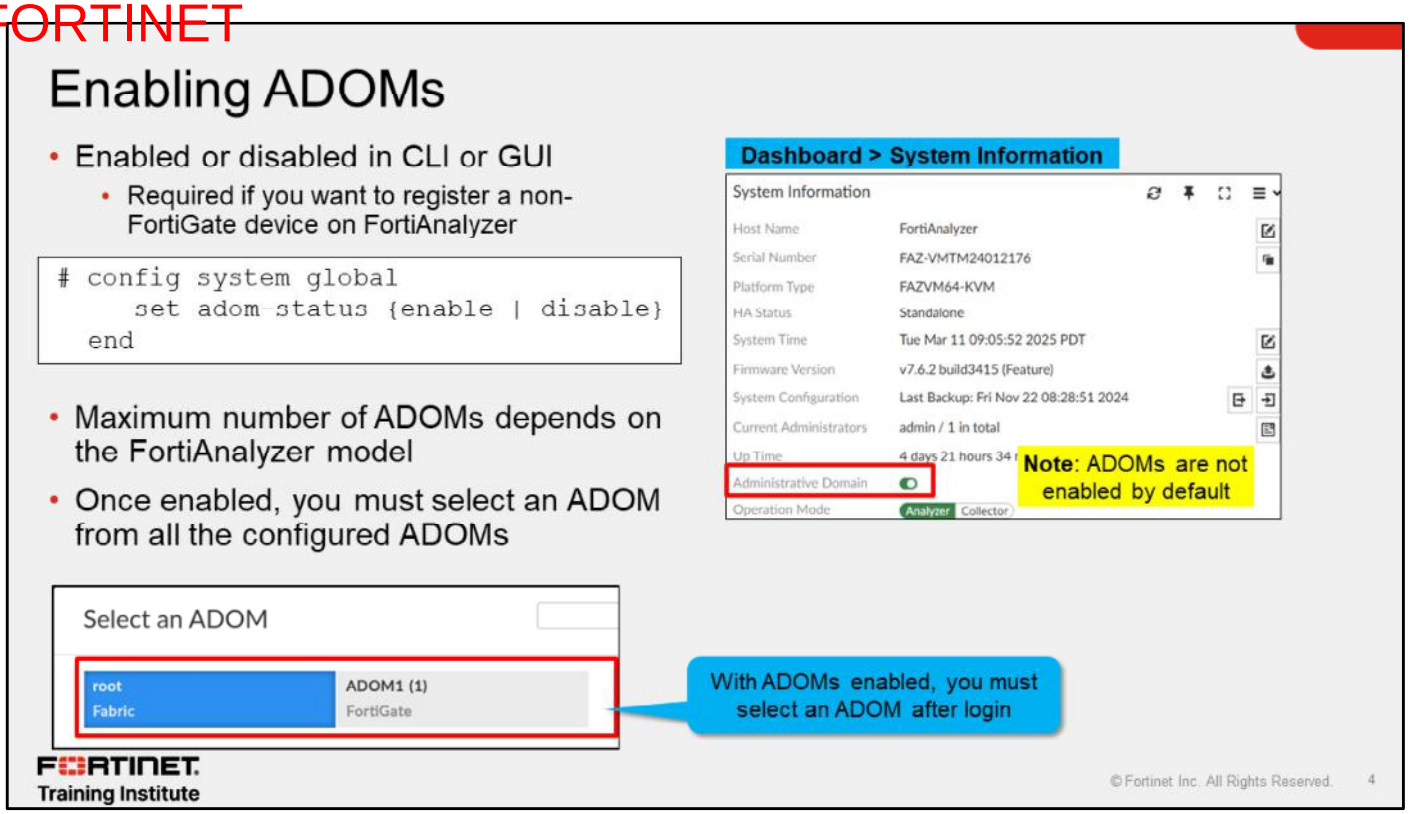
In this lesson, you will learn how to use high availability (HA) to make your FortiAnalyzer deployment more resilient.



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 in the slide.

By demonstrating competence in ADOMs, you will be able to group devices for administrators to monitor and manage. You will also be able to manage data policies and disk space allocation more efficiently.

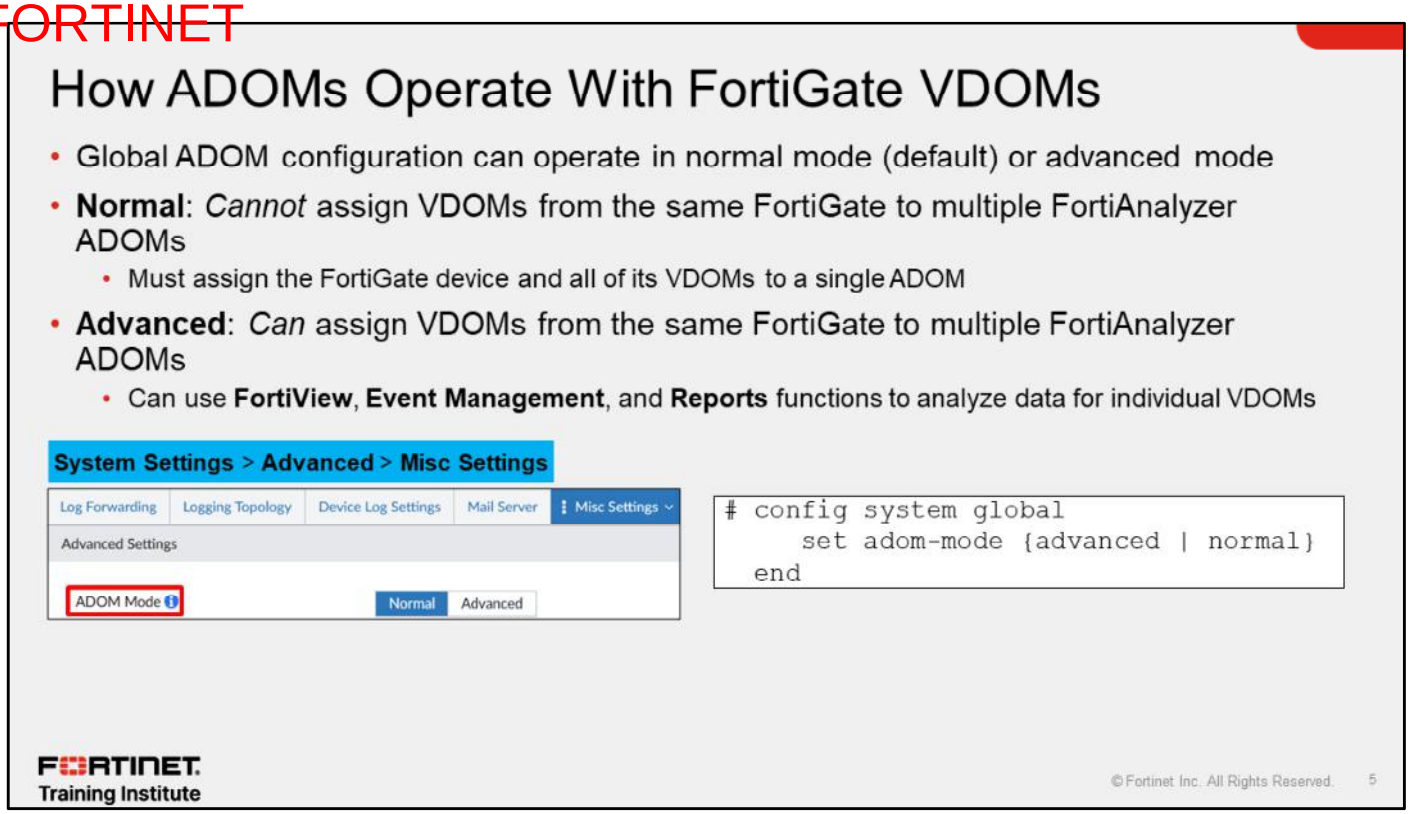


ADOMs are not enabled by default, and only administrators with Super_User access can enable and configure them.

To manage ADOMs, use the command `config system global` in the CLI or go to **System Settings** on the GUI to enable or disable them.

Once you enable ADOMs, the system will log you out to apply the new settings. The maximum number of ADOMs you can activate depends on the specific FortiAnalyzer model you are using.

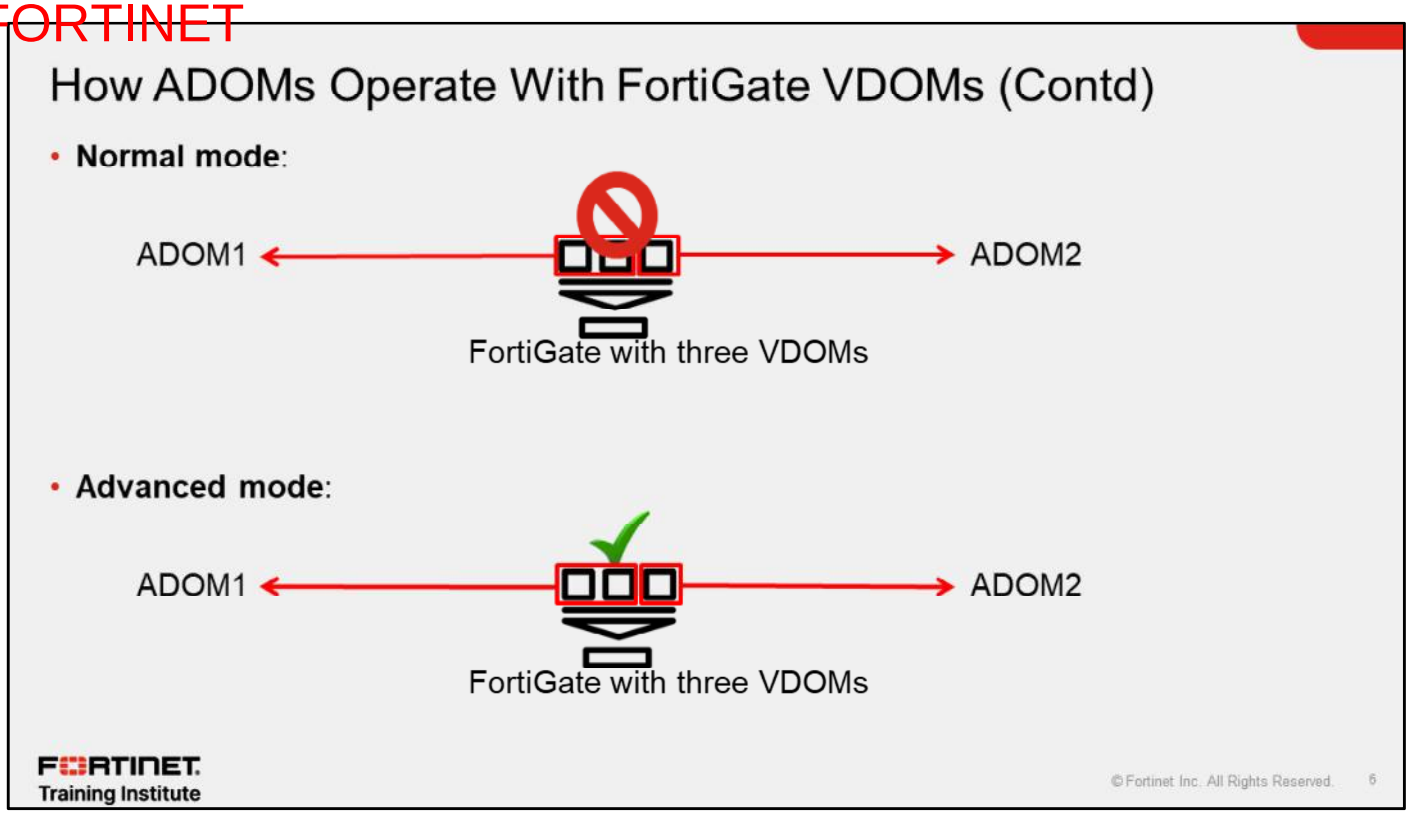
After you log in with ADOMs enabled, you must select the ADOM you want to view from the list of configured ADOMs.



A global ADOM configuration can operate in either Normal mode, which is the default mode, or Advanced mode.

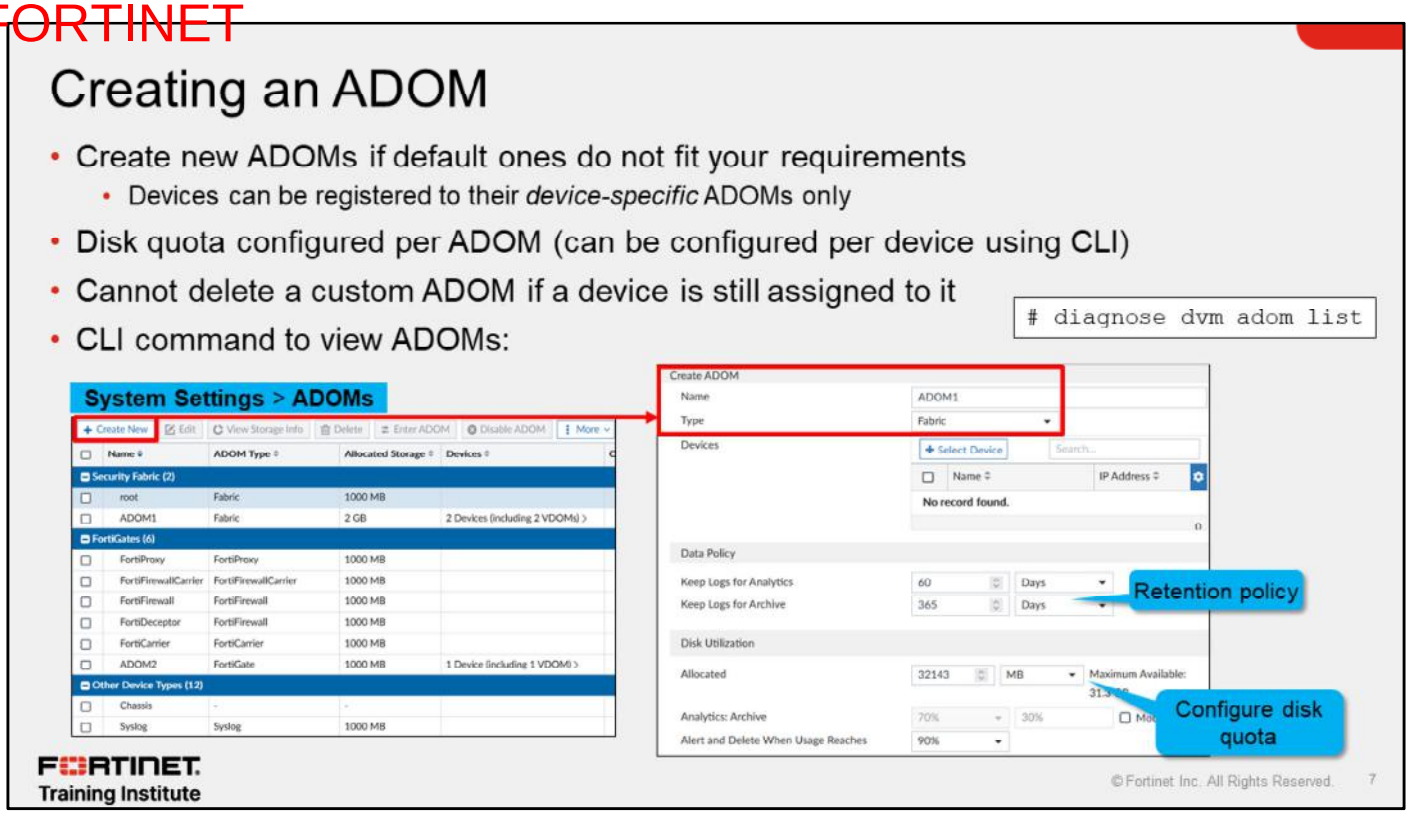
In normal mode, you *cannot* assign VDOMs from the same FortiGate to multiple FortiAnalyzer ADOMs. You must assign the FortiGate device and all of its VDOMs to a single ADOM.

In Advanced mode, you can assign VDOMs from the same FortiGate device to multiple FortiAnalyzer ADOMs. This mode allows you to use the **FortiView**, **Event Management**, and **Reports** functions to analyze data for individual VDOMs—Advanced mode results in more complicated management scenarios.



The image on this slide shows two scenarios, each consisting of a FortiGate with three VDOMs configured.

In normal mode, it is not possible to assign different VDOMs to different ADOMs. However, in advanced mode, each VDOM can be assigned to a different ADOM.

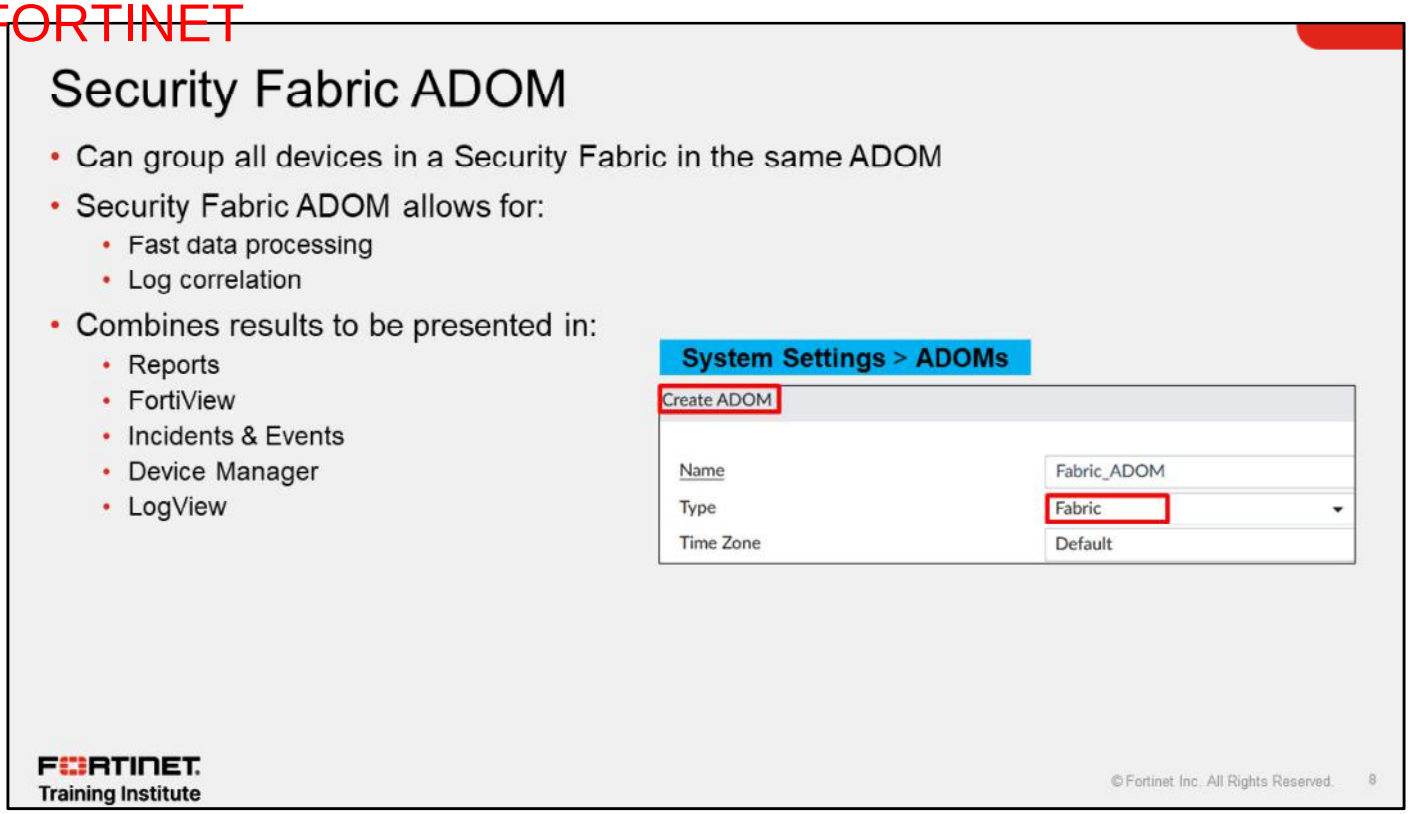


On the ADOMs page, you can view all the configured ADOMs, including the default ADOMs for all non-FortiGate devices. If the default ADOMs do not meet your needs, you can create custom ones.

When creating an ADOM, it is important to select the appropriate type that corresponds to the device you plan to add. For example, if you want to create an ADOM for a FortiGate device, you must select FortiGate as the ADOM type. By default, the ADOM type is set to Fabric for the root ADOM or when creating a new ADOM.

During the creation of a new ADOM, you also have the option to set a disk quota. This quota applies to the ADOM, rather than to the individual devices added within it. You can add quotas to individual devices using the CLI.

Additionally, you cannot delete custom ADOMs that have assigned devices until all devices are removed from that ADOM.



In FortiAnalyzer, all Fortinet devices within a Security Fabric can be grouped into the same ADOM.

This configuration facilitates rapid data processing and log correlation, allowing combined results to be displayed in various sections, including **Device Manager**, **Log View**, **FortiView**, **Incidents & Events**, and **Reports**.

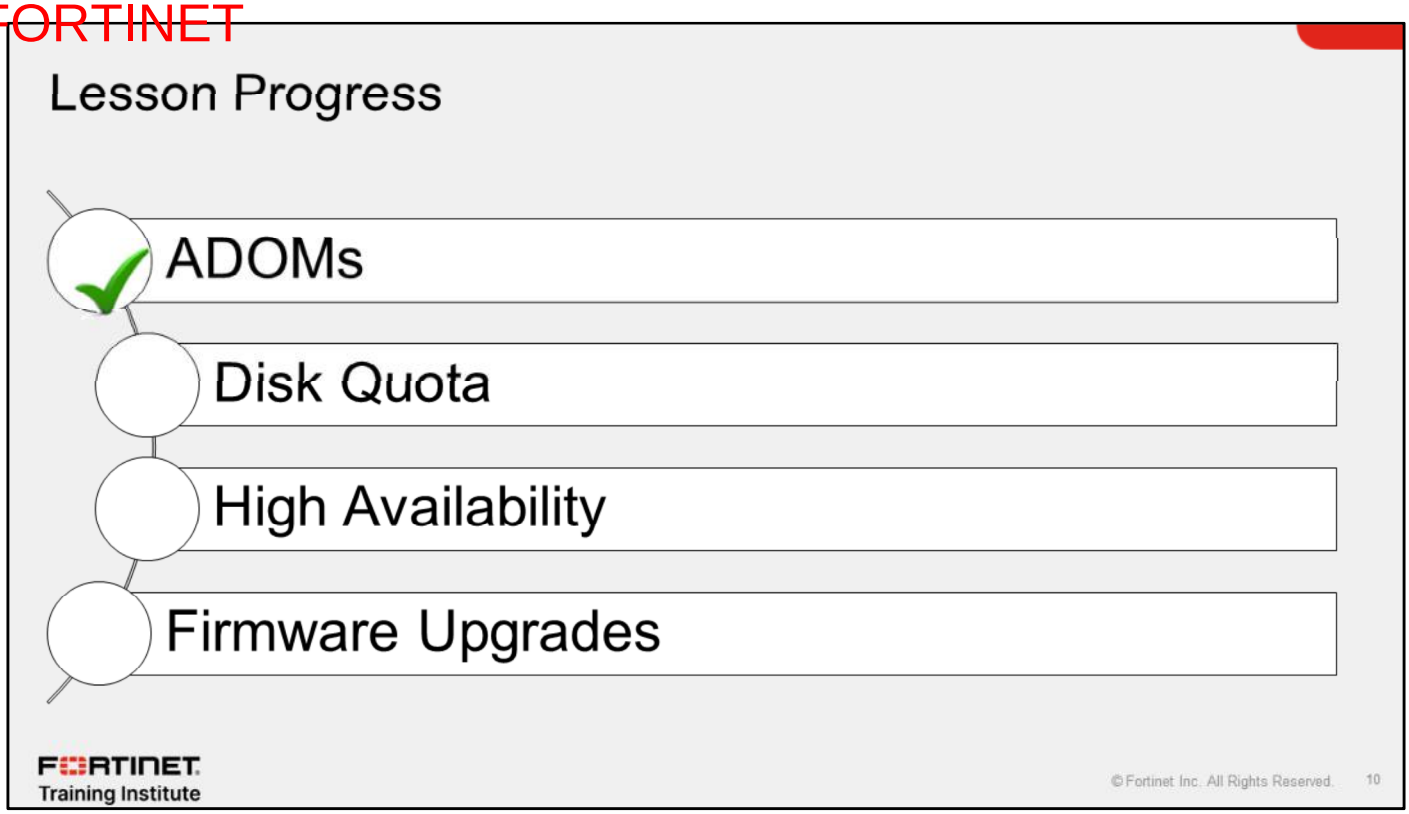
Once a Fabric ADOM is created, it appears under the **Security Fabric** section of **All ADOMs**.

Knowledge Check

1. Disk quota is assigned to the _____.
   - ✓A. ADOM
   - B. Device
2. Which statement about ADOM Advanced mode is true?
   - A. You must assign FortiGate and all its VDOMs to a single ADOM.
   - ✓B. You can assign FortiGate VDOMs from a single device to multiple ADOMs.

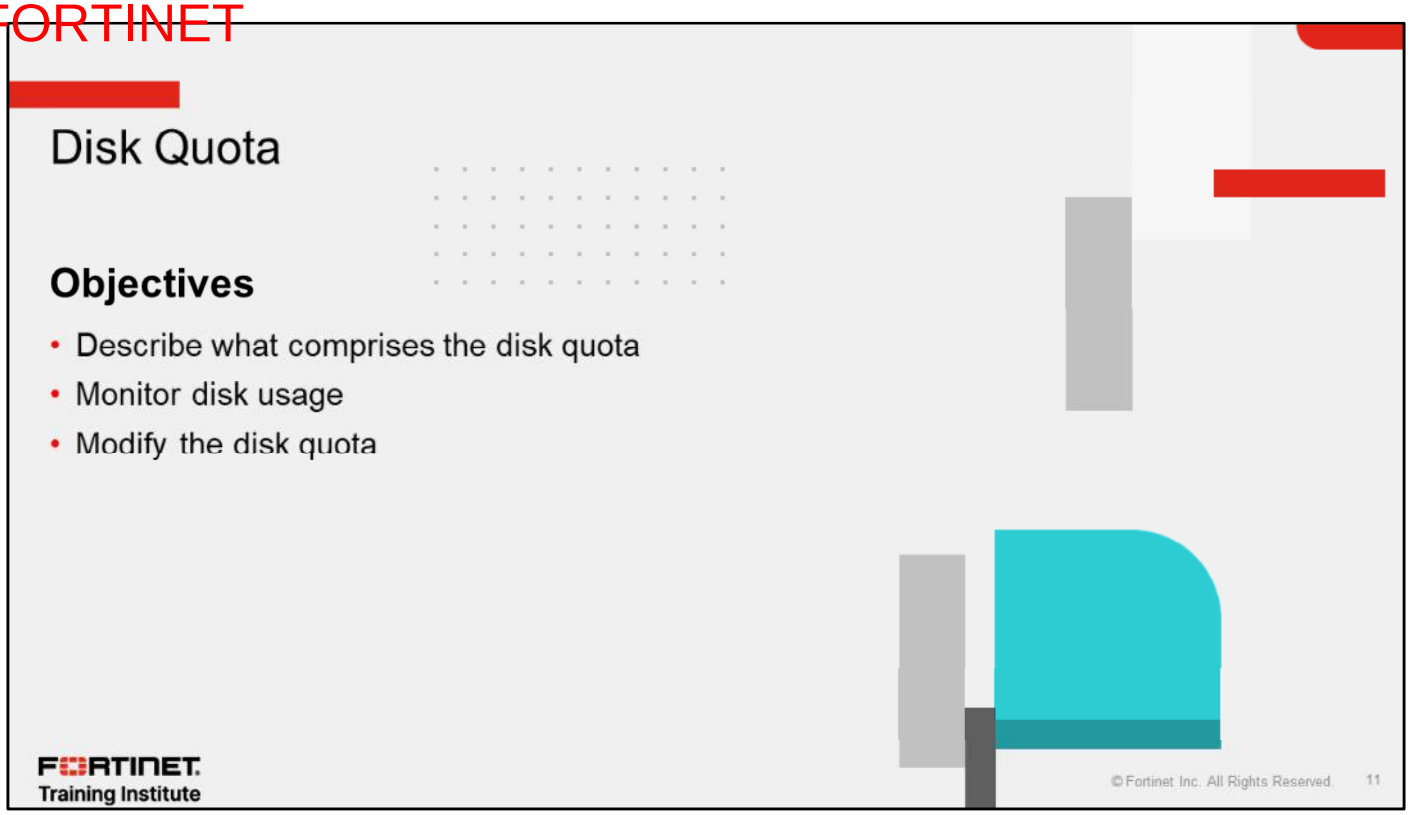
FORTINET Training Institute

 9



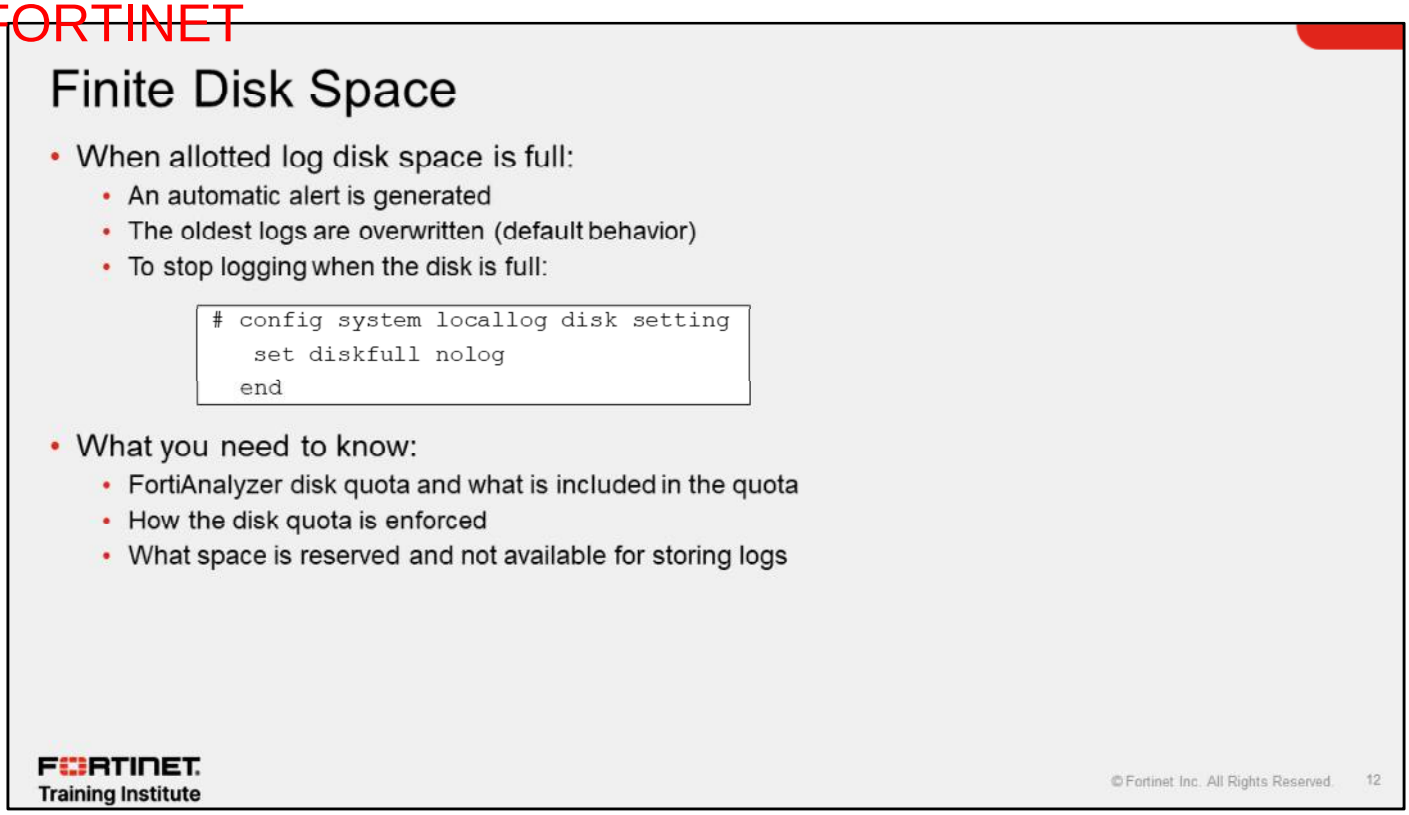
Good job! You now understand ADOMs.

Now, you will learn how to manage disk quotas.



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

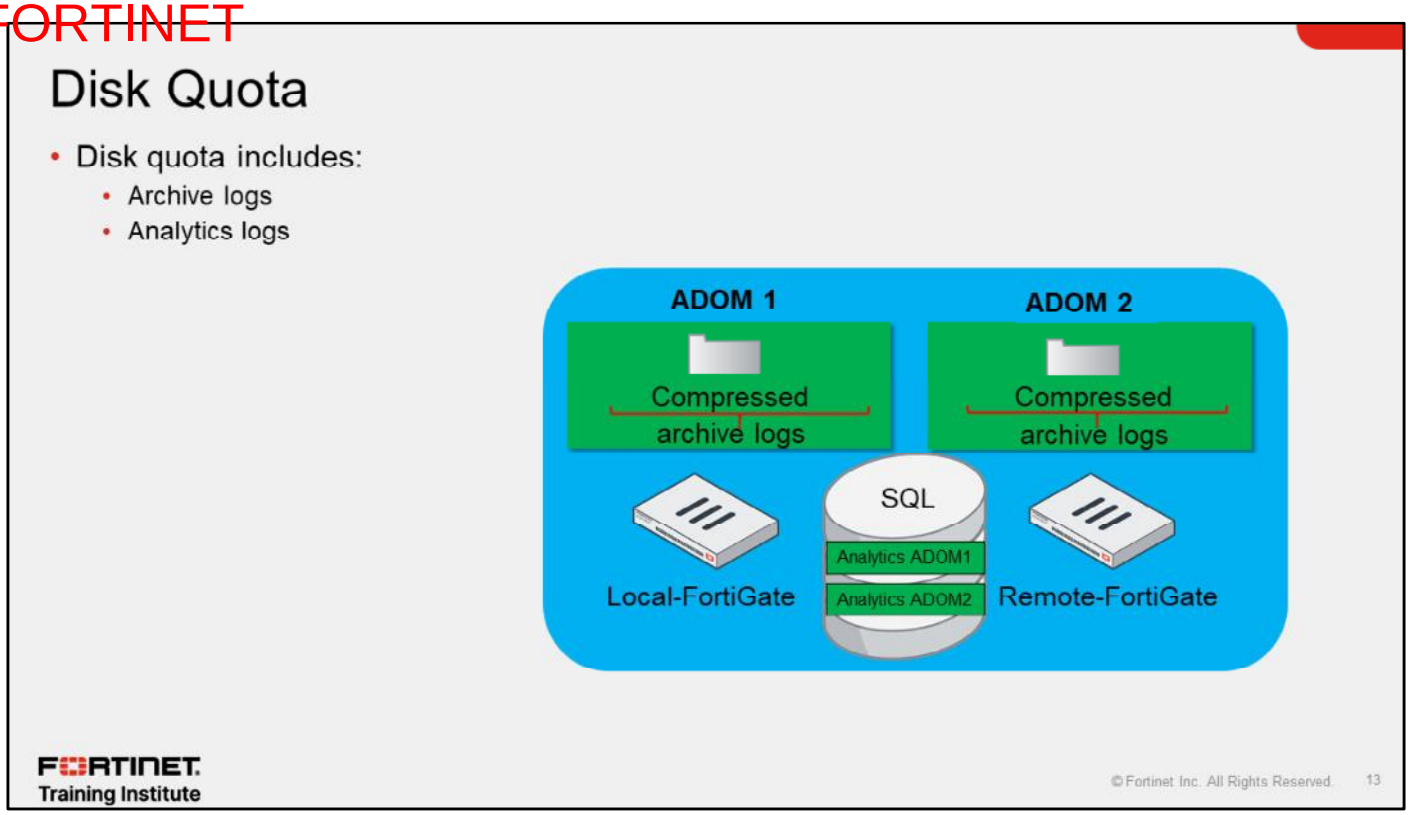
By demonstrating competence in understanding disk quota and how to modify it, you will be able to use disk quotas more effectively in your network.



FortiAnalyzer devices have limited disk space. When the allocated log disk space reaches its capacity, the following happens:

- On the Alert Message Console, FortiAnalyzer automatically generates an alert message categorized as a warning event log.
- FortiAnalyzer overwrites the oldest logs. While this is the default setting, you can modify the behavior to stop logging entirely once the disk is full.

No administrator wants to lose important log data or face compliance issues regarding data retention. Therefore, it is essential to understand your FortiAnalyzer disk quota, how it is enforced, and which space is reserved and unavailable for storing logs.



The FortiAnalyzer disk quota includes two types of logs:
- Archive logs: These are logs compressed on hard disks and offline.
- Analytics logs: These are the logs stored and indexed in the SQL database and online.

Analytics logs indexed in the SQL database require more disk space than archive logs. The only exception to this rule is when a FortiAnalyzer VM is deployed in collector mode because the SQL database is not running.

An average indexed log is 600 bytes, and an average compressed log is only 80 bytes. Consider this difference when specifying the storage ratio for analytics and archive logs. The default ratio is 70% to 30%.

Reserved Disk Quota

- FortiAnalyzer reserves 5% to 20% disk space for system usage and unexpected quota overflow
- Only 80% to 95% of the disk space is available for allocation to devices

Disk size	Reserved system disk quota
Small (< 500 GB)	20% or 50 GB, whichever is smaller
Medium (500 GB – 1000 GB)	15% or 100 GB, whichever is smaller
Large (1000 GB – 3000 GB)	10% or 200 GB, whichever is smaller
Very large (3000 – 5000 GB)	5% or 500 GB, whichever is smaller

```
# diagnose log device
```

To view the amount of reserved space

- RAID levels determine the disk size and reserved disk quota level
  - For example, a FAZ 1000C with four 1 TB hard drives configured in RAID 10 is considered a large disk (2 TB)

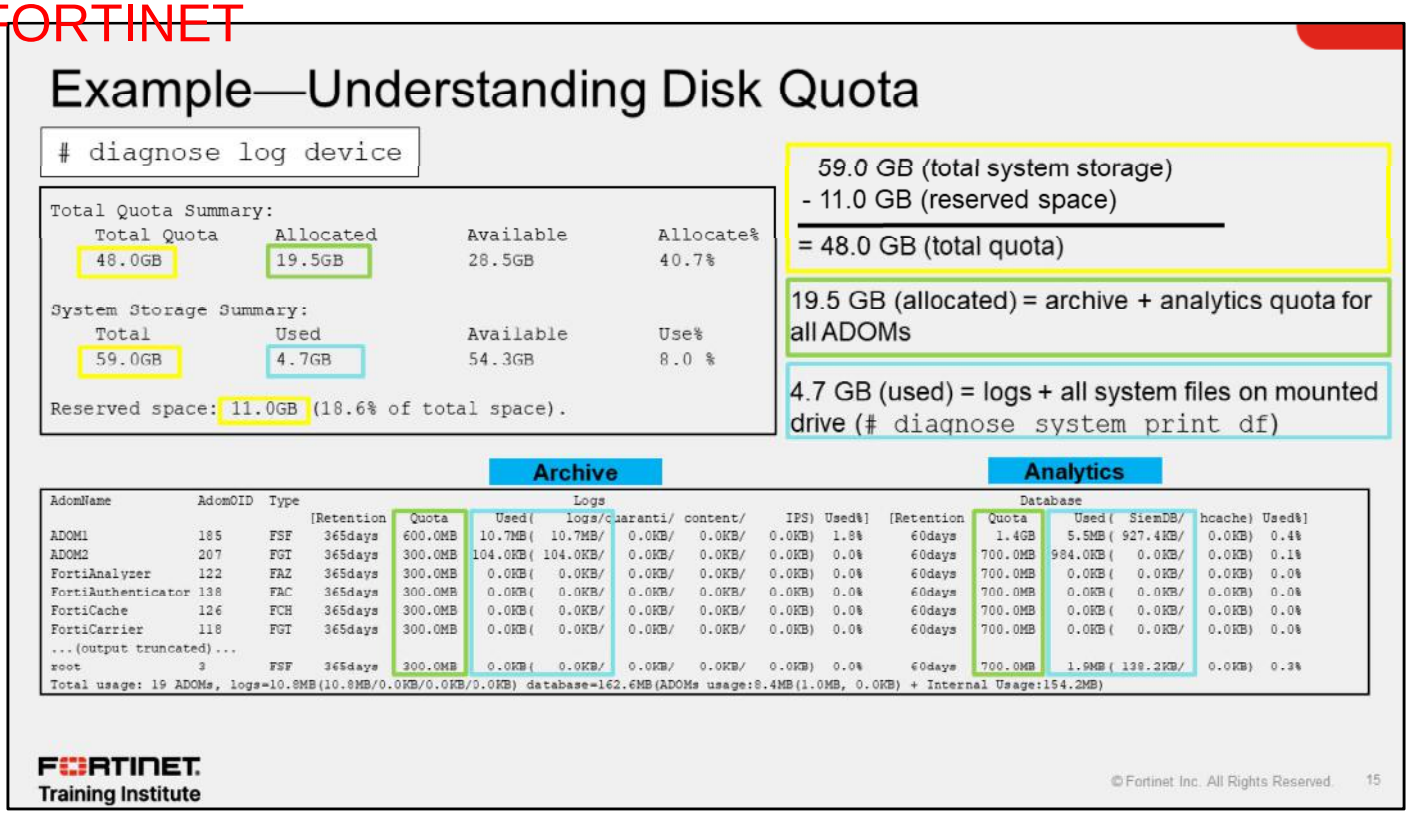
FORTINET Training Institute

 14

By default, each ADOM is allocated 1000 MB (just under 1 GB) of storage on FortiAnalyzer for log data. However, this allocation is configurable. The minimum storage limit cannot be set below 100 MB, while the maximum depends on the disk space available on the specific FortiAnalyzer device.

FortiAnalyzer reserves between 5% and 20% of the disk space for compressed files, uploaded files, and temporary report files. This reservation leaves approximately 80% to 95% of the disk space available for allocation to devices.

It's important to note that if RAID is being used, the RAID level will influence the total disk size and the reserved quota.

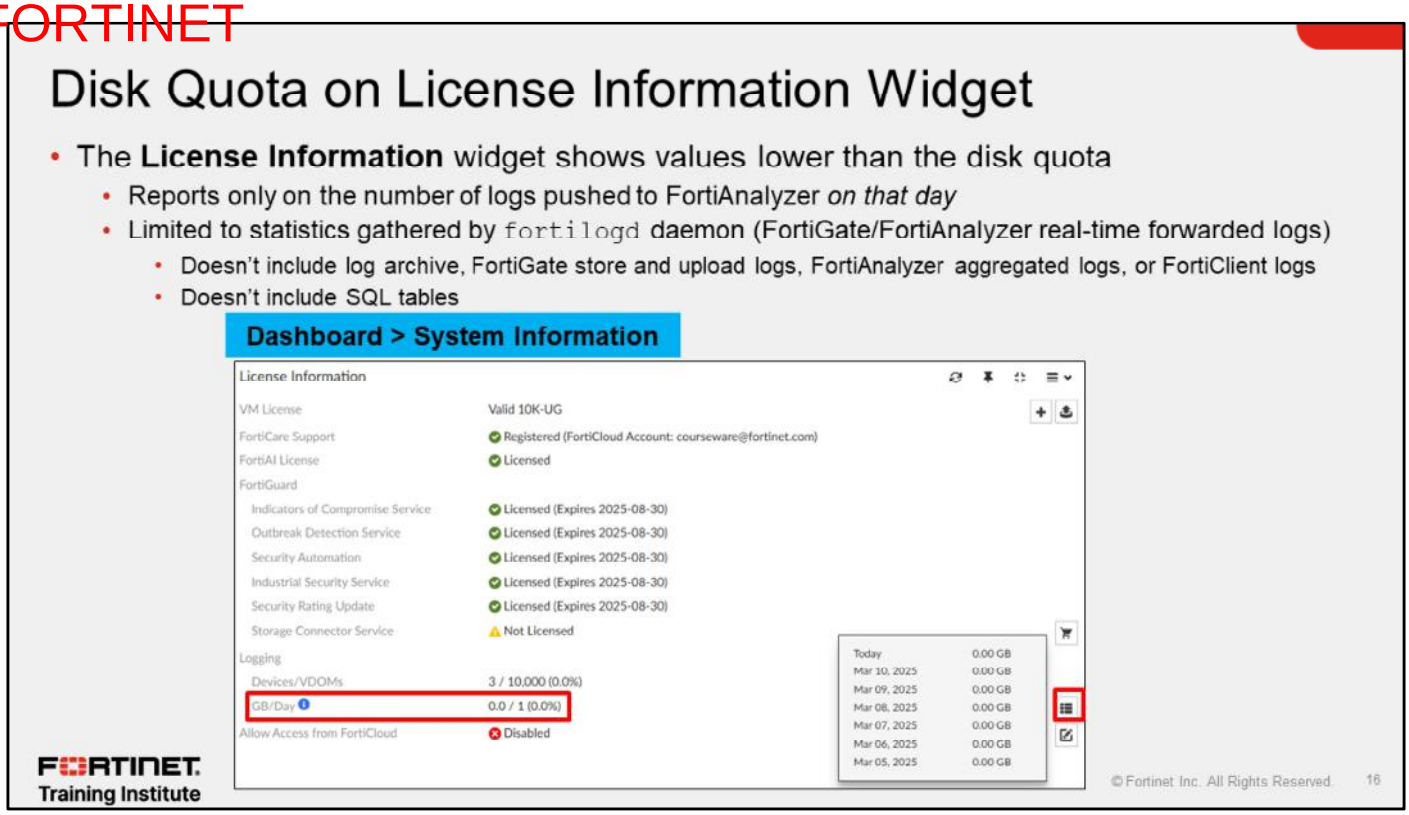


You can view your log disk usage, including usage for each ADOM, using the CLI command shown on this slide.

Determine the total quota by subtracting the reserved space from the total system storage.

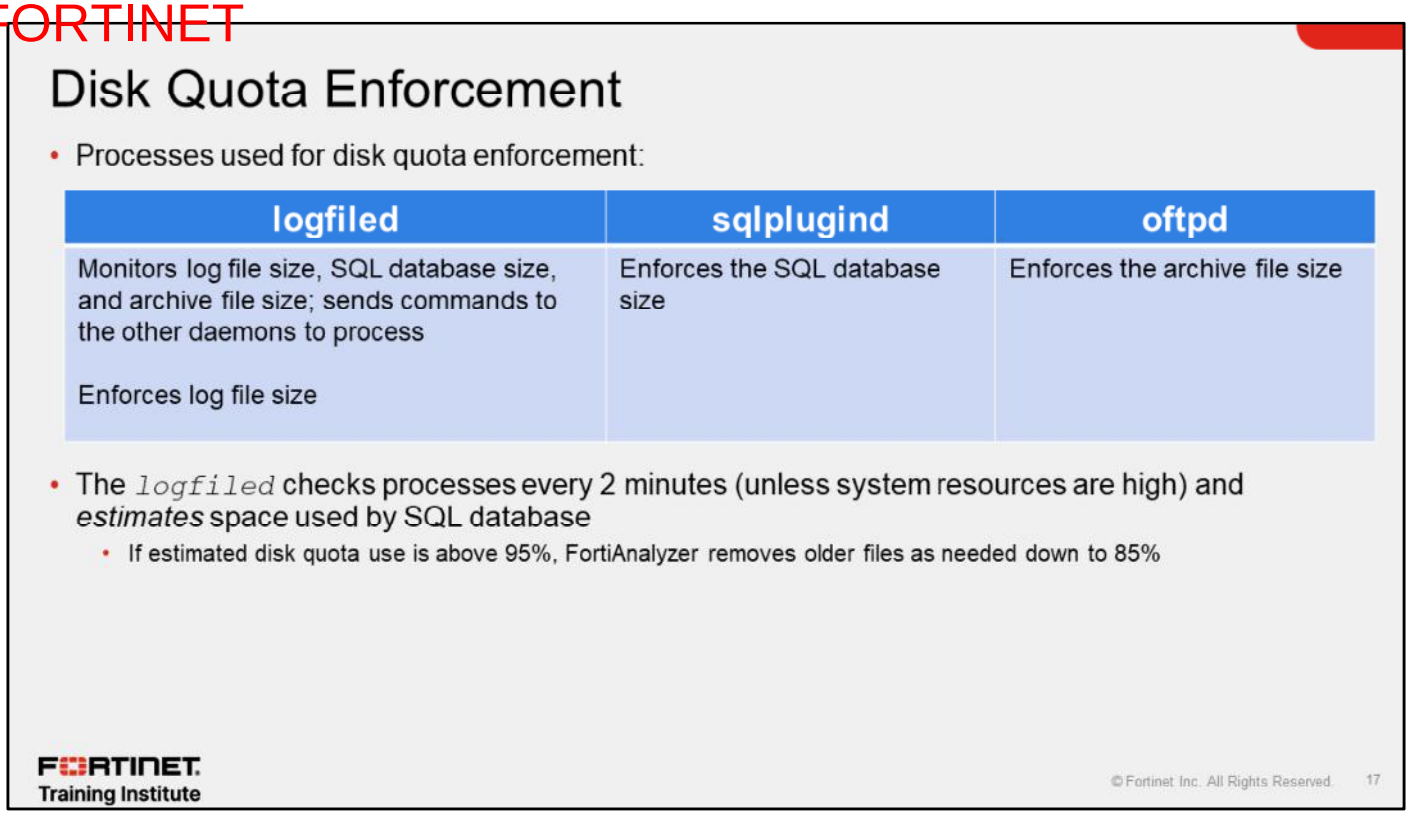
Determine the allocated space by adding the archive and analytics quota for all ADOMs.

Determine the used space by adding the archive, analytics logs, and all the system files mounted on the drive. To view the system file value, enter the CLI command `diagnose system print df`.



The **License Information** widget displays a lower value than the disk quotas. This discrepancy occurs because it reports only the number of logs pushed to FortiAnalyzer on a given day. To view the log volume for the previous six days, click the **Show Details** icon. Additionally, the widget accounts only for ingress traffic, which is limited to the raw log portion. It does not include log archives, FortiGate store and upload logs, FortiAnalyzer aggregated logs, or FortiClient logs. SQL database tables are also excluded, as FortiAnalyzer performs indexing on the logs after they have been received.

It's important to monitor your daily log limit and configured disk quotas. If you find that either is consistently nearing or exceeding the threshold, consider optimizing your FortiAnalyzer configuration by filtering out unnecessary logs or removing devices that do not need to be logged. If your network consistently generates traffic that surpasses the daily log limit, you may want to increase your licensing level. Additionally, if the disk quota is inadequate for your logging needs, you will need to allocate more resources.



Different processes are responsible for enforcing disk quotas:

· The `logfiled` process monitors other processes to enforce log file size and disk quotas.
· The `sqlplugind` process manages the size of the SQL database.
· The `oftpd` process oversees the size of archive files.

The `logfiled` daemon checks on these processes every 2 minutes, unless system resources are strained. It also estimates the space used by the SQL database. If the estimated disk usage exceeds 95%, FortiAnalyzer will delete files as necessary to reduce usage to 85%.

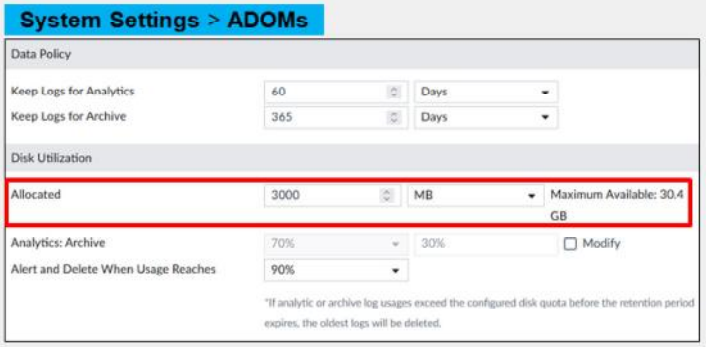
Modify ADOM Disk Quota

- Monitor log utilization and quotas

```
# diagnose log device
```

- If the volume of logs is high, consider increasing the ADOM log quota to prevent the loss of the oldest logs

- Allocating an insufficient quota to an ADOM can:
  - Hinder log retention objectives
  - Consume unnecessary CPU resources while enforcing the quota with log deletion and database trims
  - Impact reporting if quota enforcement affects analytical data before a report is complete



FORTINET Training Institute

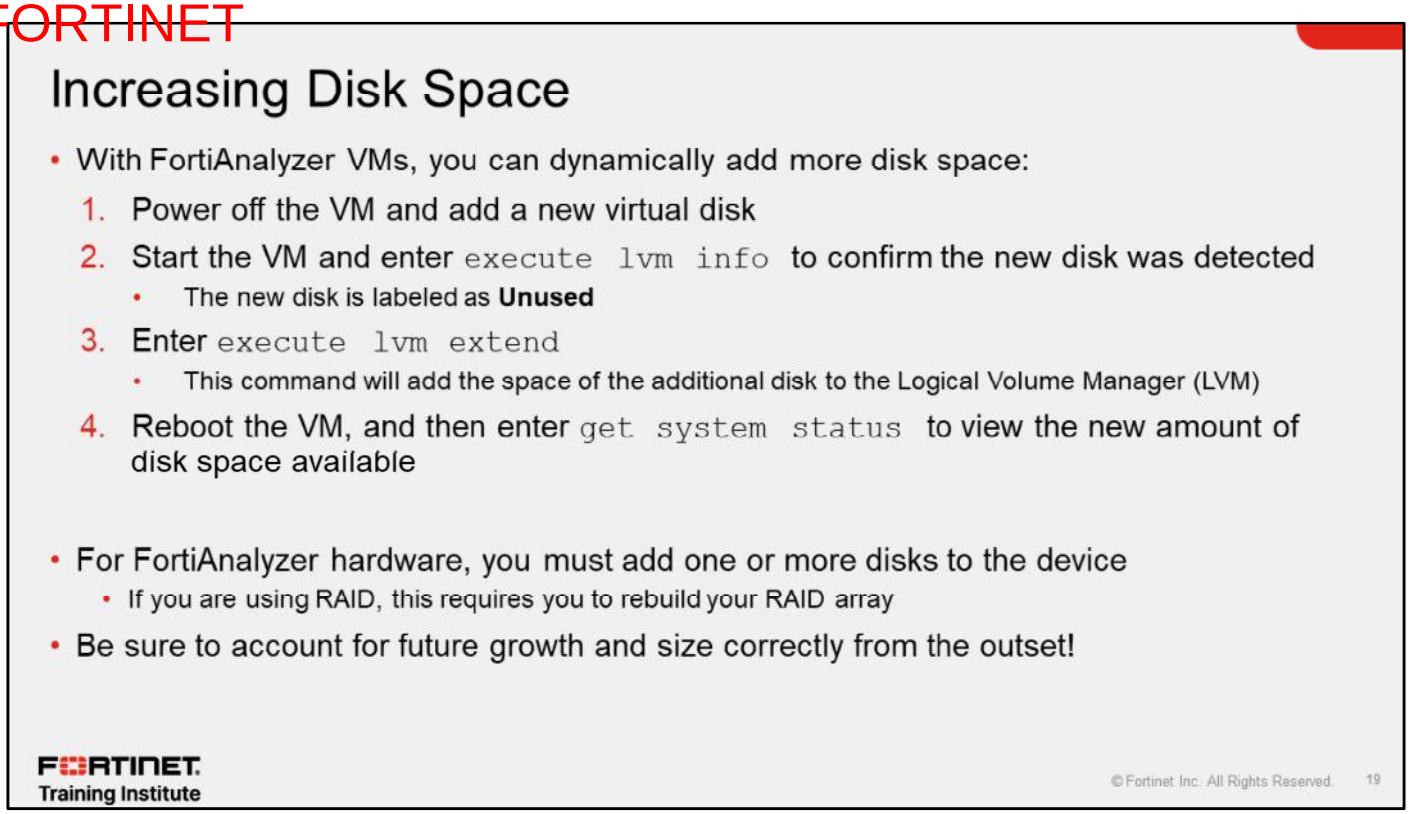
 18

Based on your log rate and device usage statistics, you may need to adjust your ADOM disk quota to avoid losing important log data.

It's essential to regularly monitor the log rate for each device within the ADOM. If you notice a high volume of logs, consider increasing the ADOM quota to ensure that the oldest logs are not discarded prematurely.

Allocating an insufficient quota to an ADOM can lead to several issues, including:

- Inability to meet your log retention objectives.
- Unnecessary CPU resource consumption due to log deletion and database trimming enforced by the quota.
- Negative impact on reporting if the quota enforcement affects analytical data before a report is complete.



If increasing the disk quota is not enough based on your monitored log rate, you may need to improve your overall disk space.

For FortiAnalyzer VMs, you can dynamically add more disk space by following the procedure shown on this slide.

For FortiAnalyzer hardware, you must add one or more disks. If you are using RAID, you must rebuild your RAID array if you add another disk. Therefore, it's essential to properly plan for future growth and sizing from the start.

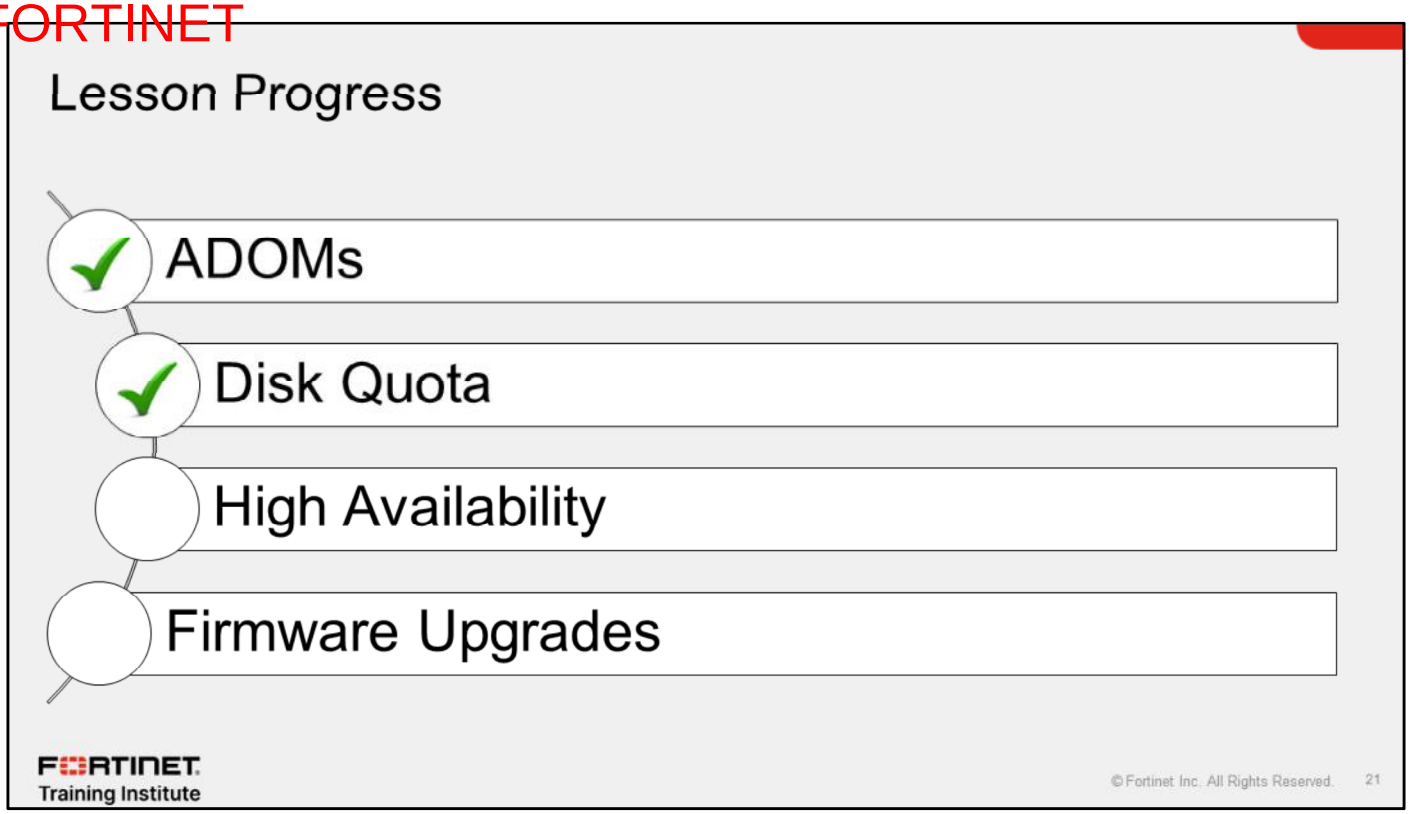
Knowledge Check

1. By default, what happens when the allotted log disk space is full?
   - ✓A. The oldest logs are overwritten.
   - B. Logging stops.

2. What is disk quota composed of?
   - ✓A. Archive logs and analytics logs
   - B. Raw logs and archive files

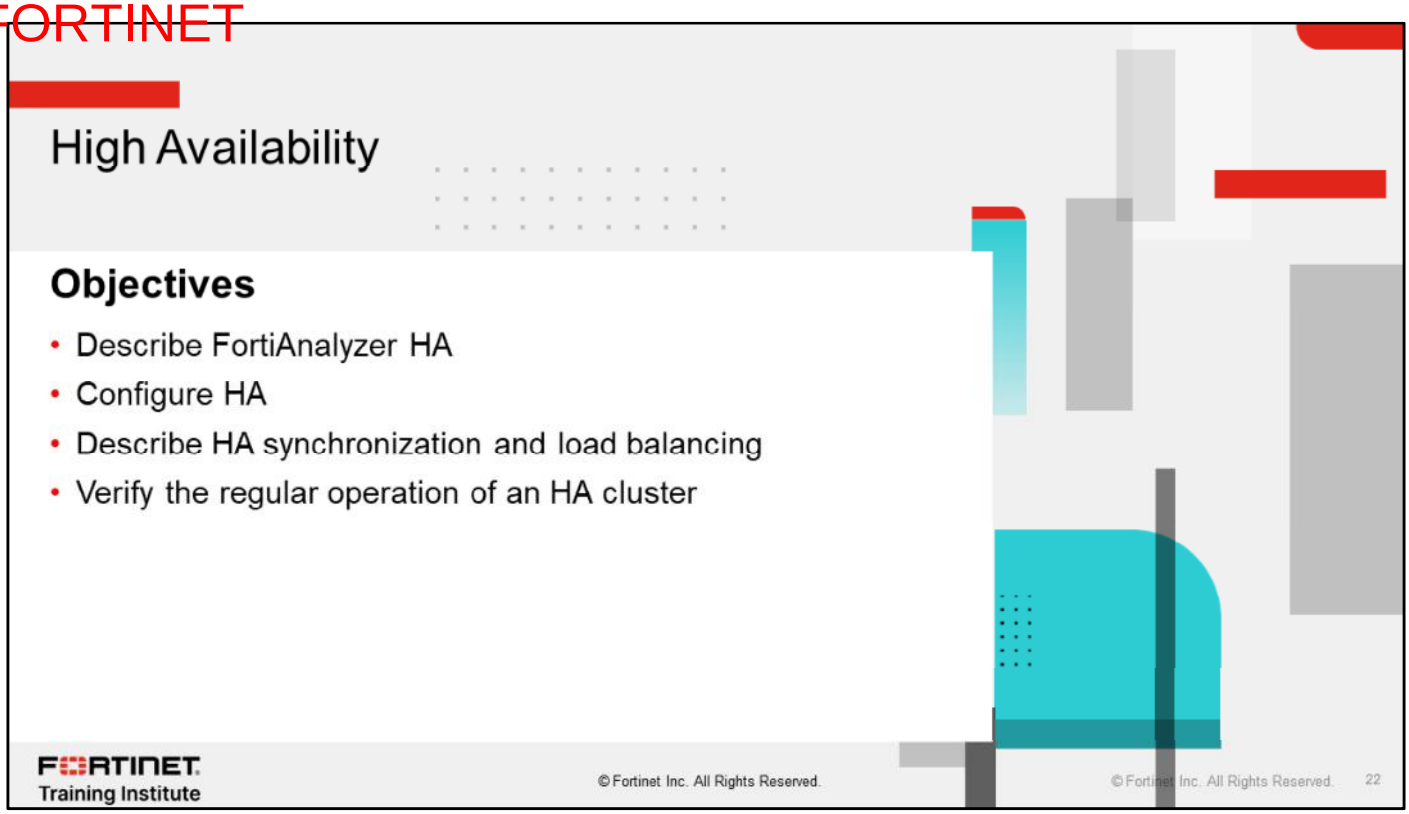
FORTINET Training Institute

 20



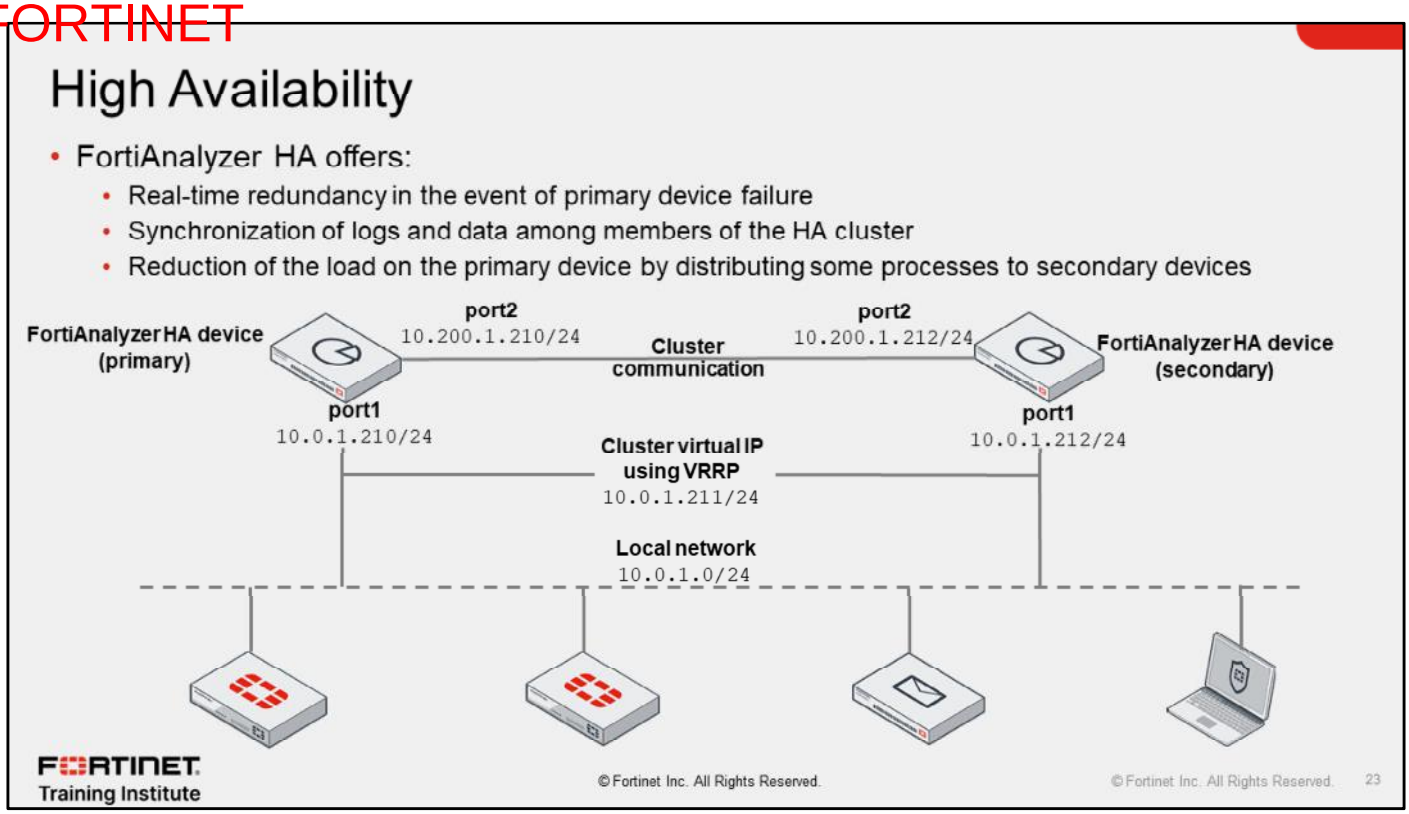
Good job! You now understand disk quotas.

Now, you will learn about FortiAnalyzer HA.



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

By demonstrating competence in configuring and troubleshooting high availability (HA), you can increase the availability of your FortiAnalyzer implementation.



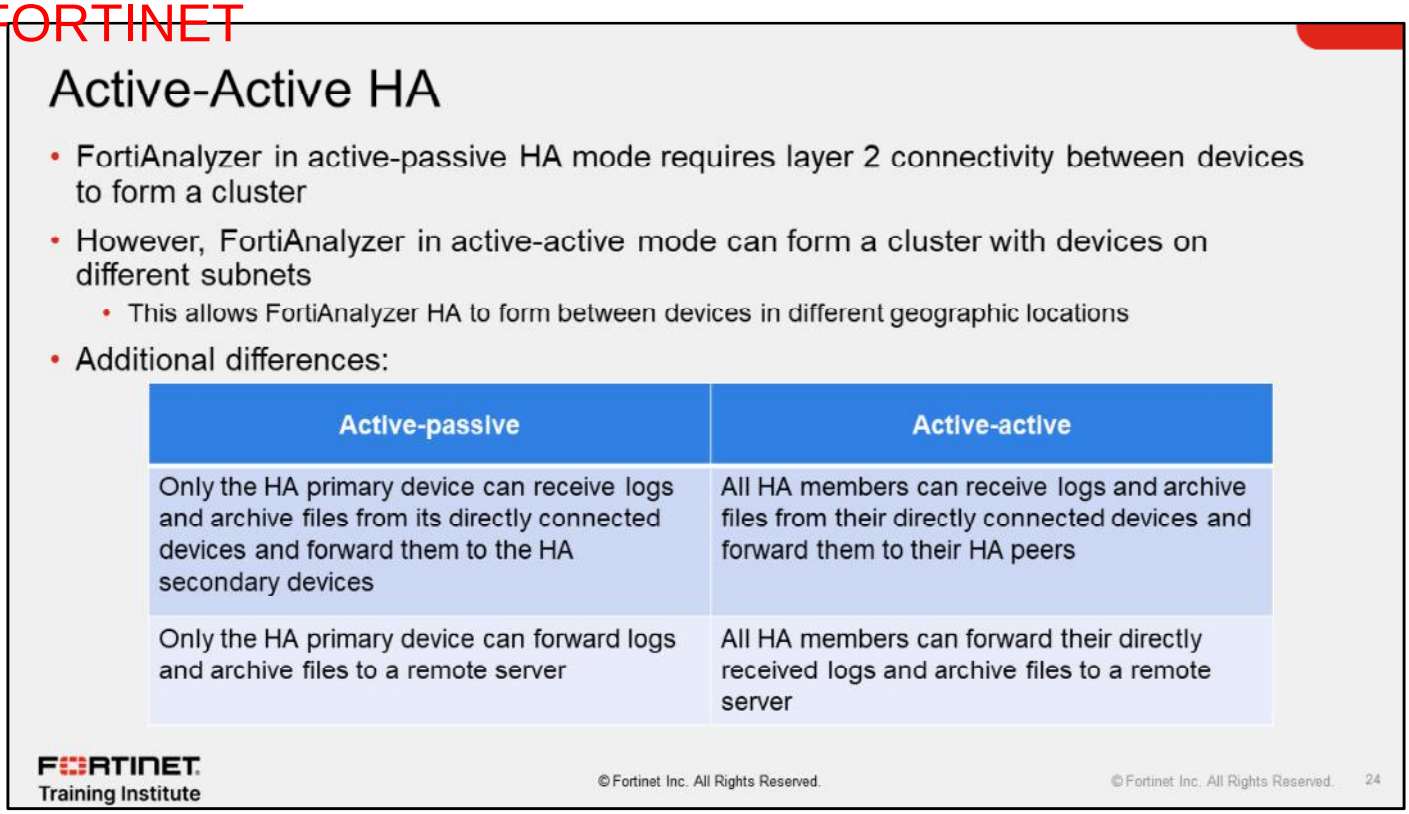
A FortiAnalyzer HA cluster offers the following advantages:

- Real-time redundancy: The cluster ensures continuous operation by automatically selecting another device as the primary if the current primary device fails.
- Secure synchronization: Logs and data are securely synchronized across multiple FortiAnalyzer devices, including system and configuration settings pertinent to HA.
- Load distribution: Secondary devices can take on additional processes like running reports and sharing the load for FortiView widgets, reducing the burden on the primary device.

A FortiAnalyzer HA cluster can consist of a maximum of four devices: one primary device and up to three secondary devices. All devices in the cluster must belong to the same FortiAnalyzer series, operate on the same firmware version, and be visible to each other in the network. Additionally, all devices must run in the same operational mode, either as an analyzer or collector.

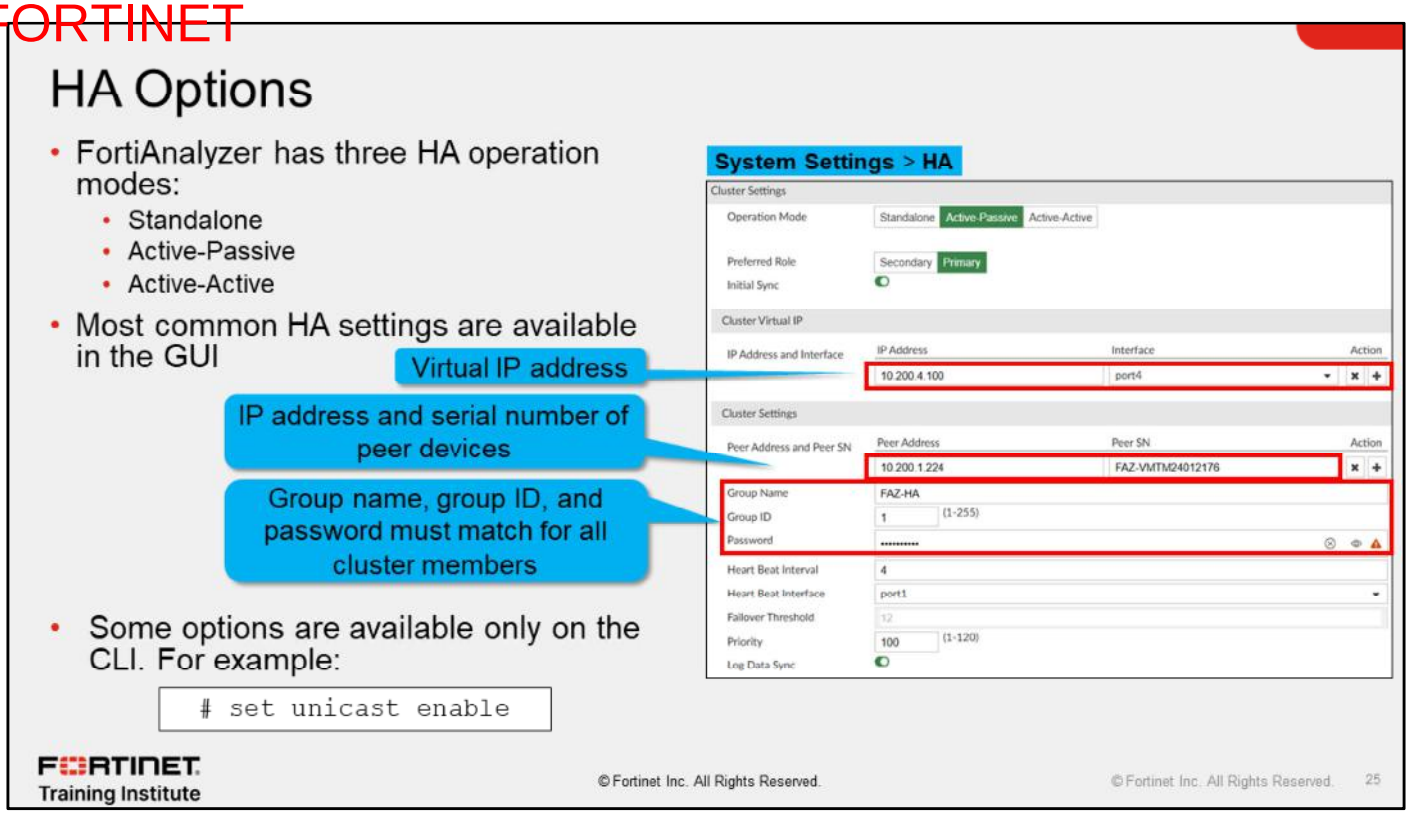
While the available disk space among cluster members does not need to match precisely, it's crucial that each device has sufficient storage for the expected logs. It is recommended that all members have similar available storage.

When using FortiAnalyzer VMs as cluster members, all VMs must be on the same platform. For example, a VM operating on VMware cannot form a cluster with a VM running on kernel-based VM (KVM). If FortiAnalyzer devices with different licenses are combined into an HA cluster, the license with the smallest number of managed devices will dictate the cluster's limits.



FortiAnalyzer HA in active-passive mode requires a layer 2 connection between HA members in order to set up the HA cluster virtual IP address. However, in active-active mode, members can be in different geographic locations and form a cluster. Instead of using a virtual IP address, you define the heartbeat interface as the interface used to communicate with the peer across different networks.

Furthermore, in active-active mode, all HA members can receive logs and archive files from their directly connected devices, and then forward them to other HA members. All HA members can also forward their directly received logs and archive files to a remote server.



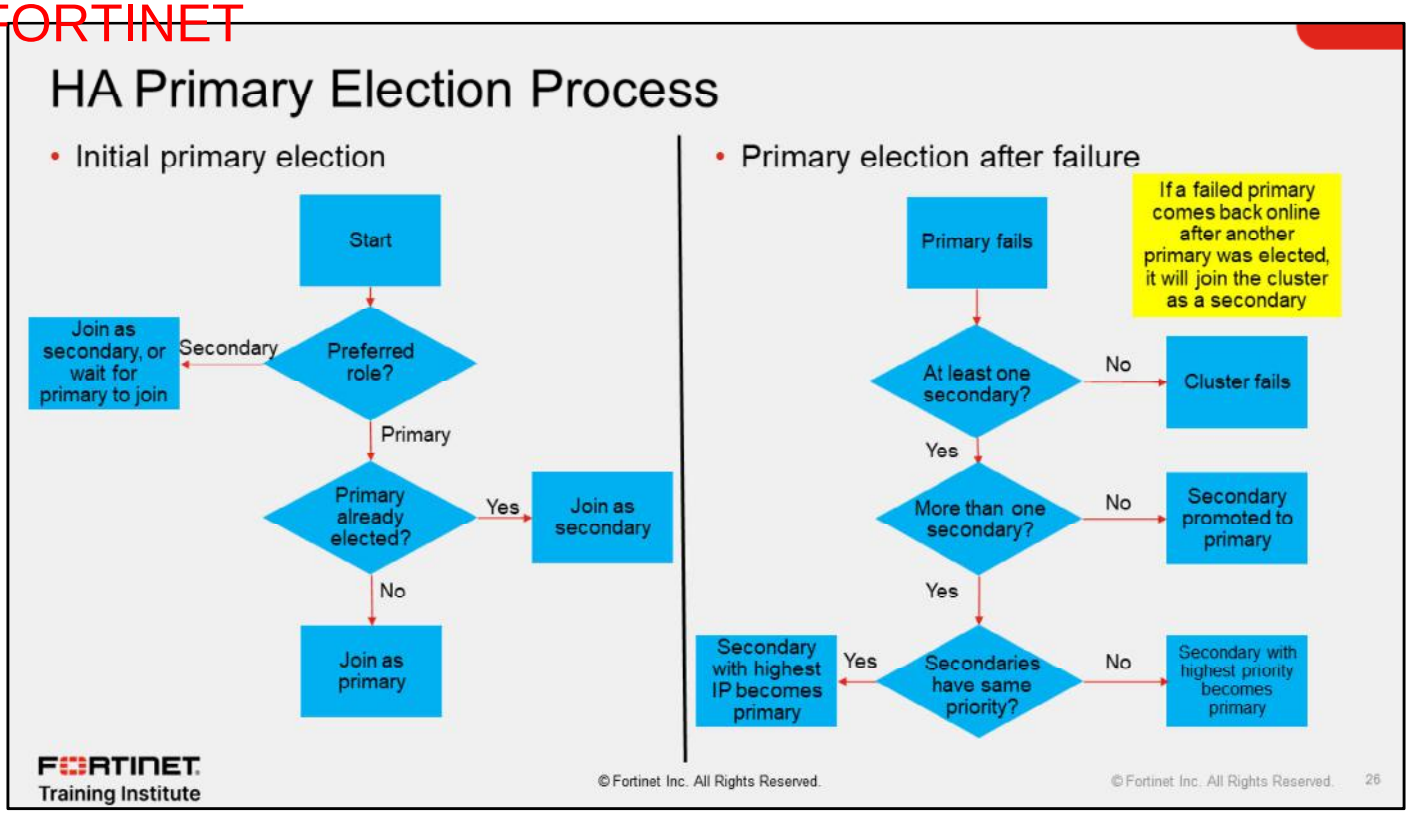
On the **HA** page, use the **Cluster Settings** section to create or change the HA configuration. To configure a cluster, set the **Operation Mode** of the primary device to **High Availability**, and then select the preferred role for the device when it joins the HA cluster.

In the **Cluster Virtual IP** section, select the interface and type the IP address for which the FortiAnalyzer device will provide redundancy. The virtual IP address is optional in active-active mode.

Once the cluster is active, the devices sending their logs must point to the cluster virtual IP address. By default, the Virtual Router Redundancy Protocol (VRRP) heartbeat packets are sent to the multicast address `224.0.0.18` and sourced from the primary IP address of the first virtual IP interface configured. You can configure a different interface to send the heartbeats, as well as set it to use unicast.

Next, add the IP addresses and serial numbers of each secondary device to the peer list of the primary device. The IP address and serial number of the primary device, along with all secondary devices, must be added to each secondary device. All cluster members must be reachable at these IP addresses to ensure proper log synchronization traffic. As shown on the previous slides, these IP addresses do not need to be on the same subnet as the cluster virtual IP address. In fact, it is advisable for them to be on separate subnets.

The primary device and all secondary devices must have the same **Group Name**, **Group ID**, and **Password**. The **Priority** setting is used during the selection of the primary device in the cluster. You can assign a value from 80 to 120, where a higher number has higher priority. The **Log Data Sync** option is enabled by default. It provides real-time log synchronization among cluster members, after the initial log synchronization.

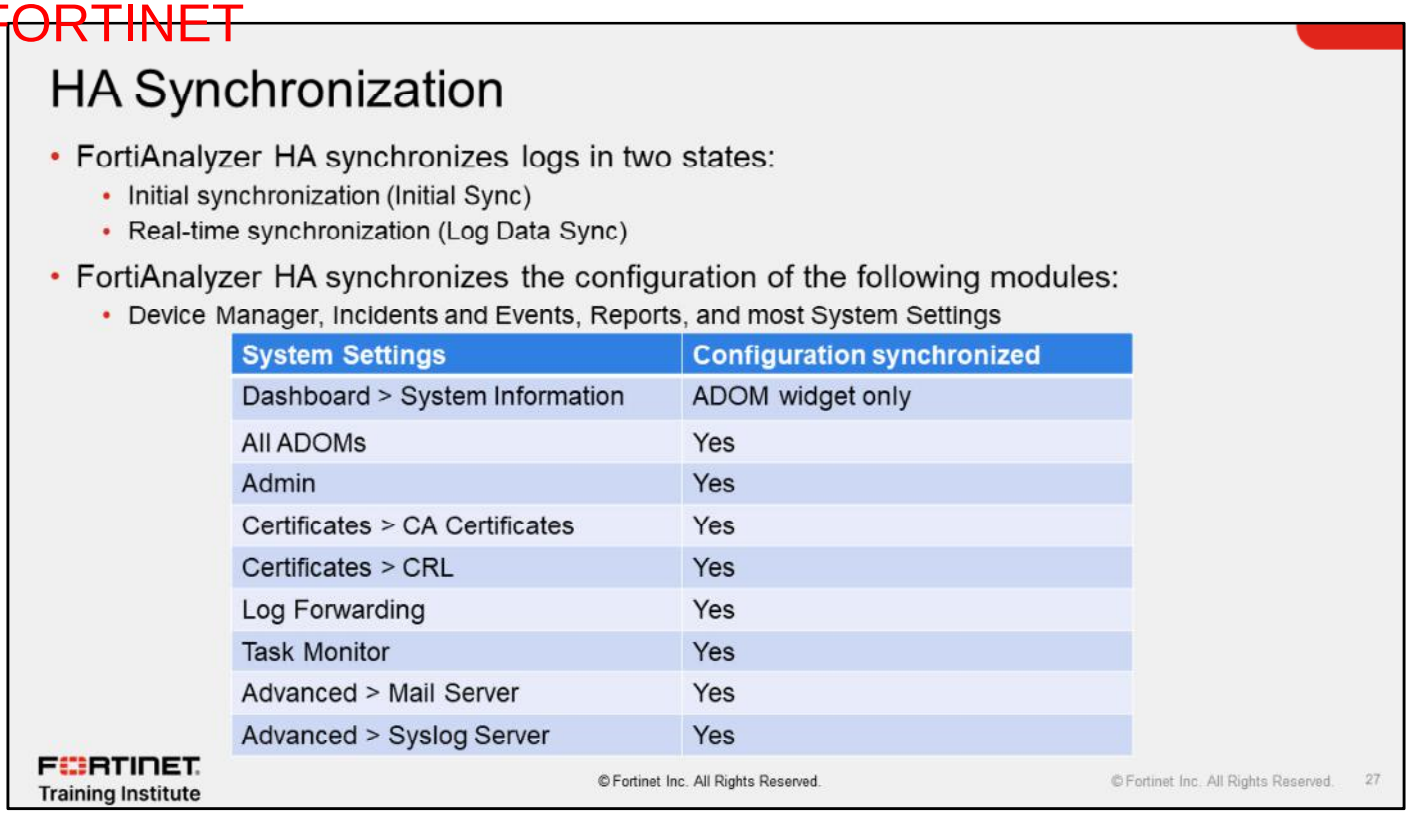


The initial selection of the primary device is determined by the preferred role that is configured. If the preferred role is set to Primary, the device becomes the primary device when it is configured first in a new HA cluster. If there is already an existing primary device, the new device will take on the role of a secondary device. By default, the role is set to Secondary, allowing the device to synchronize with the primary device. A secondary device cannot be designated as a primary device until it has been synchronized with the current primary device.

In the event of a primary device failure, FortiAnalyzer HA follows these rules to select a new primary device:

- Each device in the cluster is assigned a priority ranging from 80 to 120, with the default being 100. If the primary device becomes unavailable, the device with the highest priority is chosen as the new primary device. For example, a device with a priority of 110 will be selected over one with a priority of 100.
- If multiple devices share the same priority, the device with the highest primary IP address is selected as the new primary. For instance, 123.45.67.124 will be chosen over 123.45.67.123.
- If a new device with a higher priority or a higher IP address value joins the cluster, it will not automatically replace (or preempt) the current primary device.

By default, the only parameter checked to trigger an automatic failover is the network reachability among the cluster members. However, you can optionally configure HA to also check the status of the Postgres database process. If that process stops functioning, it will initiate a failover. This configuration can be done on the CLI using the command `set healthcheck DB` under the `system HA` configuration mode.



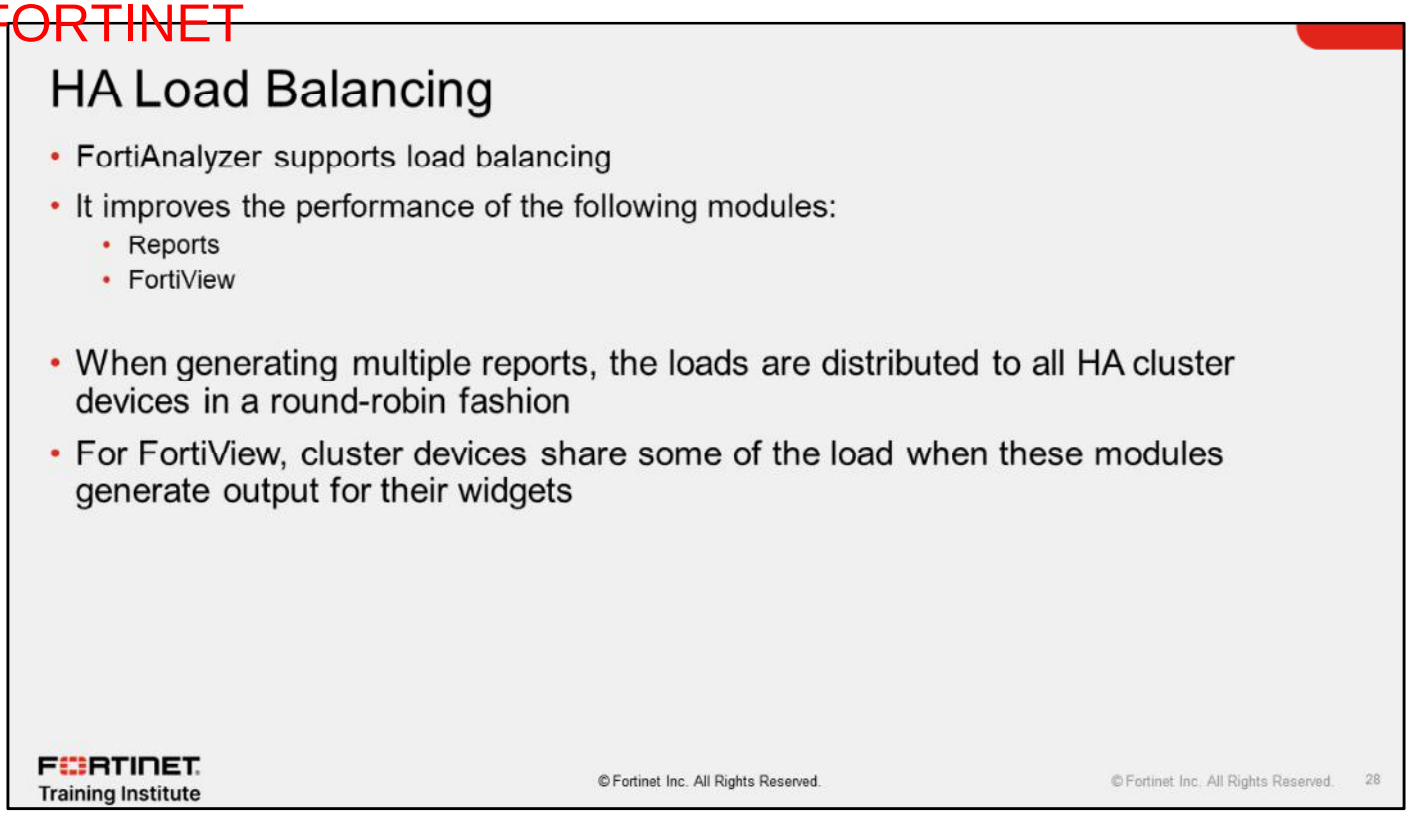
To ensure that logs are synchronized among all HA devices, FortiAnalyzer HA synchronizes logs in two states: initial synchronization and real-time synchronization.

Initial synchronization: The primary device synchronizes its logs with new devices added to the cluster. Once initial synchronization is complete, the secondary device automatically reboots and rebuilds its log database using the synchronized logs. You can monitor the status in the **Cluster Status** window, in the **Initial Logs Sync** column.

Real-time synchronization: After the initial log synchronization is finished, the HA cluster transitions into the real-time log synchronization state. **Log Data Sync** is enabled by default for all devices in the HA cluster. When active in the primary device, it forwards logs in real time to all secondary devices. This ensures that both primary and secondary devices maintain synchronized logs. If the primary device fails, the designated secondary device will assume the role of the new primary device and continue synchronizing logs with secondary devices. If you wish to use a FortiAnalyzer device solely as a standby (not as a secondary), you do not need real-time log synchronization and can disable **Log Data Sync**.

Configuration synchronization provides redundancy and load balancing among the cluster devices. A FortiAnalyzer HA cluster synchronizes the configuration of the following modules to all devices in the cluster:
- Device Manager
- Incidents and Events
- Reports
- Most system settings

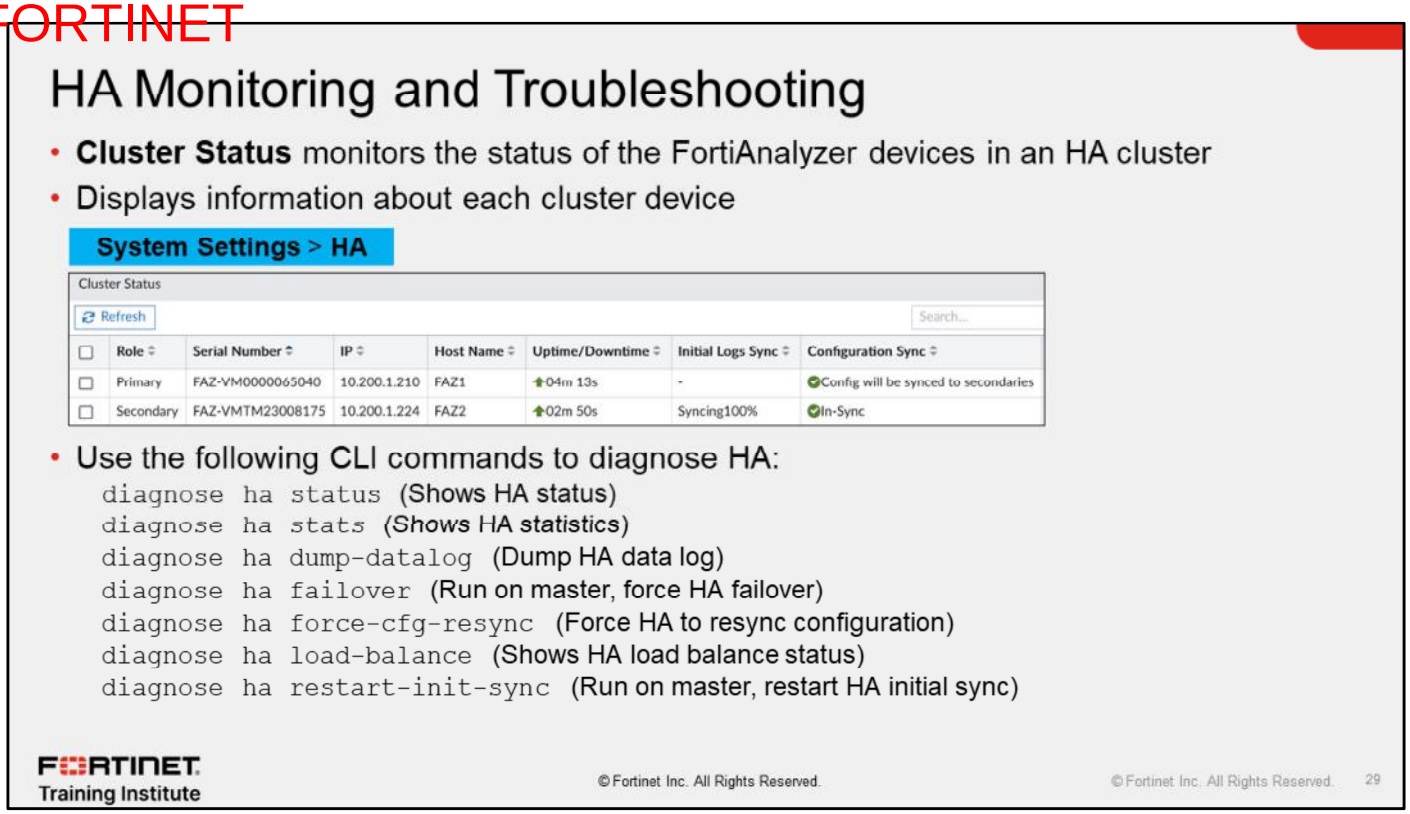
FortiAnalyzer HA synchronizes most system settings in the HA cluster. The table on this slide shows some of the settings that are synchronized. Refer to the *FortiAnalyzer Administration Guide* for the complete list.



Because FortiAnalyzer HA synchronizes logs among HA units, the HA cluster can balance the load and improve overall responsiveness. Load balancing enhances the following modules:

- Reports
- FortiView

When generating multiple reports, the loads are distributed to all HA cluster devices in a round-robin fashion. When a report is generated, the report is synchronized with other devices so that the report is visible on all HA device members. Similarly, for FortiView, cluster devices share some of the load when these modules generate output for their widgets.



On the **Cluster Status** page, you can monitor the status of FortiAnalyzer devices in an HA cluster. This window displays information about the role of each cluster device, the HA status of the cluster, and the HA configuration of the cluster. The following information is displayed:

- **Role**
- **Serial Number**
- **IP**
- **Host Name**
- **Uptime/Downtime**
- **Initial Logs Sync**
- **Configuration Sync**
- **Message**

You can use the CLI command `diagnose ha status` to display the same HA status information. This slide also shows other useful CLI diagnosis commands to monitor and troubleshoot HA.

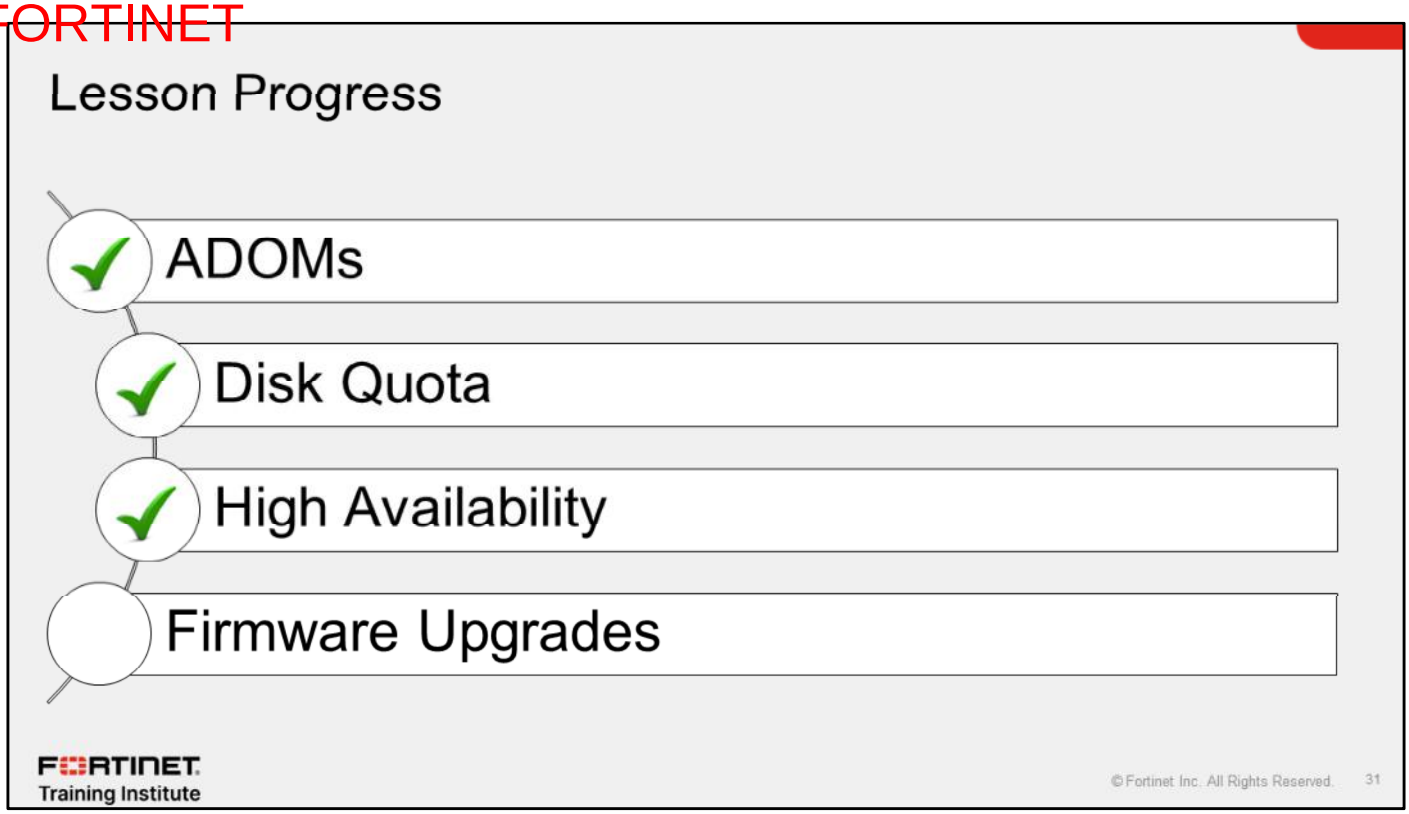
Knowledge Check

1. Which value is checked first when selecting a new primary device in the event of a FortiAnalyzer HA failure?
   - A. Device IP address
   - ✓B. Device priority

2. Which of these modules does a FortiAnalyzer HA cluster synchronize during configuration synchronization?
   - ✓A. Reports
   - B. Network

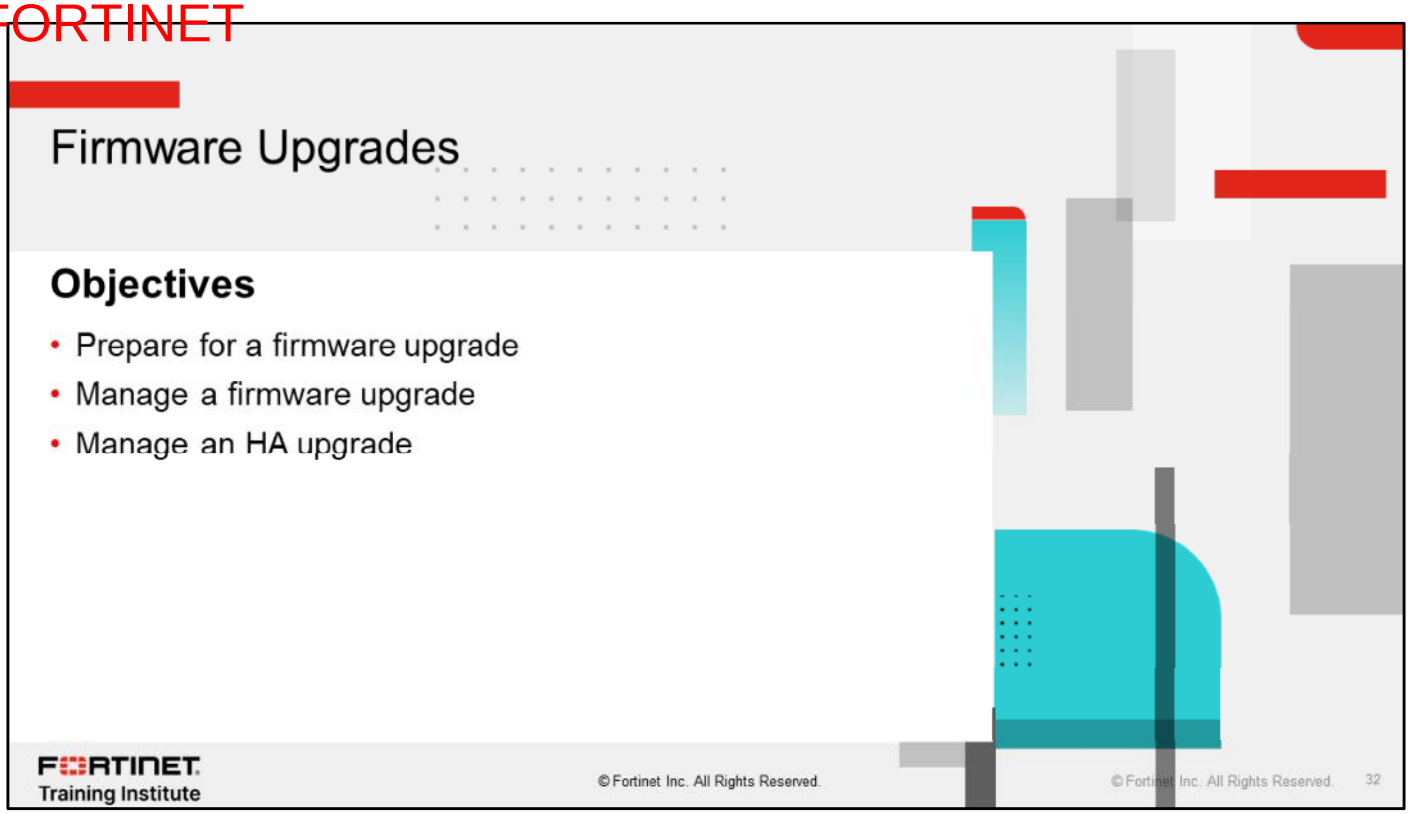
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30



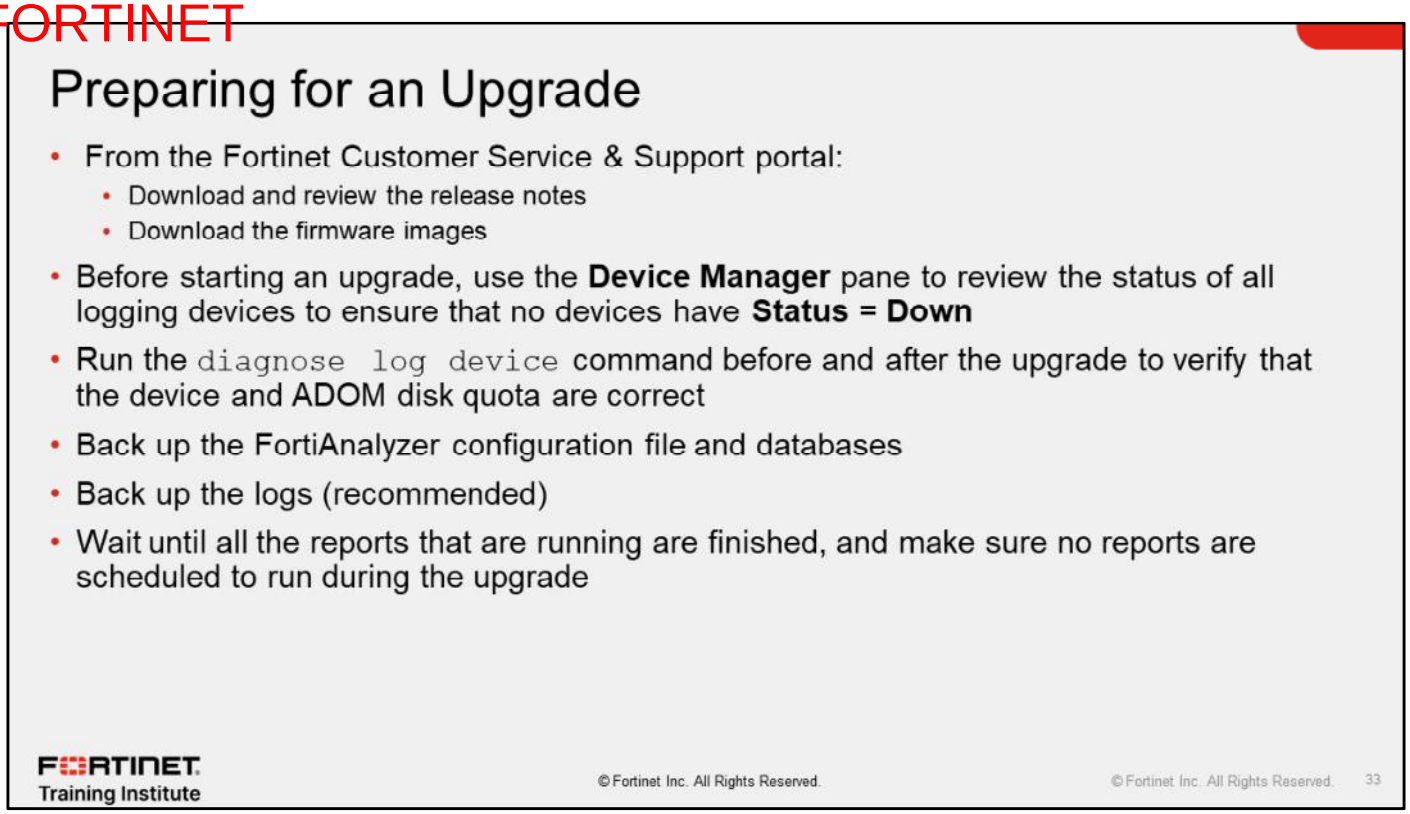
Congratulations! You have completed this lesson.

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



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

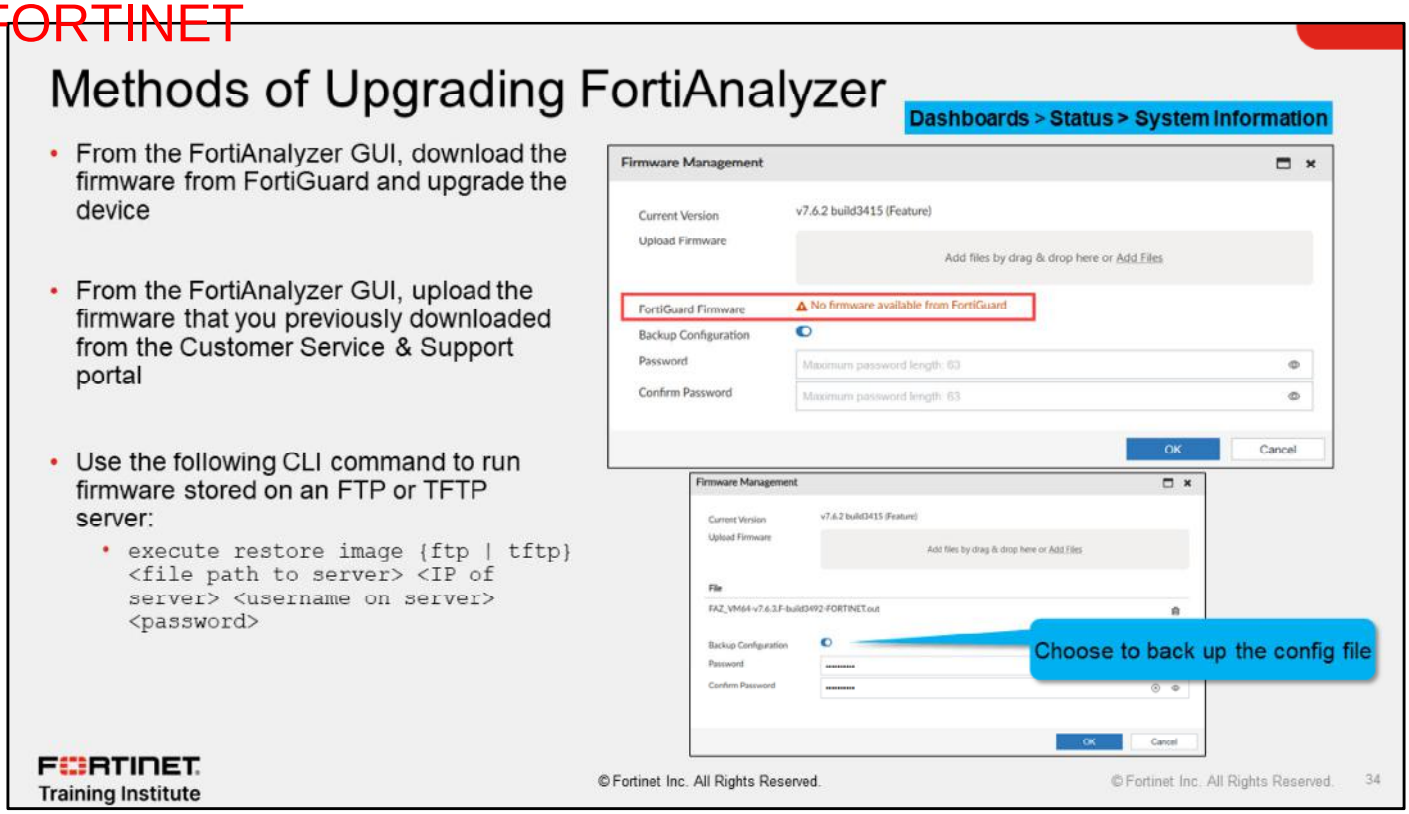
By demonstrating competence in upgrading FortiAnalyzer firmware, you will be able to upgrade FortiAnalyzer.



To ensure a smooth upgrade of FortiAnalyzer, follow these steps:

1. Review the release notes and download the firmware images from support.Fortinet.com.
2. Check the status of all logging devices to ensure that no devices have a status of **Down**.
3. Run the `diagnose log device` command and save its output.
4. After completing the upgrade, run the command again to verify that device and ADOM disk quotas are correct.

It is crucial that you back up the FortiAnalyzer configuration files and databases. It is also recommended that you back up logs before performing the upgrade. Make sure to wait until all active reports are completed and confirm that no reports are scheduled to run during the upgrade.



You can use the following methods to upgrade the FortiAnalyzer firmware:

- From the FortiAnalyzer GUI, download the firmware from FortiGuard and upgrade the device.
- From the FortiAnalyzer GUI, upload the firmware that you previously downloaded from support.Fortinet.com.
- Optionally, you can upgrade firmware stored on an FTP or TFTP server using the CLI command shown on the slide.

To prevent timeouts, it is recommended that you upload the firmware from a server that is in the same location as FortiAnalyzer.

Completing the Firmware Upgrade

- After the upgrade is finished, the **FortiAnalyzer Setup** wizard appears
- If the database needs rebuilding, you can monitor the rebuild status by double-clicking **Rebuilding DB** on the toolbar.
  - Look for the **Rebuilding log database was completed** message
- Review the event logs under **System Settings** to check for errors

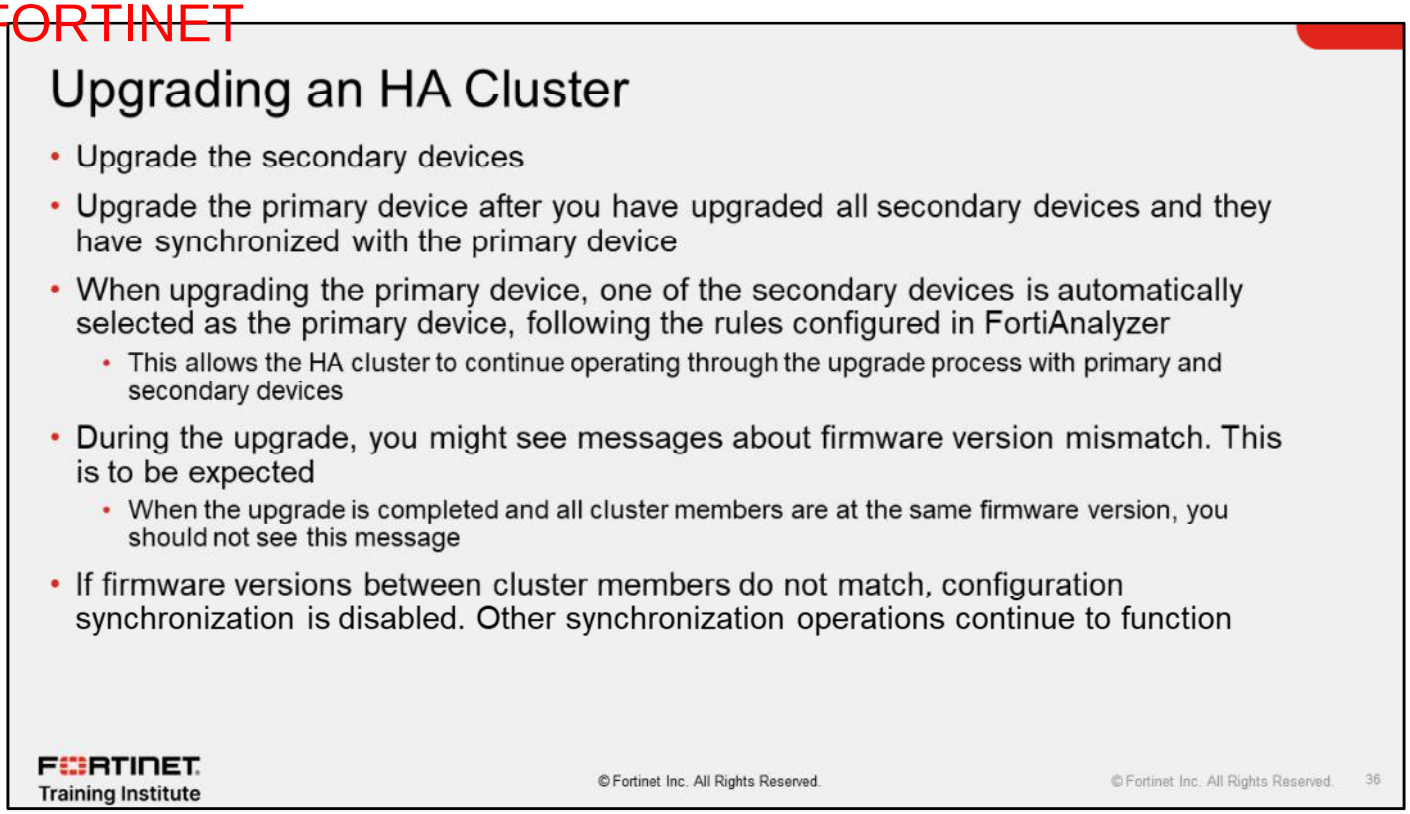
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

When the upgrade is complete, the FortiAnalyzer Setup wizard appears. Click **Begin**. Alternatively, you can click **Later** to finish the wizard at another time.

If the database needs rebuilding, you can monitor the rebuild status by double-clicking the **Rebuilding DB** status in the toolbar. The rebuild process has two steps. When it's finished, you will see the message **Rebuilding log database was completed**.

Review the event logs under **System Settings** for any errors.



You can upgrade the firmware of an operating FortiAnalyzer cluster in the same way you would a standalone FortiAnalyzer device. Upgrade the secondary devices first. Upgrade the primary device last, after all secondary devices have been upgraded and synchronized with the primary device.

When you upgrade the primary device, one of the secondary devices is automatically selected to be the primary device following the rules configured in FortiAnalyzer. This allows the HA cluster to continue operating through the upgrade process with primary and secondary devices.

During the upgrade, you might see messages about firmware version mismatch. This is to be expected. When the upgrade is completed and all cluster members are at the same firmware version, you should not see this message.

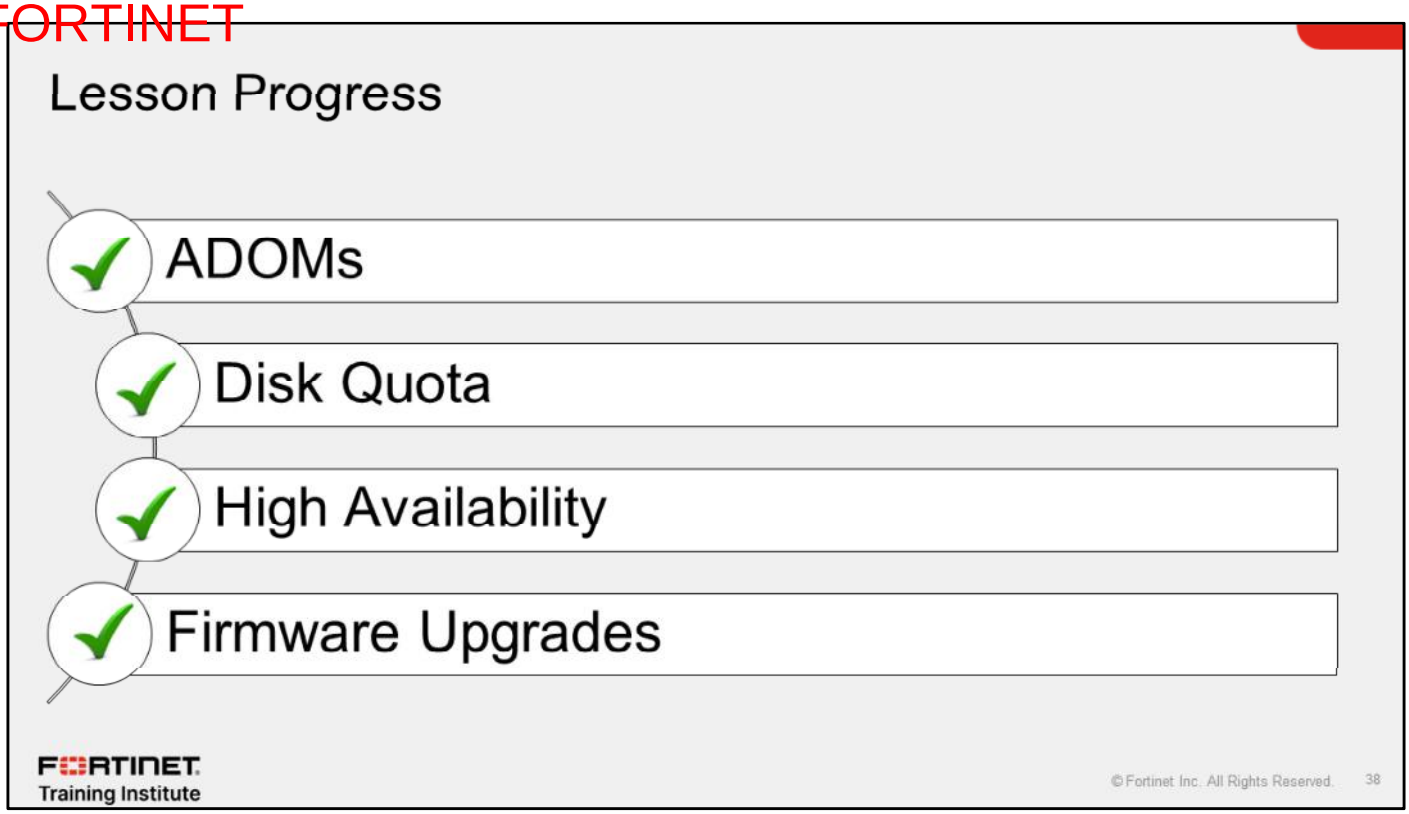
If the firmware upgrade involves multiple steps, it is recommended that you complete each step for both the primary and the secondary devices before proceeding to the next step.

Knowledge Check

1. When upgrading FortiAnalyzer devices in a cluster, which device should you upgrade first?
   - ✓ A. Primary device
   - B. Secondary device

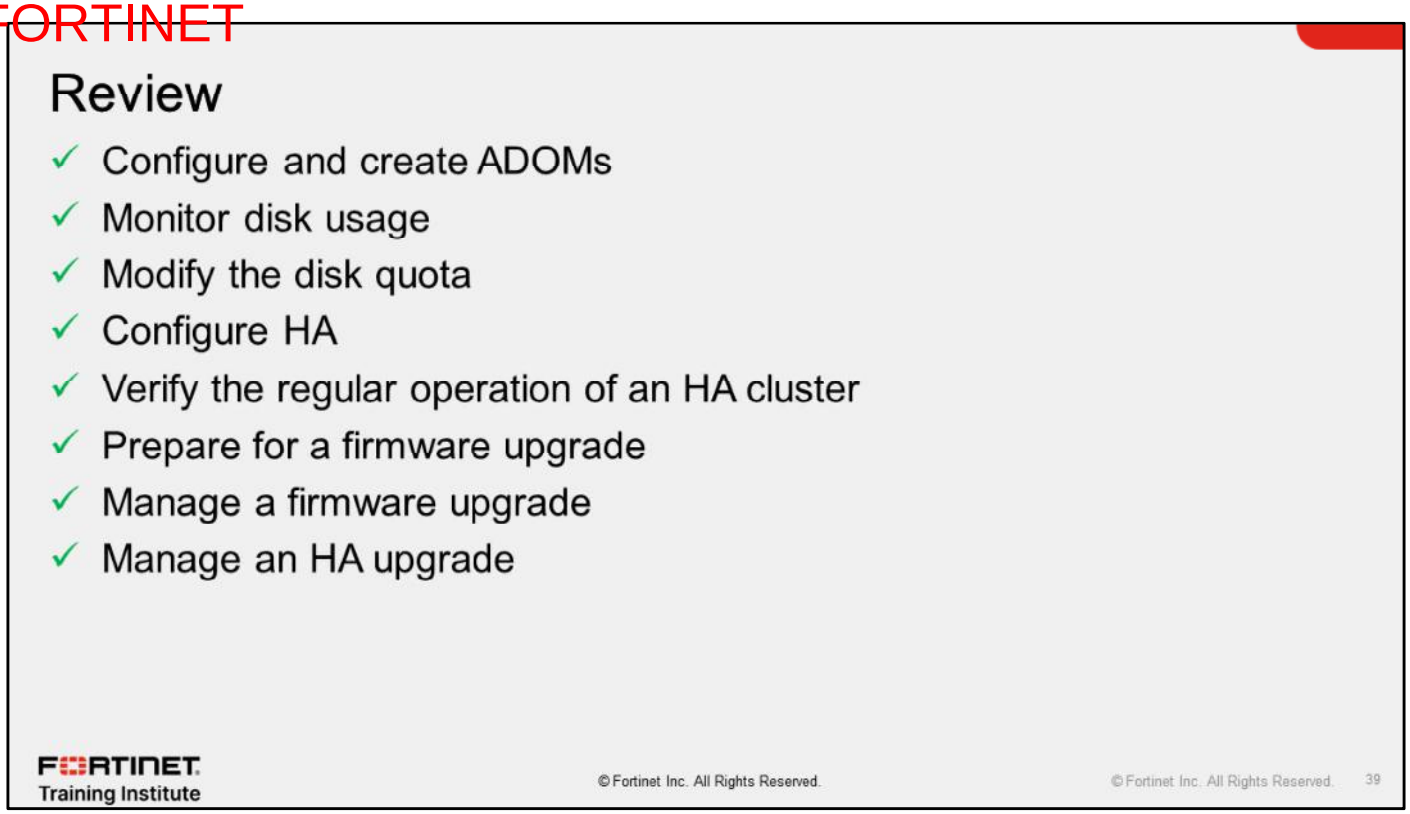
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37



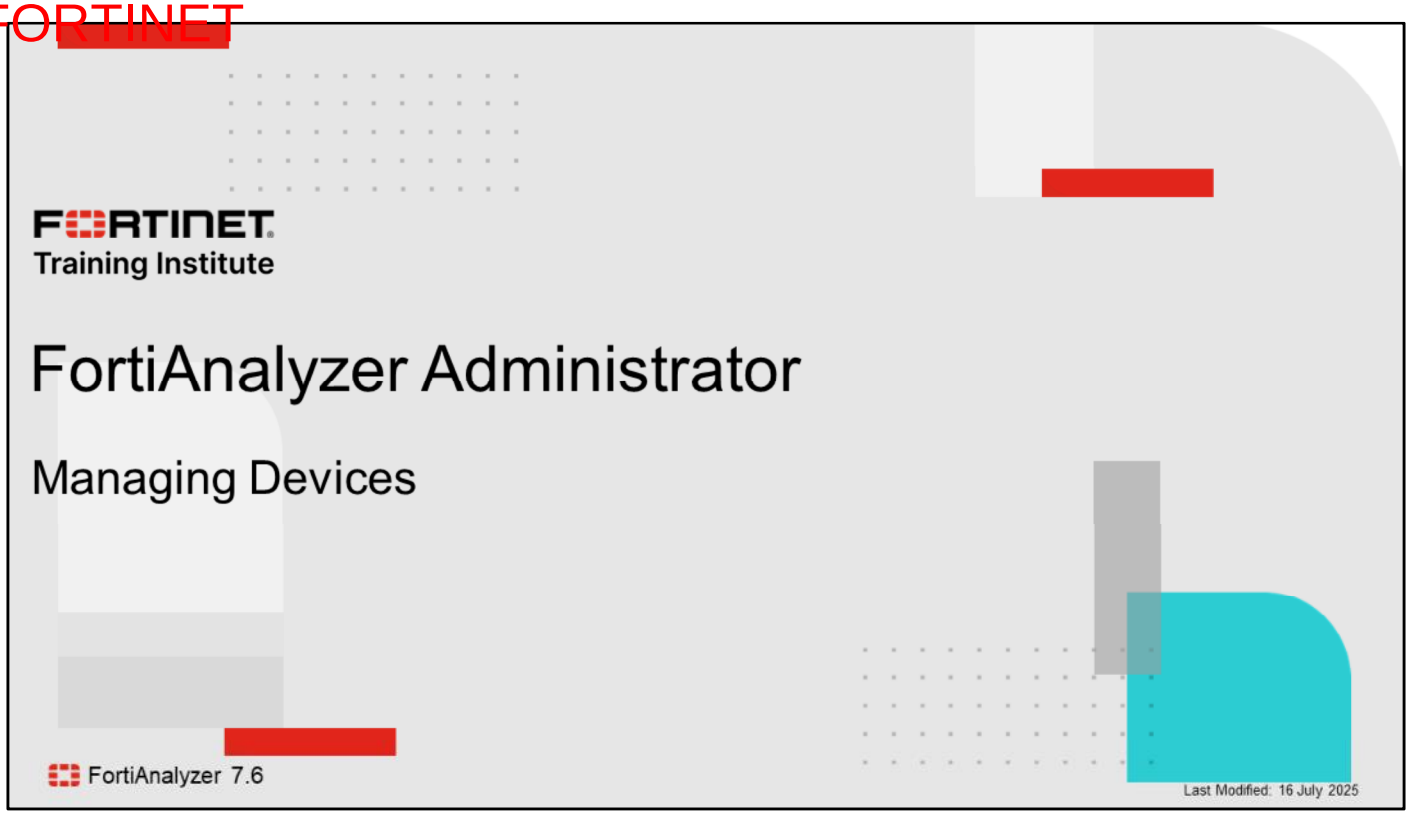
Congratulations! You have completed this lesson.

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

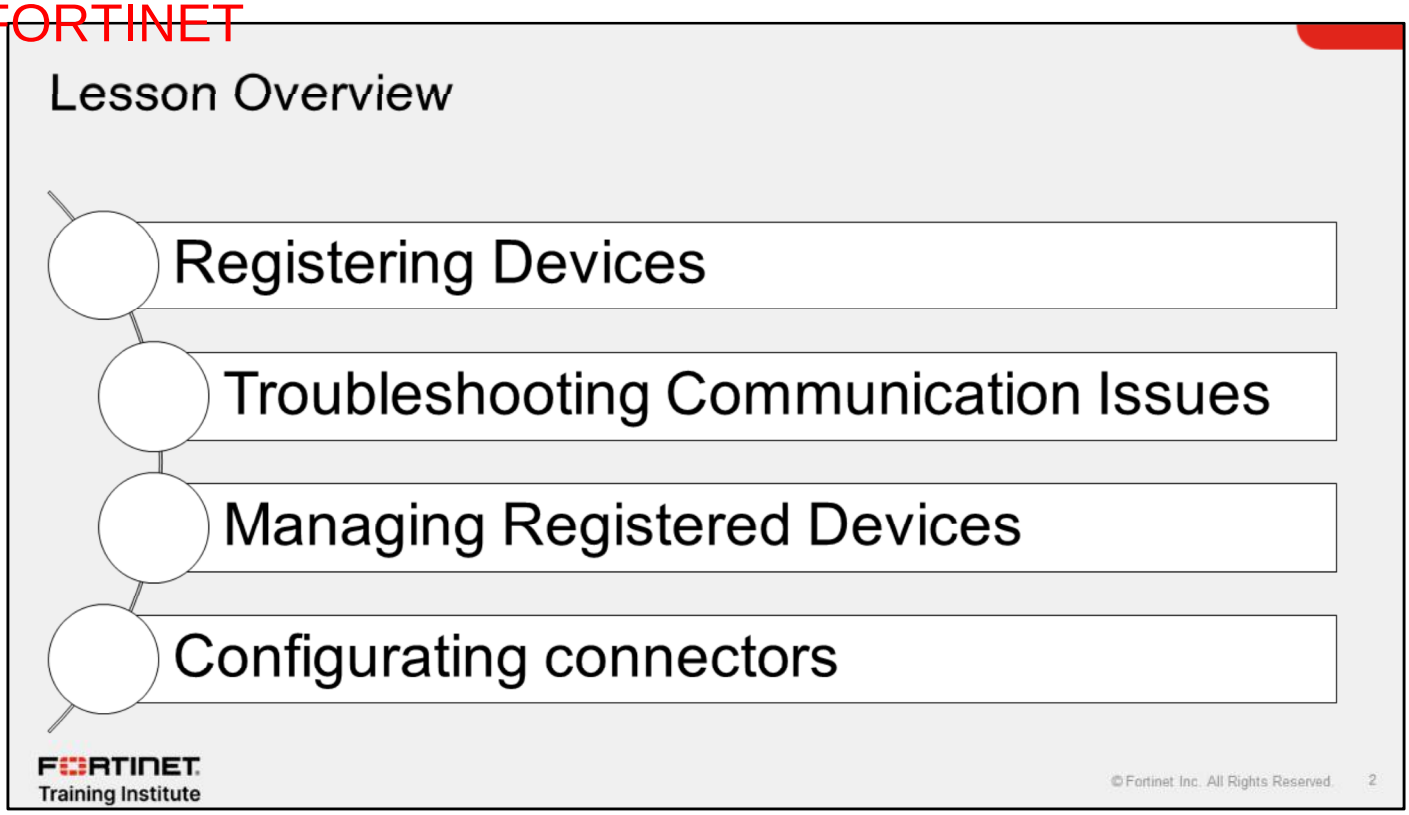


This slide show the objectives that you covered in this lesson.

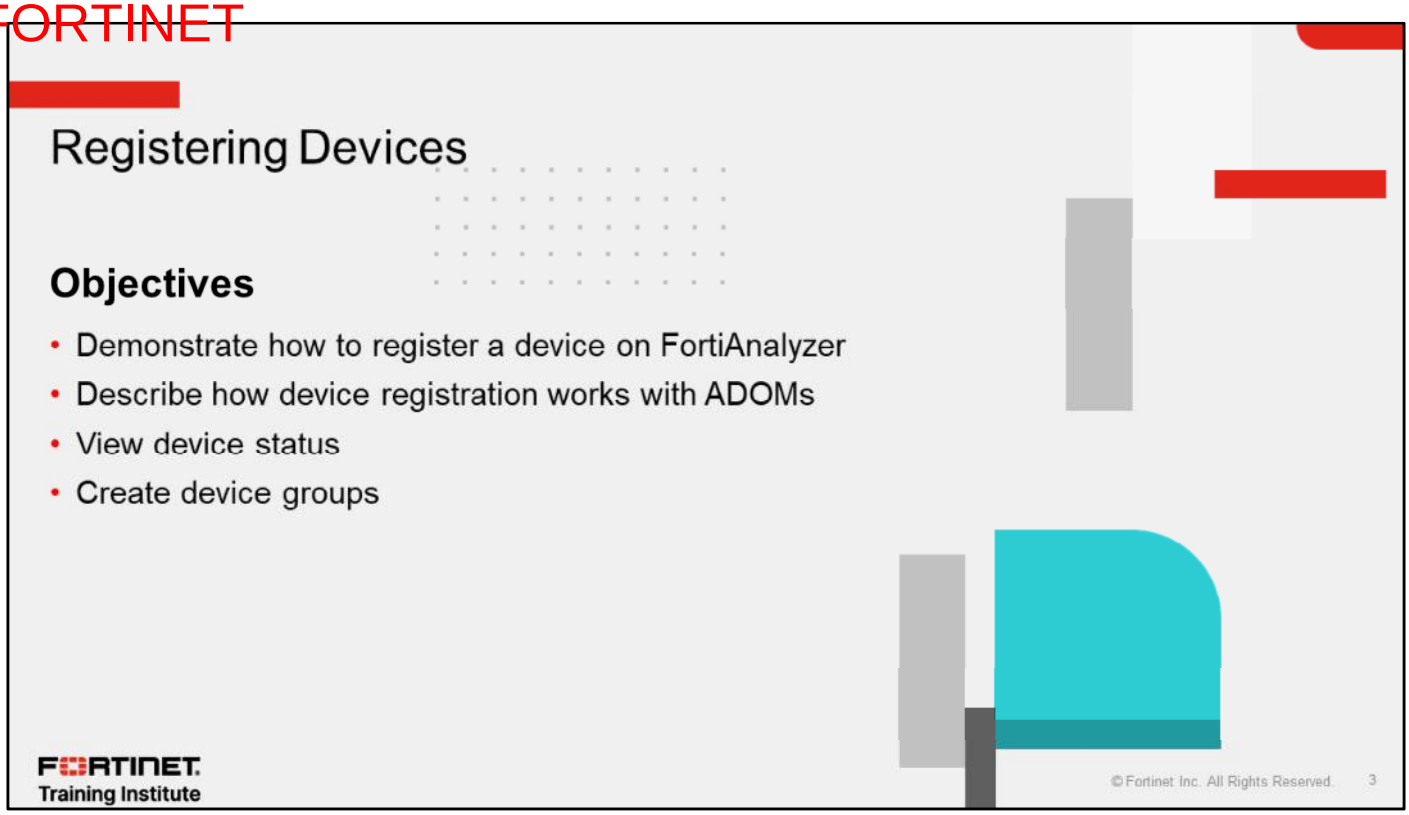
By mastering the objectives covered in this lesson, you learned how to use administration and management functions to better defend FortiAnalyzer—and how to use HA to make your FortiAnalyzer device more resilient against hardware failures.



In this lesson, you will learn how to register devices on FortiAnalyzer for log collection, as well as how to troubleshoot communication between FortiAnalyzer and its registered devices.

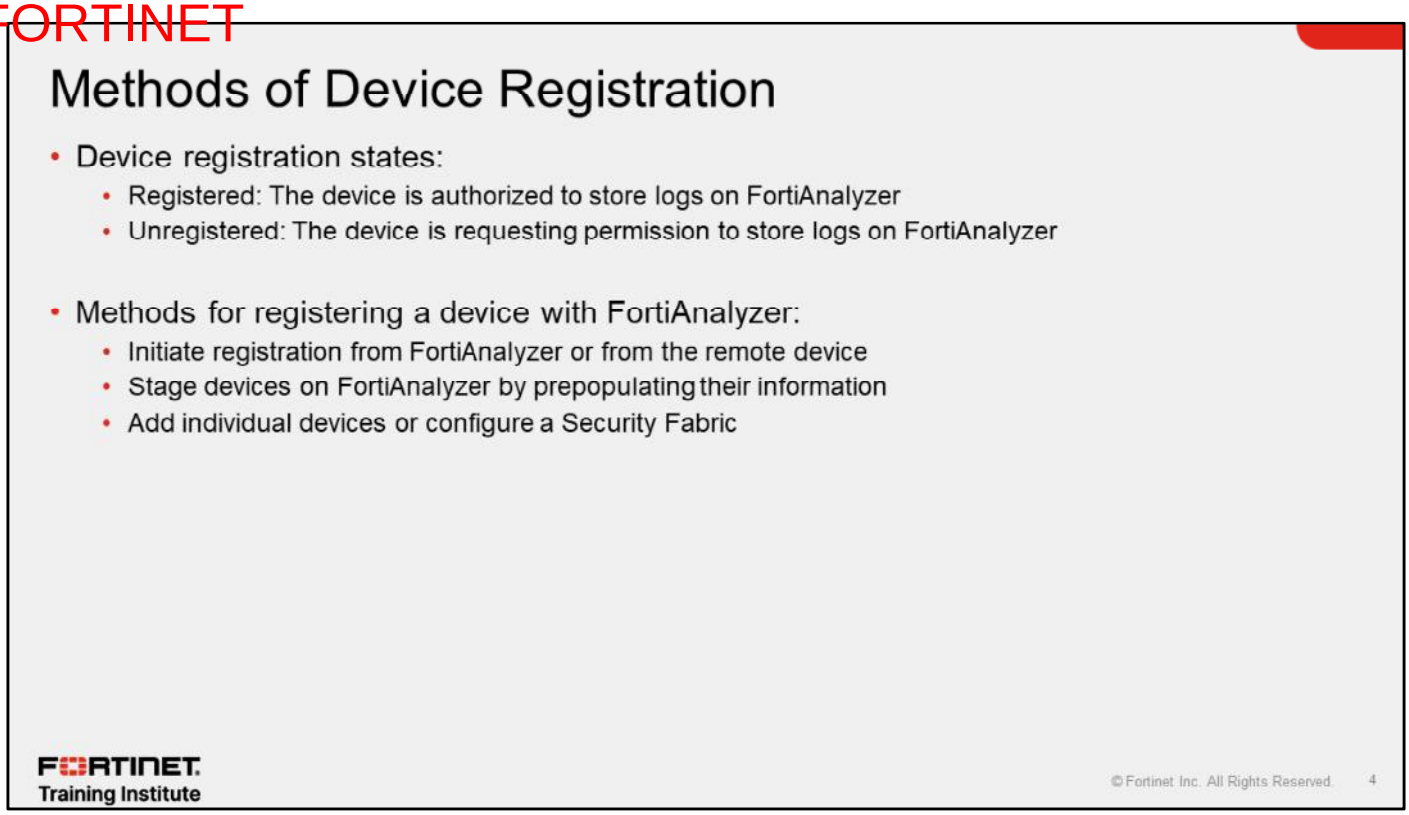


In this lesson, you will explore the topics shown on this slide.



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

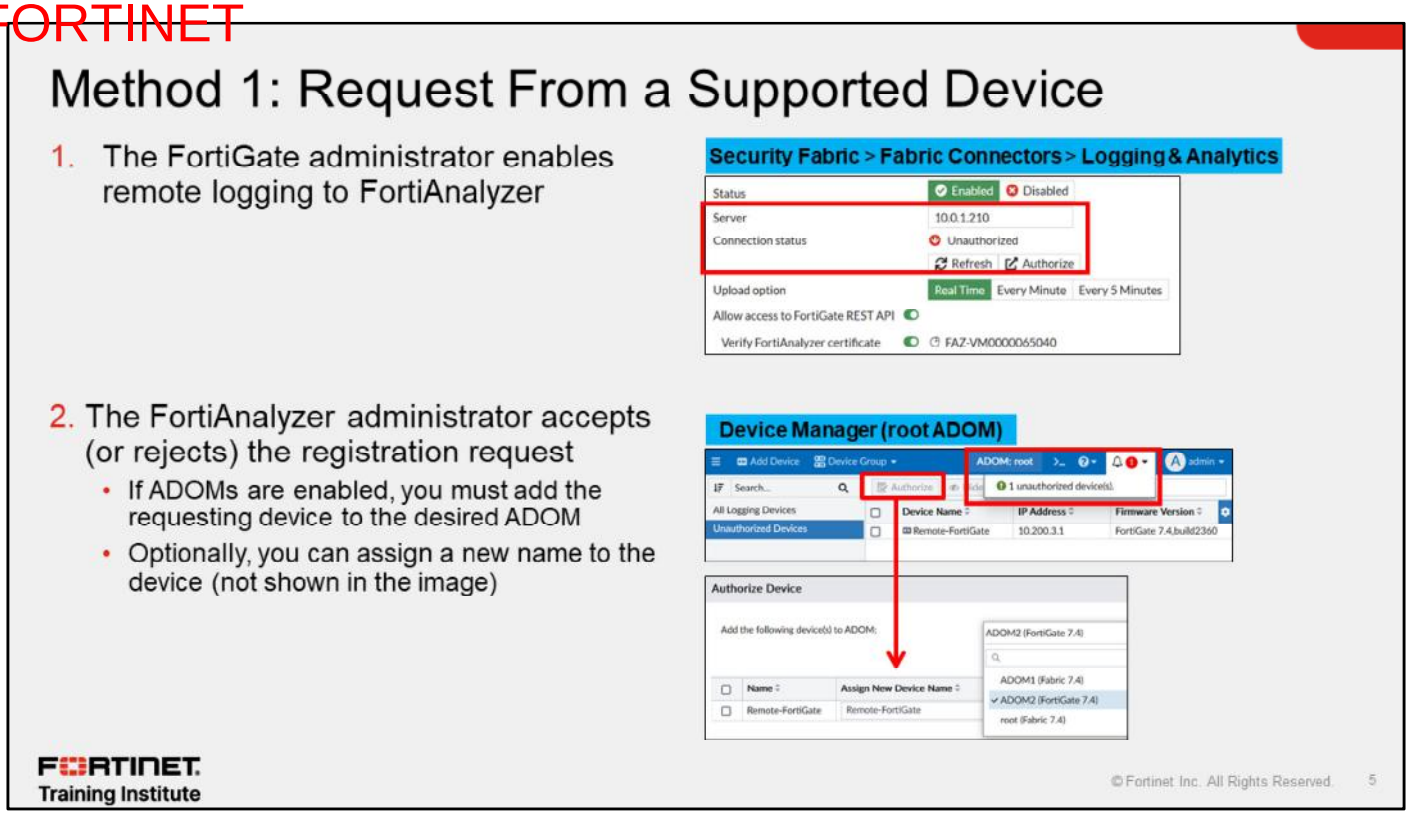
By demonstrating competence in device registration, you will be able to configure FortiAnalyzer to collect logs from registered devices.



For FortiAnalyzer to start collecting logs from a device, that device must become a registered device on FortiAnalyzer. To FortiAnalyzer, there are only two types of devices: those that are registered and those that are unregistered. A registered device has been *authorized* to store logs on FortiAnalyzer, whereas an unregistered device is *requesting* to store logs on FortiAnalyzer.

There are various ways you can register a device with FortiAnalyzer. A supported device can send a registration request. The FortiAnalyzer administrator can either accept or deny the request. You can also add devices on FortiAnalyzer using the **Add Device** wizard. You can add a device based on its serial number or a pre-shared key. If the device is supported and all its details are correct, FortiAnalyzer registers the device.

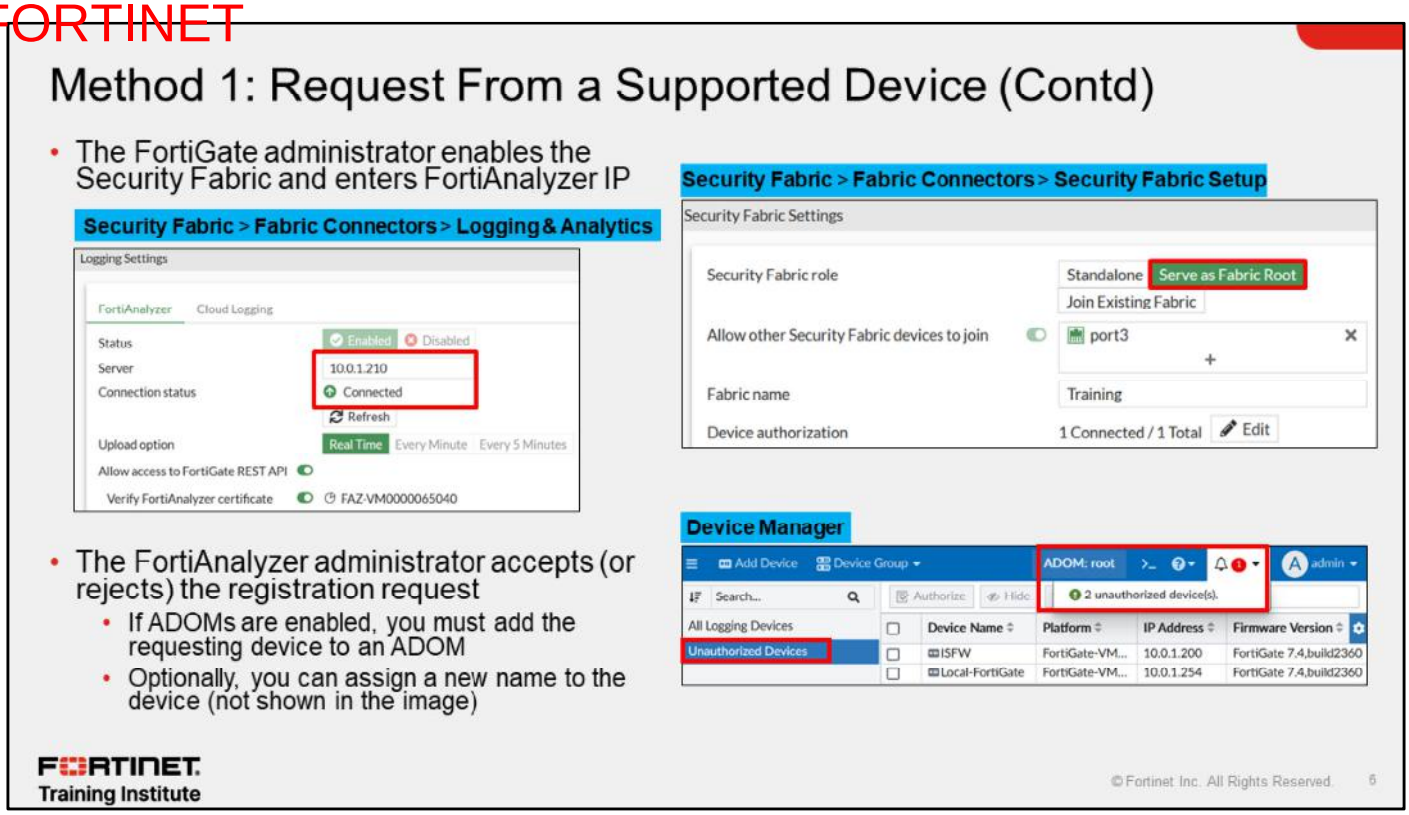
FortiGate can also initiate a connection to the FortiAnalyzer **Security Fabric Authorization** window, log in to FortiAnalyzer, and approve devices.



There are two ways to initiate a request from a FortiGate device.

In the first method, you must configure the FortiAnalyzer IP address and enable logging on the FortiGate device. After you click **Apply**, and if the request reaches FortiAnalyzer successfully, you must confirm the serial number of the FortiAnalyzer device if the **Verify FortiAnalyzer certificate** setting is enabled. If you click **Test Connectivity**, FortiGate will display as **Unauthorized** at this stage. This is because the FortiAnalyzer administrator has not yet accepted the *request to register*. At this stage, FortiGate is still an unregistered device.

After the supported device makes the request, it automatically appears under the root ADOM in **Device Manager**. The FortiAnalyzer administrator should review the details of the unauthorized device and, if satisfied, authorize the device. Upon acceptance of the registration request, if ADOMs are enabled, you can keep FortiGate in the root ADOM or add it to any custom FortiGate ADOMs you have configured, as illustrated on this slide.



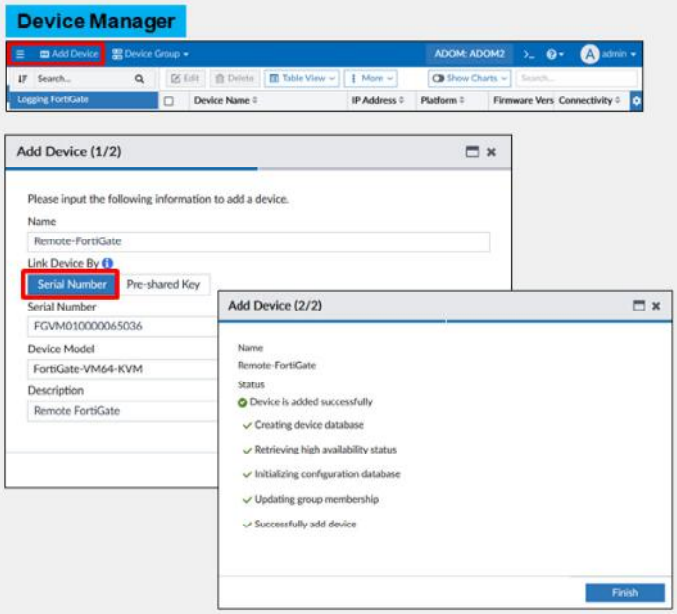
When you enable the Security Fabric on FortiGate, it automatically enables FortiAnalyzer logging by default. After you configure the FortiAnalyzer IP address on the root FortiGate, all the Fabric member devices receive the central logging configuration. Additionally, all unregistered Fabric members send registration requests to FortiAnalyzer. If you enable **Verify FortiAnalyzer certificate**, you must confirm the FortiAnalyzer serial number on the root FortiGate.

Although the registration requests from the Fabric members are triggered simultaneously, the FortiAnalyzer administrator must review and authorize each request individually. All the FortiGate devices connected through the Fabric should be added under a single ADOM. However, it is also possible to separate the FortiGate devices and assign them to different ADOMs if needed.

Method 2: Add Device Wizard Using a Serial Number

1. Add a device using **Device Manager**
2. Type the required device information in the wizard

- If ADOMs are enabled, the device is automatically registered to its device-specific, prebuilt ADOM
  - If you've already created a custom ADOM based on the device type you are registering, switch to that ADOM *before* adding a device using the wizard

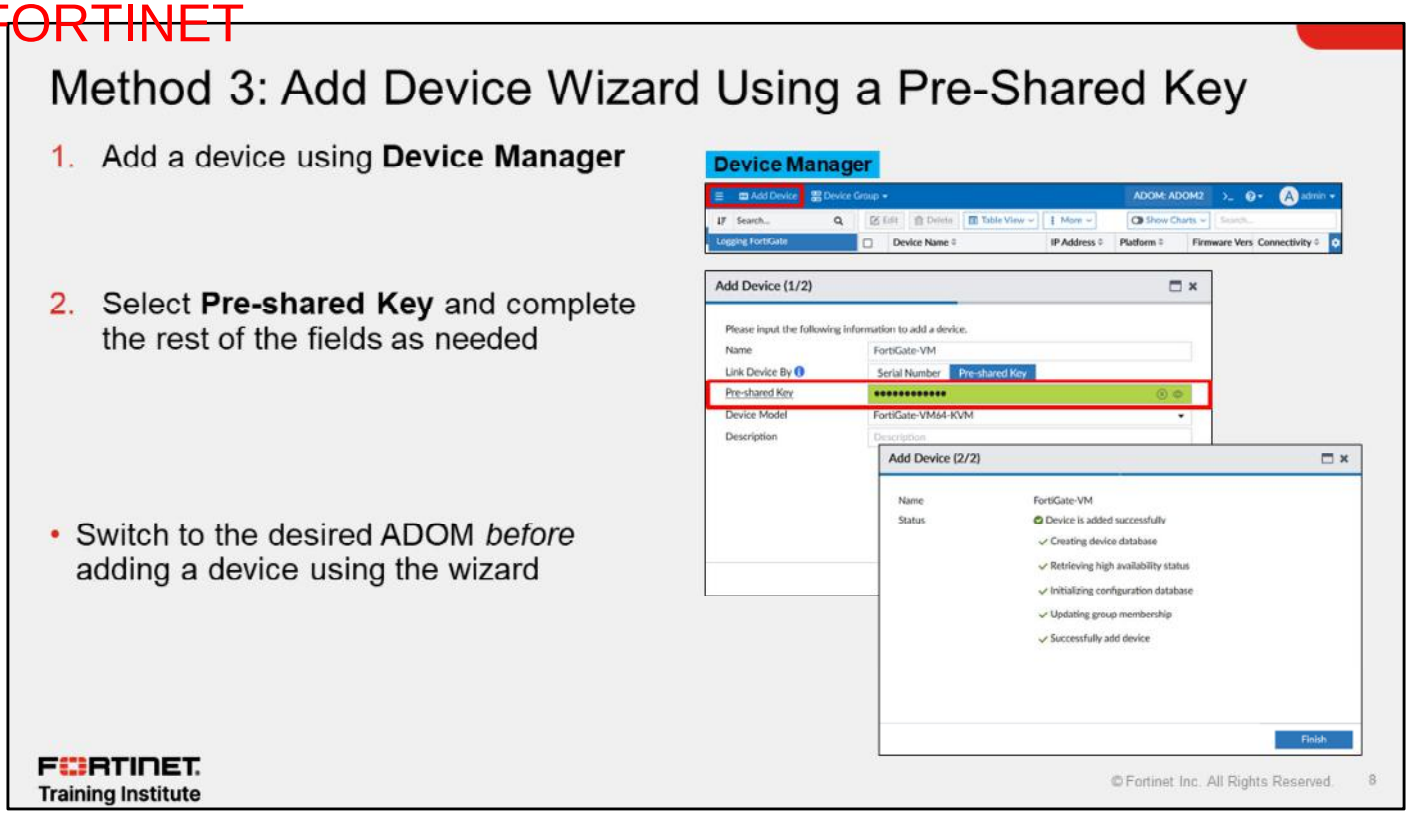


FORTINET Training Institute

 7

With this method, you use the device registration wizard in the FortiAnalyzer **Device Manager**. The FortiAnalyzer administrator proactively initiates and ultimately performs the registration. The administrator must have the specific serial number of the device. If FortiAnalyzer successfully verifies the device information, the device appears under **Device Manager**.

If ADOMs are enabled, the device is automatically registered to its device-specific ADOM. However, if you have already created a custom ADOM and want to add the device directly to that ADOM instead, switch to the ADOM *before* adding a device using the wizard.



With this method, you also use the **Add Device** wizard in the FortiAnalyzer **Device Manager**. The FortiAnalyzer administrator proactively initiates and ultimately performs the registration. The administrator must set a pre-shared key and provide other details about the device, such as the device model. After FortiAnalyzer verifies the device information, the device appears under **Device Manager**.

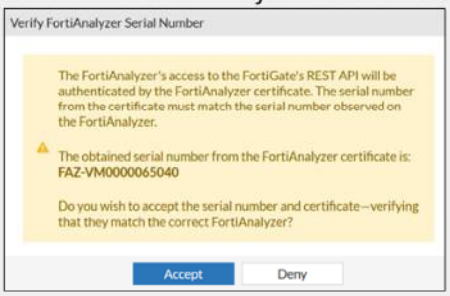
If ADOMs are enabled, the device is automatically registered to its device-specific ADOM. However, if you have already created a custom ADOM and want to add the device directly to that ADOM instead, switch to the ADOM *before* adding a device using the wizard.

Method 3: Add Device Wizard Using a Pre-Shared Key (Contd)

- Enter the pre-shared key on the FortiGate CLI

```
# config log fortianalyzer setting
    set status enable
    set server "<FortiAnalyzer IP>"
    set serial "<FortiAnalyzer Serial>"
    set preshared-key "<password>"
  end
```

- Authorize FortiAnalyzer on FortiGate

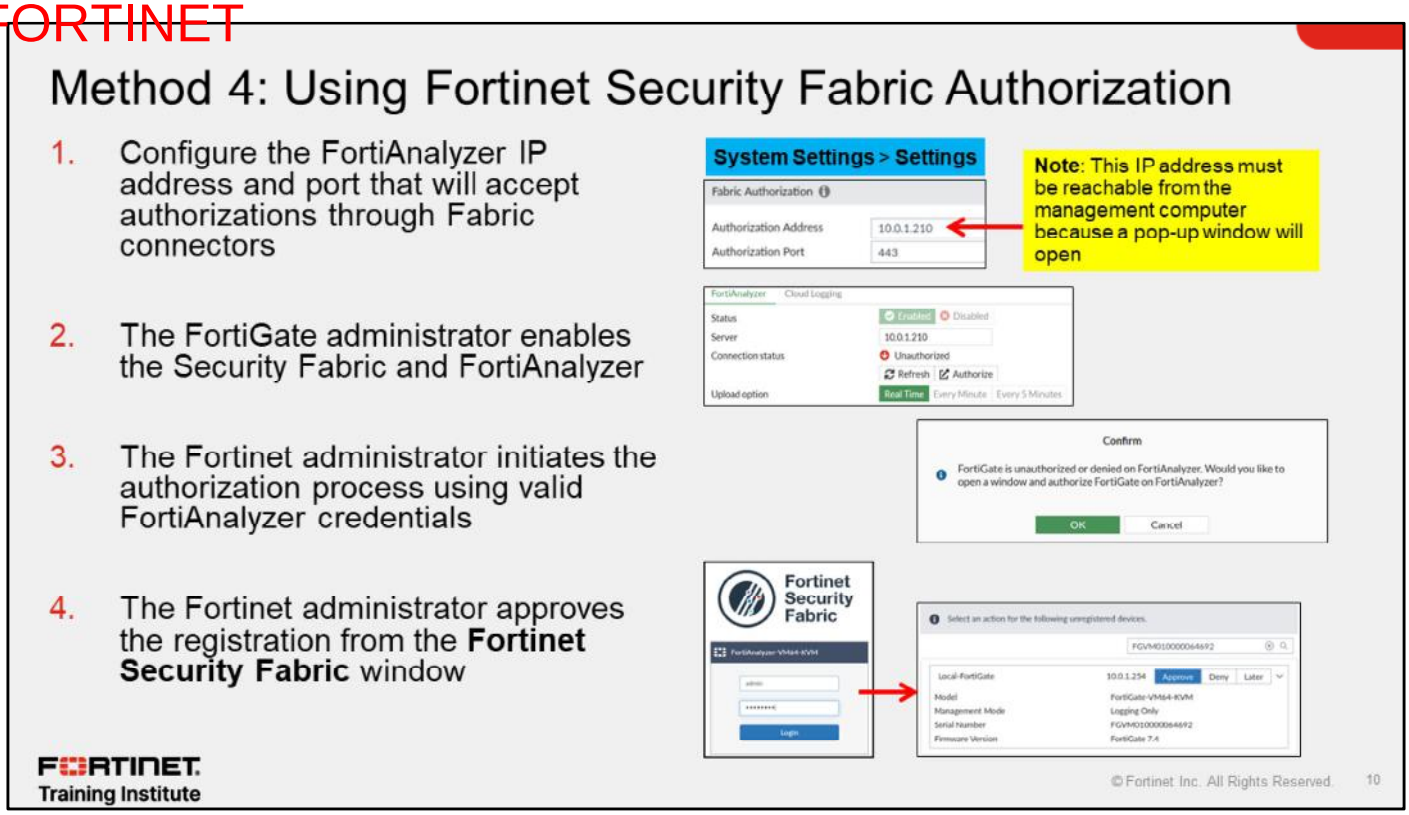


FORTINET Training Institute

 9

Next, configure the pre-shared key on the FortiGate CLI, along with the FortiAnalyzer IP address and serial number. After configuring the device, you need to verify the FortiAnalyzer serial number and authorize the connection if **Verify FortiAnalyzer certificate** is enabled on FortiGate.

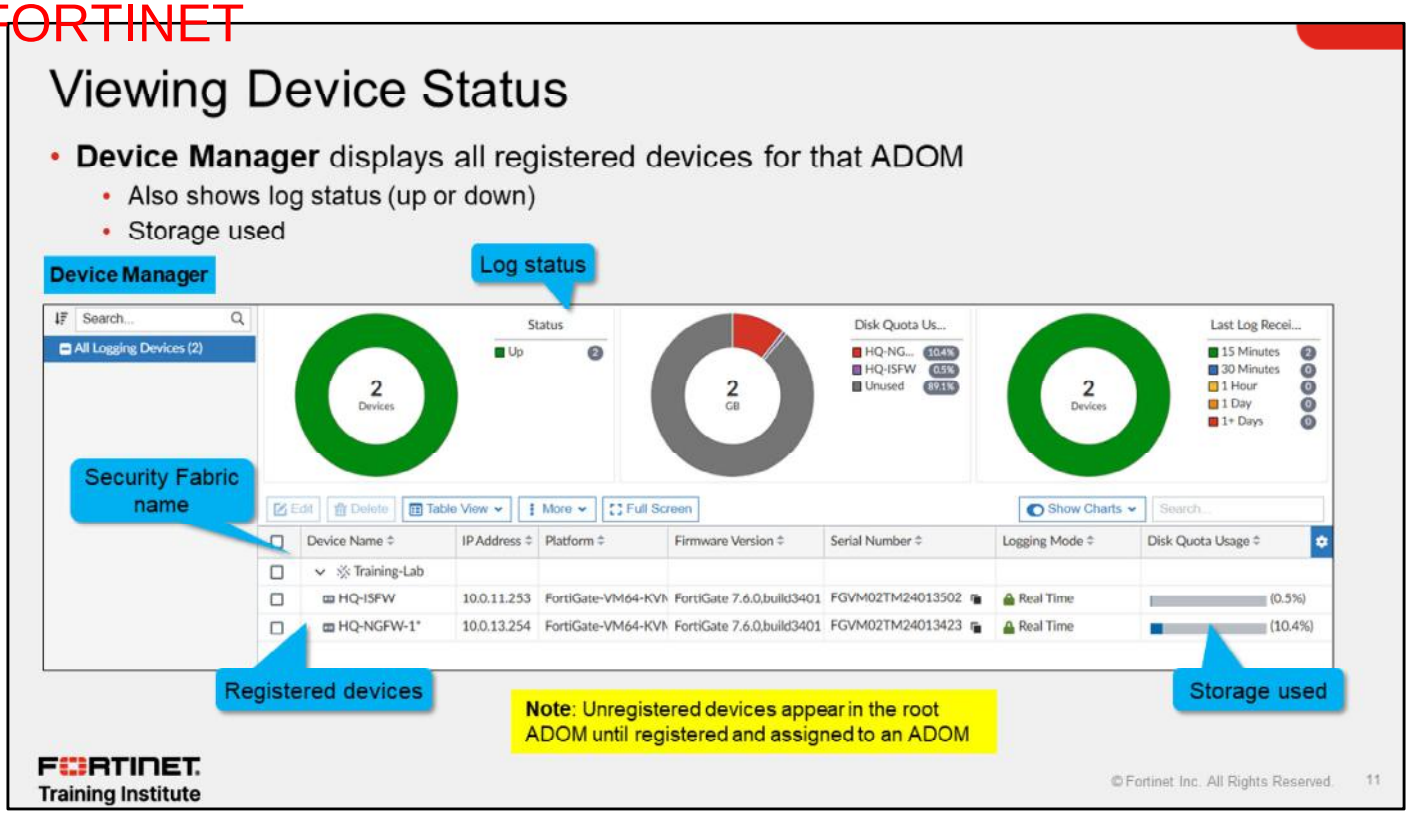
Note that you can add only FortiGate devices using this method.



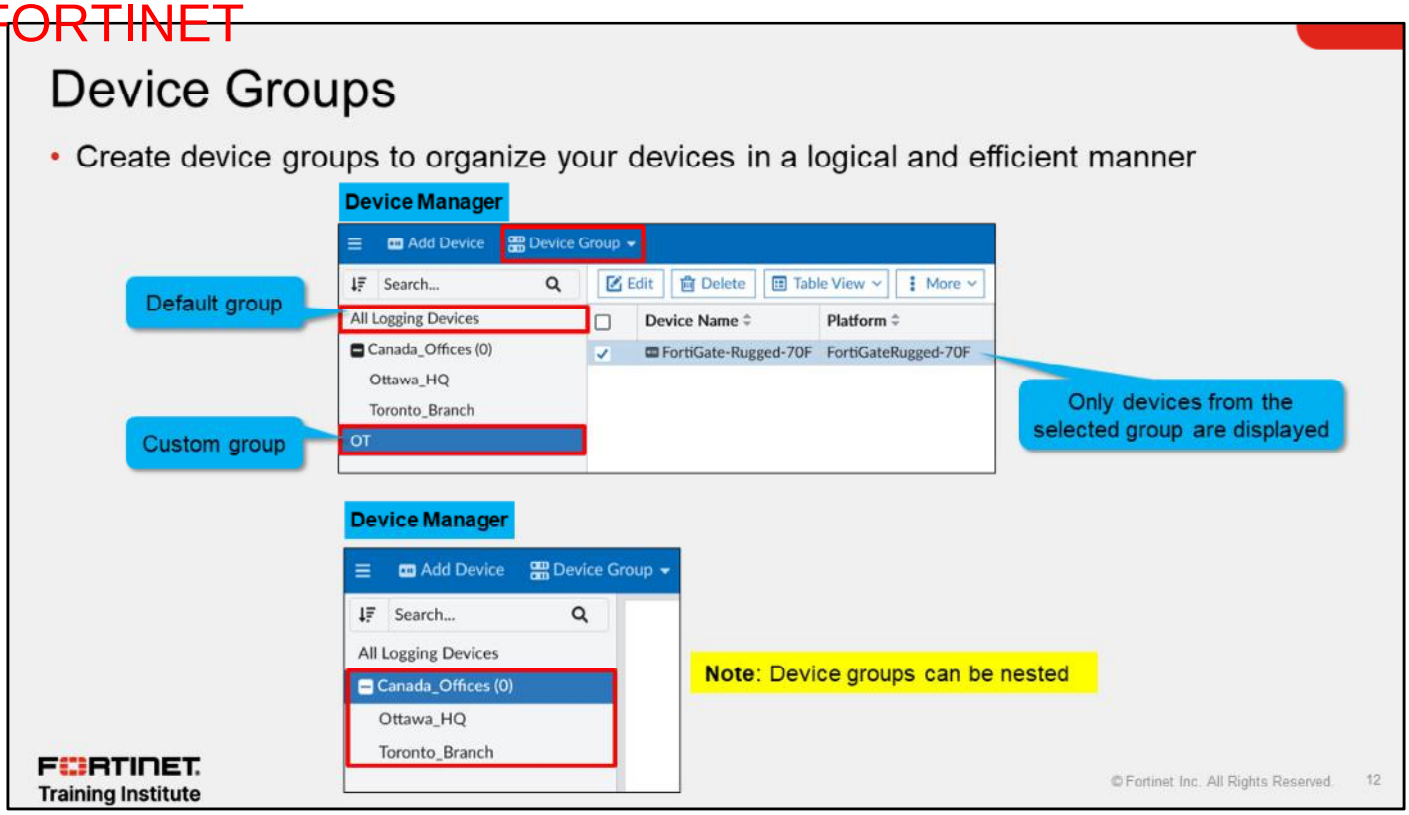
To use this method, you must first configure FortiAnalyzer to accept authorizations through Fabric connectors. You must type the IP address and port that will be used to receive the requests. By default, port 443 is used.

Next, the FortiGate administrator enables the Security Fabric to use FortiAnalyzer for logging and then initiates the authorization process by clicking **OK** in the window shown in step 3 on the slide. Alternatively, you can click **Authorize,** as shown in step 2.

To complete the registration process, the FortiGate administrator must have valid credentials on FortiAnalyzer. To do so, click **Approve** in the **Fortinet Security Fabric** window.



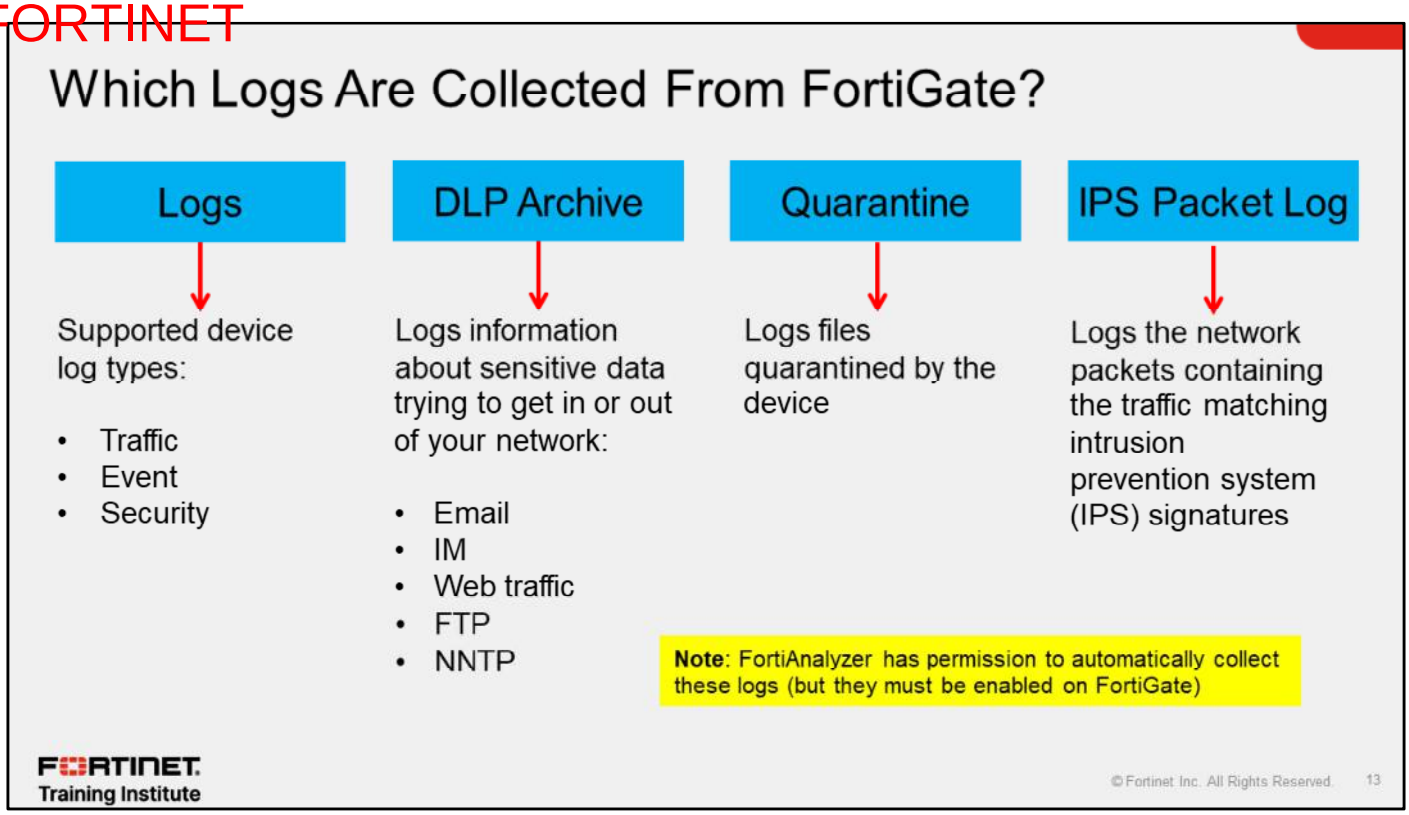
After registering a Fortinet device, you can access it on the **Device Manager** tab of the associated ADOM. Additionally, you can conveniently review details regarding log status and storage utilization for that ADOM. Meanwhile, unregistered devices appear under the root ADOM until you approve and assign them to a designated ADOM.



By default, FortiAnalyzer adds all registered devices to a default device group called **All Logging Devices**. However, you can create custom device groups for your organization. For example, you can create custom groups based on physical location and functionality.

Additionally, you can nest device groups. In the example shown on this slide, a device group named **Canada_Offices** contains a nested group with two branches.

Do *not* add spaces in the names of custom device groups.



When a FortiGate device is registered, FortiAnalyzer automatically collects the following types of logs if they are enabled on FortiGate:

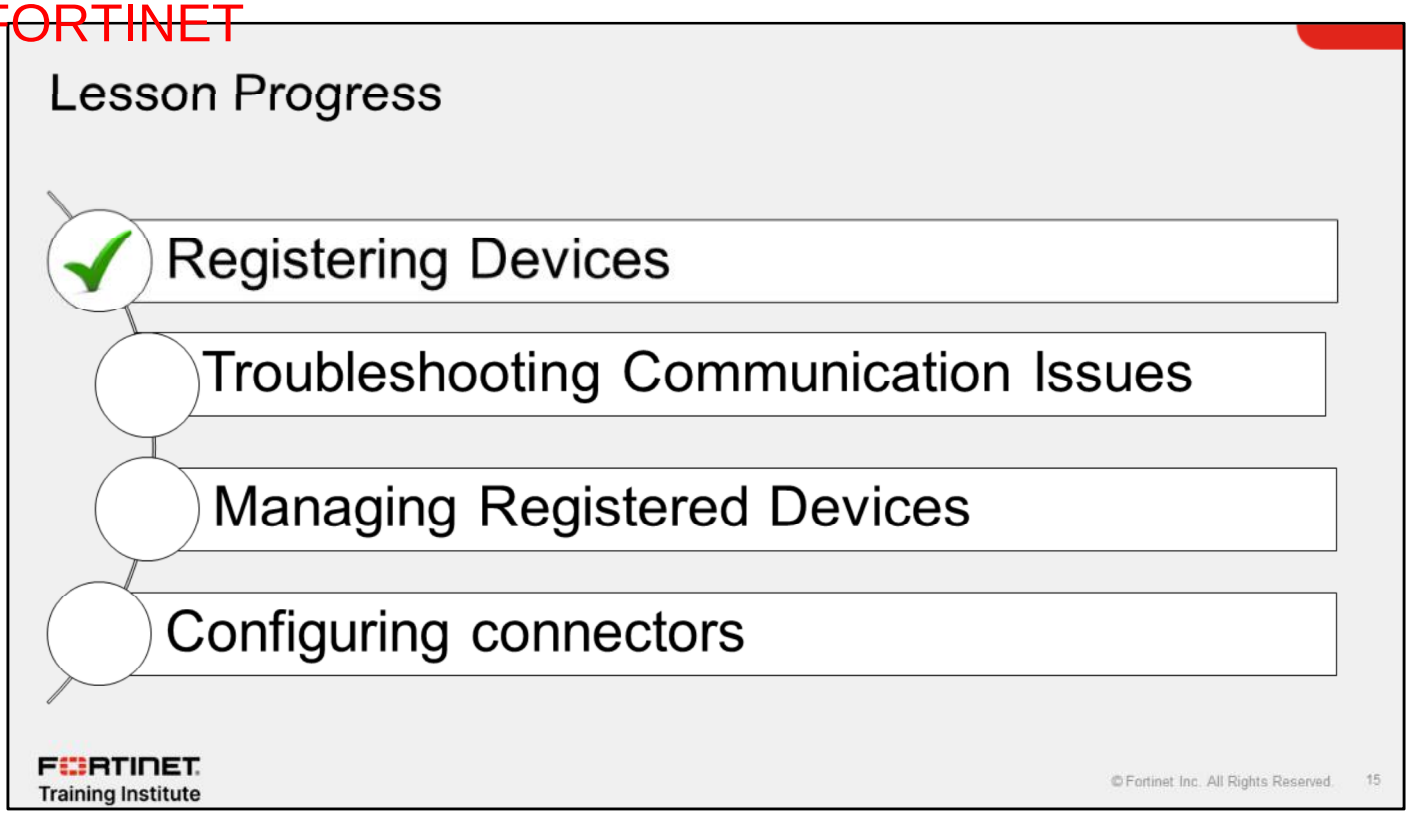
- Logs: This log type details traffic, events, and security information.
- DLP Archive: This log type details any sensitive data trying to get in or out of your network.
- Quarantine: This log type details files placed in quarantine by the device sending the logs.
- IPS Packet Log: This log type details information about network packets containing the traffic matching IPS signatures.

Knowledge Check

1. Which statement about device registration is correct?
   - A. The logging device must initiate the registration request.
   - ✓ B. Both the logging device and FortiAnalyzer can initiate the registration request.

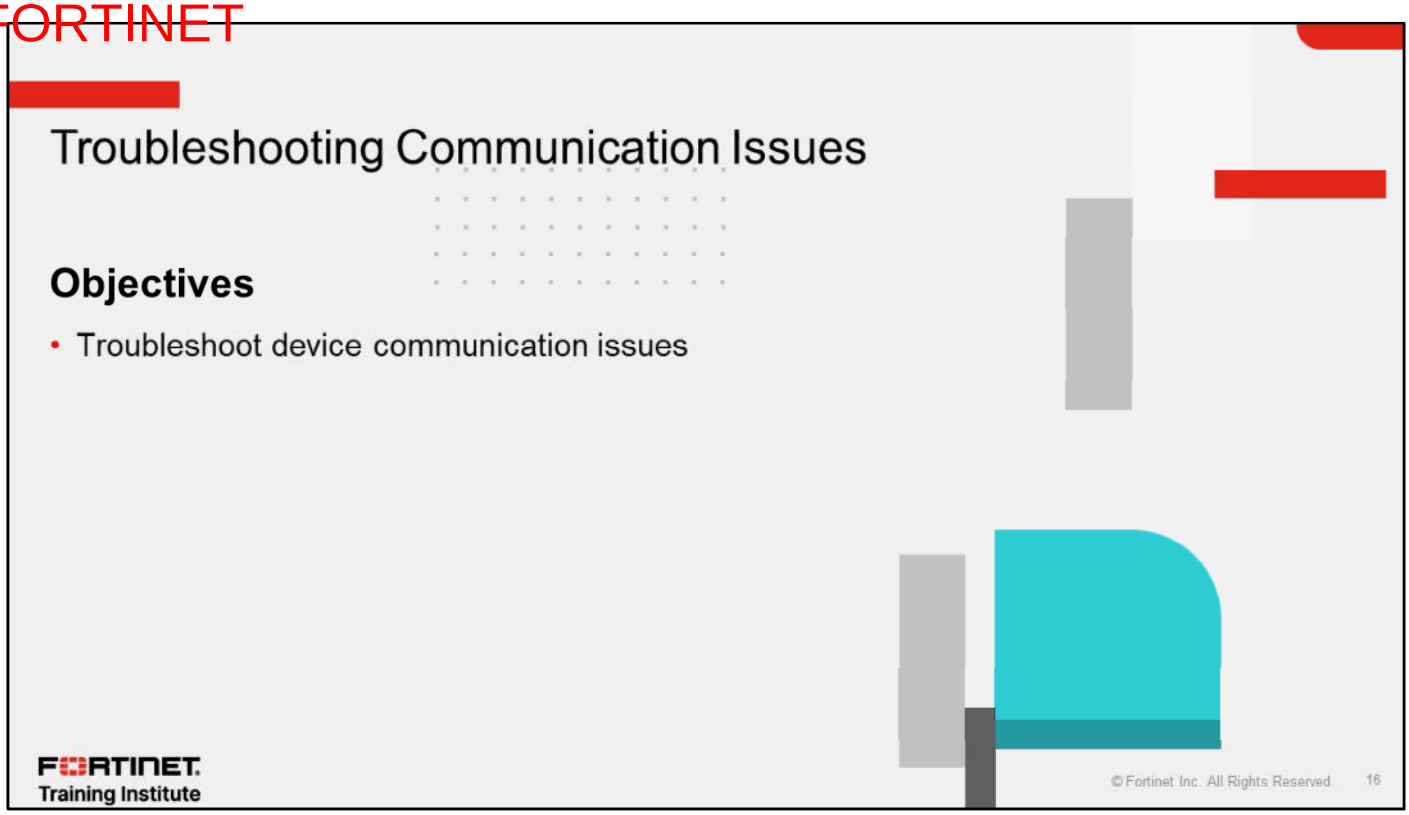
FORTINET Training Institute

 14



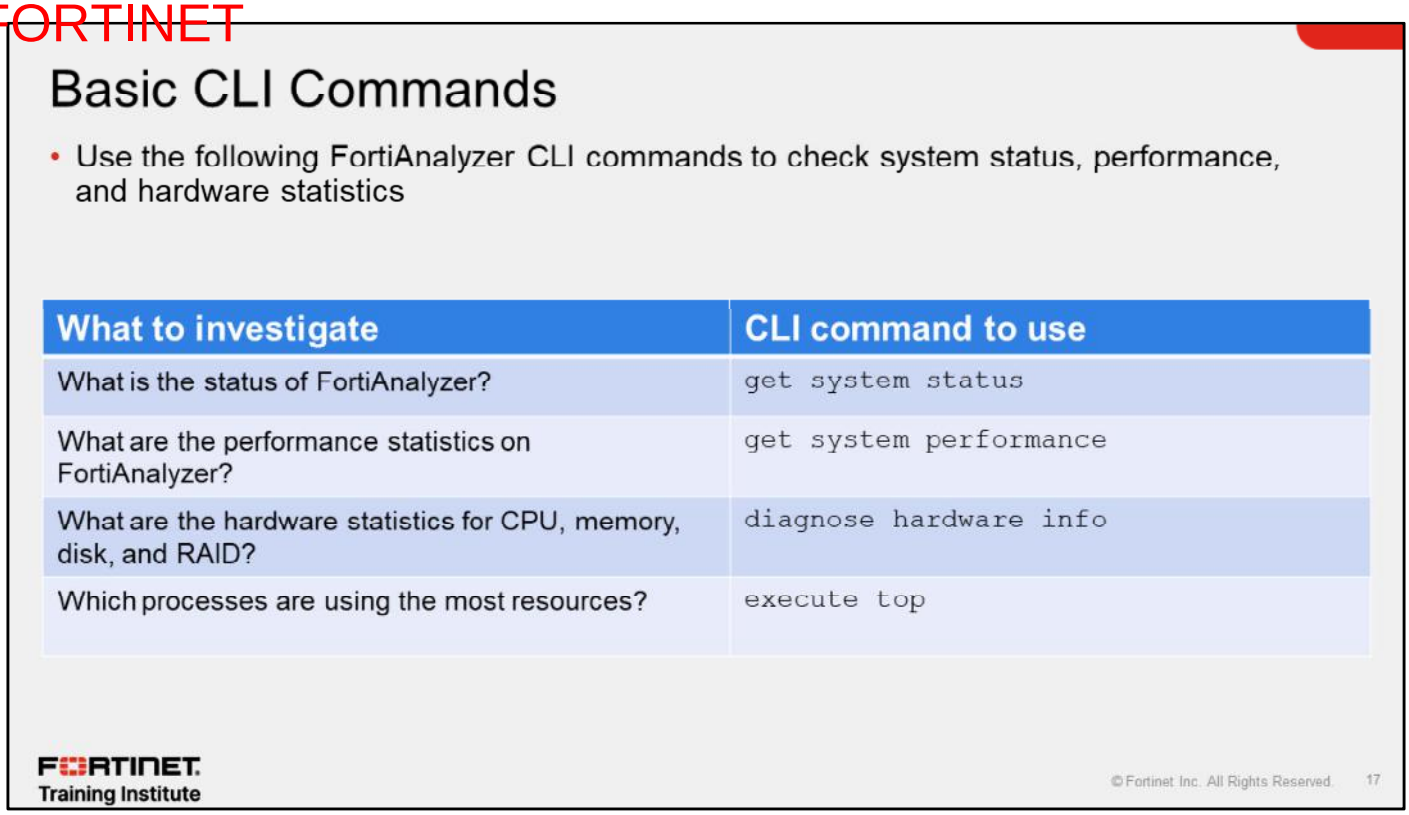
Good job! You now understand how to register a device.

Now, you will learn ways to troubleshoot communication issues between FortiAnalyzer and your registered devices.

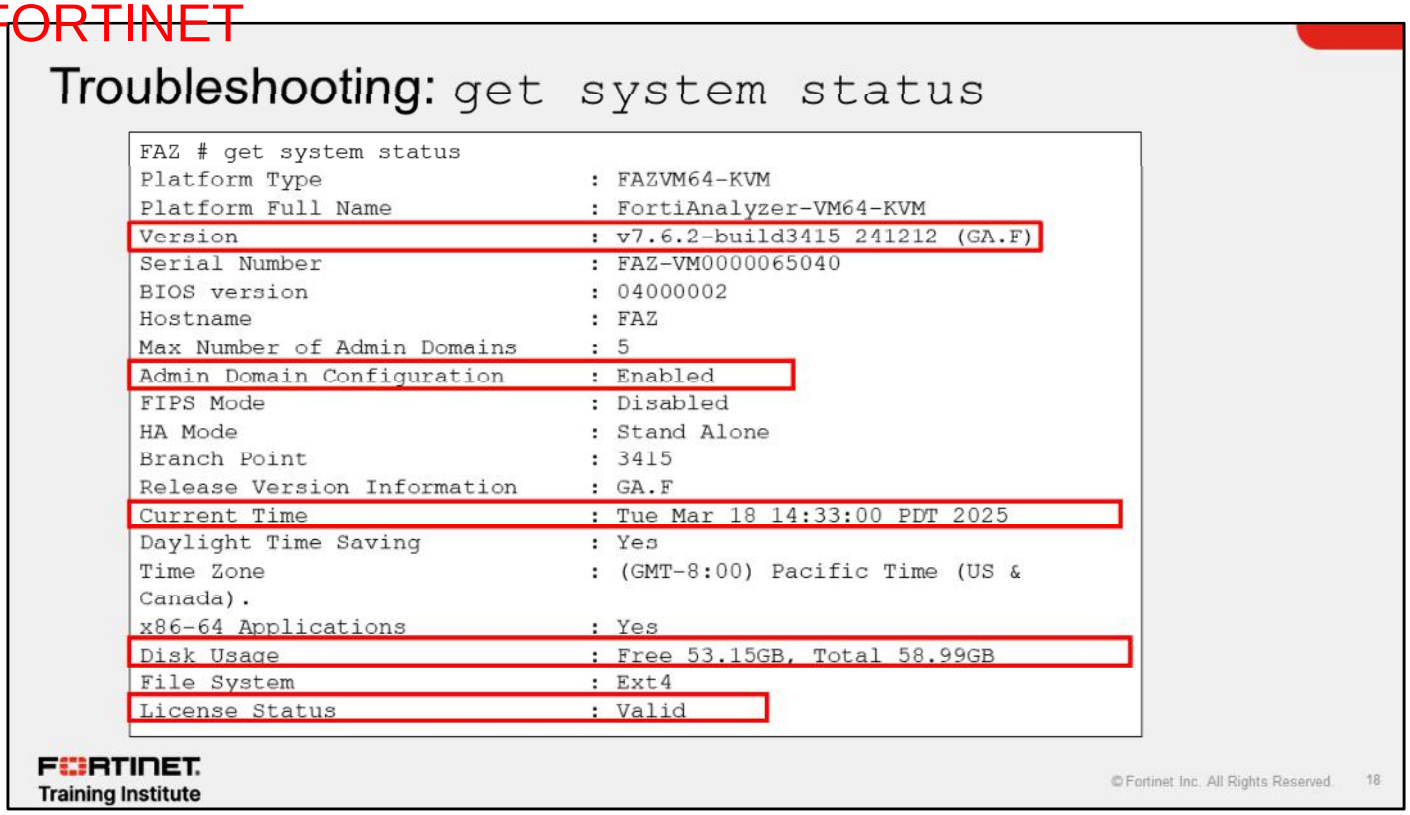


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in device communication troubleshooting, you will be able to efficiently troubleshoot issues that could prevent log collection.

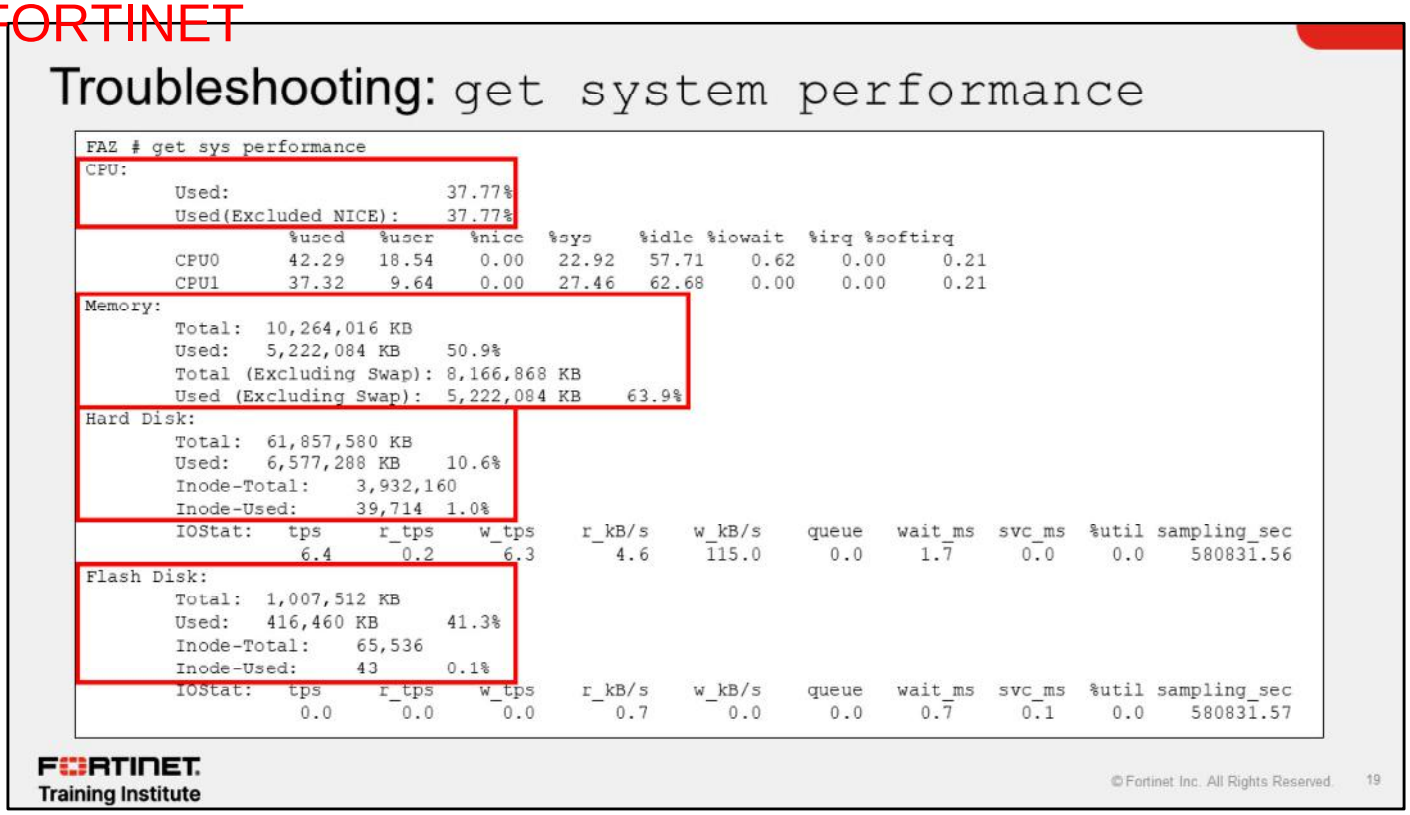


This slide shows some basic CLI commands that you can use to check system status, performance, hardware statistics, and processes.



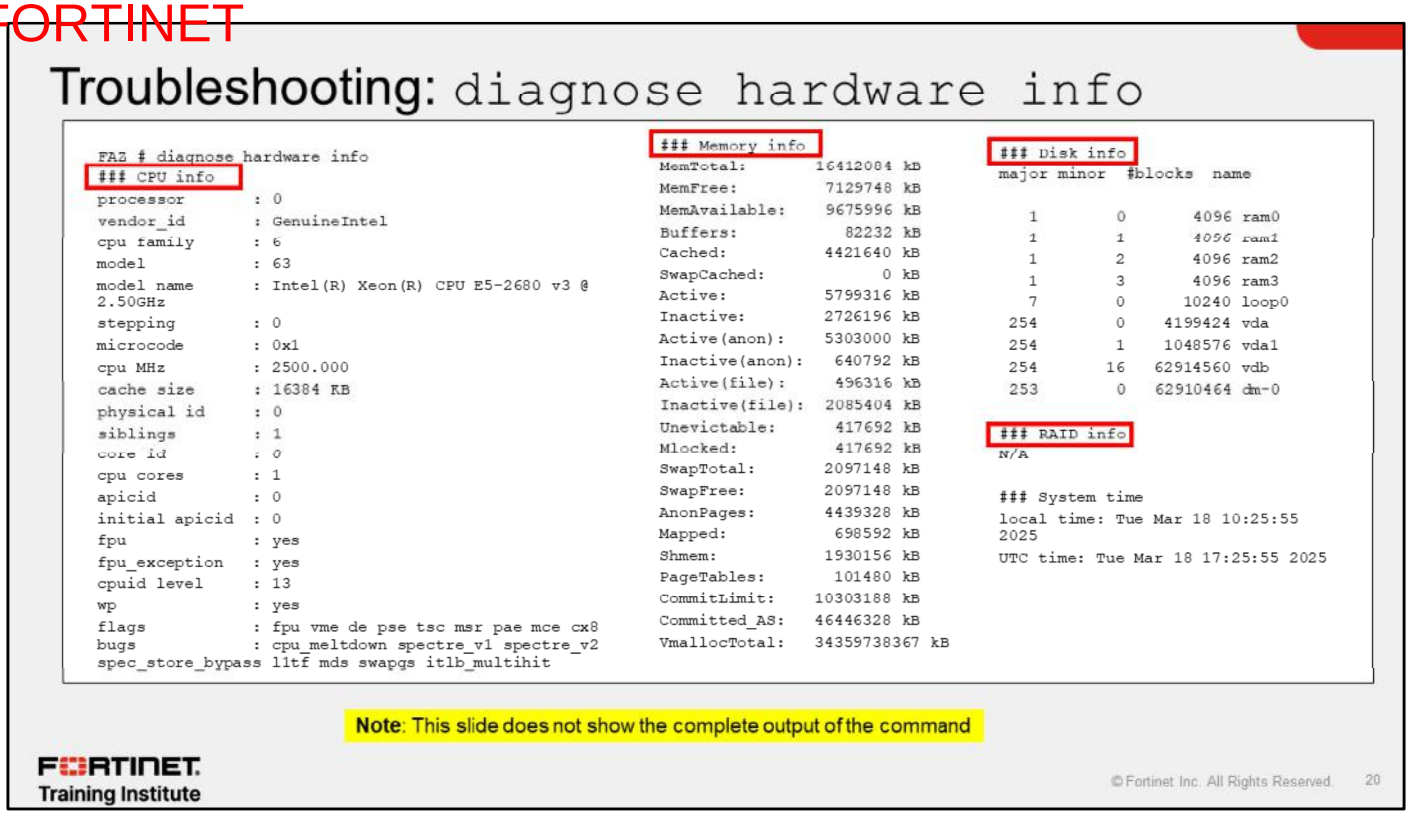
When using the `get system status` command to troubleshoot system issues, the following information can be helpful:

- `Version`: Ensure the FortiAnalyzer firmware version is compatible with your registering device. For supported firmware versions, see the *FortiAnalyzer Release Notes*.
- `Admin Domain Configuration`: Ensure ADOMs are enabled if you attempt to register a non-FortiGate device.
- `Current Time`: Ensure your date and time are set according to your needs. The FortiAnalyzer system time must be accurate for many features to work, including scheduling, logging, and SSL-dependent features. While you can manually set the date and time, it is recommended that you synchronize with a Network Time Protocol (NTP) server.
- `Disk Usage`: Ensure you have enough free disk space to accept and store logs from registered devices.
- `License Status`: Ensure you have a valid license. This is for a VM only.



When using the `get system performance` command to troubleshoot system issues, look at the used space for CPU, memory, hard disk, and flash disk. If any of these are *nearing* capacity, you may experience issues with log collection. The used capacity does not need to be at 100% before you encounter problems. For example, the space assigned to a hard disk quota is not fully available for logs because some is reserved for system usage and unexpected quota overflow.

For FortiAnalyzer VMs, a minimum of 16 GB of memory is recommended.



The `diagnose hardware info` command provides valuable details about the CPU, memory (RAM), and disks. The memory and RAID sections can be instrumental in troubleshooting system issues.

The `Memory info` section provides a more granular breakdown of memory than the `get system performance` command. For example, the total memory from the `get system performance` command includes the total and swap memory. The `diagnose hardware info` command shows a more detailed breakdown of all memory components.

Swap memory refers to the disk space available when the physical memory is full, and the system requires more memory. For a temporary period, inactive pages in memory are moved to the swap space.

If RAID is used as a high-performance storage solution, the RAID level impacts the determination of disk size and reserved quota level.

Troubleshooting: execute top

```
top - 11:03:59 up 19:30,  0 users,  load average: 0.29, 0.27, 0.22
Tasks: 245 total,   1 running, 244 sleeping,   0 stopped,   0 zombie
%Cpu(s):   1.8/1.0     3[|||                              ]

  PID USER      PR  NI    VIRT    RES  %CPU  %MEM     TIME+ S COMMAND
 2585 root      20   0  165.3m 133.2m   2.6   0.8  34:19.03 S /bin/python /us
 1025 root      20   0   97.6m  39.0m   1.3   0.2  11:04.17 S forticldd.main
 1032 root      20   0  833.3m 105.2m   1.3   0.7  12:36.29 S oftpd
 3486 postgres  20   0 2844.2m  30.5m   1.0   0.2   0:20.11 S postgres
  249 root      20   0   87.6m  35.1m   0.7   0.2   5:06.77 S cmdbsvr
 1028 root      20   0  395.1m  39.2m   0.7   0.2  10:54.60 S logfwd.main
 2607 root      20   0  158.6m 128.2m   0.7   0.8   7:22.42 S airflow schedul
    8 root      20   0    0.0m   0.0m   0.3   0.0   1:27.66 I rcu_sched
```

Note: This slide does not show the complete output of the command

FORTINET Training Institute

 21

The `execute top` command provides real-time information about processes on FortiAnalyzer. You can see the process ID, CPU usage, memory usage, and other information. Use the `get system performance` command to check resource usage. If it is high, use the `execute top` command to get detailed information about how resources are allocated.

You can press `h` while the command is running to bring up a help window, which lists common shortcuts and their descriptions. Depending on which shortcut you press, you can sort by different criteria or toggle different summaries.

Device and ADOM Status Check

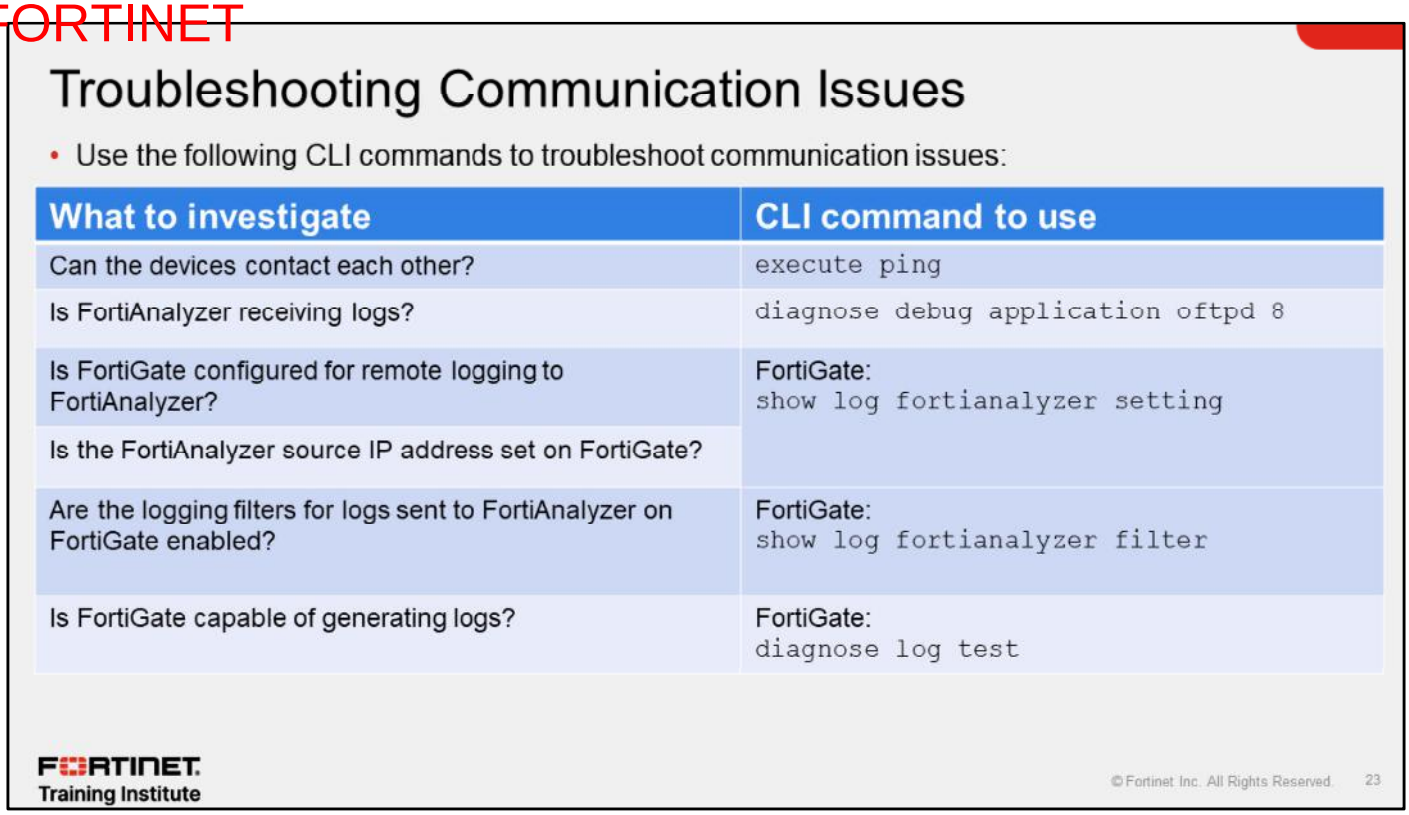
- Use the following FortiAnalyzer CLI commands to check the device and ADOM status

What to investigate	CLI command to use
Which devices and IP addresses are connected to FortiAnalyzer?	`diagnose test application oftpd 3`
Which ADOMs are enabled and configured?	`diagnose dvm adom list`
Which devices or VDOMs are currently registered and unregistered?	`diagnose dvm device list`

FORTINET Training Institute

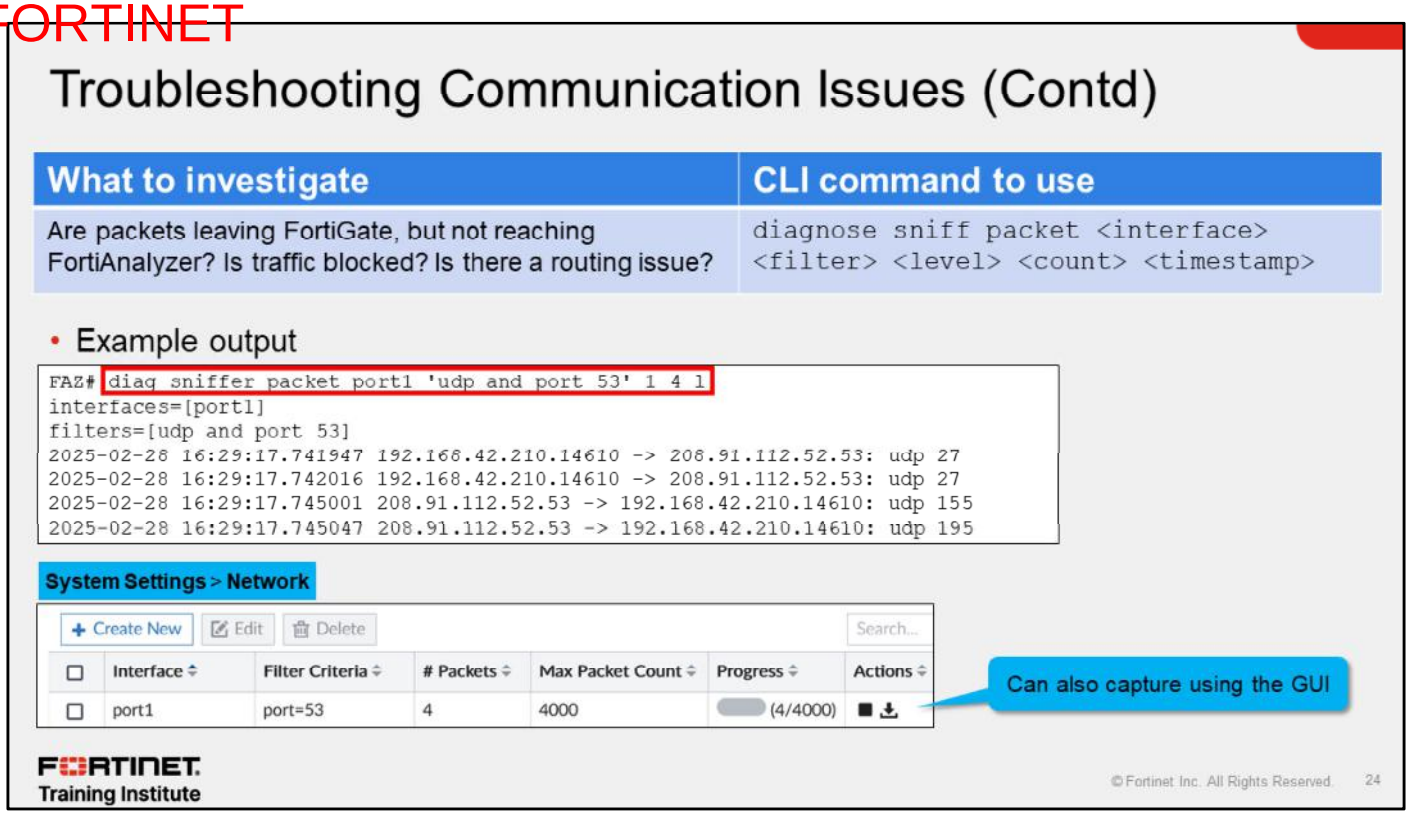
 22

This slide shows the FortiAnalyzer CLI commands you can run to discover which devices and IP addresses are connected to FortiAnalyzer, which ADOMs are enabled and configured, and which devices are registered and unregistered.



If you are experiencing communication issues between other devices and FortiAnalyzer, ensure that both devices can reach each other. Use the `execute ping` CLI command on either device to verify reachability (ping must be enabled and allowed by all intermediate firewalls).

Other questions to ask:
- Is FortiGate configured for remote logging to FortiAnalyzer?
- Is the FortiAnalyzer receiving logs? You can run an `oftpd` debug to verify log forwarding.
- Is the FortiAnalyzer source IP address set on FortiGate? This is important if FortiAnalyzer is accessed over a VPN that allows only a specific subnet.
- Are the logging filters for logs sent to FortiAnalyzer enabled on FortiGate?
- Is FortiGate capable of generating logs, and can FortiAnalyzer receive them? If you don't see any logs on FortiGate, you must examine the logging issue on FortiGate, before troubleshooting FortiAnalyzer.

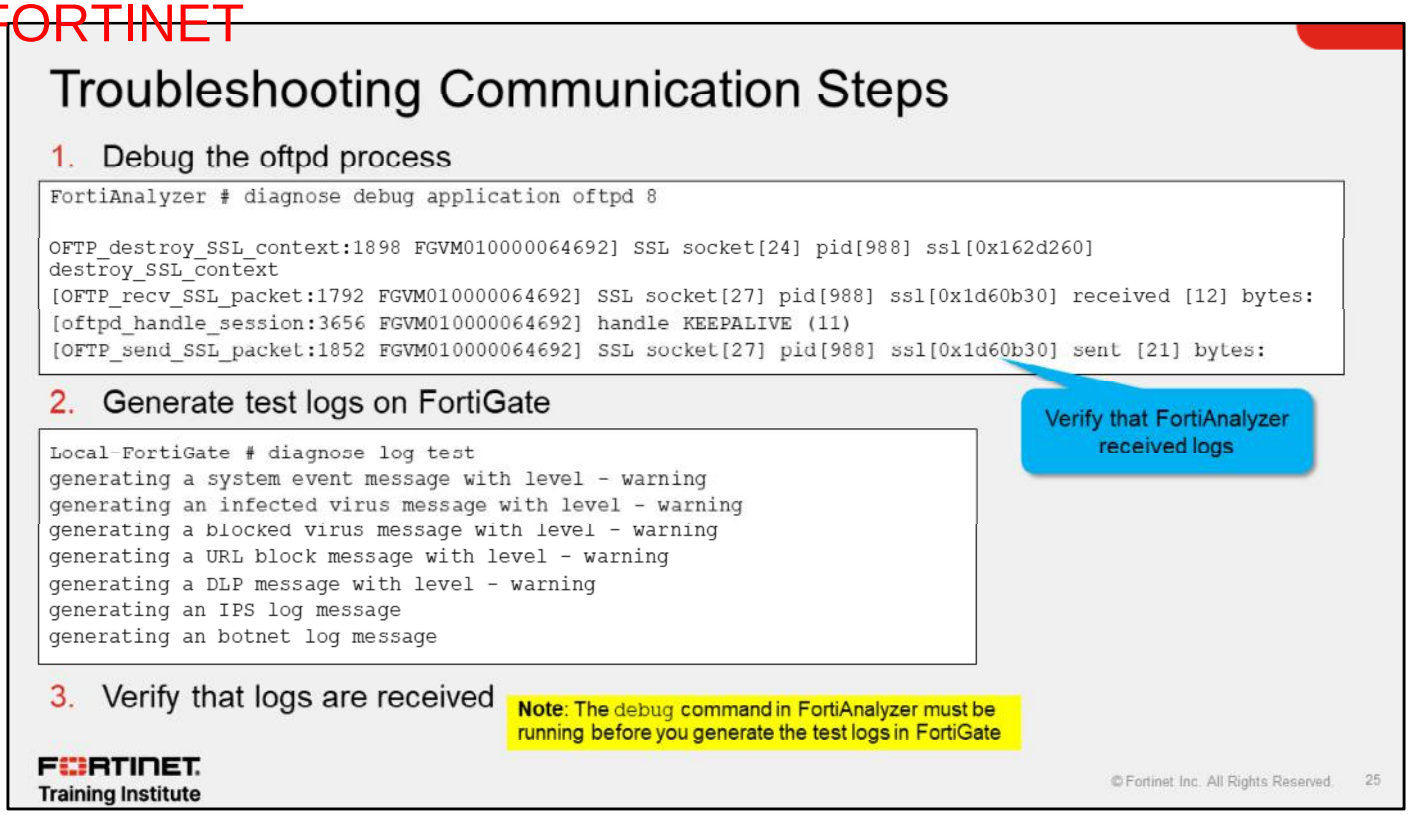


You can also run sniffers on both devices to see if packets leaving FortiGate are reaching FortiAnalyzer. If packets are leaving FortiGate but not reaching FortiAnalyzer, look at other devices in the network because an intermediate router or firewall may be blocking the traffic or routing it inappropriately.

FortiAnalyzer has a built-in packet sniffer available on the GUI and CLI. It supports versatile filters and verbosity levels 1–3. The higher the verbosity level, the more information the capture contains. For troubleshooting purposes, Fortinet Technical Support may request level-3 captures.

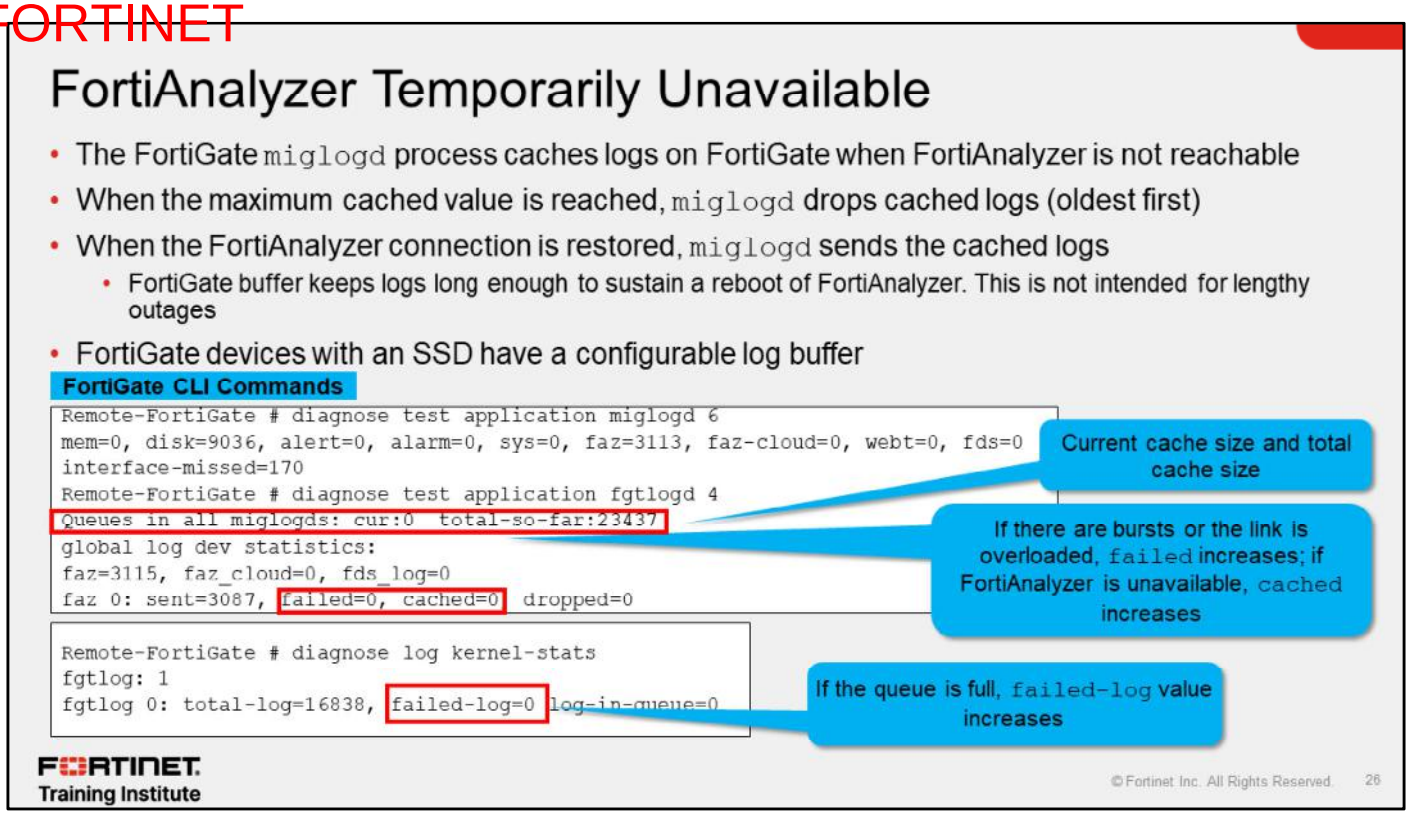
In the CLI example shown on this slide, the capture has the following characteristics:
- Traffic on port1
- UDP port 53 (DNS traffic)
- Level 1 verbosity
- Capture limit of four packets
- Local time

For more syntax information, consult the *CLI Reference* guide for FortiAnalyzer on docs.fortinet.com.



You can use the following commands at the same time to troubleshoot communication issues:

1. Run the `diagnose debug application oftpd 8` command on FortiAnalyzer to view current log activity.
2. Run the `diagnose log test` command on FortiGate to send some test logs to FortiAnalyzer.
3. Review the output shown on this slide. If everything is working as expected and logs are being received, you should see some entries on FortiAnalyzer.



If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its `miglogd` process to cache the logs. The cache has a maximum size, and the `miglogd` process drops cached logs, starting with the oldest ones first.

When the connection between the two devices is restored, the `miglogd` process sends the cached logs to FortiAnalyzer. The FortiGate buffer keeps logs long enough to sustain a restart of FortiAnalyzer (if you upgrade the firmware, for example). This is not intended for a lengthy FortiAnalyzer outage.

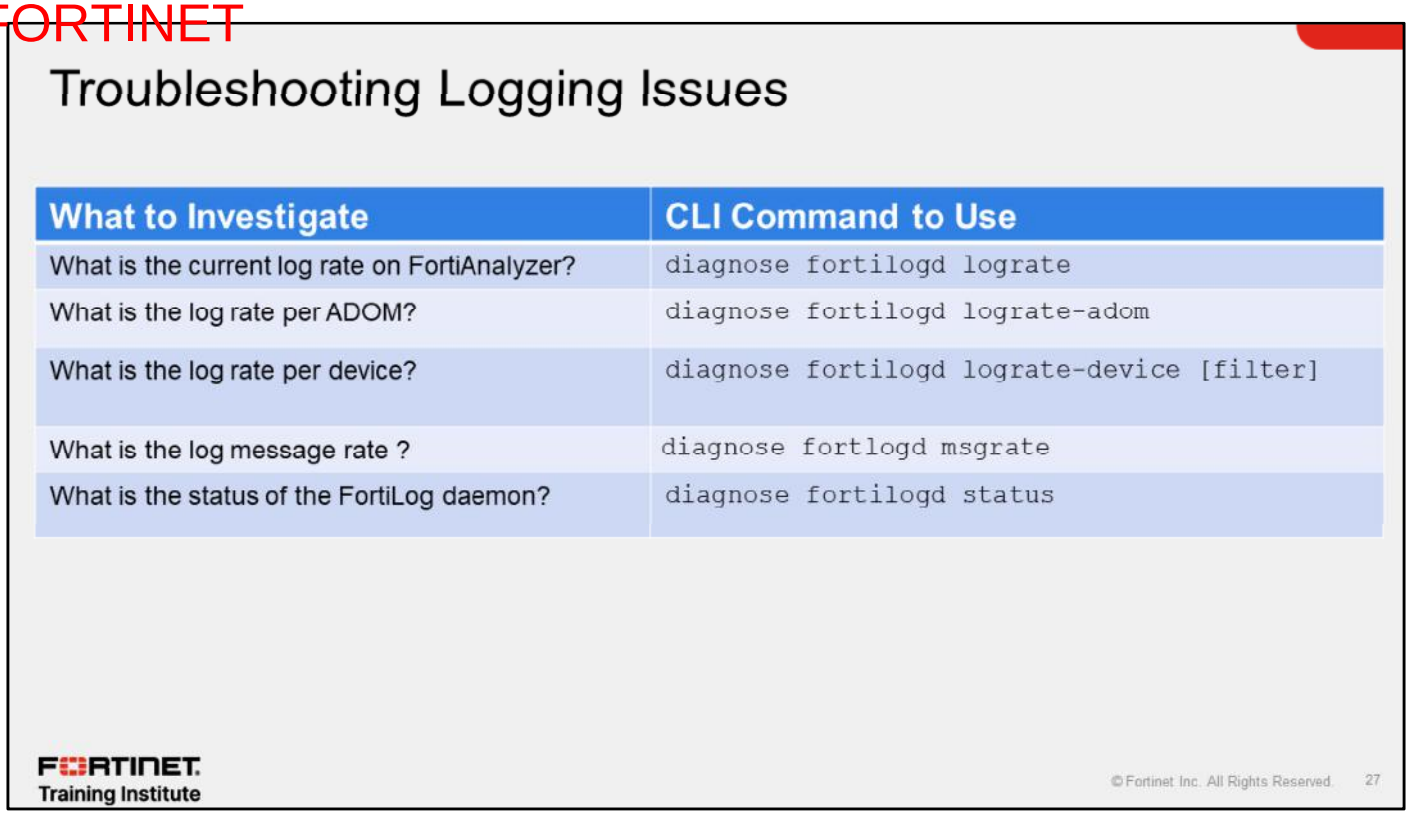
On FortiGate, the CLI commands `diagnose test application miglogd 6` and `diagnose test application fgtlogd 4` display logging statistics, including the current and maximum cache sizes.

The CLI command `diagnose log kernel-stats` shows an increase in `failed-log` if the cache is full and logs must be dropped.

FortiGate devices with an SSD disk have a configurable log buffer. If the memory log buffer is full when the connection to FortiAnalyzer is unreachable, FortiGate can buffer logs on the disk. FortiGate will seamlessly transmit the logs from the disk buffer once the connection to FortiAnalyzer is successfully reestablished.

To change the buffer size, use the following commands:

```
config system global
    set faz-disk-buffer-size <integer> ; <integer> disk queue size of
FortiAnalyzer within range 0-4506 MB (0 = disabled)
end
```



If you suspect that the FortiAnalyzer is having issues logging, use the commands shown on this slide to check the FortiLog daemon. You can check the log rate on FortiAnalyzer, log rate per ADOM, and log rate per registered device.

You can also check the log message rate on FortiAnalyzer and the status of the FortiLog daemon.

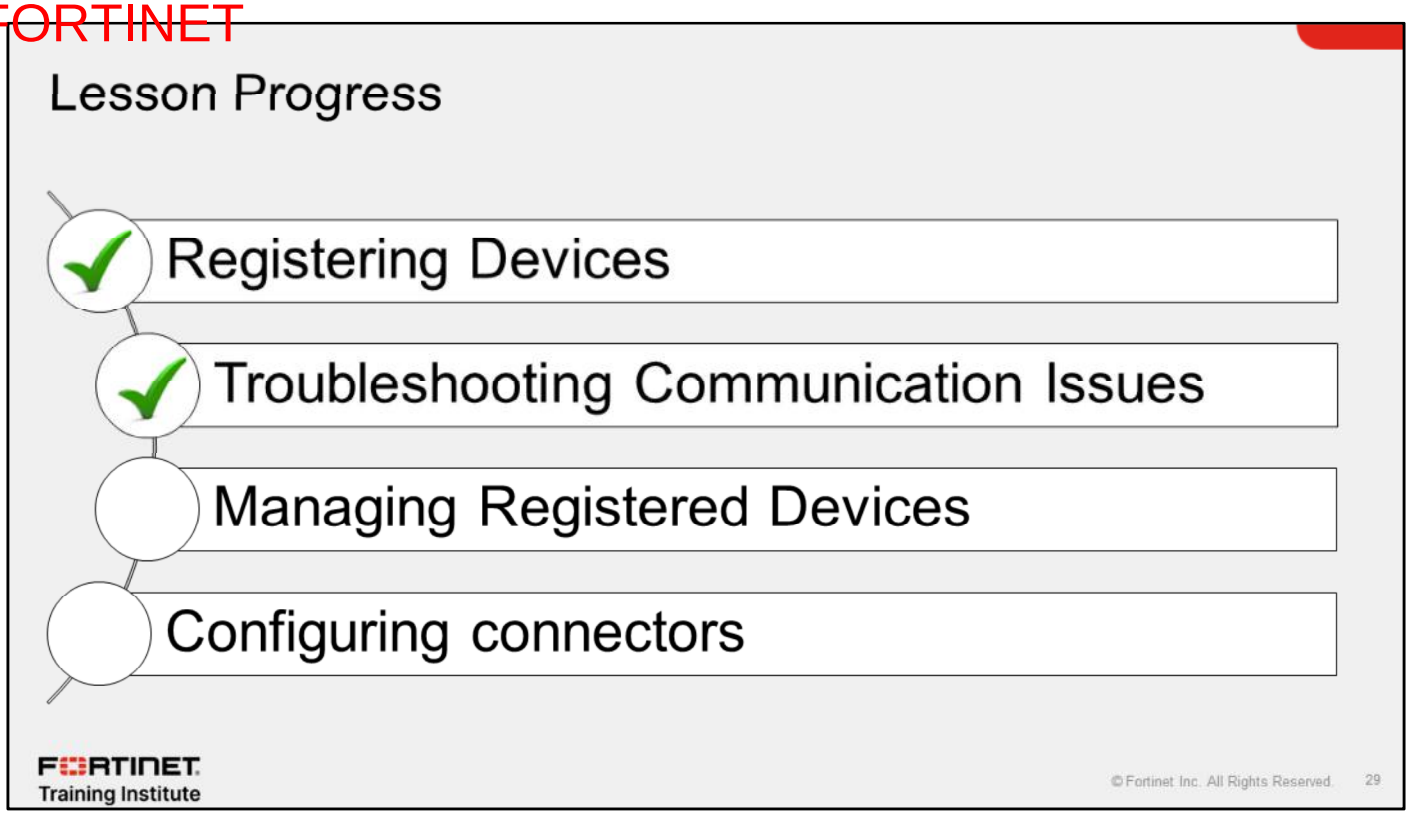
Knowledge Check

1. Which CLI command can you use to determine if ADOMs are enabled?
   - ✓ A. `get system status`
   - B. `show system performance`

2. What can the CLI command `diagnose test application oftpd 3` help you determine?
   - A. That ADOMs are enabled and configured
   - ✓ B. The devices and IP addresses that are connecting to FortiAnalyzer

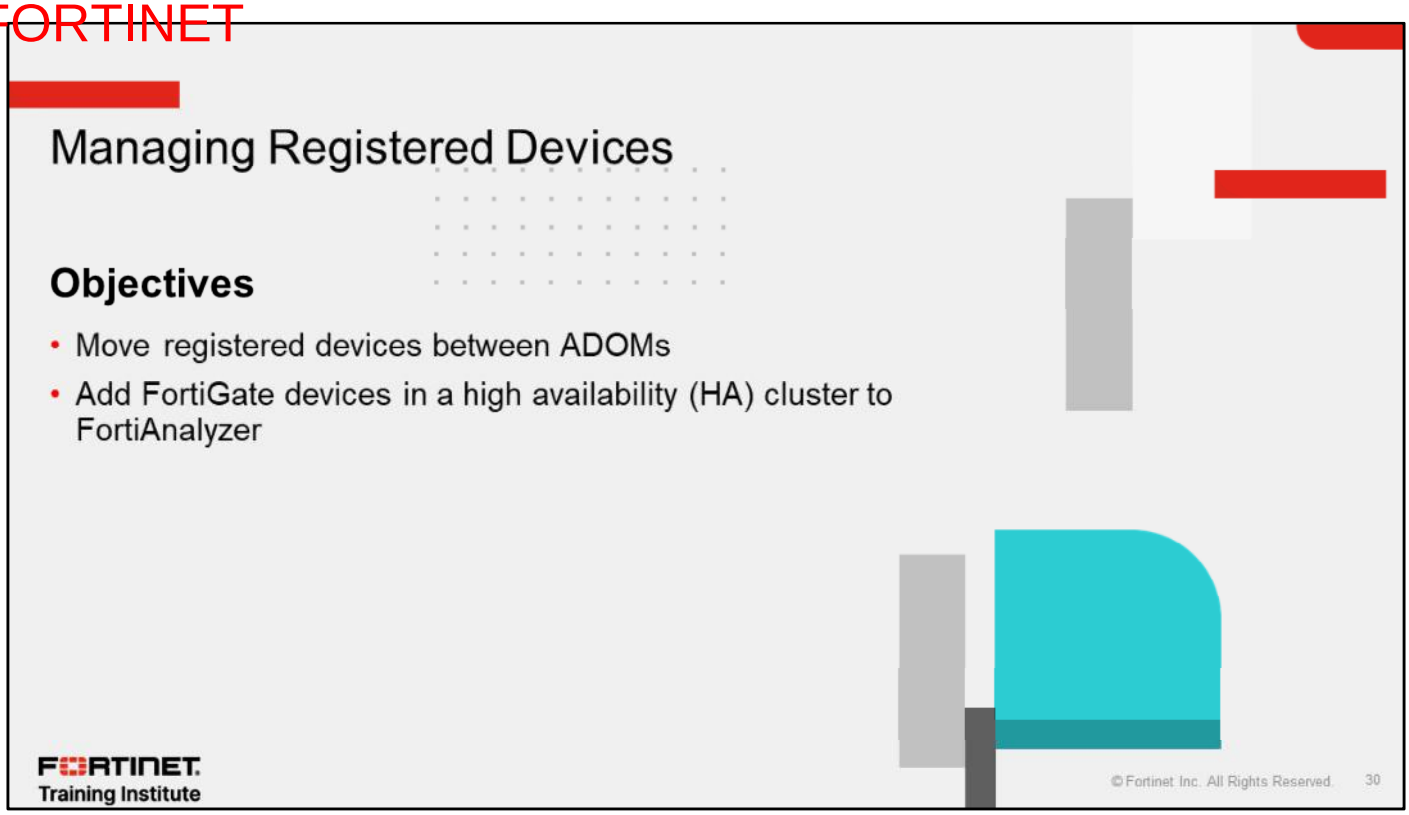
FORTINET Training Institute

 28



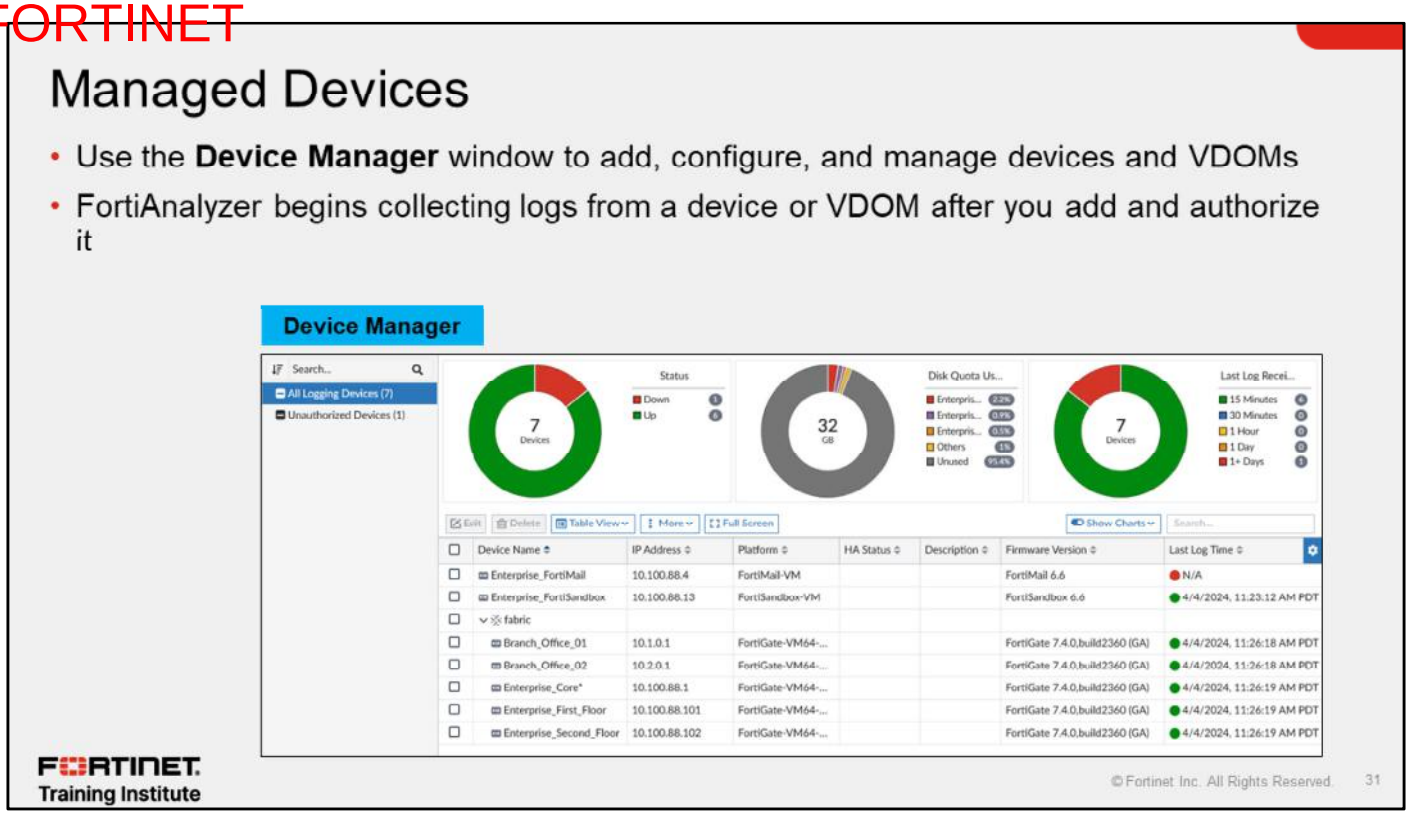
Good job! You now understand how to troubleshoot communication issues.

Now, you will learn how to manage registered devices.



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

By demonstrating competence in moving devices between ADOMs and adding FortiGate devices in an HA cluster, you will be able to manage registered devices effectively in your network.



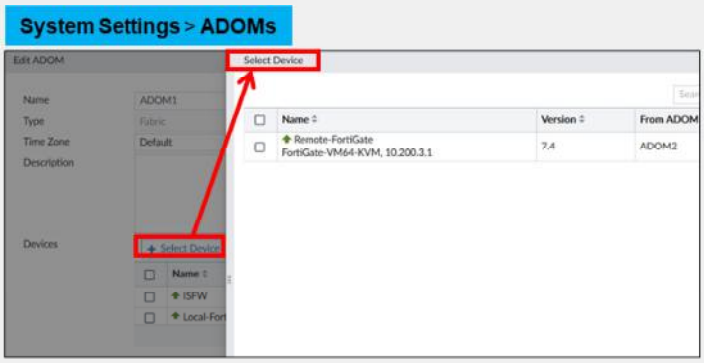
Use the **Device Manager** window to add, configure, and manage devices and VDOMs.

After you add and authorize a device or VDOM, FortiAnalyzer begins collecting logs from it. You can configure the FortiAnalyzer unit to forward logs to another device.

FortiAnalyzer supports collection and analysis of logs from almost all Fortinet devices. Go to `docs.fortinet.com` for a complete list of all the devices that FortiAnalyzer supports.

Moving Registered Devices Between ADOMs

- Do not move devices between ADOMs unless absolutely necessary
- You can move devices between ADOMs after registration
  - By default, restricted to administrators with Super_User access
- You do not need to create a new ADOM if you upgrade your FortiGate firmware
  - Not necessary to separate ADOMs by FortiOS version



FORTINET Training Institute

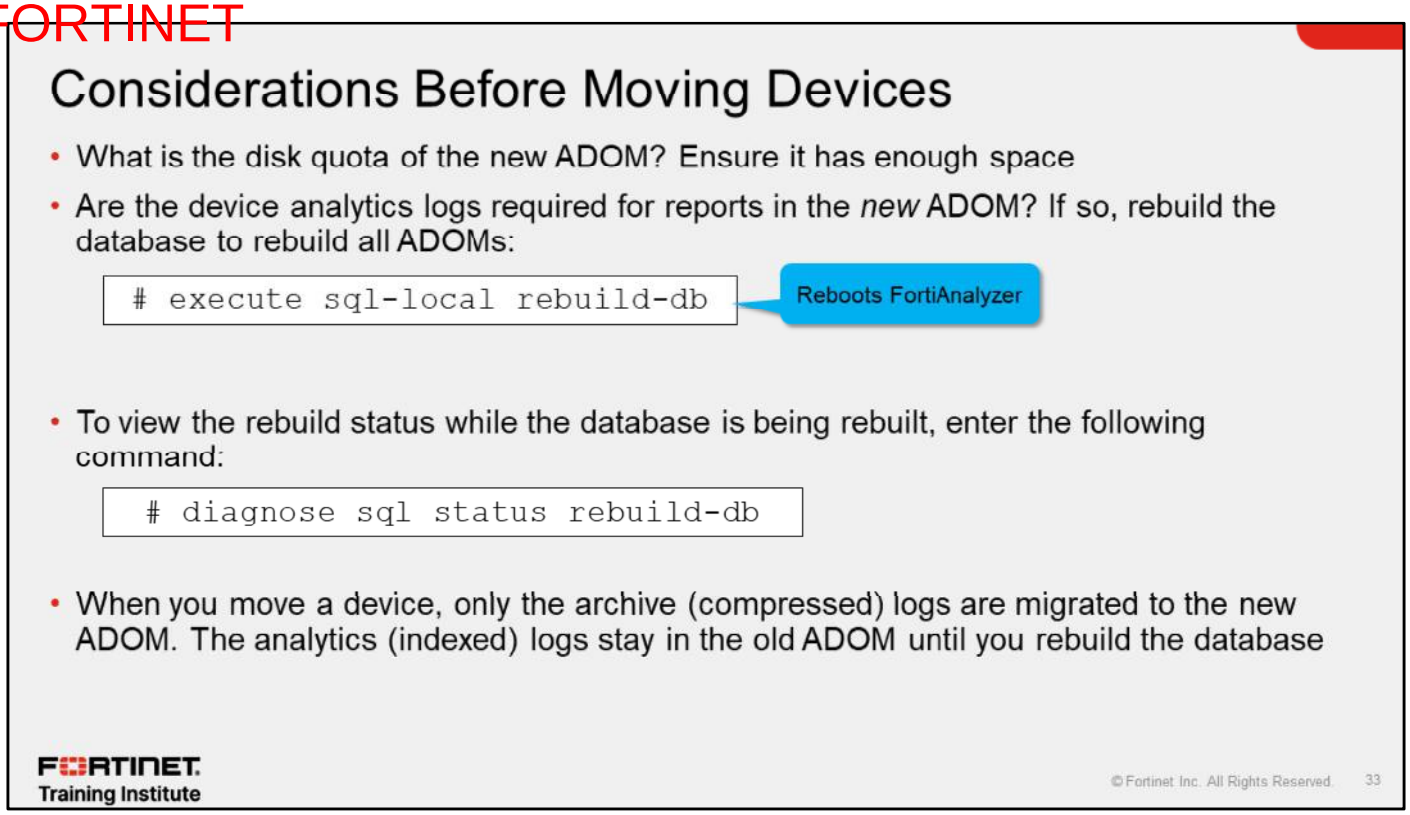
 32

You can move devices between ADOMs after registration on the **ADOMs** page.

While it's not advisable to move devices between ADOMs unless necessary, there are cases where it can be beneficial. For example, if you have a mix of low-volume and high-volume log rates in one ADOM, it is recommended to place the low-volume log rate devices in one ADOM and the high-volume log rate devices in another. This separation helps prevent quota enforcement from negatively impacting the low-volume log devices.

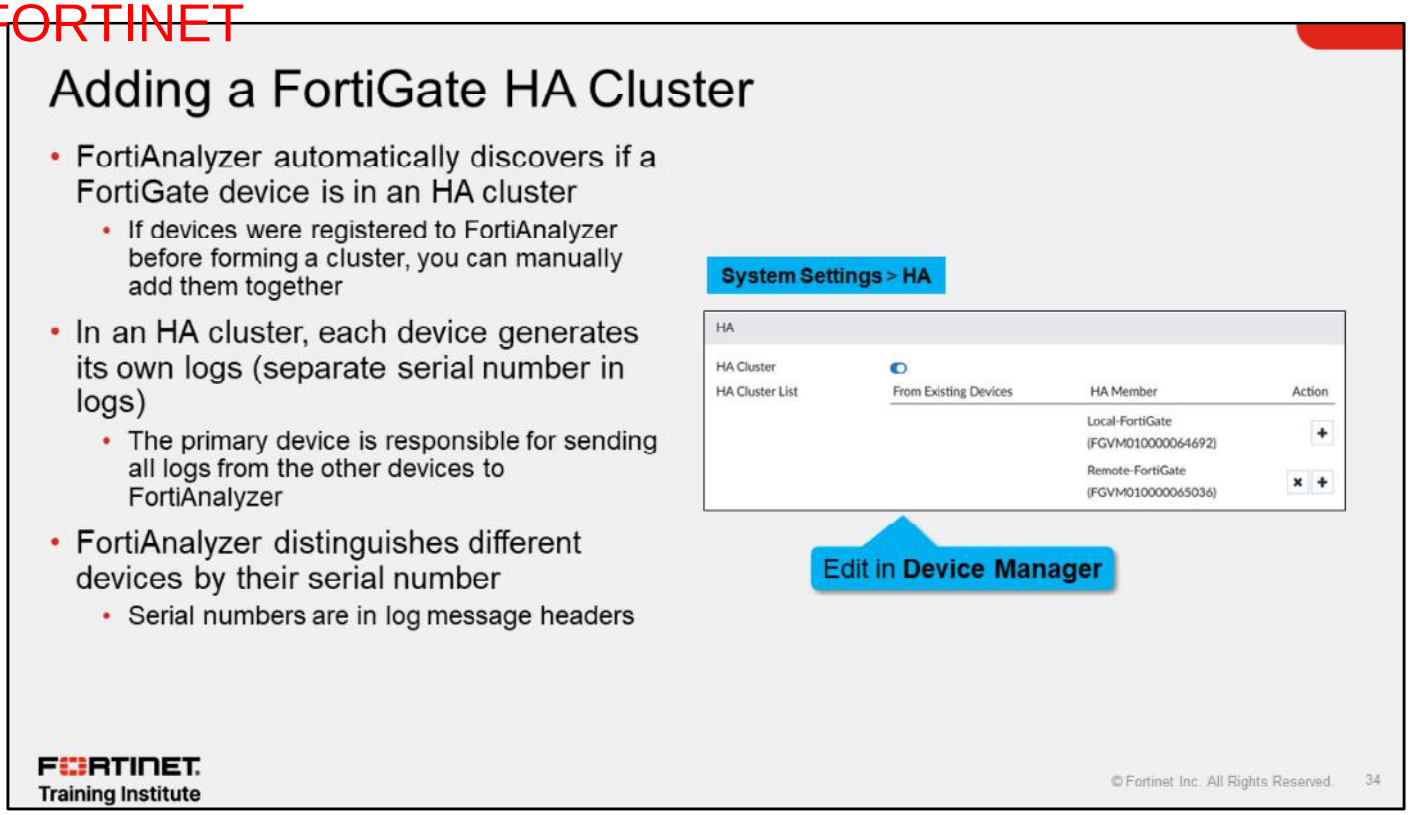
To move devices between ADOMs, edit the custom ADOM where you want to add the device and then select the device to add to it.

You do not need to move devices into a new ADOM when you upgrade your FortiGate firmware.



There are some important considerations when moving devices between ADOMs, especially if logs are already being collected for the device you are moving:

- What is the disk quota of the new ADOM? Ensure the new ADOM has enough space.
- Are the device analytics logs required for reports in the new ADOM? If so, you must rebuild the new ADOM SQL database. Only the archive logs (compressed logs) are migrated to the new ADOM when you move a device. The analytics logs (indexed logs) stay in the old ADOM until you rebuild the database.
- Do you want to see the device analytics logs in the old ADOM? If not, you need to rebuild the old ADOM SQL database. Otherwise, they are removed according to the data policy.



FortiAnalyzer automatically detects if a FortiGate device is part of an HA cluster. If you register your device with FortiAnalyzer before adding it to a cluster, you can manually add the cluster within FortiAnalyzer.

In an HA cluster, only the primary FortiGate device communicates directly with FortiAnalyzer. The nodes in the HA cluster send their logs to the primary FortiGate device, which forwards them to FortiAnalyzer.

To enable a cluster, edit the registered device on FortiAnalyzer in **Device Manager** and enable **HA Cluster**. You can either add existing devices to the cluster or manually enter the serial numbers for each device.

FortiAnalyzer identifies different devices by their serial numbers, which are included in the headers of all the log messages it receives.

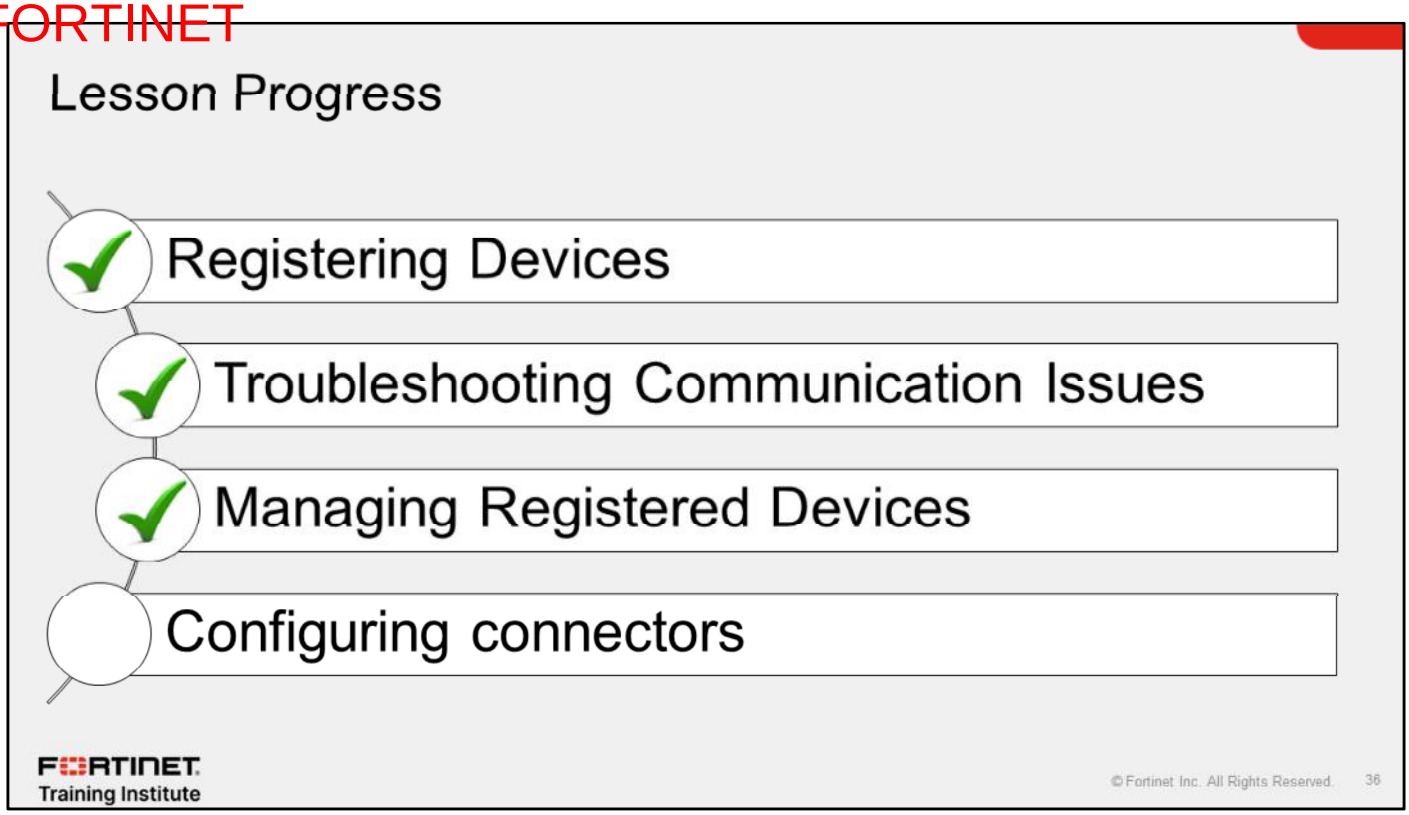
Knowledge Check

1. When you move a FortiGate device to a different ADOM, which type of log is migrated to the new ADOM without requiring a database rebuild?

✓ A. Archive logs
B. Analytic logs

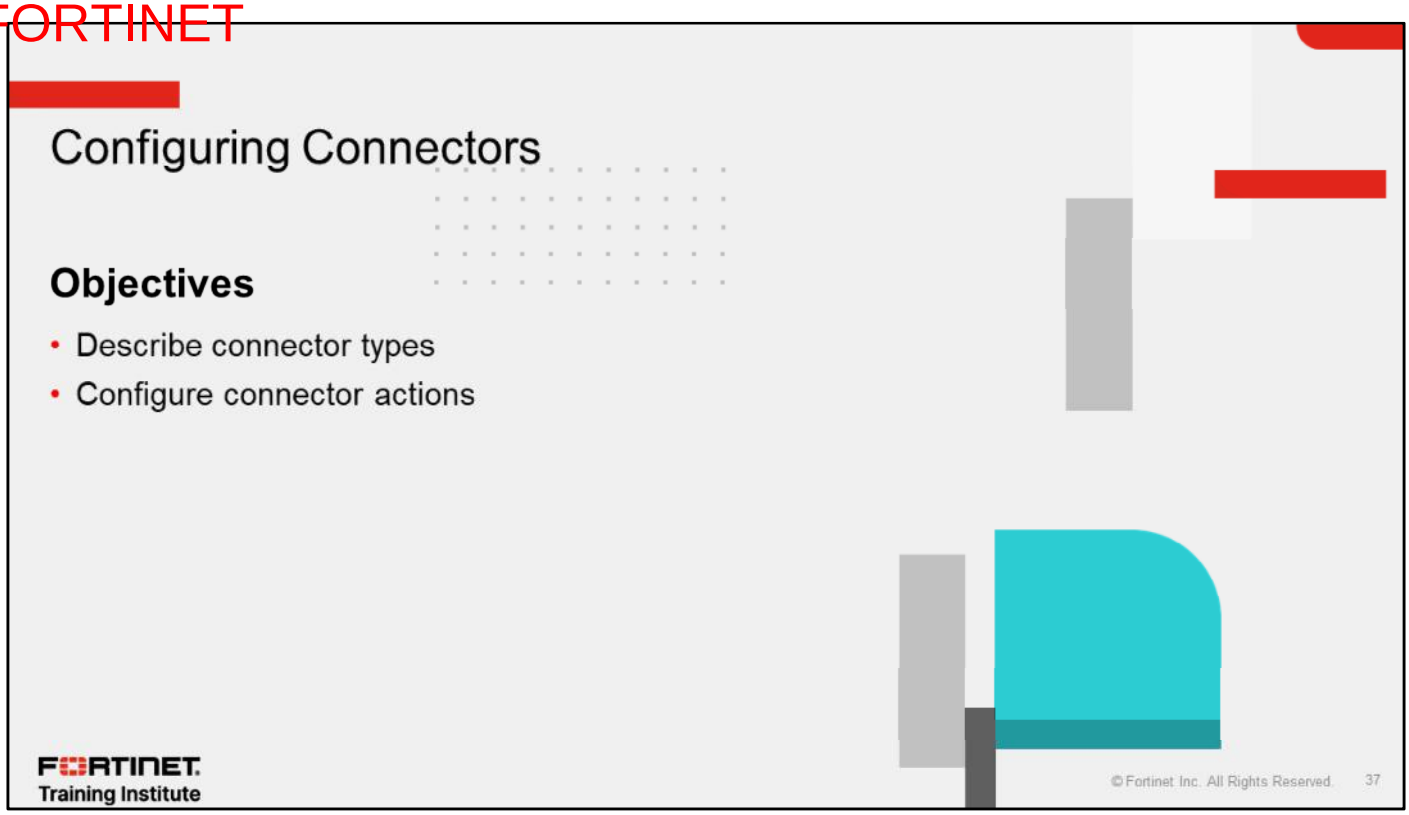
FORTINET Training Institute

 35



Good job! You now understand how to manage registered devices on FortiAnalyzer.

Now, you will learn about connectors.

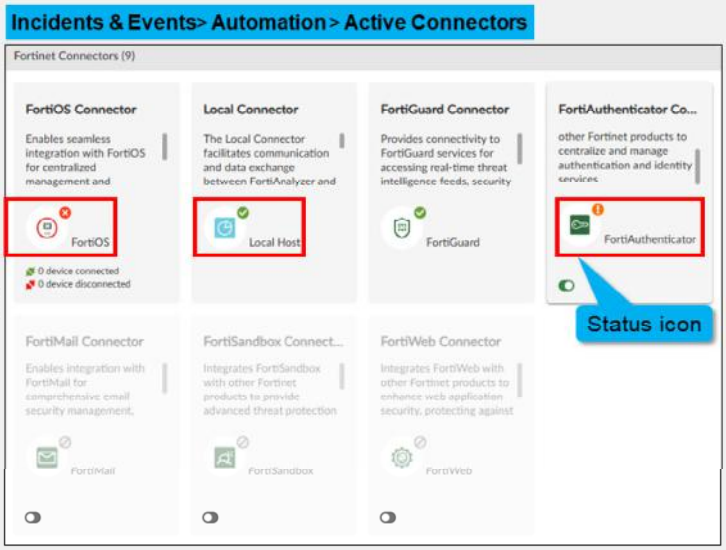


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring connectors, you will understand how FortiAnalyzer uses connectors to automate actions to be performed on other Fortinet devices.

Connectors

- Allow playbooks to interact with devices in the Security Fabric and other standalone devices
- Determine which actions can be performed by playbook tasks
- The local connector does not need any additional configuration
  - All other connector types must be configured
- Have a color-coded status icon:
  - Green: connection successful
  - Orange: connection unknown
  - Red: connection down



FORTINET Training Institute

 38

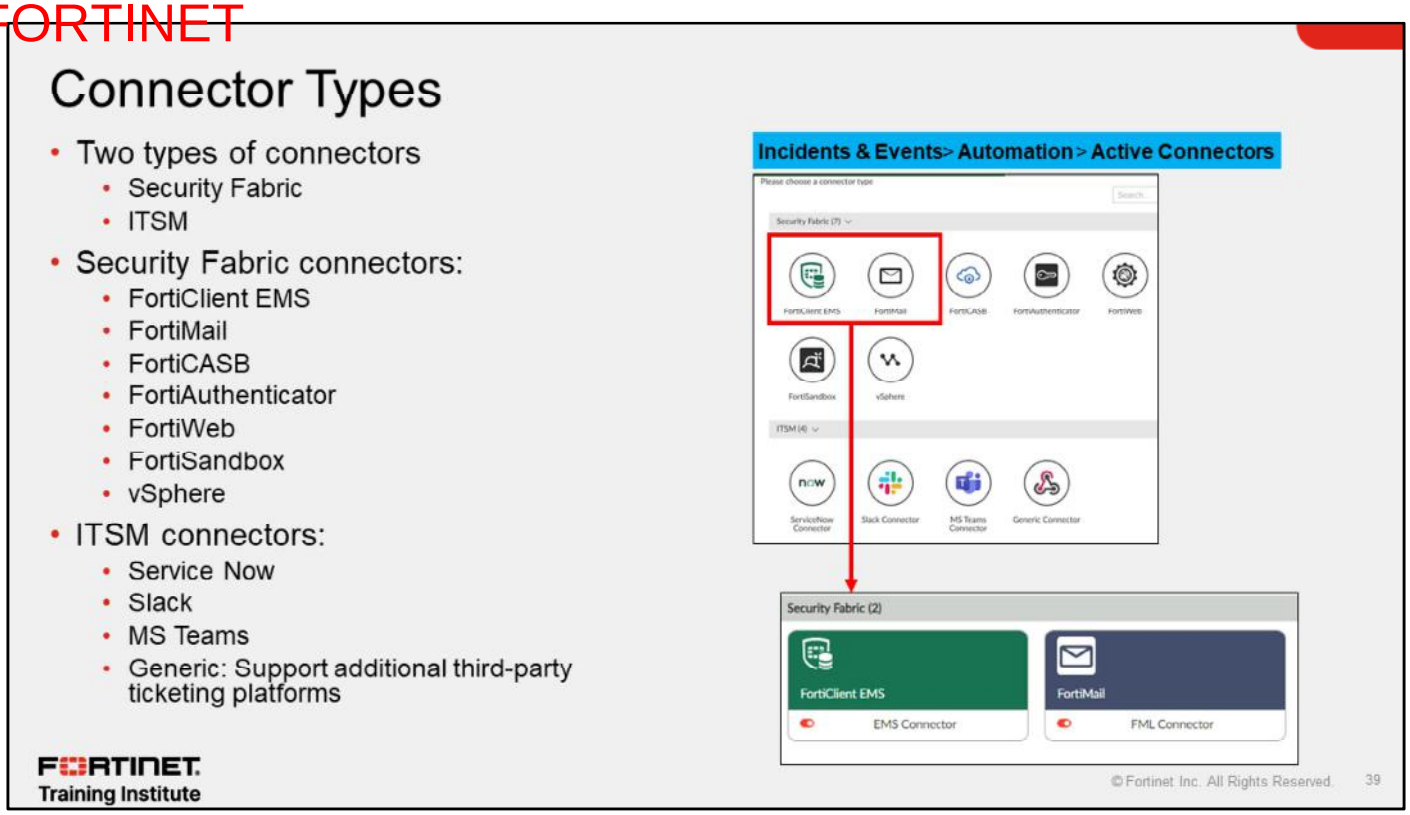
Connectors determine which automated actions playbooks can perform. Each connector type supports different actions.

You can quickly determine the API connection status of a connector, which is indicated by a colored status icon.

By default, you can use the local connector in playbooks without any additional configuration. All other connectors require extra configuration.

The connector status icon is colour-coded. Green means the connection is successful, orange means the connection is unknown, and red means the connection is down.

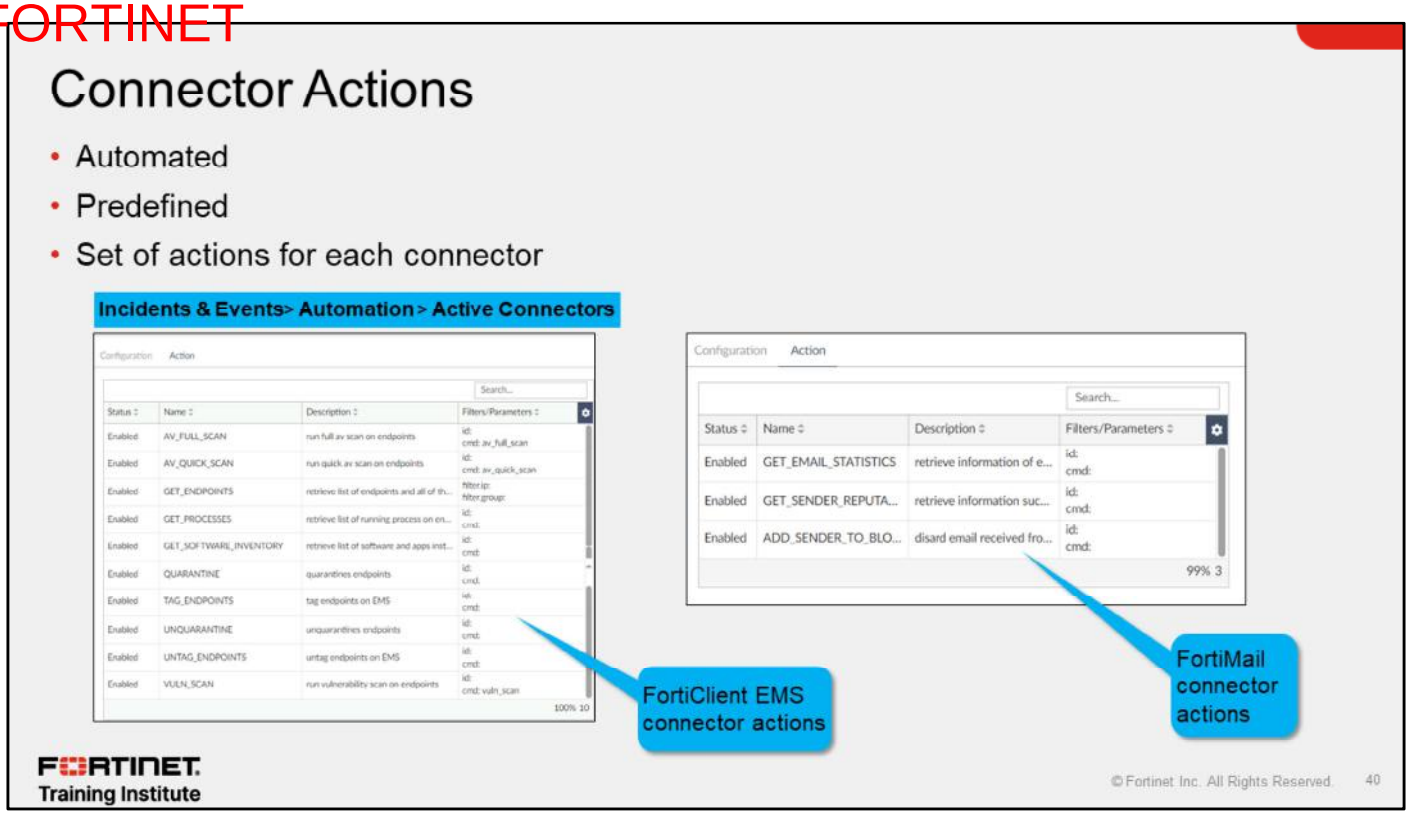
For example, the FortiOS connector is listed when you add the first FortiGate device to FortiAnalyzer. To access the actions related to the FortiOS connector, you must enable an automation rule triggered by an incoming webhook call on the FortiGate device.



FortiAnalyzer has two types of connectors that you can configure on the **Fabric Connectors** page: Security Fabric and IT service management (ITSM).

Security Fabric connectors include FortiClient EMS, FortiMail, and FortiCASB connectors.

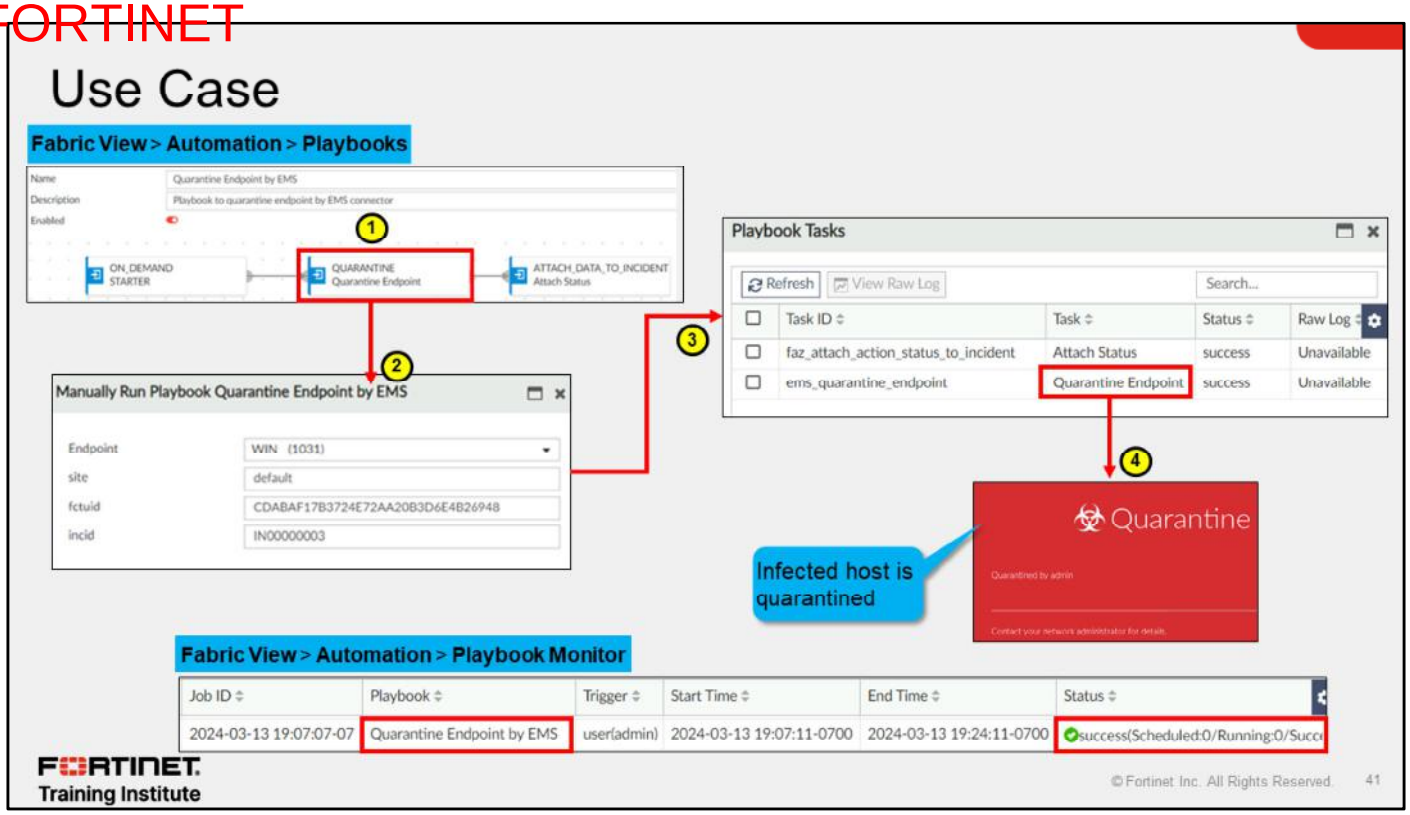
ITSM connectors include connecting to third-party service management or ticketing software such as Service Now, Slack, MS Teams, and so on. FortiAnalyzer also supports a generic connector type to facilitate integration with additional third-party ticketing software.



Each connector has its own set of predefined actions. These actions are automated and are performed in playbooks.

An example of when you might use a connector action in your network is to have a FortiClient EMS connector regularly retrieve a list of endpoints or perform quarantine actions on compromised endpoints.

All connector actions are predefined and cannot be modified.



This slide shows an example of a playbook using the FortiClient EMS connector.

FortiAnalyzer has generated an event indicating that a host is infected after downloading a malicious file. The analyst has configured a playbook with a FortiClient EMS connector to quarantine infected hosts.

The analyst performs the following actions:
1) Manually runs the playbook because it is configured for an on-demand trigger.
2) Enters the FortiClient host details, including endpoint number, FortiClient UID, FortiClient site, and an existing incident ID.

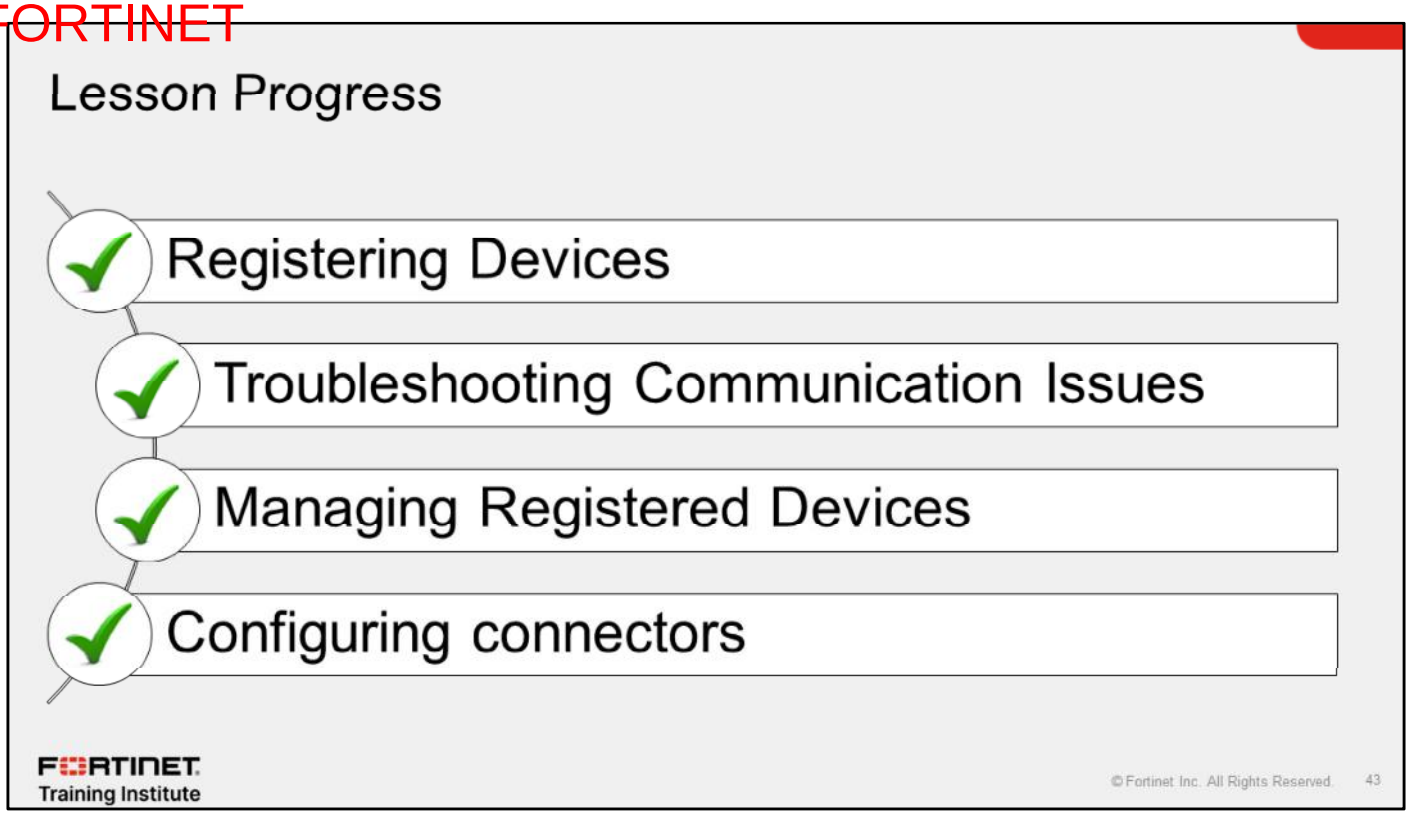
The playbook automates the following actions:
1) Executes a quarantine task on the infected host using the FortiClient EMS connector and attaches all related data to the incident.
2) Quarantines the host so the malicious file cannot move laterally and infect other hosts in the network.

Knowledge Check

1. Which color indicates an unknown connection status on FortiAnalyzer?
   - A. Green
   - ✓ B. Orange
   - C. Black
   - D. Red

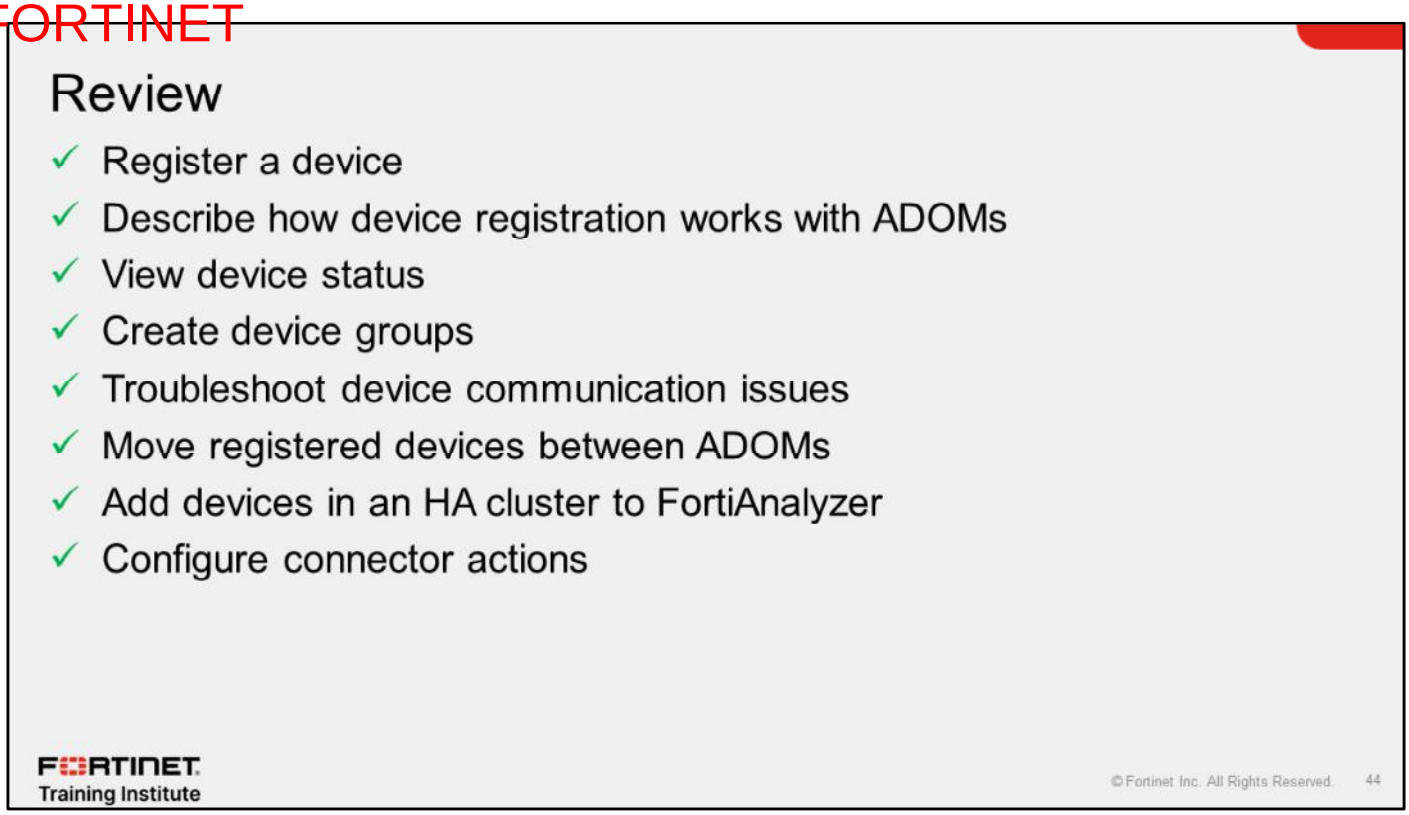
FORTINET Training Institute

 42



Congratulations! You have completed this lesson.

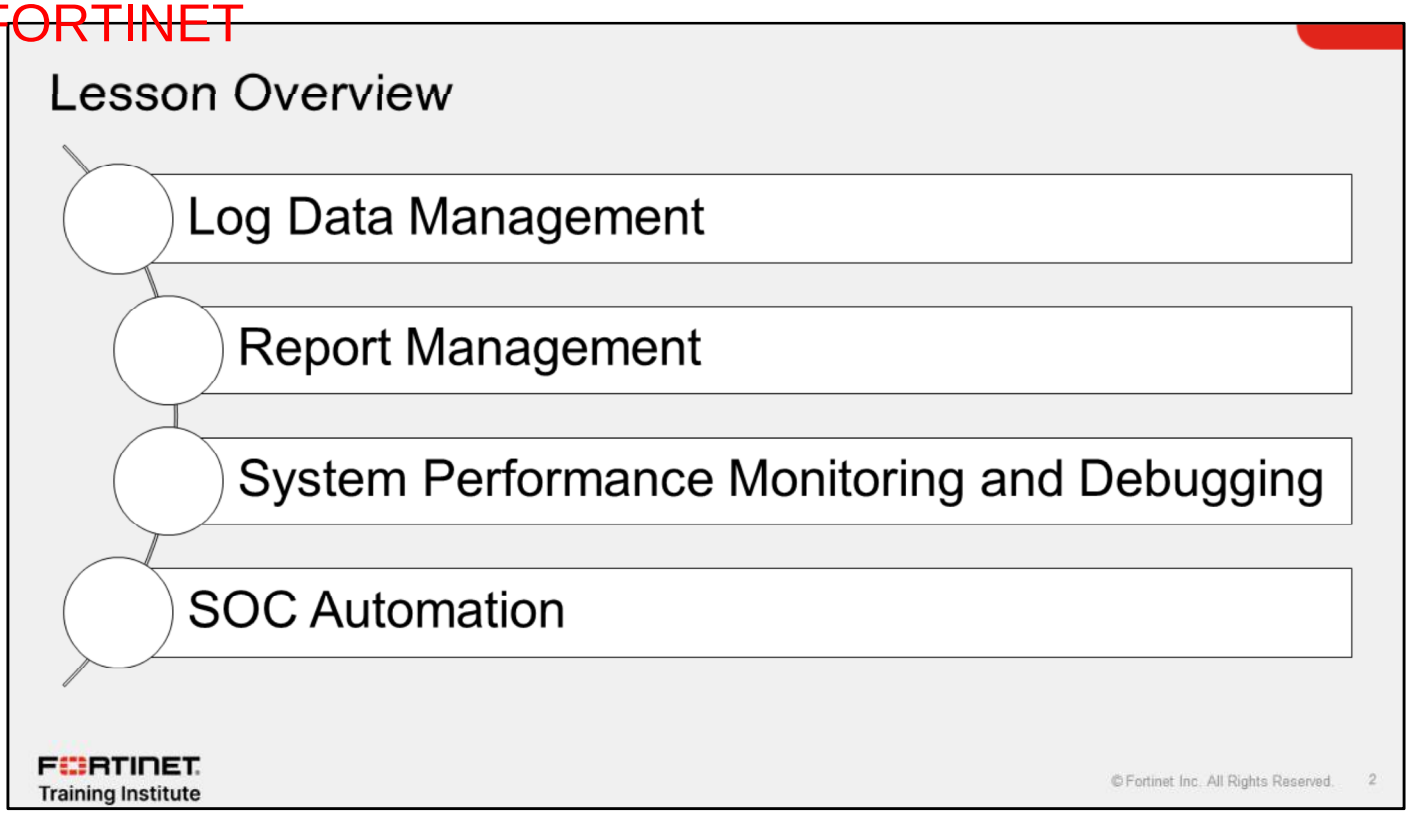
Now, you will review the objectives that you covered in this lesson.



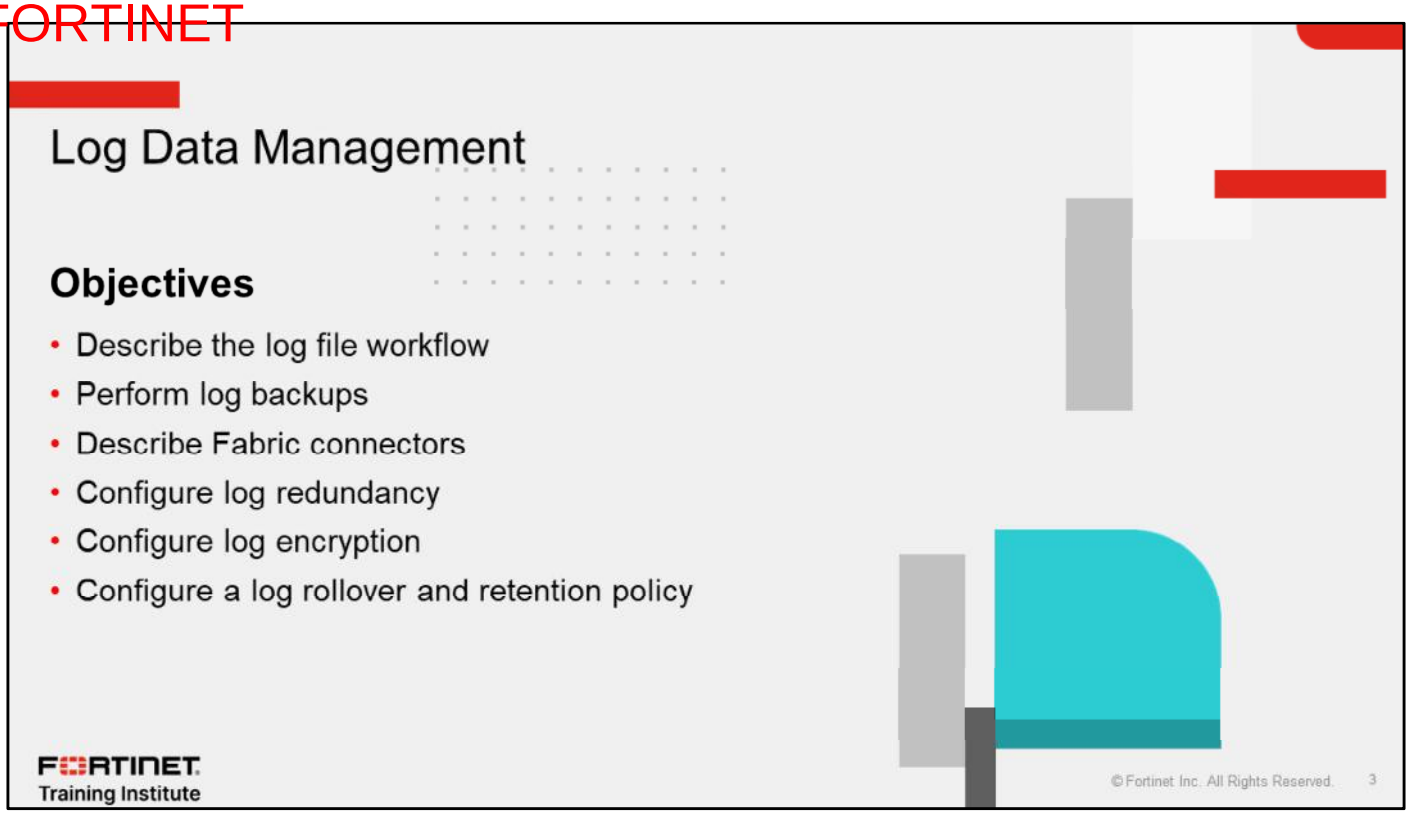
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to add, manage, and maintain devices in your network.

In this lesson, you will learn how to protect and manage logs on FortiAnalyzer. You will also learn about basic report concepts and common report management tasks.

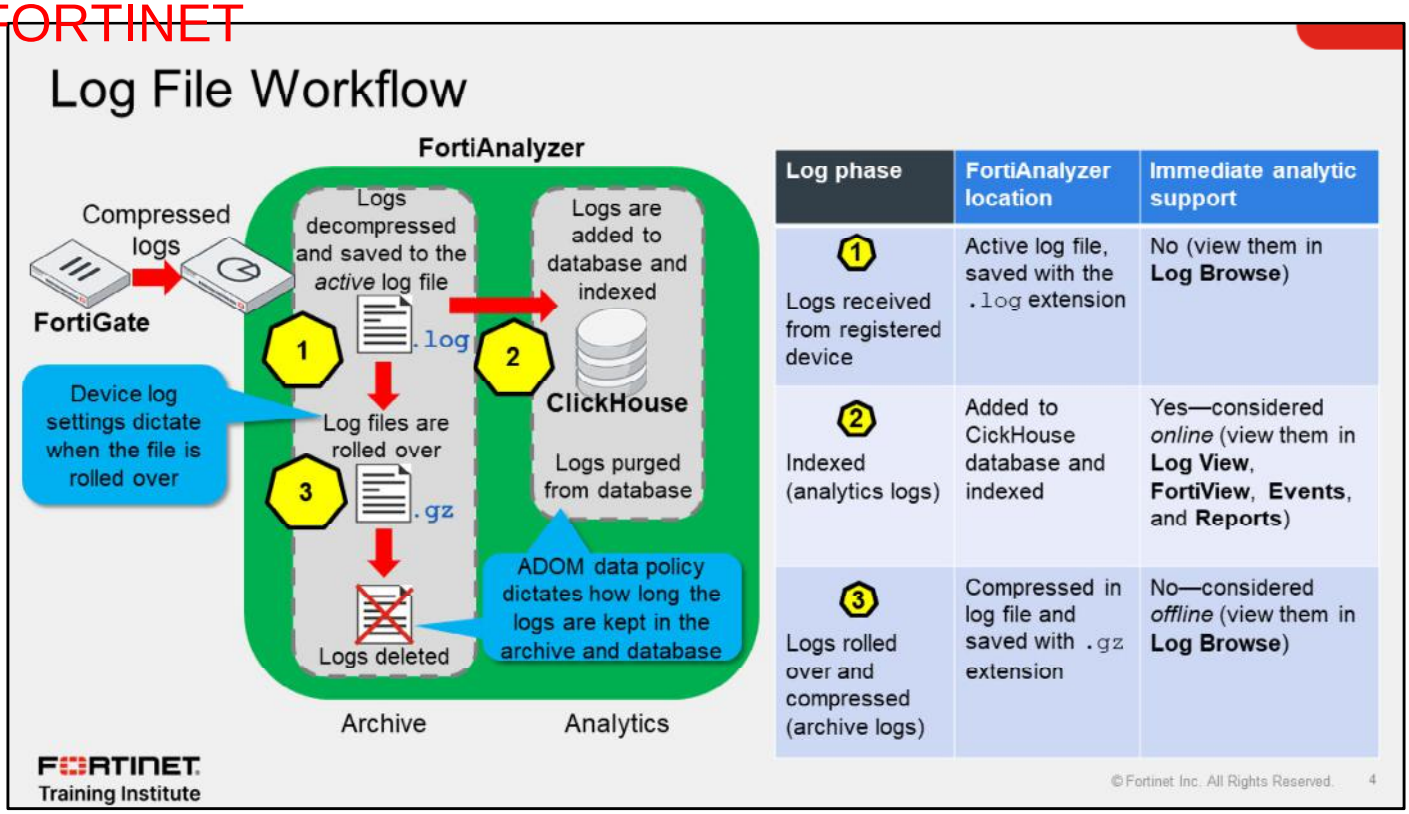


In this lesson, you will learn about the topics shown on this slide.



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

By demonstrating competence in understanding the log file workflow and the different ways you can protect your log data, you will be able to meet organizational and legal requirements for logs.



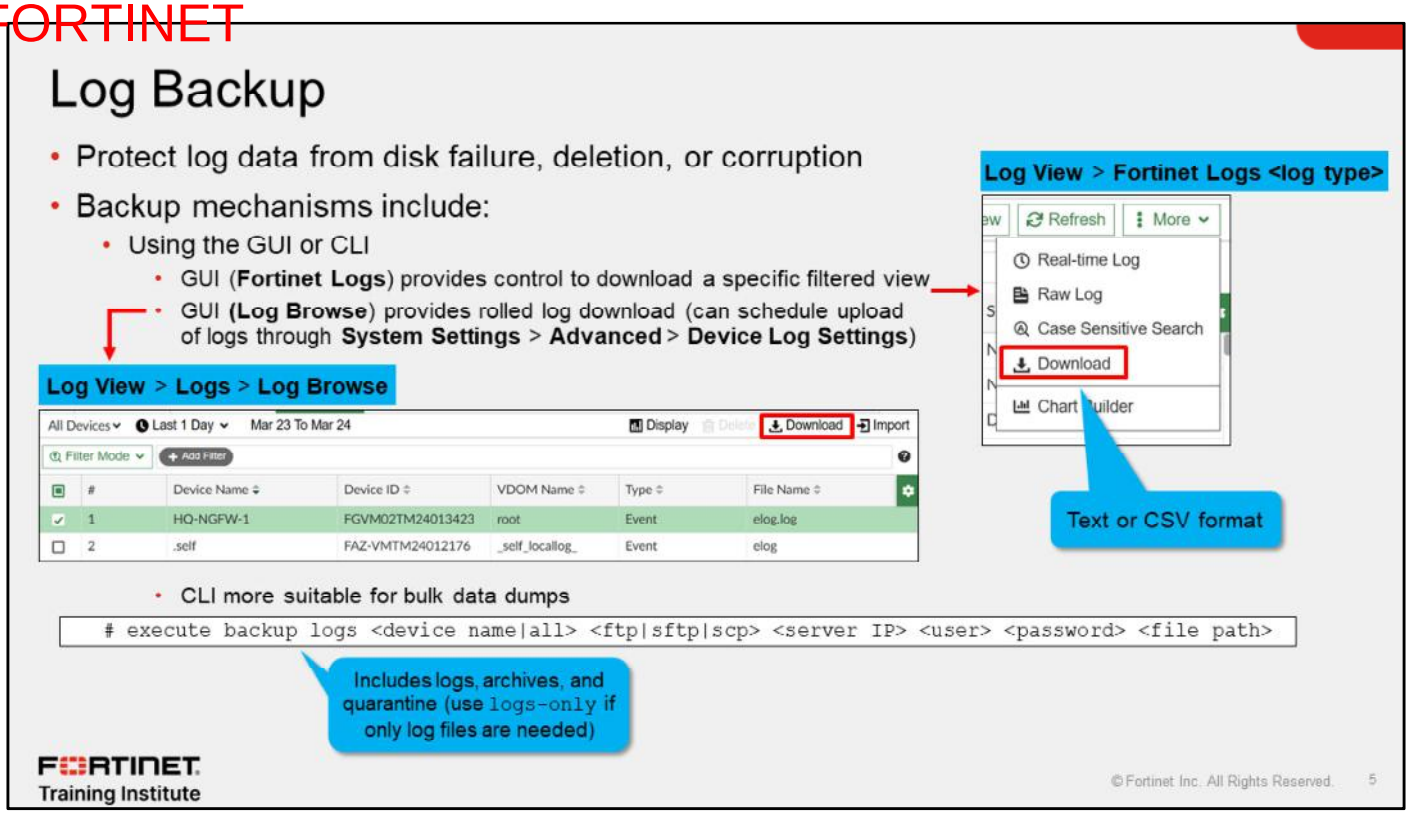
Log phase	FortiAnalyzer location	Immediate analytic support
1 Logs received from registered device	Active log file, saved with the `.log` extension	No (view them in **Log Browse**)
2 Indexed (analytics logs)	Added to CickHouse database and indexed	Yes—considered *online* (view them in **Log View**, **FortiView**, **Events**, and **Reports**)
3 Logs rolled over and compressed (archive logs)	Compressed in log file and saved with `.gz` extension	No—considered *offline* (view them in **Log Browse**)

When registered devices send logs to FortiAnalyzer, logs enter the following automatic workflow:

1. FortiAnalyzer decompresses all received logs and saves them in a log file on the FortiAnalyzer disk. The log file has the extension *.log*. For example, FortiAnalyzer saves FortiGate logs with the names *tlog.log* and *elog.log* for traffic and event logs, respectively. Note that the *tlog.log* file includes FortiGate security logs.

2. At the same time, FortiAnalyzer indexes the saved logs in the ClickHouse database to support analysis. Logs in the indexed phase are known as *analytics* logs. These logs are considered online and offer immediate analytic support. FortiAnalyzer purges analytics logs from the SQL database according to the ADOM data policy.

3. Eventually, when the log file reaches a configured size or a set schedule, FortiAnalyzer rolls over the log file. The process of rolling over consists of renaming the file, adding a timestamp, and then compressing it, which adds the `.gz` extension. These files are known as *archive* logs and are considered offline, so they don't offer immediate analytic support. Combined, they count toward the archive quota and retention limits, and FortiAnalyzer deletes them based on the ADOM data policy.



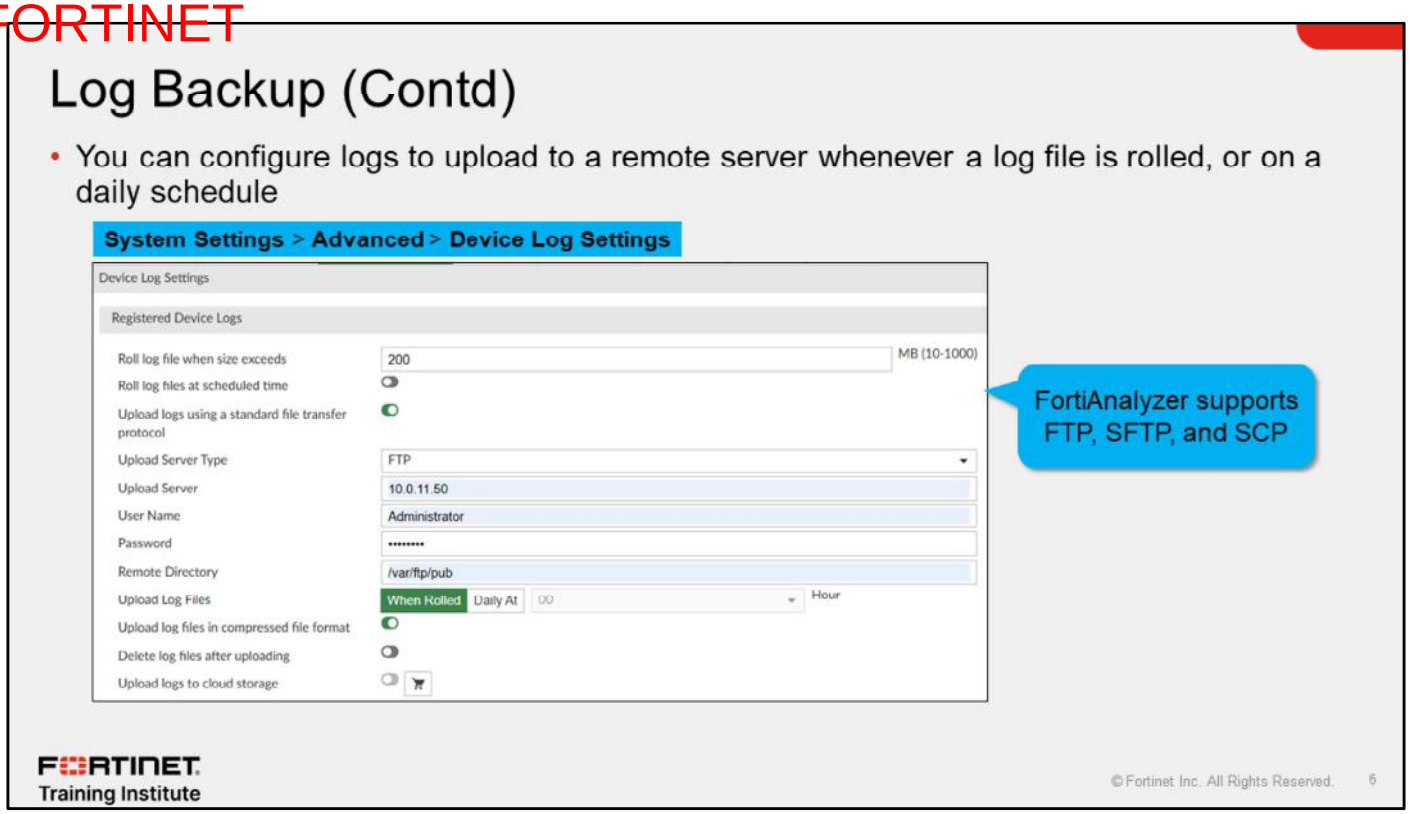
You should not consider RAID as a replacement for backing up your logs. You can back up your logs through the GUI or CLI.

On the FortiAnalyzer GUI, you can download a specific filtered view or you can download all rolled logs. You can also upload logs to an FTP, SFTP, or SCP server on a scheduled basis.

On the CLI, you can send a backup of all logs to a specified device or devices. FortiAnalyzer compresses the log files before sending them, so the transfer of the logs does not happen right away. The destination server must process and archive the logs, which can take some time. You must also ensure that the destination server has enough disk space for this potentially large volume of data.

You can also restore logs using the GUI and the CLI.

Use **LogView** when downloading a smaller subset of data. To download a large volume of data, use the **LogBrowse** page.

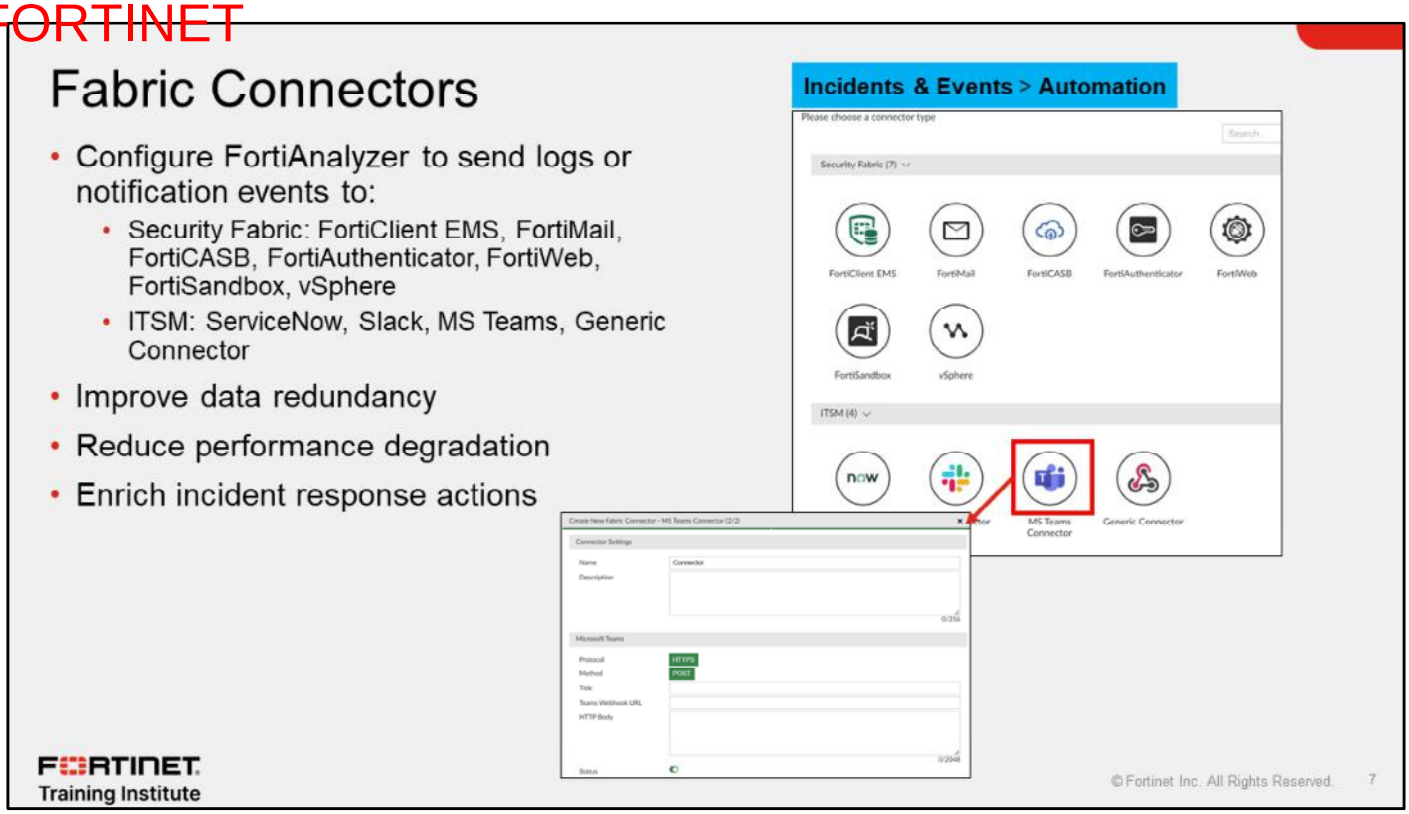


You can configure FortiAnalyzer to upload logs to a remote server whenever a log file is rolled or based on a daily schedule.

FortiAnalyzer supports FTP, SFTP, and SCP for log upload.

If you enable **Upload log files in compressed file format**, FortiAnalyzer compresses the device log files before uploading them, resulting in smaller logs and faster upload times.

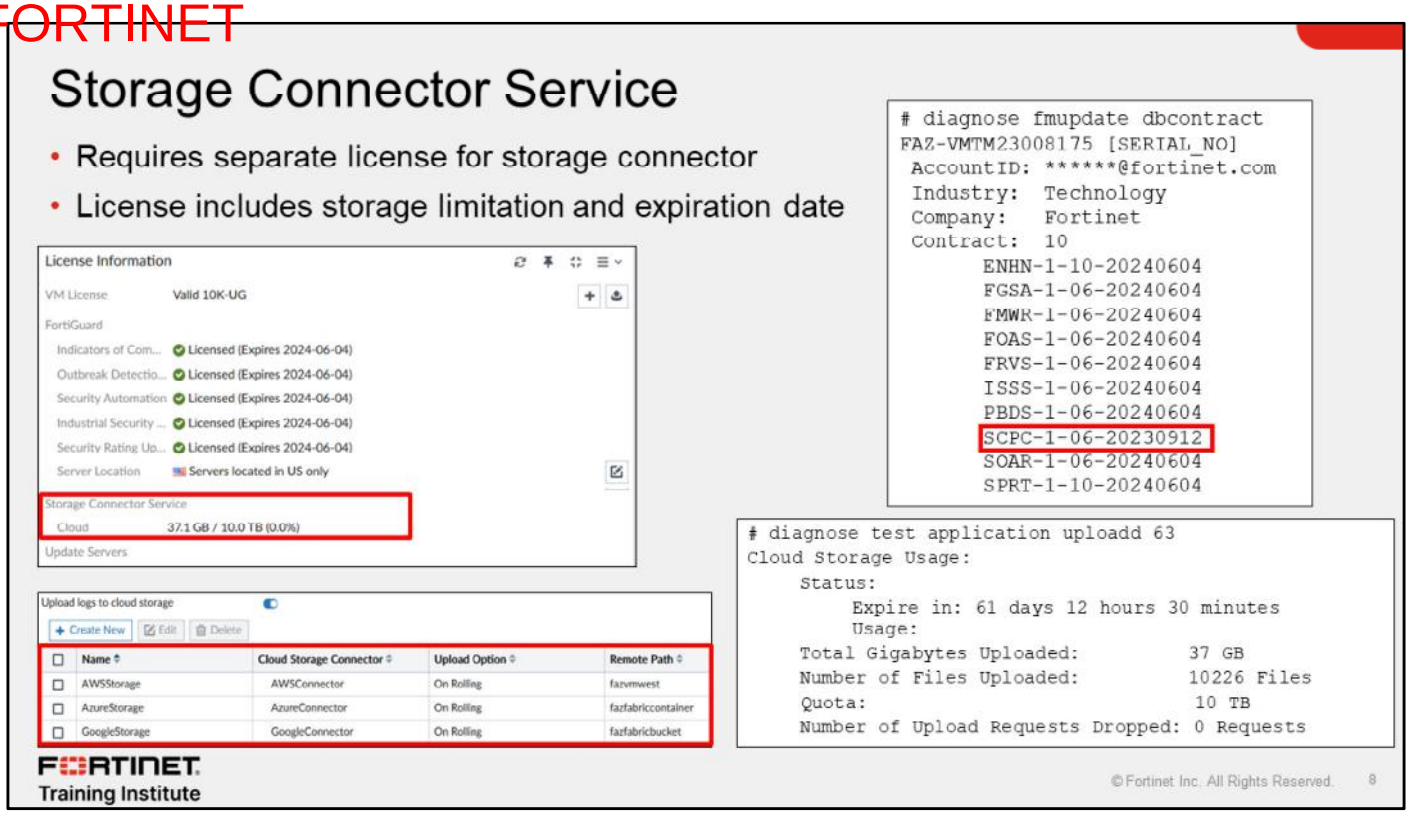
If you enable **Delete log files after uploading**, FortiAnalyzer removes the device log files from local storage after uploading them to the remote server.



FortiAnalyzer supports integration with other products through Fabric connectors.

Security Fabric connectors enrich the incident response-related actions available on FortiAnalyzer, such as automating actions by triggering playbooks.

IT service management (ITSM) connectors enable FortiAnalyzer to send notifications to ITSM platforms when a new incident is created or for any subsequent updates. This approach is more efficient than third-party platforms polling information from the FortiAnalyzer API at predefined intervals, which could result in FortiAnalyzer performance degradation.



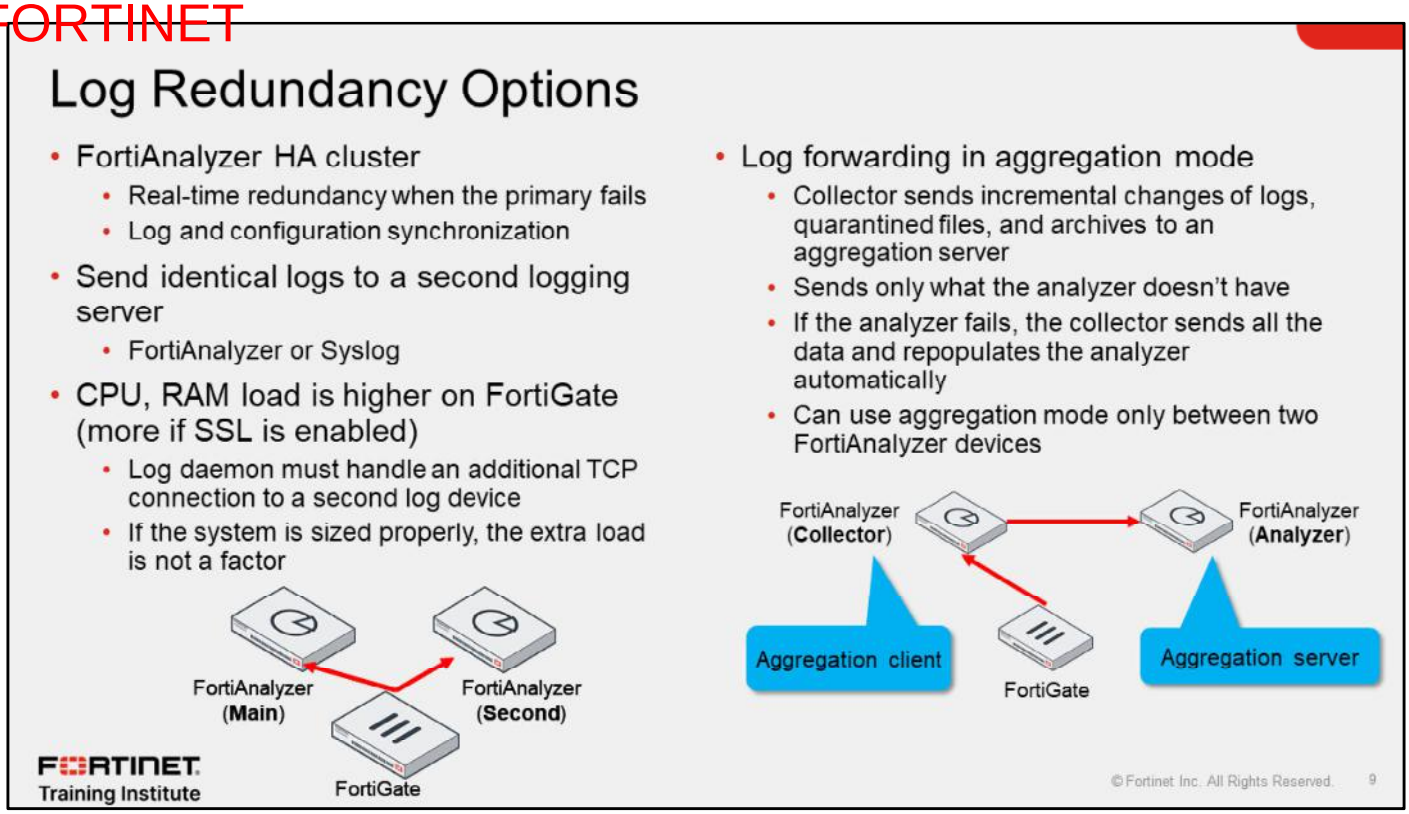
To send logs to cloud platforms, you must purchase a separate license for the Storage Connector Service. This license includes constraints that limit the amount of data you can upload to the cloud platform. The licenses also have an expiry date. This is usually valid for one year. The license does not limit how much storage you can use on the cloud provider. It limits only the *amount* of data that you can transfer. To configure this feature, you must have an account with the correct permissions to access the cloud storage. Refer to the *FortiAnalyzer Administration Guide* for more details.

If uploaded logs exceed data storage limitations before the license expires, you must renew the license to continue using this service.

After uploading the license, you can enable the **Upload logs to cloud storage** feature on the **Device Log Settings** page, and then select cloud storage platforms.

You can use the `diagnose fmupdate dbcontract fds` command to determine the license validity and expiry details.

The `diagnose test application uploadd 63` command provides details, such as usage quota, total data upload in GB, total number of files uploaded, number of days remaining until license expiry, and number of uploaded requests that were dropped.

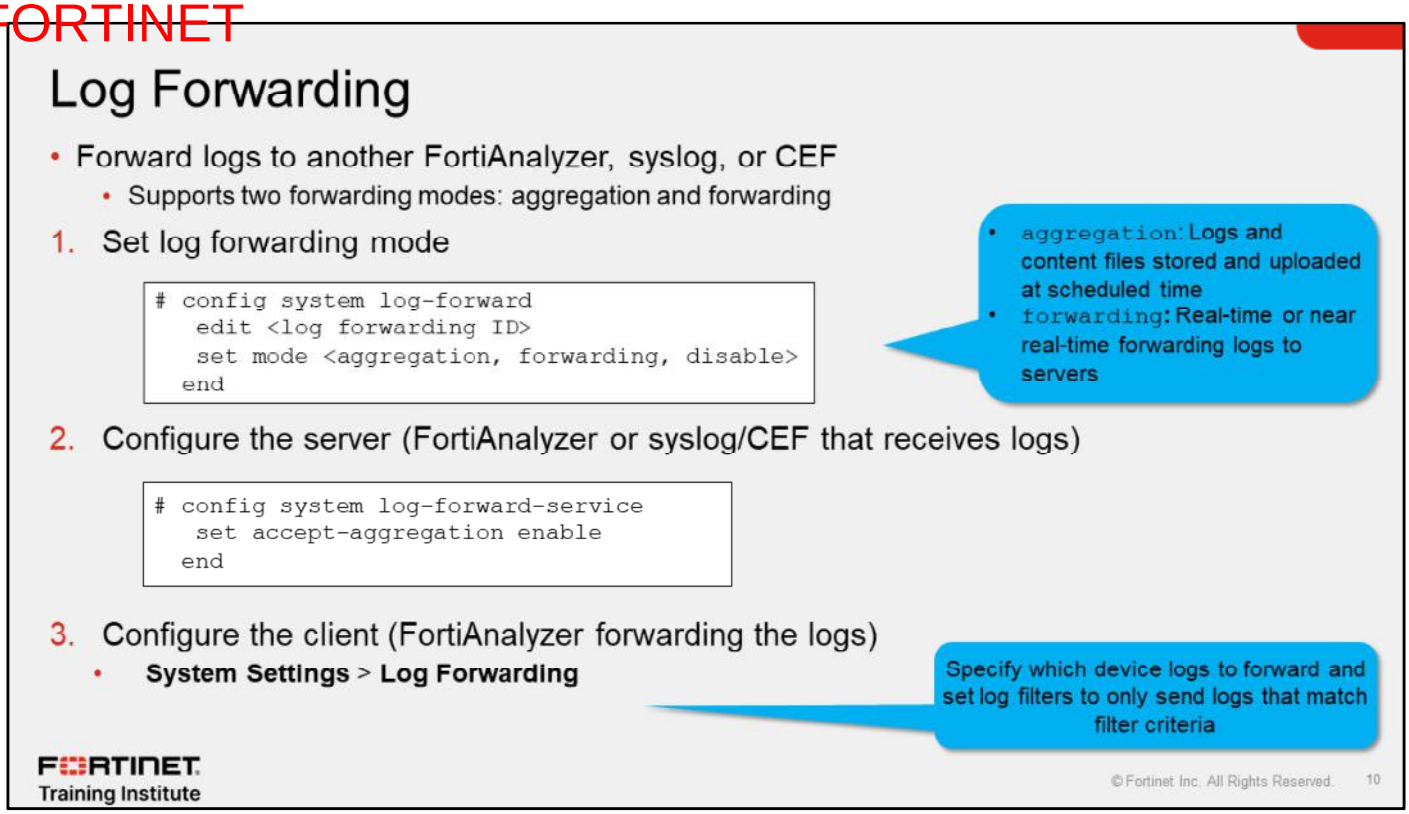


To protect your logs during log delivery, you can add redundancy to your environment. In a FortiGate-FortiAnalyzer environment, there are a few options.

One option is to configure a FortiAnalyzer HA cluster. FortiAnalyzer high availability (HA) provides real-time redundancy when a FortiAnalyzer primary device fails. If the primary device fails, another node in the HA cluster becomes the primary device. The primary device synchronizes logs and data securely among multiple FortiAnalyzer devices. It also synchronizes system and configuration settings applicable to HA and provides load balancing for processes, such as running reports.

Another option is to configure FortiGate to send an identical set of logs to a second logging server, such as a second FortiAnalyzer or a syslog server. Note that this method increases the load on FortiGate because the log daemon must handle an additional TCP connection to the second logging server. However, this extra load is not a factor when you use correct system sizing. This option is unavailable for smaller FortiGate devices that do not support a second device.

A third option is to configure log forwarding in aggregation mode. Generally, your central (aggregating) device is a larger FortiAnalyzer, but this is not a requirement. The collector sends the logs' delta (incremental changes) to the aggregation server. The two devices compare what they have stored, and the collector sends only what the analyzer doesn't have. This reduces the amount of traffic and provides a level of redundancy. If the analyzer device fails, the collector sends all the data it has and repopulates the restored analyzer automatically. Aggregation mode is supported only between two FortiAnalyzer devices.

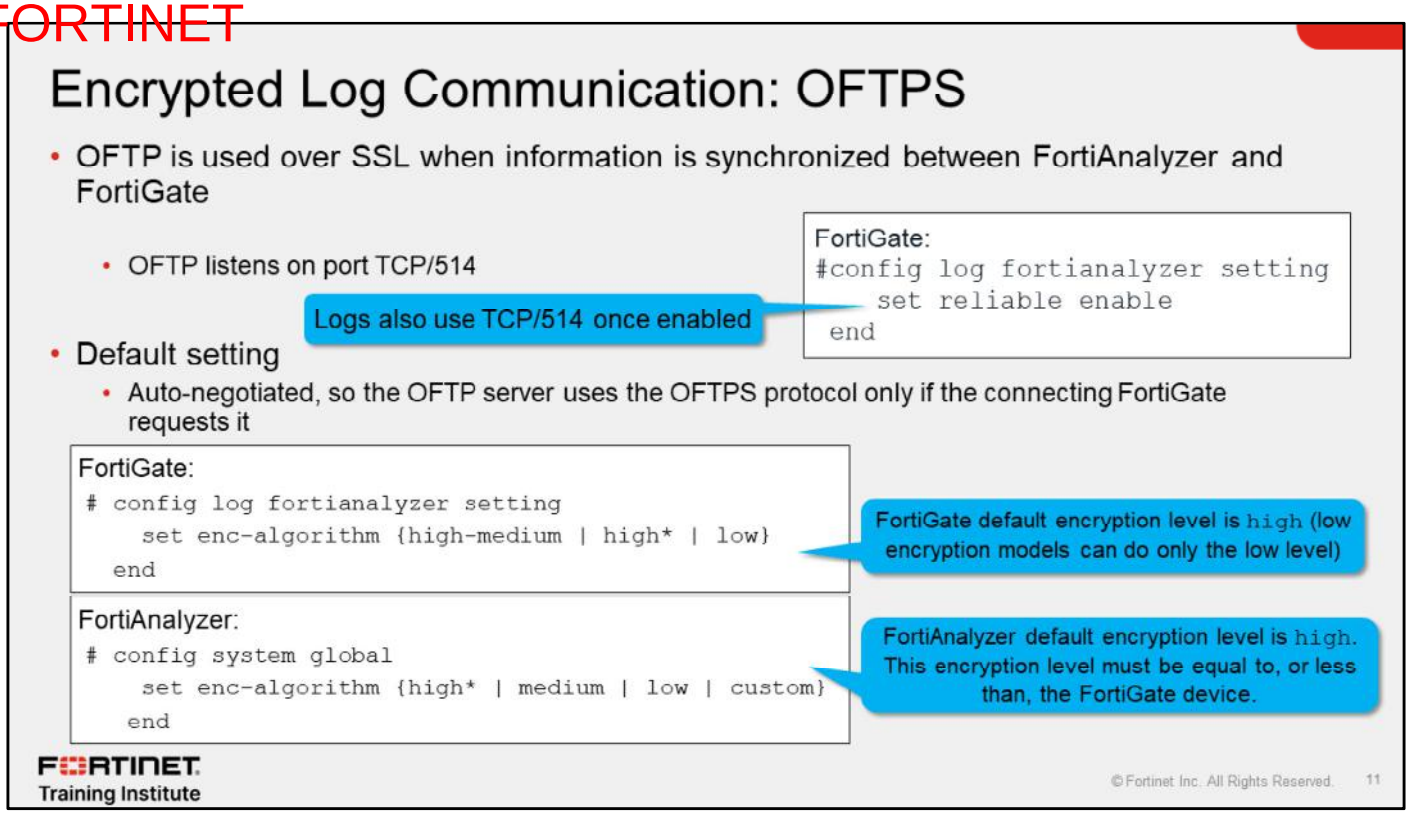


You can run log forwarding in modes other than aggregation mode, which applies only to two FortiAnalyzer devices. In forwarding mode, FortiAnalyzer can also forward logs in real time to a syslog server (such as FortiSIEM), a common event format (CEF) server, or another FortiAnalyzer. You can also forward logs to a public cloud service through an output plugin. When FortiAnalyzer forwards logs to another FortiAnalyzer, the forwarding device takes the client role, while the recipient device takes the server role.

To configure log forwarding, you must complete the following:

1. Select the log forwarding mode: aggregation or forwarding.
    - Forwarding mode forwards logs as they are received.
    - Aggregation mode stores logs and content files and uploads them to the FortiAnalyzer server at a scheduled time.
2. Configure the server (the log recipient). Forwarding mode requires configuration on only the client side. In aggregation mode, you must configure the FortiAnalyzer server to accept the client logs.
3. Configure the client (the FortiAnalyzer forwarding the logs). Here, you can specify which device logs to forward and apply log filters to send only logs that match filter criteria.

In addition to forwarding logs, the FortiAnalyzer client retains a local copy, which is subject to the data policy settings for archive logs on the FortiAnalyzer client.

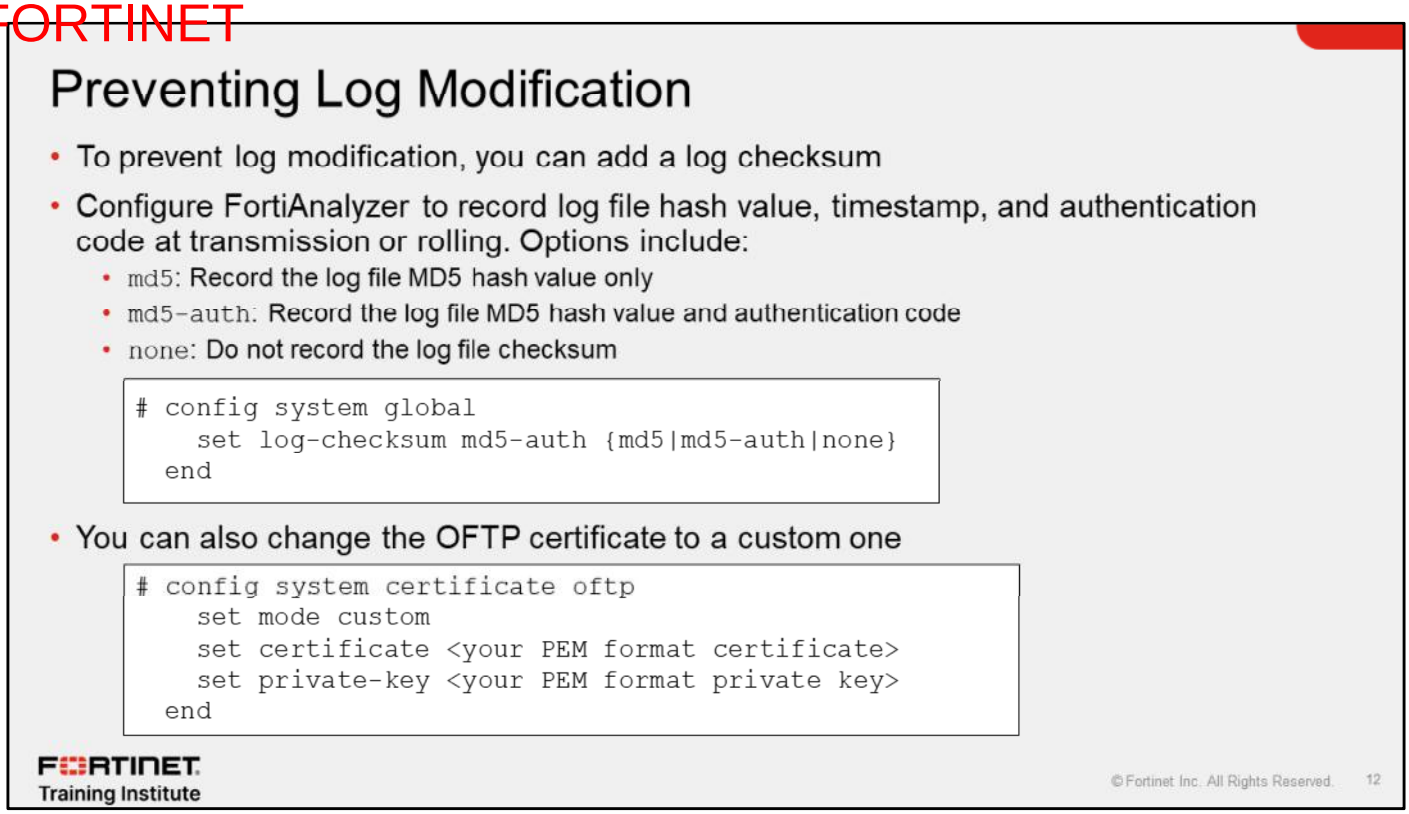


In the default configuration, FortiGate and FortiAnalyzer communicate using two communication streams: the Optimized Fabric Transfer Protocol (OFTP) communication stream, which is encrypted, and the log communication stream, which is not.

FortiAnalyzer and FortiGate use OFTP over SSL when information is synchronized between them. OFTP listens on port TCP/514. Port UDP/514 is used for unencrypted log communication.

Using the commands shown on this slide, you can protect log communication between devices through encryption, with the desired encryption level. After you enable secure log transfer, logs are also transferred between FortiGate and FortiAnalyzer using port TCP/514.

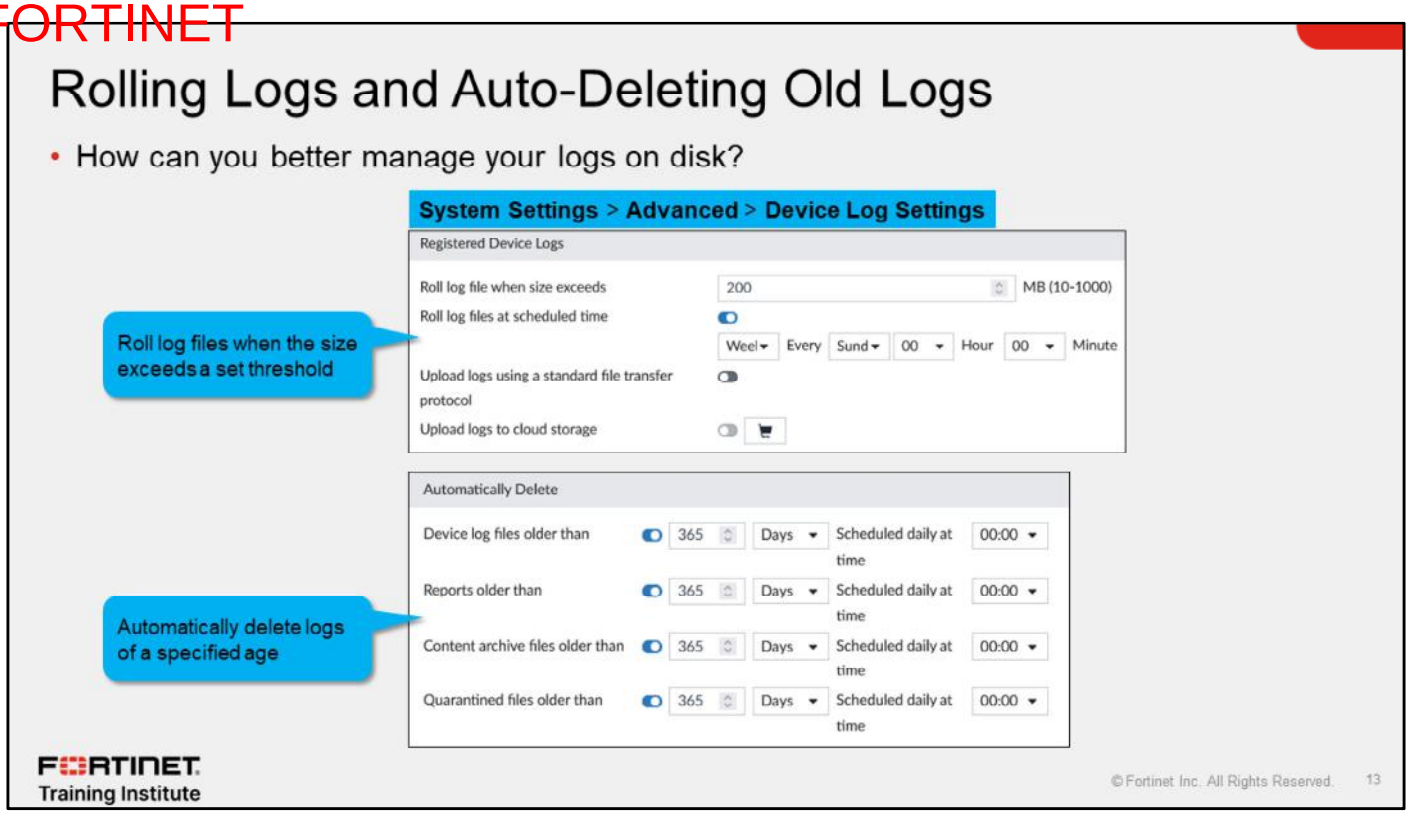
SSL communications are auto-negotiated between FortiAnalyzer and FortiGate, so the OFTP server uses SSL-encrypted FTP only if the connecting FortiGate uses it. By default, both FortiGate and FortiAnalyzer use the *high* encryption level. The FortiAnalyzer encryption level *must* be equal to or less than the FortiGate device. If you set the algorithm to *custom* on FortiAnalyzer, you can manually define a list of cipher suites.



You can add a log checksum using the `config system global` command to prevent logs from being tampered with while in storage. You can configure FortiAnalyzer to record a log file hash value, timestamp, and authentication code when the log is rolled and archived, and when the log is uploaded (if that feature is enabled). This can also protect against man-in-the-middle (MITM) for the transmission from FortiAnalyzer to an SSH File Transfer Protocol (SFTP) server during log upload.

The following log checksums are available:
- `md5`: Record log file MD5 hash value only.
- `md5-auth`: Record log file MD5 hash value and authentication code.
- `none`: Do not record the log file checksum.

You can also change the OFTP certificate to a custom one using the `config system certificate oftp` command. You need a Privacy Enhanced Mail (PEM) formatted certificate and associated PEM-formatted private key.



Aside from changing your disk log quota, you can enforce global settings to help manage your logs.

You can configure the following:
- Specify a global log roll policy to roll or upload logs when the size exceeds a set threshold.
- Specify a global automatic deletion policy for all log files, quarantined files, reports, and content archive files on FortiAnalyzer.

All deletion policies are always active on FortiAnalyzer. Therefore, you should carefully configure each policy. For example, suppose the disk utilization policy reaches its threshold before the global automatic file deletion policy for FortiAnalyzer. In a case like this, FortiAnalyzer automatically deletes the archive logs for the affected device. Conversely, if the global automatic file deletion policy reaches its threshold first, FortiAnalyzer deletes the oldest archive log, regardless of the log storage settings associated with the device.

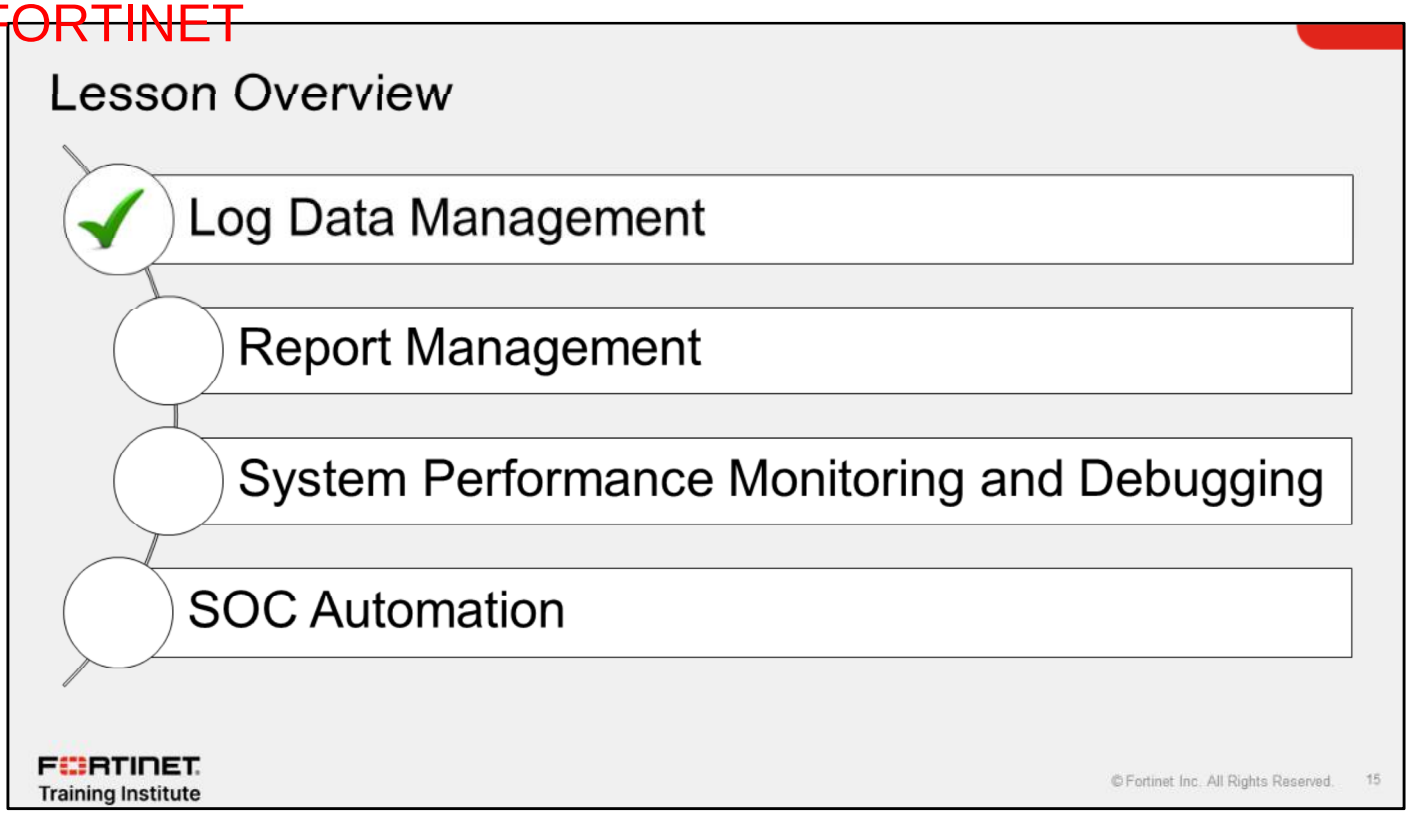
Knowledge Check

1. Which log forwarding mode stores logs and content files, and uploads them to another FortiAnalyzer server at a scheduled time?
   - A. Forwarding mode
   - ✓ B. Aggregation mode

2. Compressed logs on FortiAnalyzer are known as _____ logs.
   - ✓ A. archive logs
   - B. analytics logs

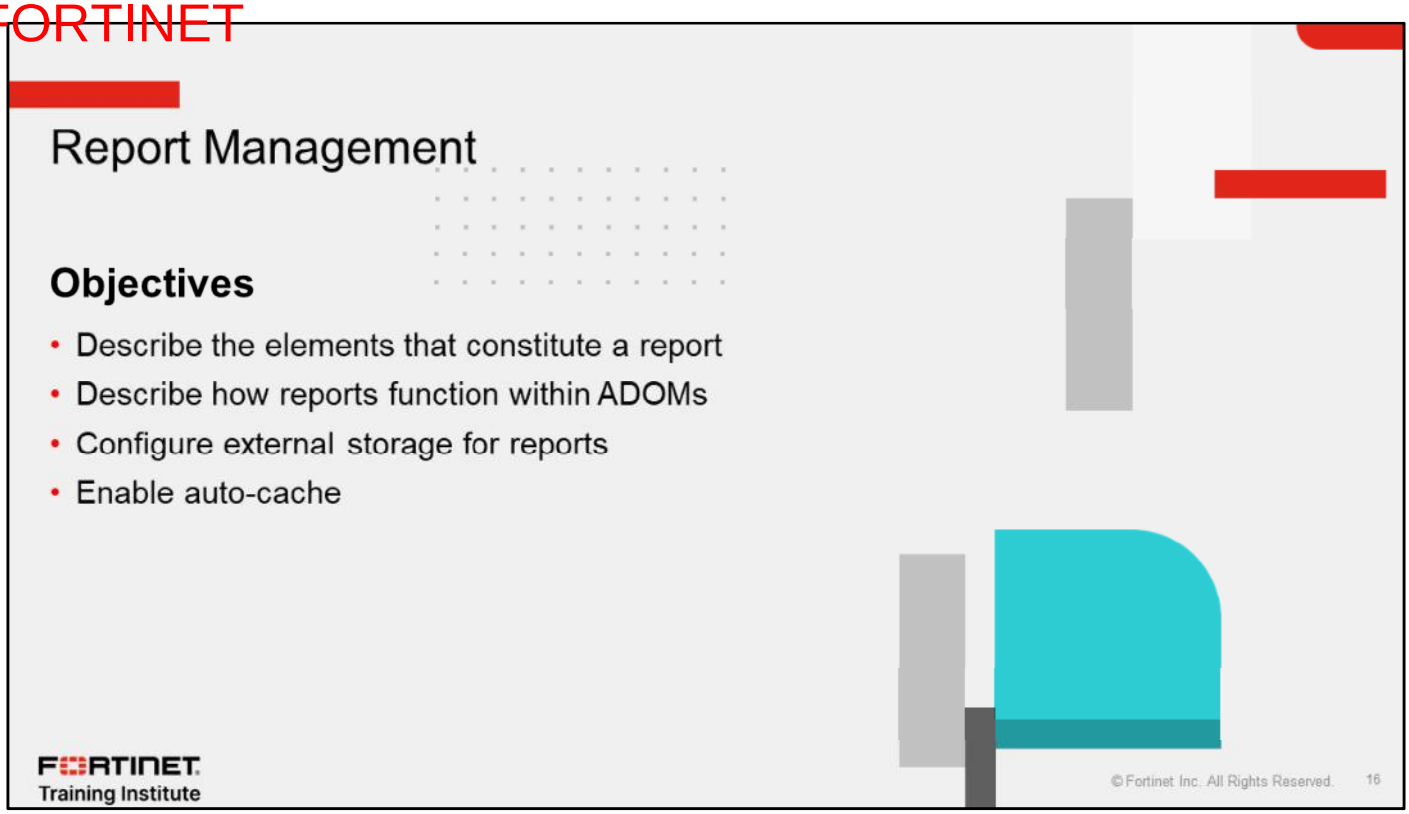
FORTINET Training Institute

 14



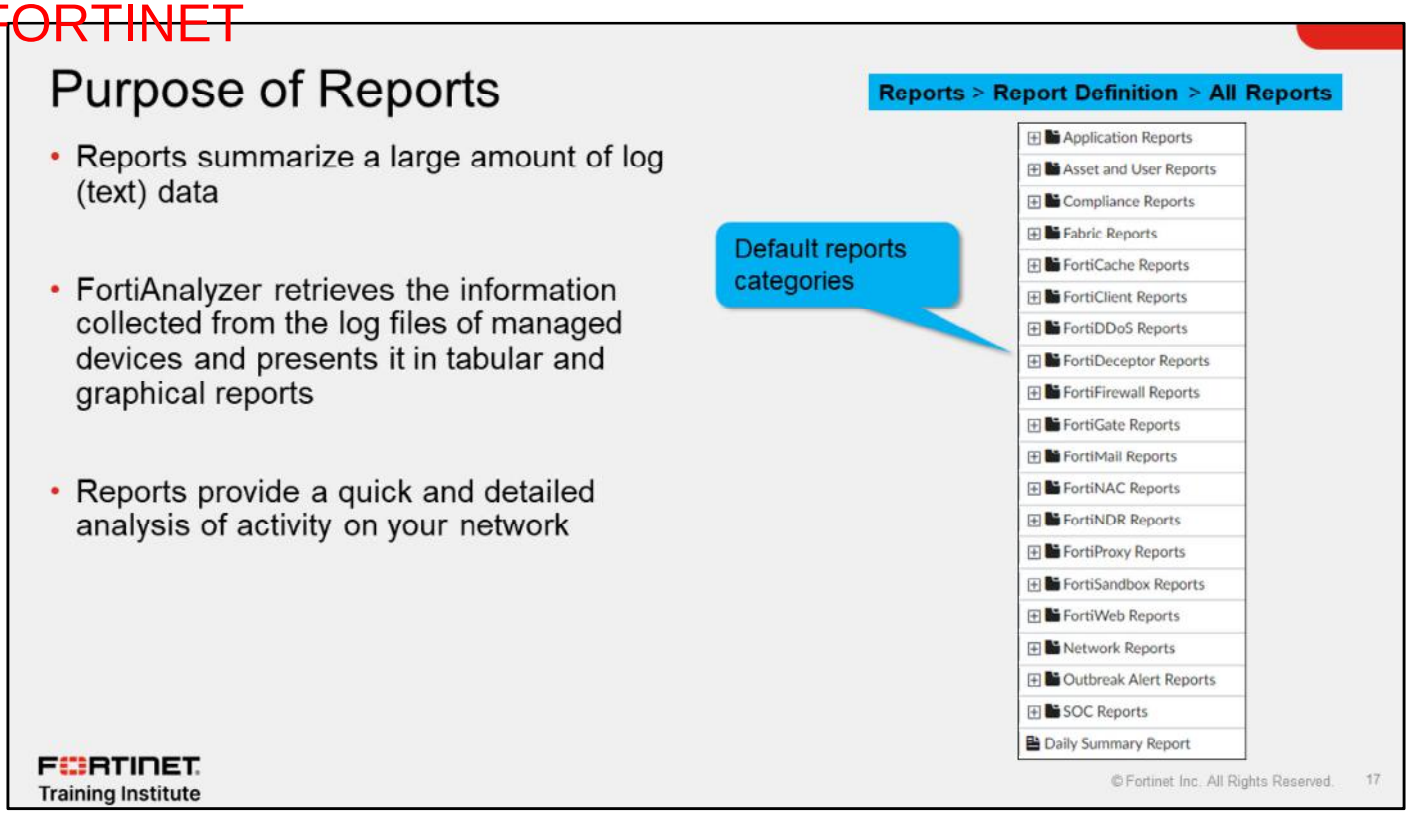
Good job! You now understand how to manage your log data.

Now you will learn about managing reports.



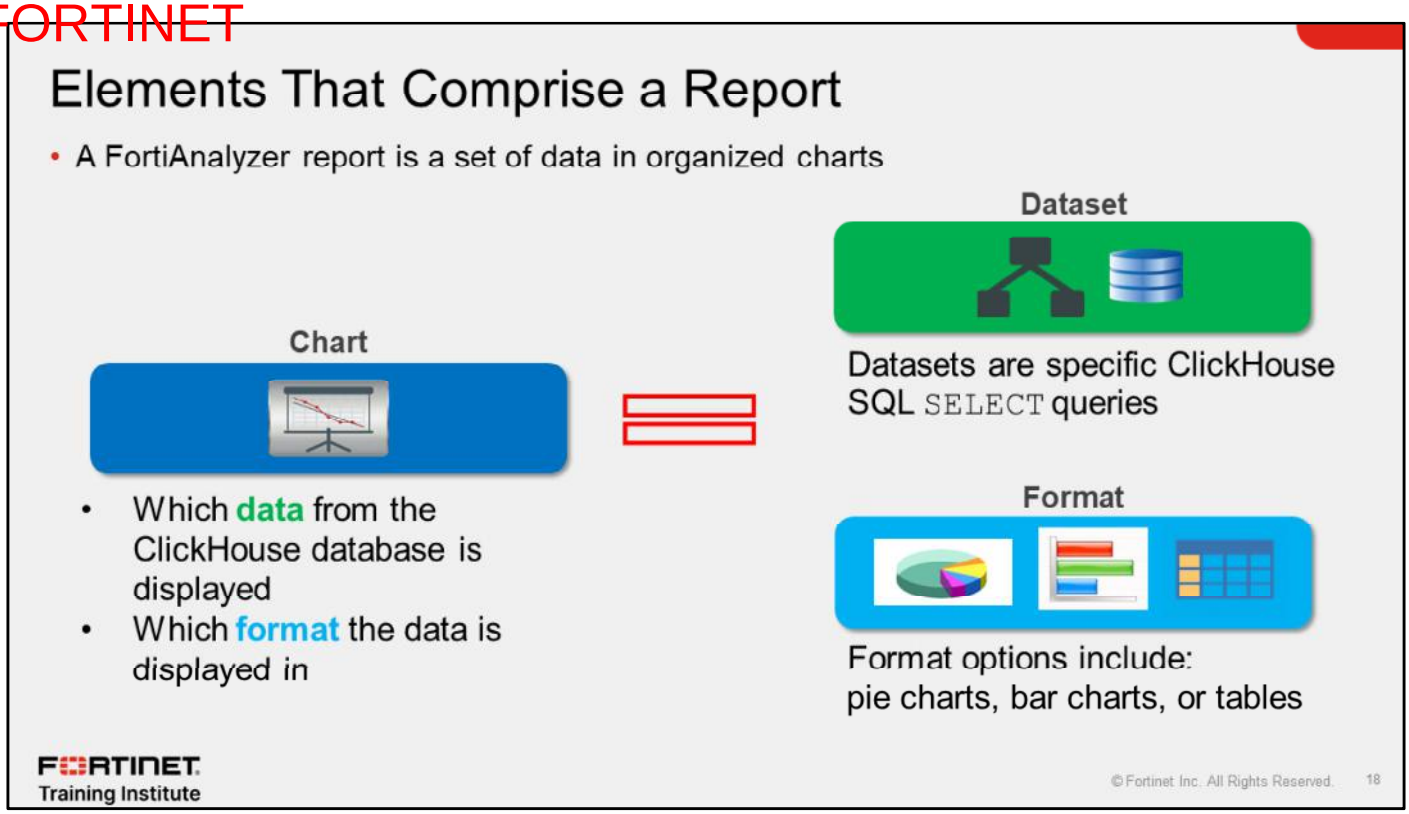
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in report management, you will be able to use reports more effectively to extract collected log data from your database. You will be able to also handle, store, and more efficiently control reports and report generation.



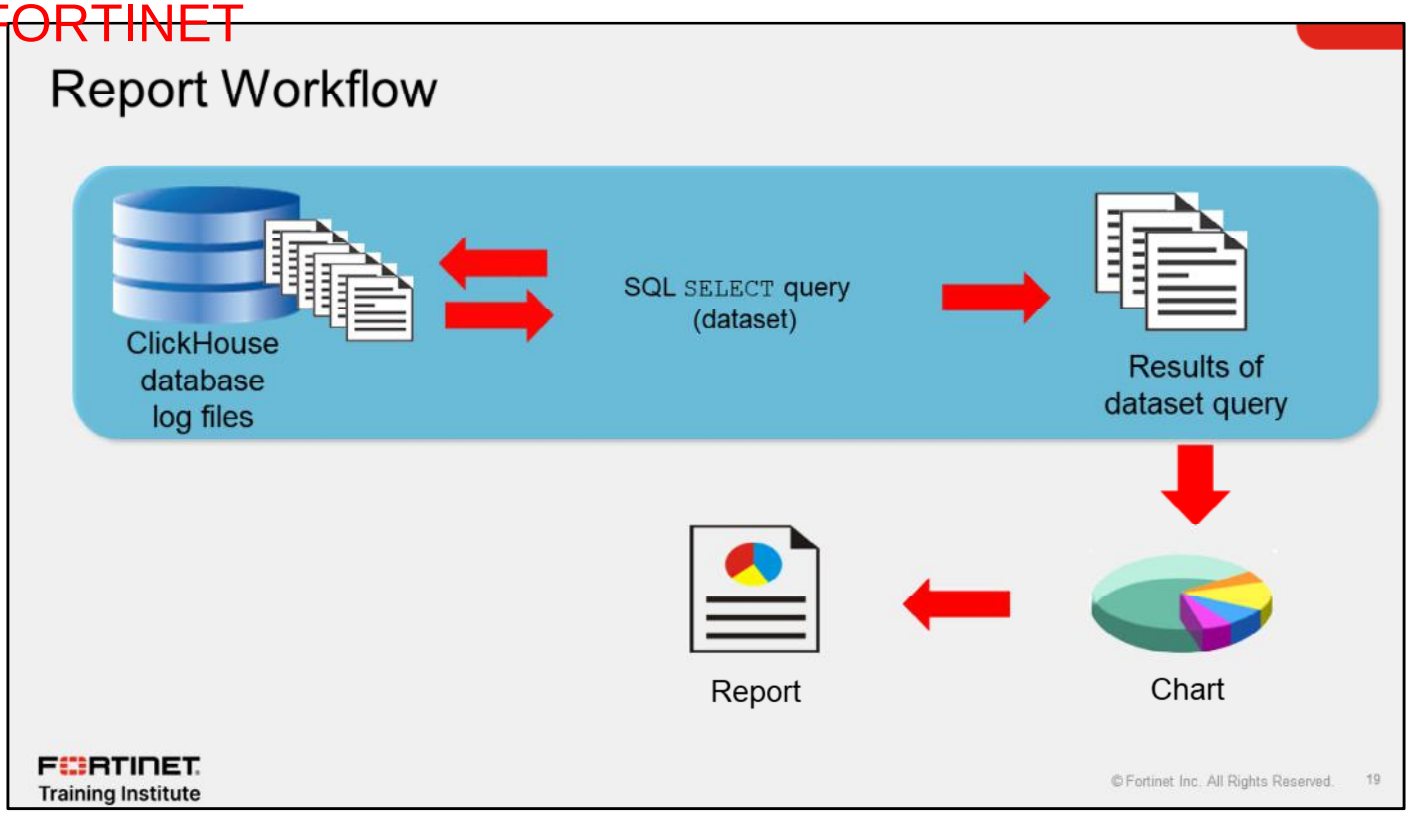
The purpose of a report is to summarize large amounts of logged data. Based on configured report parameters, FortiAnalyzer extracts data and presents it in a graphical manner that makes it easier—and quicker—to digest. The patterns and trends that reports reveal are several data points within your database. Still, it would be difficult and time-consuming to locate, cross-reference, and analyze multiple log files manually, especially if you don't know what trend or pattern you are looking for. Once configured, reports provide a quick and detailed analysis of activity on your network. You can use that information to understand your network better or improve your network security.

Note that reports generally do not provide recommendations or indicate problems. Administrators must be able to look beyond the data and charts to see what is happening within their network.



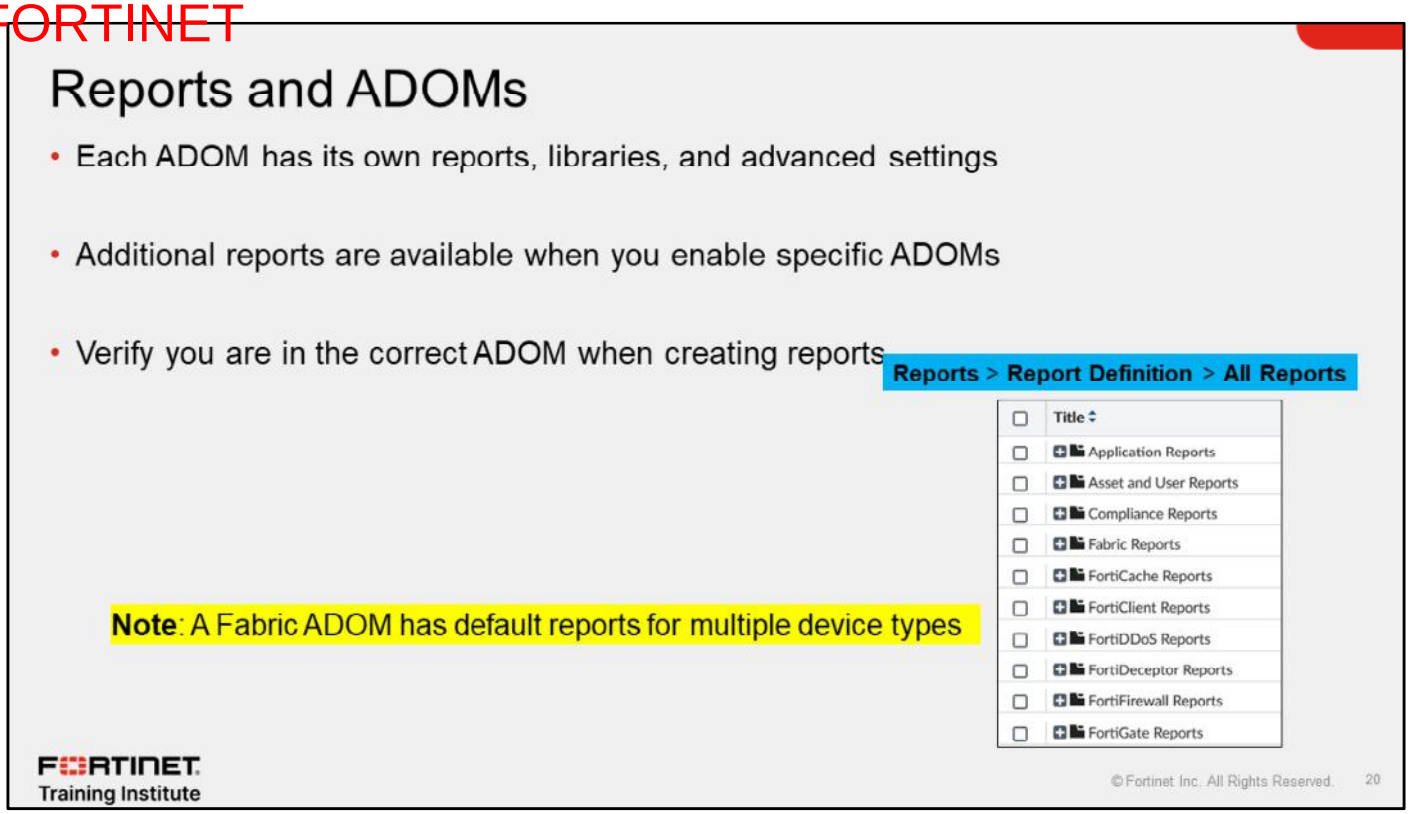
A FortiAnalyzer report is a set of data organized in charts. Charts consist of two elements:

- Datasets, which are ClickHouse SQL `SELECT` queries that extract specific data from the database
- Formatting, which controls how the data is displayed (for example, pie charts, bar charts, or tables)



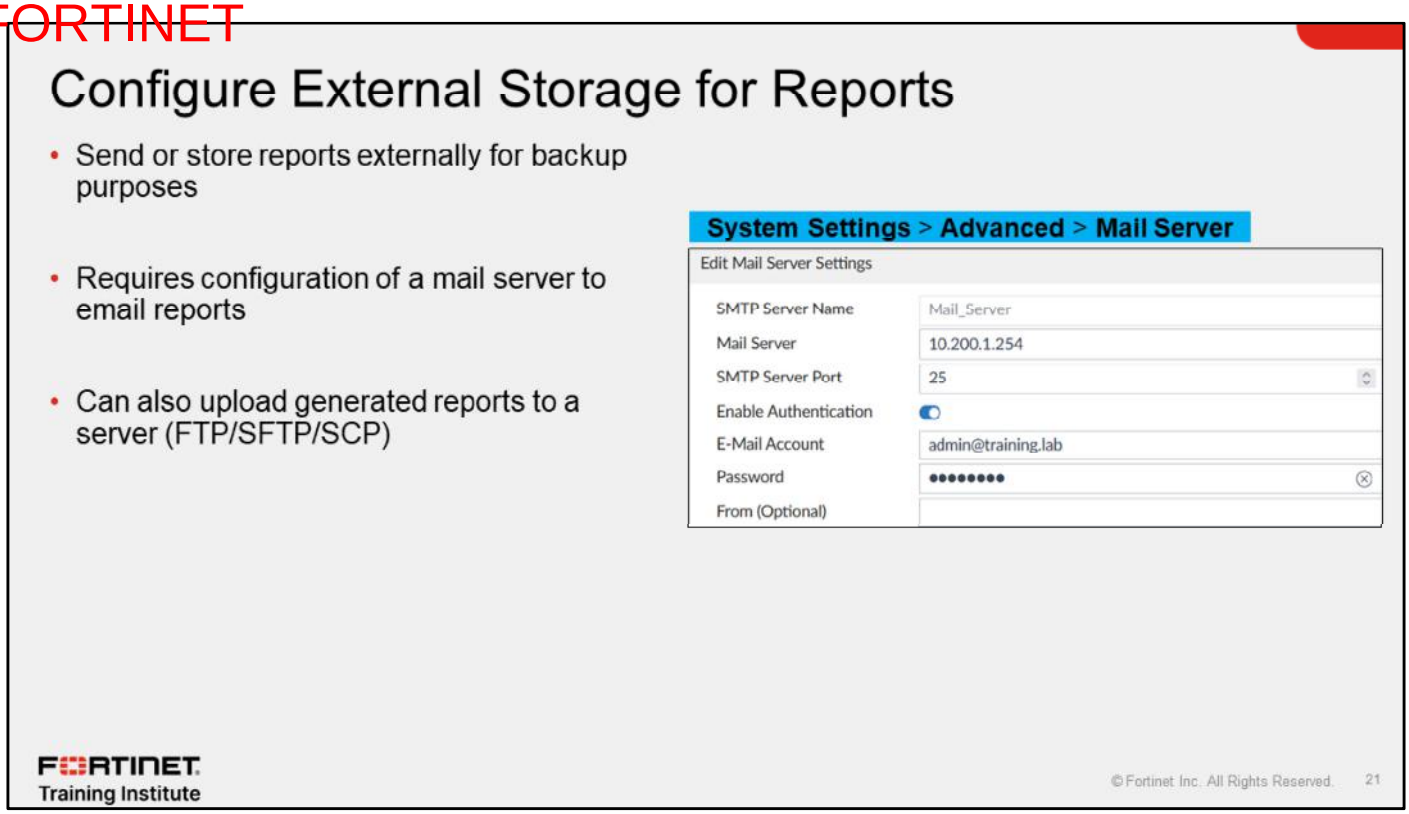
As the graphic on this slide shows, the ClickHouse database contains all the logs. An SQL `SELECT` query polls the database for specific information and extracts a subset of data stored in the logs.

This subset of data populates a chart, and one or more charts exist within a report.



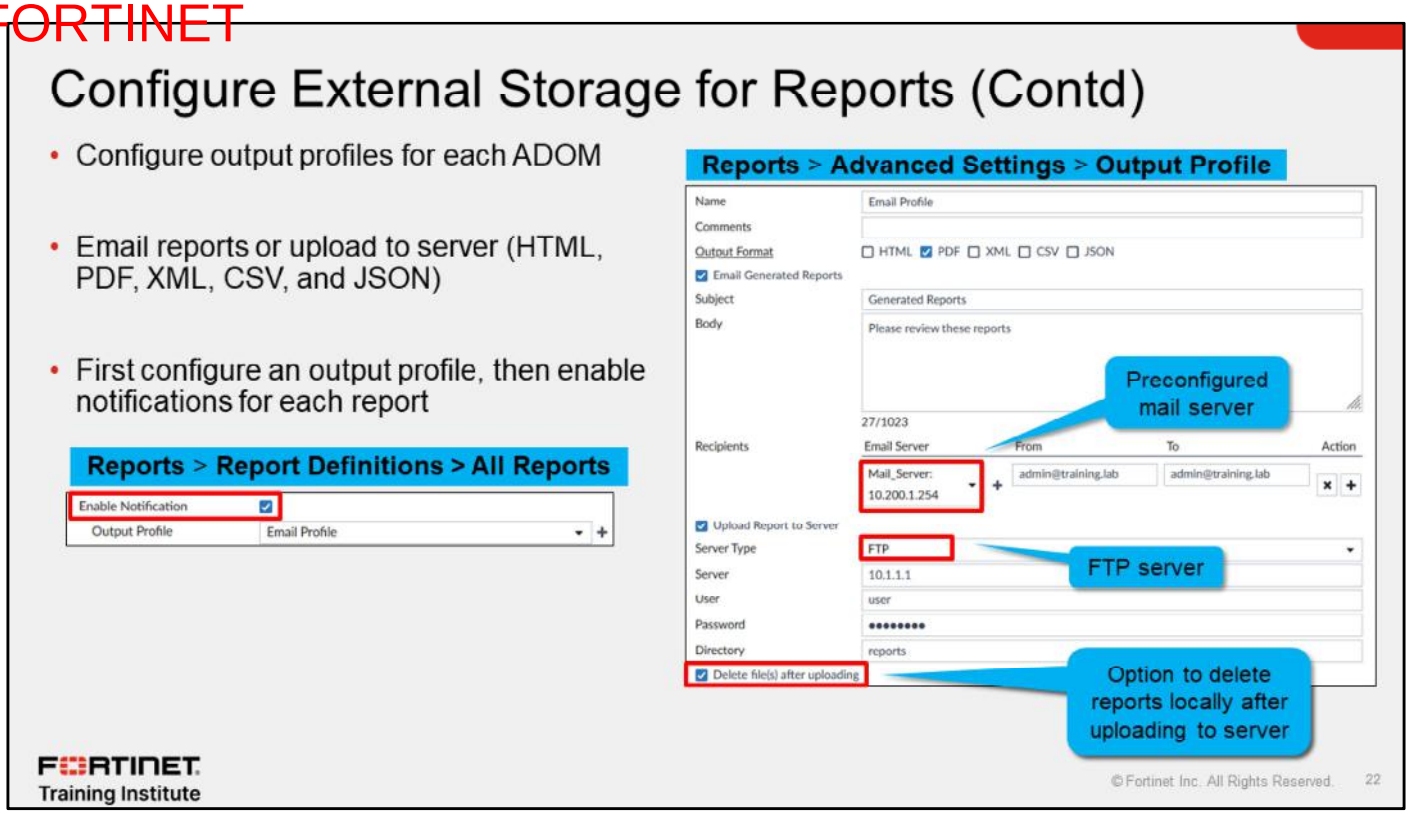
When you enable ADOMs, each ADOM has its own reports, libraries, and advanced settings. As such, ensure you are in the correct ADOM before selecting a report.

Additional reports for specific Fortinet devices are available only when you enable ADOMs. This slide does not show all the available default report types. You can configure and generate reports for these devices within their respective ADOMs. These devices also have device-specific charts and datasets.



You can configure FortiAnalyzer to email generated reports to specific administrators, or to upload generated reports to an external server.

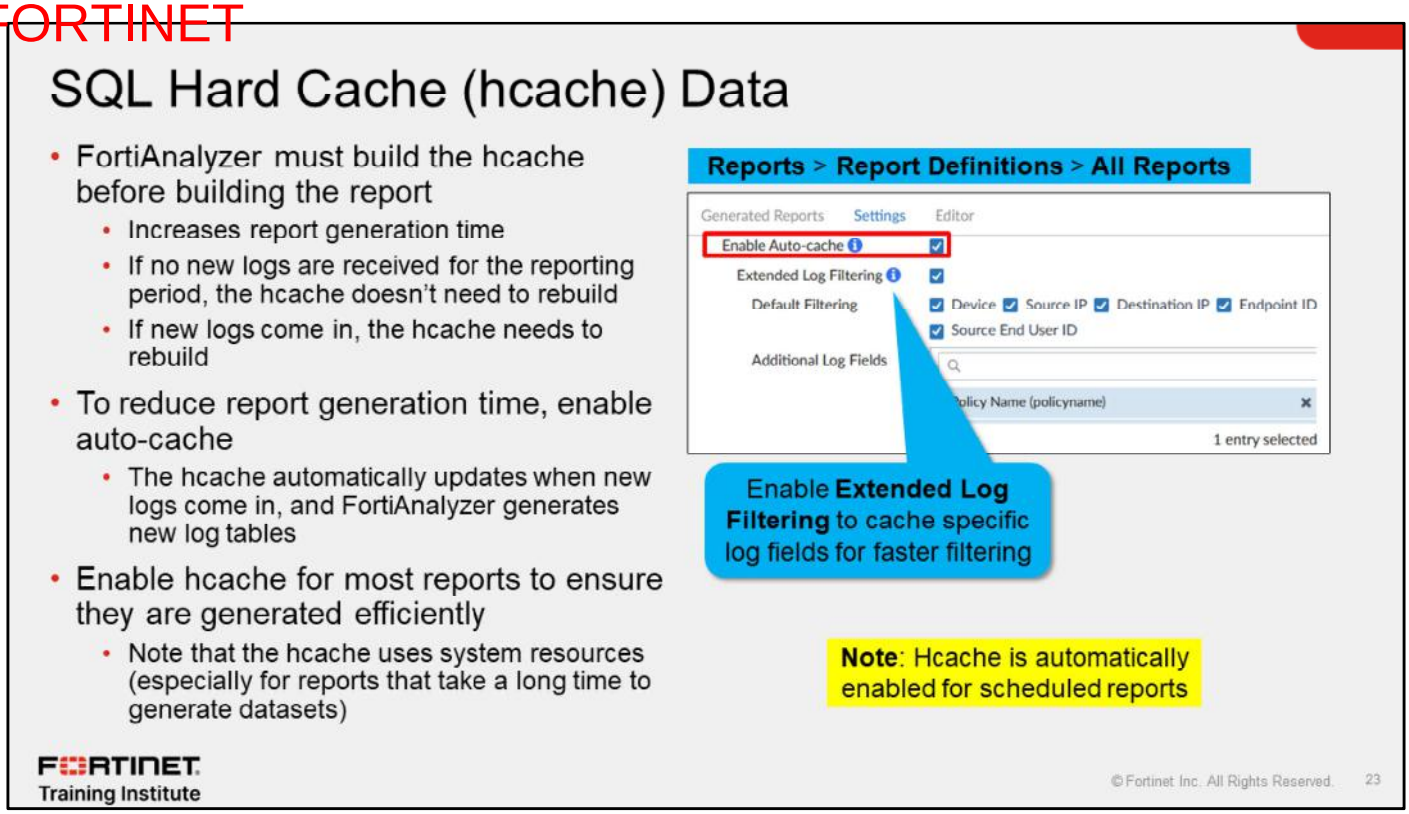
To use any of these external storage methods, you must first set up the back end. To email generated reports, you must first configure a mail server, as this slide shows. To upload logs to a server, you must first configure the mail server to accept connections from FortiAnalyzer.



To send reports to an external location, you must enable notifications in each report and select an appropriate output profile.

An output profile specifies the following:
- The format of the report, such as HTML, PDF HTML, XML, CSV, and JSON
- Whether to email generated reports or upload to a server. You can specify one option, both options, or create multiple output profiles. Server options include FTP, SFTP, and SCP.
- Whether to delete the report locally after uploading to the server

If you enable ADOMs, each ADOM has its own output profiles.



When FortiAnalyzer generates a report, the system builds the charts from precompiled SQL hard-cache data, known as the hcache. If the hcache is not built when you run the report, the system must create the hcache first and then build the report. This adds time to the report generation. However, if FortiAnalyzer does not receive any new logs for the reporting period, when you run the report a second time, it is much faster because the hcache data is already precompiled.

To boost report performance and reduce report generation time, you can enable auto-cache in the report settings. In this case, when new logs arrive, FortiAnalyzer automatically updates the hcache and generates new log tables.

Note that hcache is automatically enabled for scheduled reports. If you are not scheduling a report, you may want to consider enabling hcache. This ensures that reports are generated efficiently. However, be aware that this process uses system resources, especially for reports that require a long time to assemble datasets. Monitor your system to ensure it can handle it.

Additionally, you can enable **Extended Log Filtering** to cache specific log fields for faster filtering.

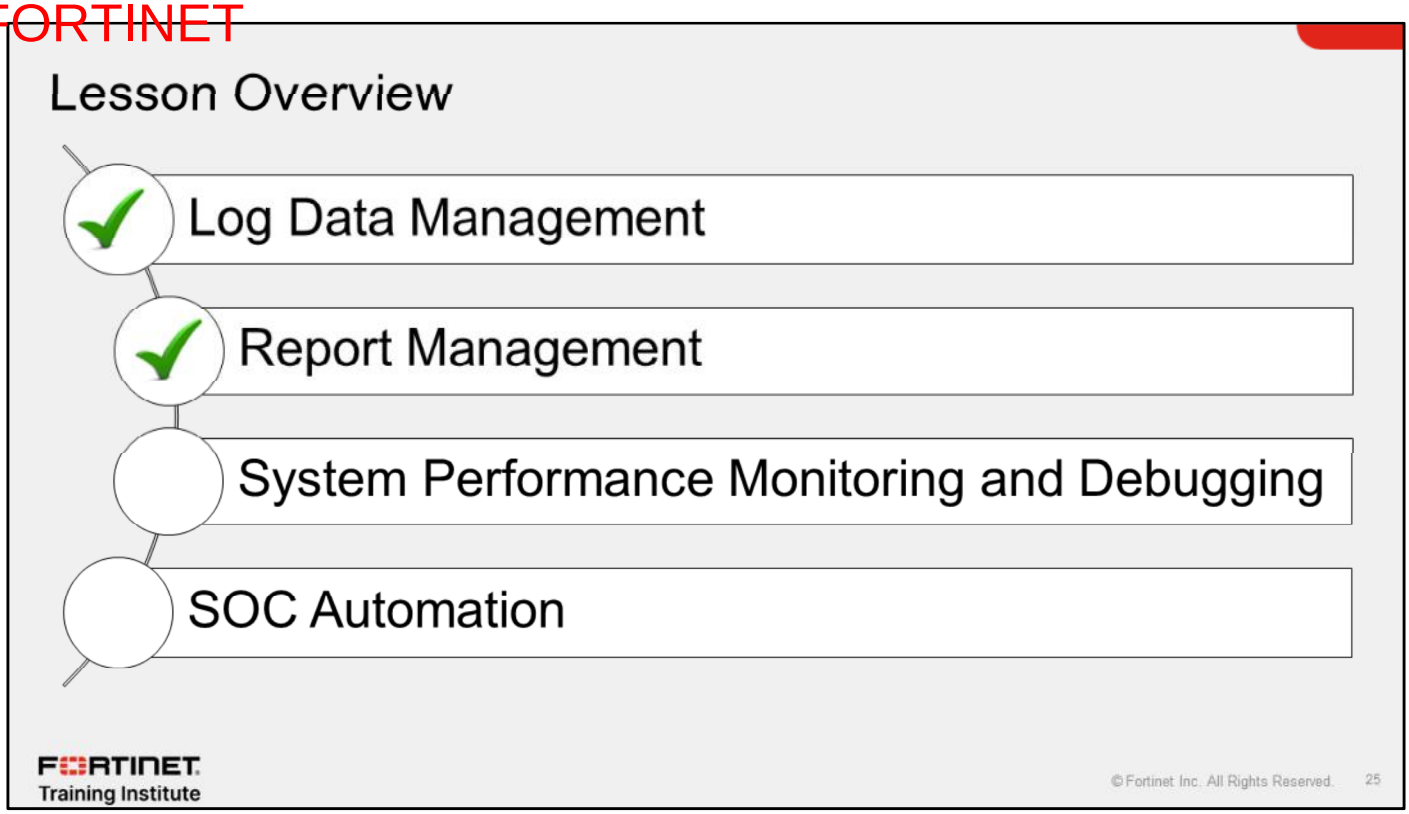
Knowledge Check

1. On FortiAnalyzer, what is a dataset?
   - A. The database schema available to perform queries
   - ✓ B. A specific SQL SELECT query that retrieves data from the database

2. What is a benefit of enabling hcache in FortiAnalyzer reports?
   - A. It increases the efficiency of the storage used by reports.
   - ✓ B. It reduces the time required to generate reports.

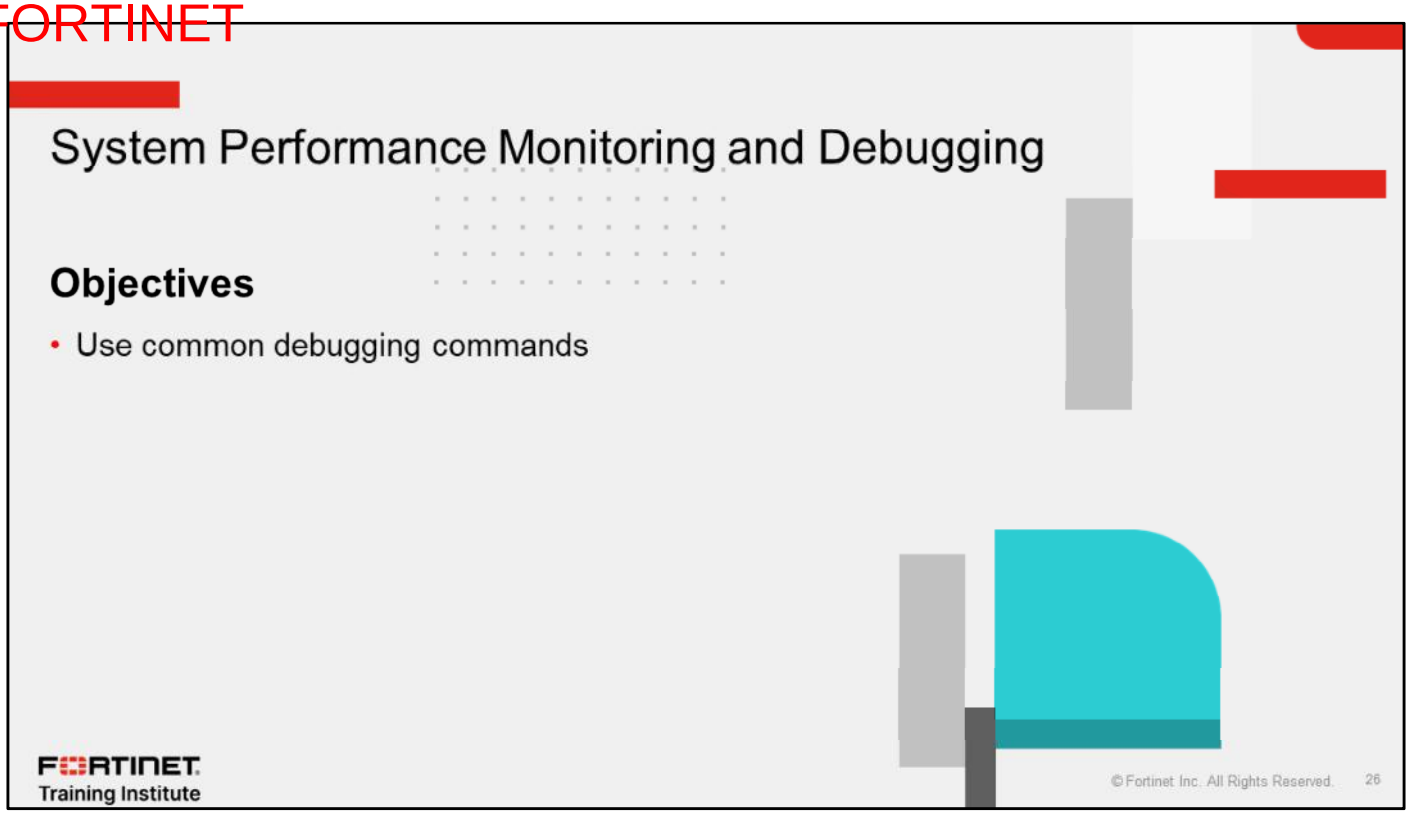
FORTINET Training Institute

 24



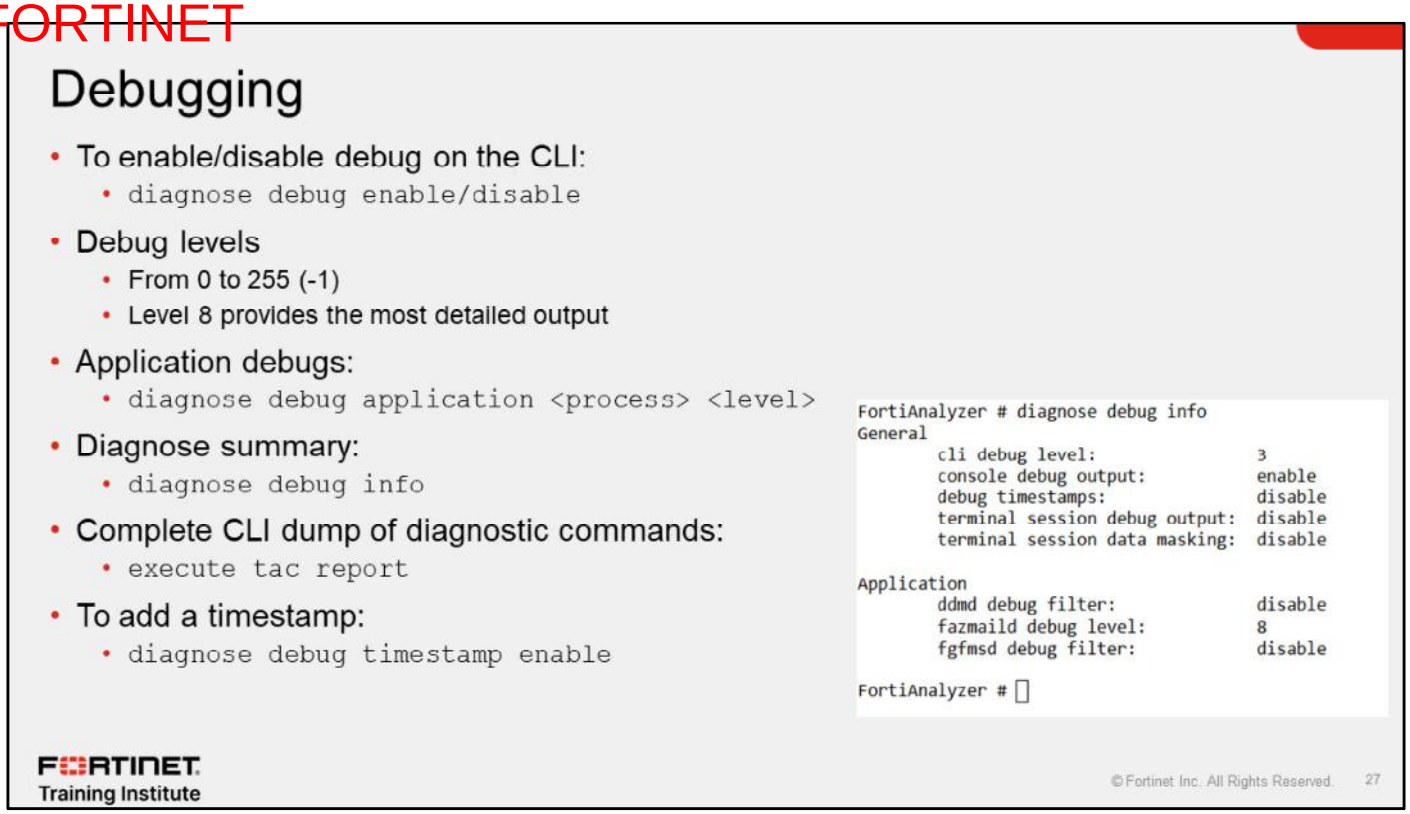
Good job! You now understand how to manage reports on FortiAnalyzer.

Now you will learn about system performance monitoring.



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

By demonstrating competence in system performance and debugging, you will be able to use the FortiAnalyzer CLI to debug common FortiAnalyzer issues.

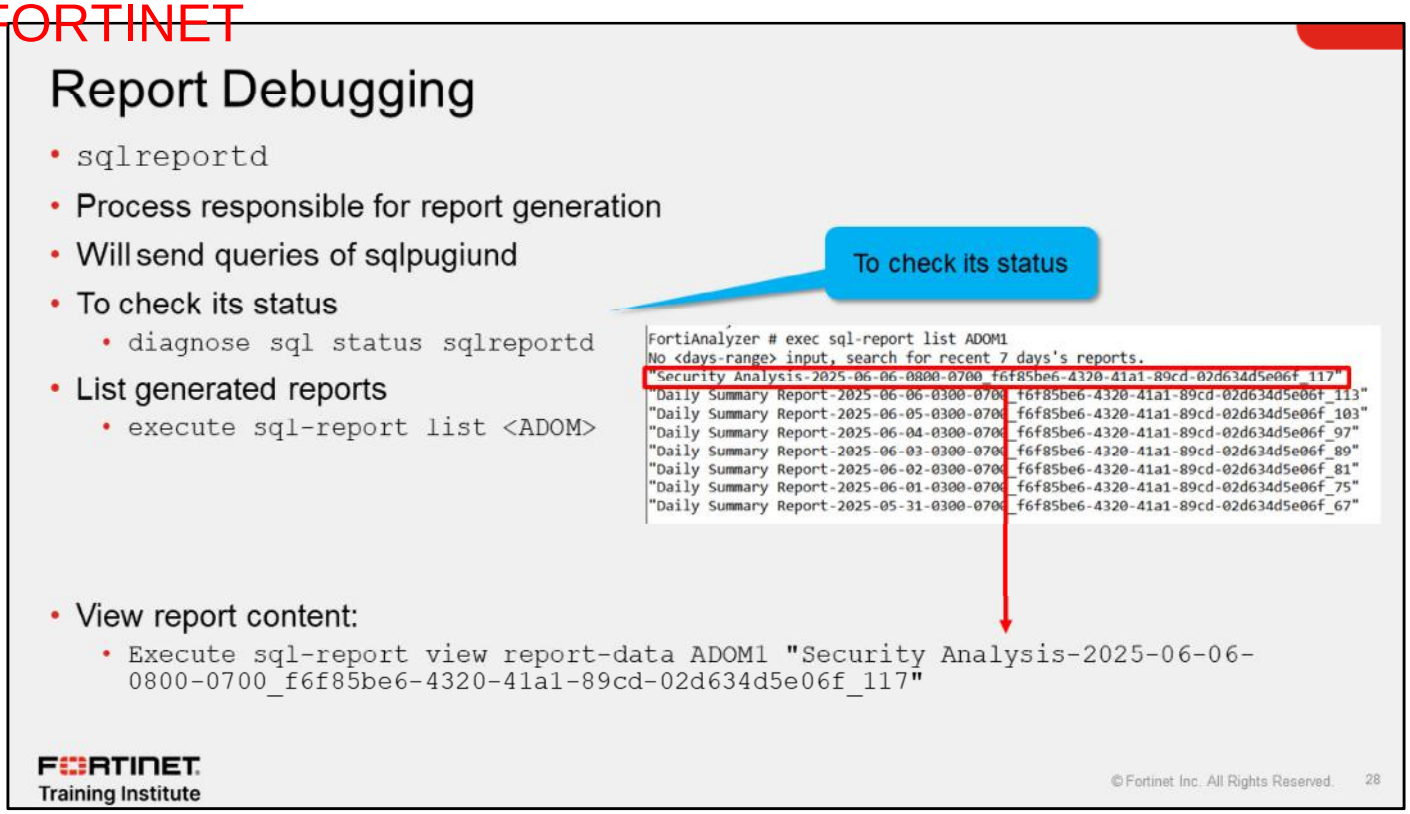


Using the CLI, you can enable and disable debugging for most processes on the FortiAnalyzer. The debug levels range from 0 to 255, with 8 giving the most detailed output.

Run the `diagnose debug application` command and define the process and the level at which you want to debug it.

The `diagnose debug info` command shows which level the debug is currently at.

The `execute tac report` command gives a dump of all diagnostic commands on the FortiAnalyzer.



The `sqlreportd` is the process responsible for generating reports on FortiAnalyzer.

Using the commands shown on this slide to check the status of the `sqlreportd` process, list all generated reports on FortiAnalyser, and view the content of the reports.

Report Debugging (Contd)

- Check and clean report queue
  - `diagnose report status`
  - `diagnose report clean`

```
FortiAnalyzer # diagnose report status
Max pending rpts: 100000
Current pendings: 0
Max running rpts: 1
Current runnings: 0
Semaphore state : initialized (1)
  Sem value     : 1 unlocked

Longest run report: adom[ADOM1], title:Security Analysis, duration:1m36s
```

- Run report from CLI (useful to get useful debugs)
  - `execute sql-report run <ADOM> <name/title>`

```
FortiAnalyzer # exec sql-report run ADOM1
<name/title>    Please select one of the available SQL report schedule names or titles:

ADOM: ADOM1
NAME    TITLE
1       - Security Analysis
10000   - User Security Analysis
10002   - Bandwidth and Applications Report
10003   - Email Report
10004   - Admin and System Events Report
10006   - Threat Report
10007   - IPS Report
10008   - Detailed Application Usage and Risk
10009   - Top 20 Categories and Applications (Bandwidth)
10010   - Top 20 Categories and Applications (Session)
10011   - Top Allowed and Blocked with Timestamps
10012   - User Detailed Browsing Log
10013   - Hourly Website Hits
10014   - Top 20 Category and Websites (Bandwidth)
10015   - Top 20 Category and Websites (Session)
10016   - Top 500 Sessions by Bandwidth
10017   - User Top 500 Websites by Bandwidth
```

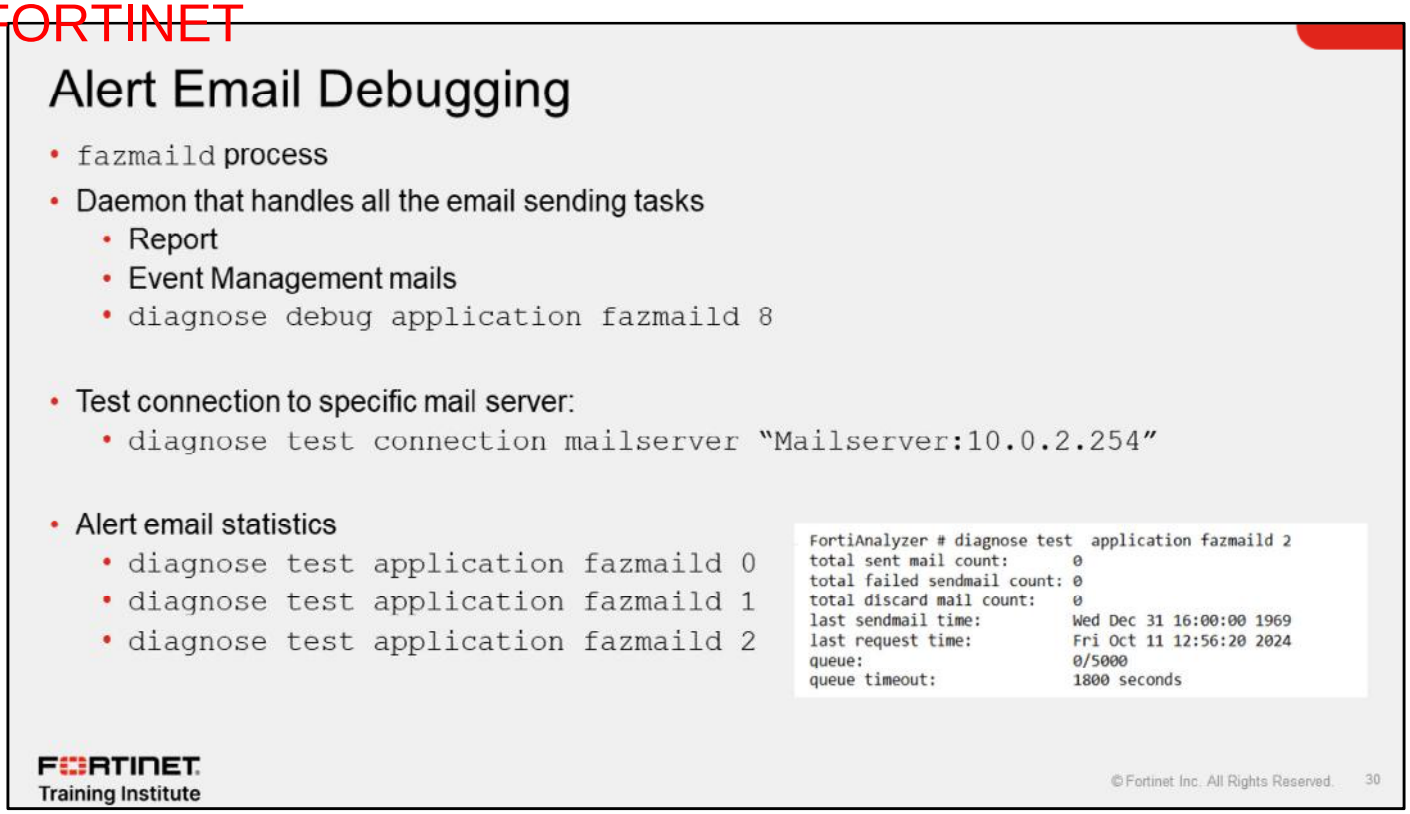
FORTINET Training Institute

 29

Run the `diagnose report status` command to check the report queue.

Too many reports waiting to be run in the FortiAnalyzer reporting queue could cause it to hang or become slow. Run the `diagnose report clean` command to wipe the report queue clean.

To see the debugs of a running report, use the `execute sql-report run <ADOM> <name/title>` command.

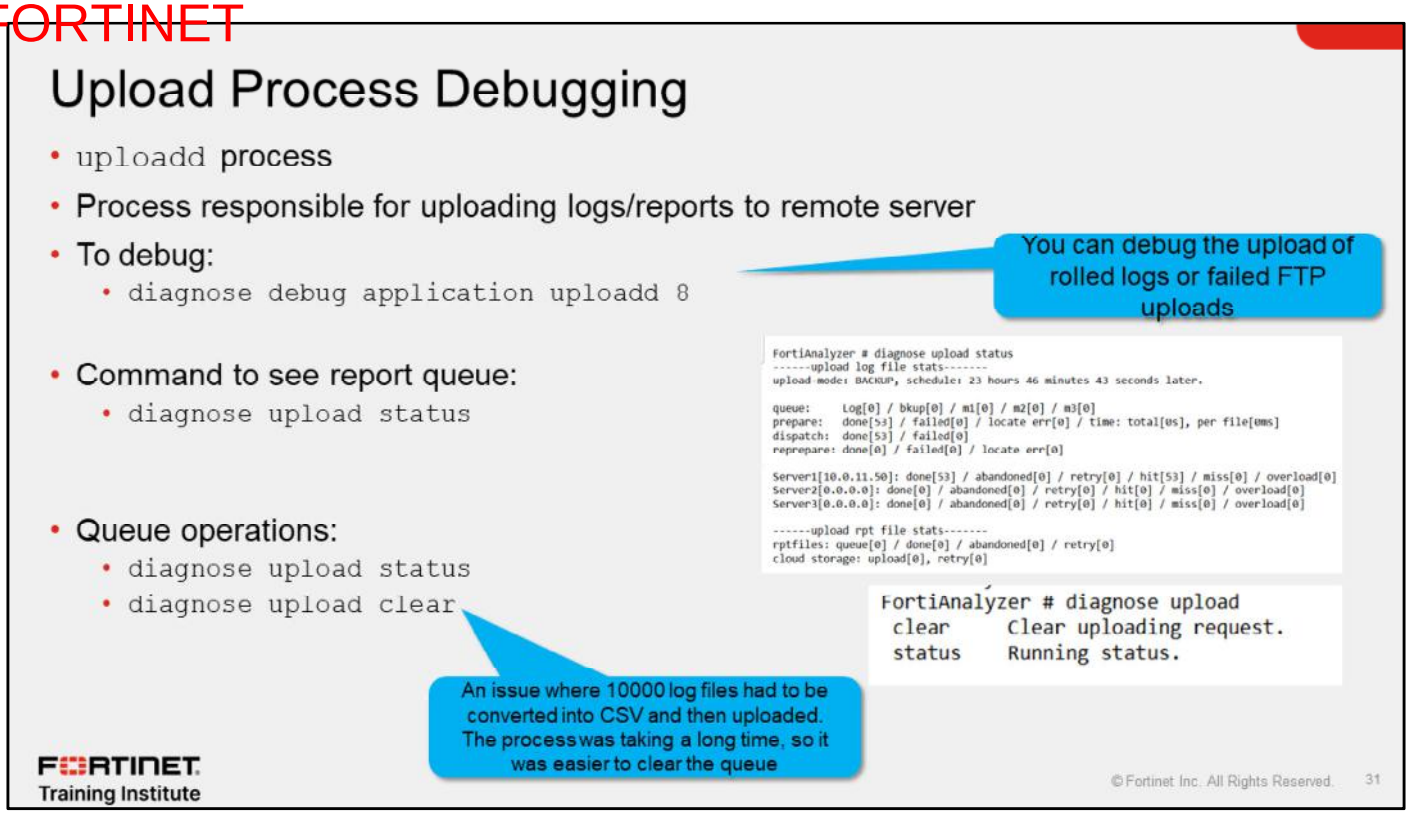


The `fazmaild` is the daemon the FortiAnalyzer that handles all email sending tasks.

The `diagnose debug application fazmaild 8` command shows all reports and event management mails that the FortiAnalyzer sent.

You can test connection to specific mail server by running the command shown on the slide.

The `diagnose test application fazmaild 2` command gives a count of all the emails sent by the FortiAbalyzer.



The `uploadd` process is responsible for uploading logs and reports to a remote server.

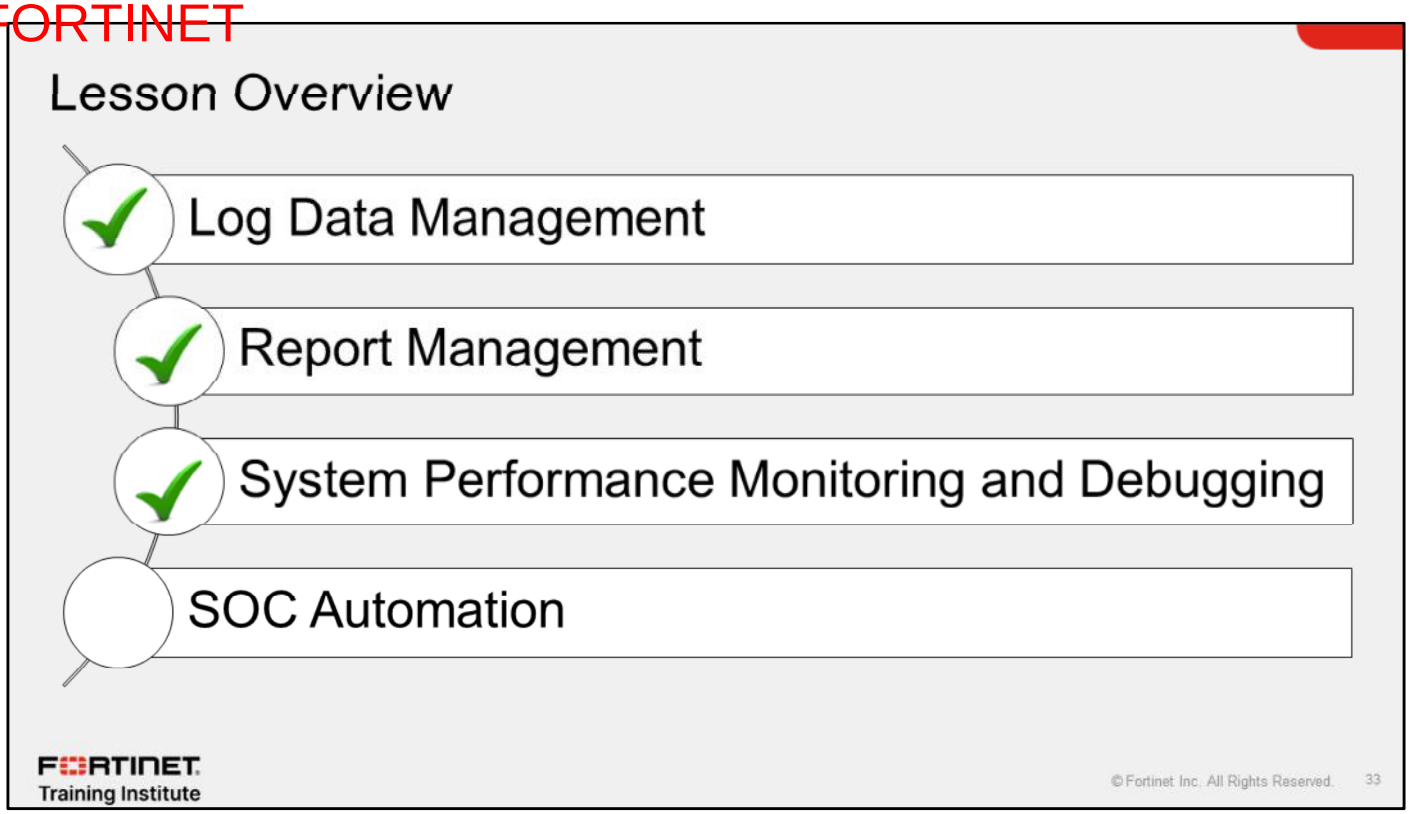
The commands to diagnose and debug the uploading process are shown on this slide.

Knowledge Check

1. Which process on FortiAnlayzer is responsible for uploading reports to remote server?
   A. sqlreportd
   B. uploadd
   ✓ C. fazmaild
   D. sqlplugind

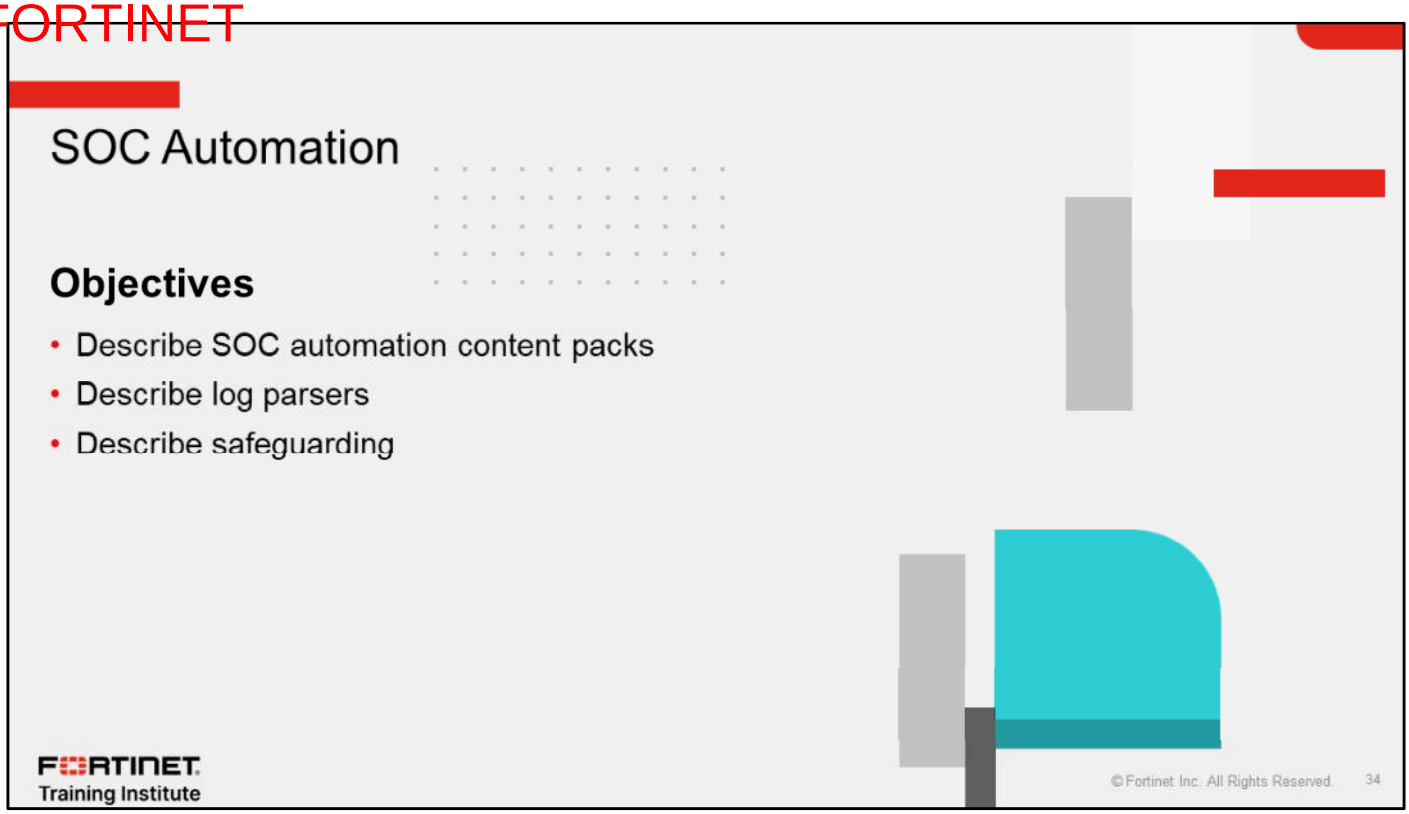
FORTINET Training Institute

 32



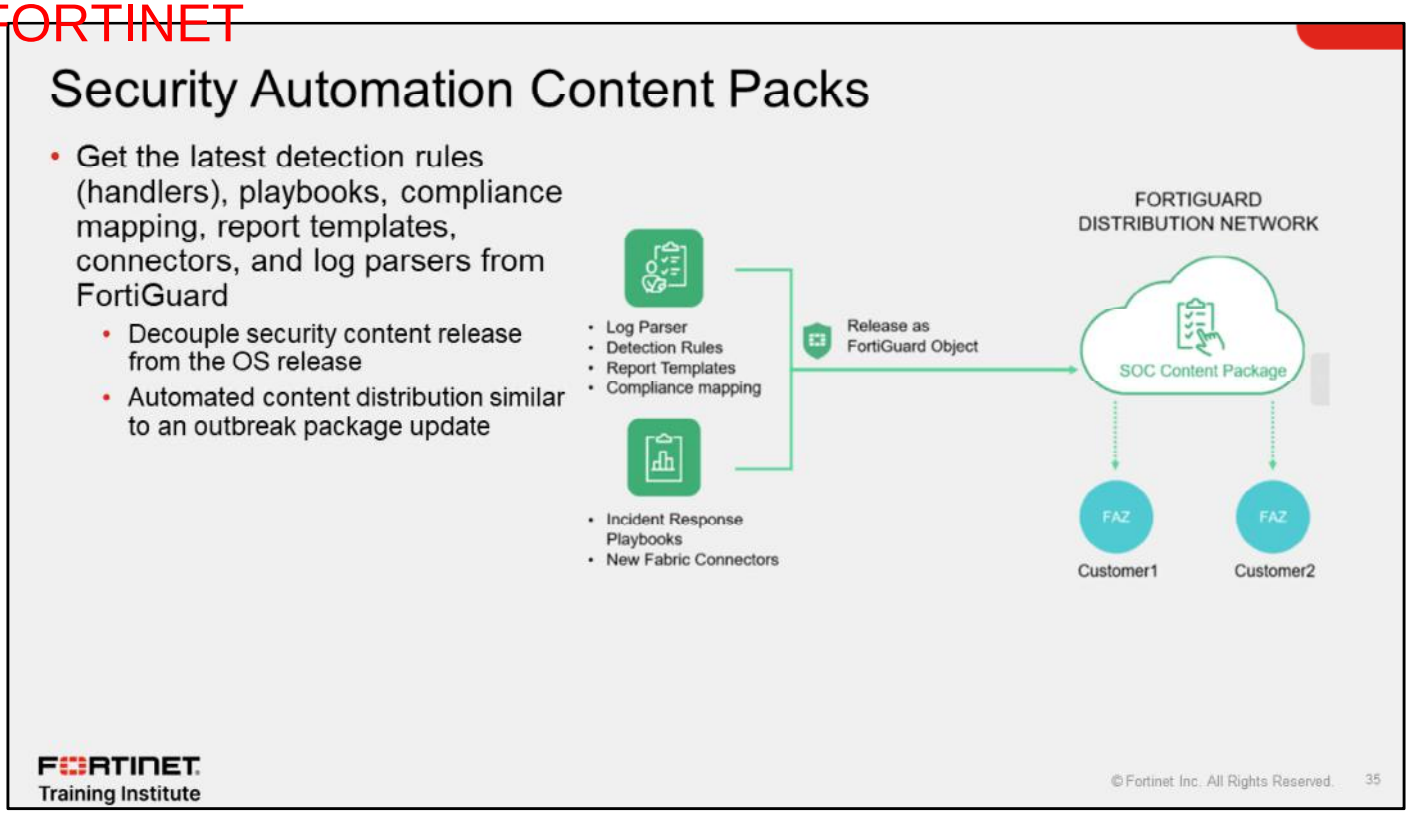
Good job! You now understand how to monitor system performance and use the debug commands.

Now, you will learn SOC automation.



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

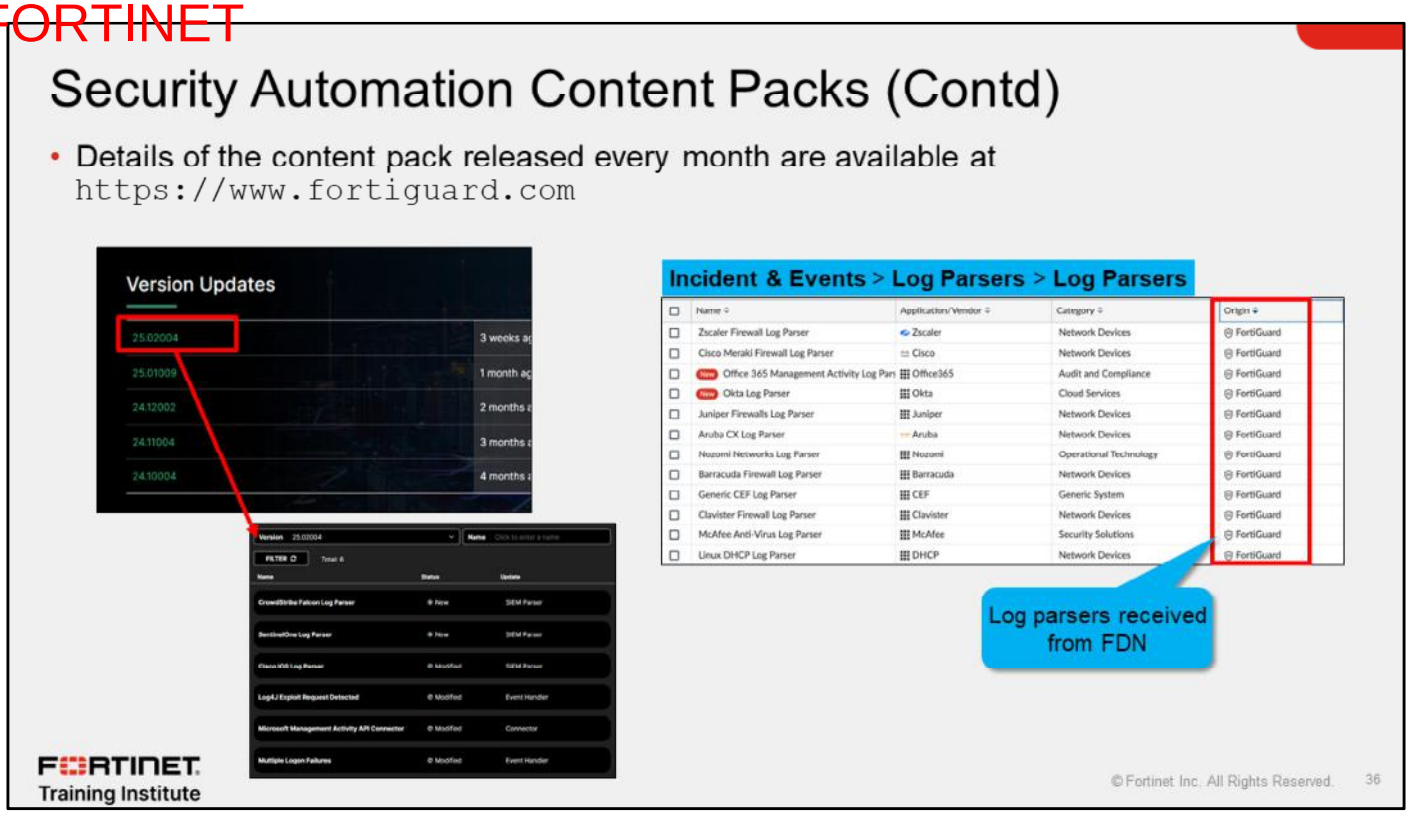
By demonstrating competence in SOC autmation, you will be able to use FortiAnalyzer in a more optimized way.



The FortiAnalyzer SOC Automation Service, integrated with native security information and event management (SIEM) and security orchestration, automation, and response (SOAR) capabilities on the platform, offers a comprehensive suite of features, including, but not limited to, third-party log parsers, advanced correlation rules, automation connectors, incident response playbooks, advanced analytics, and premium reports.

These tools empower security operations teams to swiftly detect, investigate, and respond to security incidents.

You need a separate license for the FortiAnalyzer SOC Automation Service content packs.

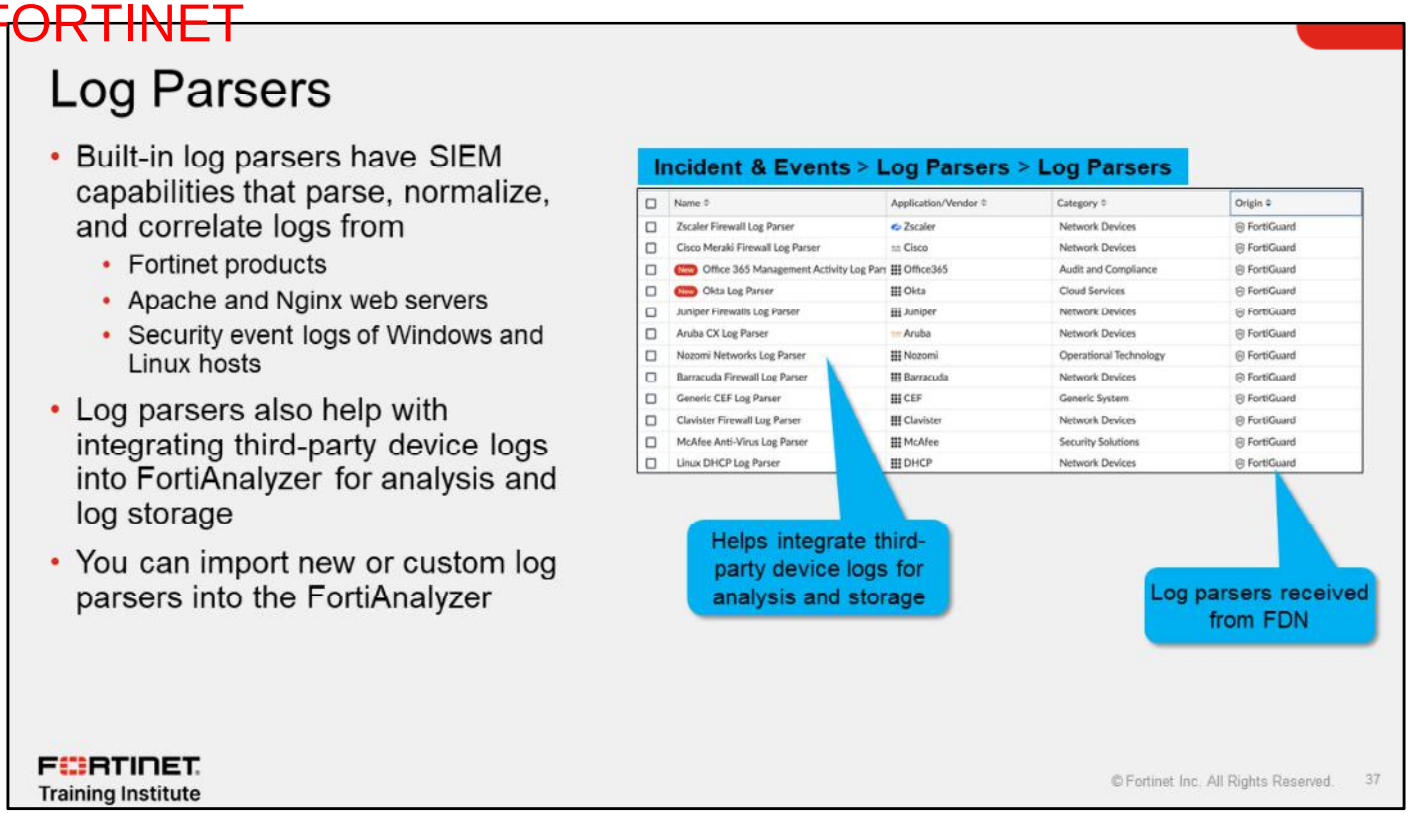


The details of the content pack released every month are available on the FortiGuard Labs website.

When you have a valid Security Automation Service license, the content pack release is applied automatically in FortiAnalyzer when available from the FortiGuard distribution server.

This service includes prebuilt and customizable reports that provide deep insights into security events and trends. The included event handlers help automate incident-handling processes for faster response. Playbooks are automated security workflows delivered from FortiGuard that enable proactive defense mechanisms. The content packs also come with SIEM parsers, which have advanced log parsing capabilities for better threat correlation and analysis.

All log parsers from content packs have the **Origin** value of **FortiGuard**, and the latest installation will include the **New** tag, as shown in the image on this slide.



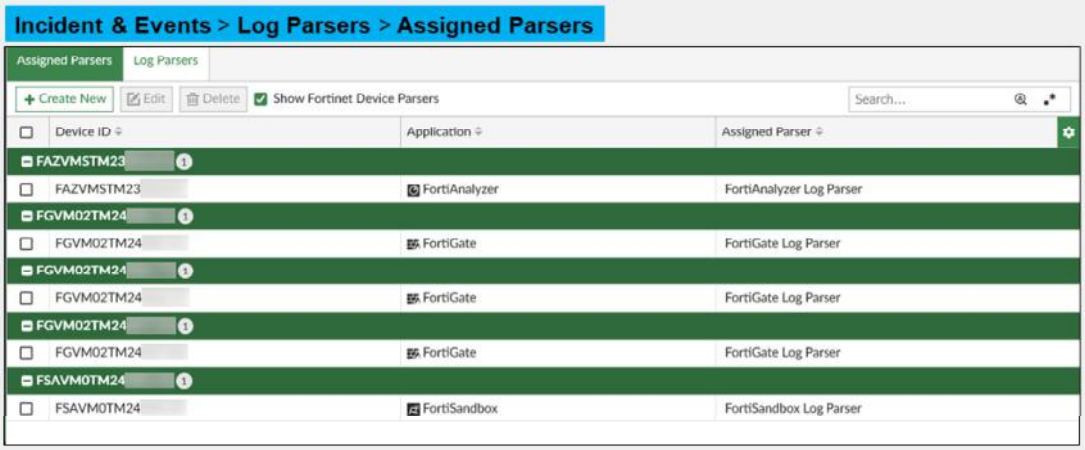
FortiAnalyzer SIEM capabilities parse, normalize, and correlate logs from Fortinet products, Apache and Nginx web servers, and the security event logs of Windows and Linux hosts (with Fabric Agent integration). SIEM logs are displayed in **Log View** > **Logs** > **All** and can be used when generating reports.

FortiAnalyzer predefines parsing and does not require administrators to configure it manually. The predefined SIEM log parsers can be managed on the **Log Parsers** page. This page includes predefined log parsers, log parsers from FortiGuard, and any custom log parsers that you have imported.

Log parsers also help integrate third-party device logs into FortiAnalyzer for analysis and log storage. In the image shown on this slide, FortiAnalyzer is licensed to receive SOC automation content packs, which come with custom log parsers from third-party devices such as Cisco, Juniper, Aruba, Checkpoint, and so on.

Assigned Parsers

- The assigned parsers tab shows all the devices and applications, and their current log parser assignments in a table view



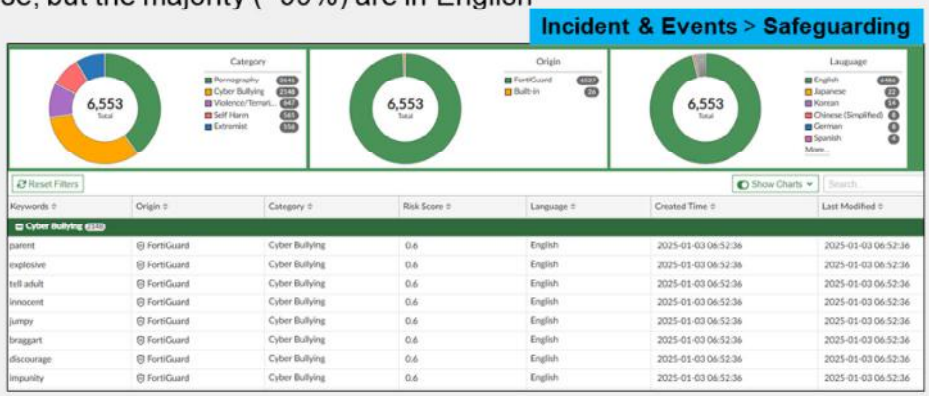
FORTINET Training Institute

 38

The **Assigned Parsers** tab displays all the devices and applications and their current log parser assignments in a table view.

Safeguarding

- Over 6,000 keywords (FortiGuard and built-in) are available, with updates provided through FortiGuard downloads
  - Keyword categories: Keywords are categorized into pornography, cyberbullying, violence/terrorism, self-harm, and extremism
- Visual insights: Donut charts display **Category**, **Origin**, and **Language** data
- Safeguarding database contains keywords in languages other than English, such as Japanese and Chinese, but the majority (~99%) are in English



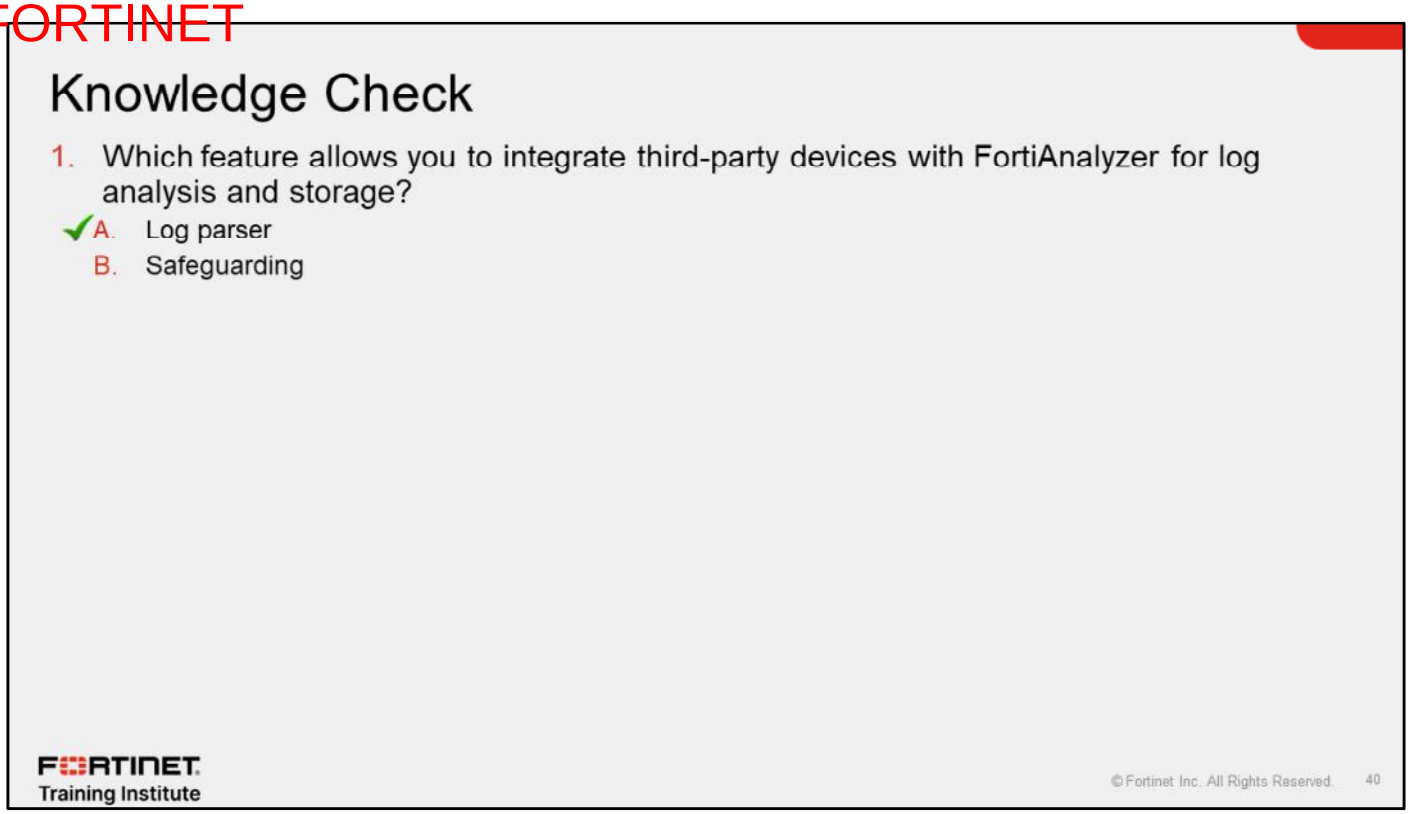
FORTINET Training Institute

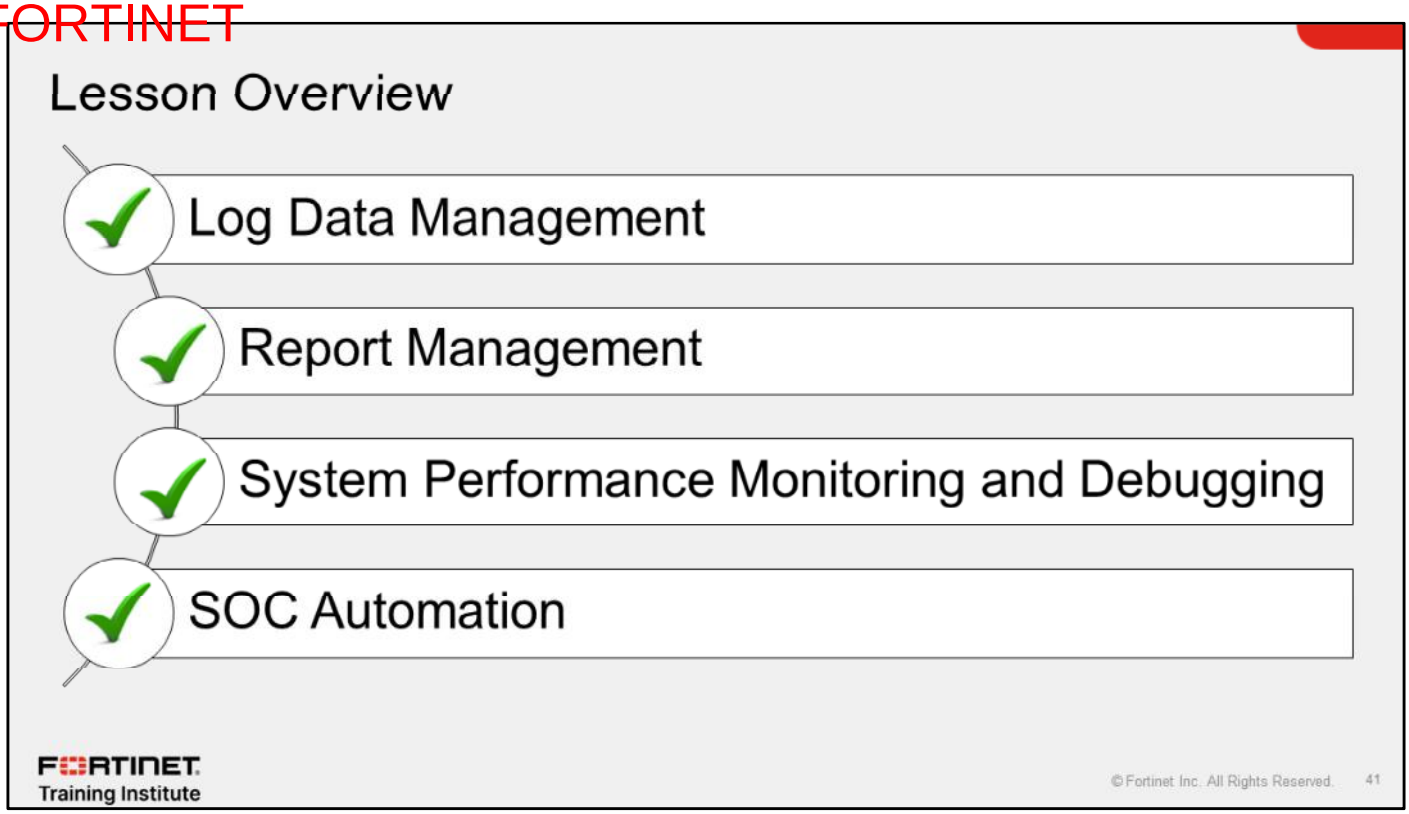
 39

The safeguarding feature on FortiAnalyzer identifies keywords for harmful content on the network. These keywords are used in reports and event handlers so you can respond accordingly. A use case would be for schools where cyberbullying or self-harm content being browsed by students can be brought to the immediate attention of the teachers so that timely action can be taken to prevent future mishaps.

While there are some built-in keywords, FortiAnalyzer must be connected to the FortiGuard distribution servers to display all the safeguarding keywords on this page. The keywords are automatically updated from FortiGuard, and the administrator cannot include new words in this category.

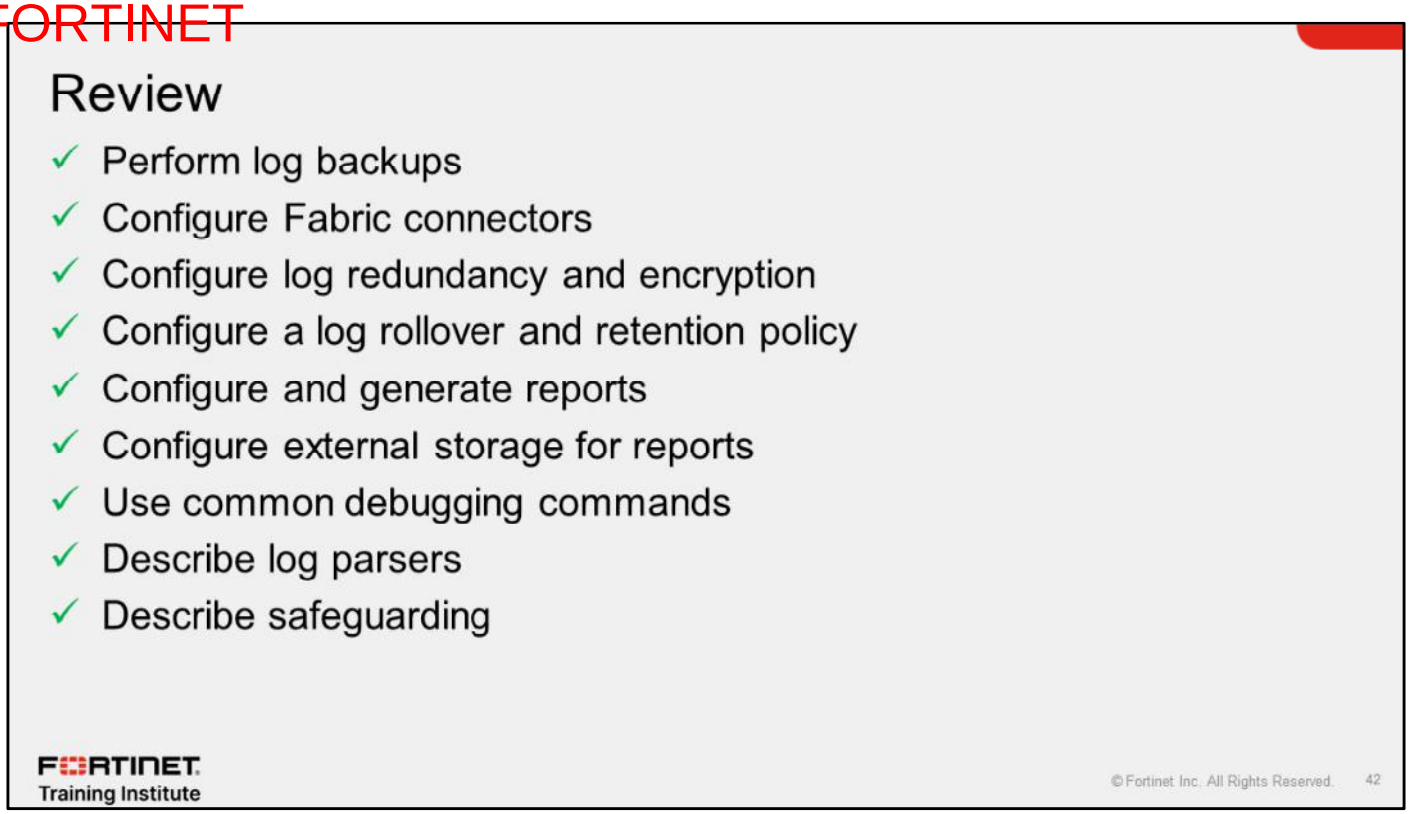
The safeguarding database contains keywords in languages other than English, such as Japanese, Chinese, etc. However, the majority (~99%) are in English.





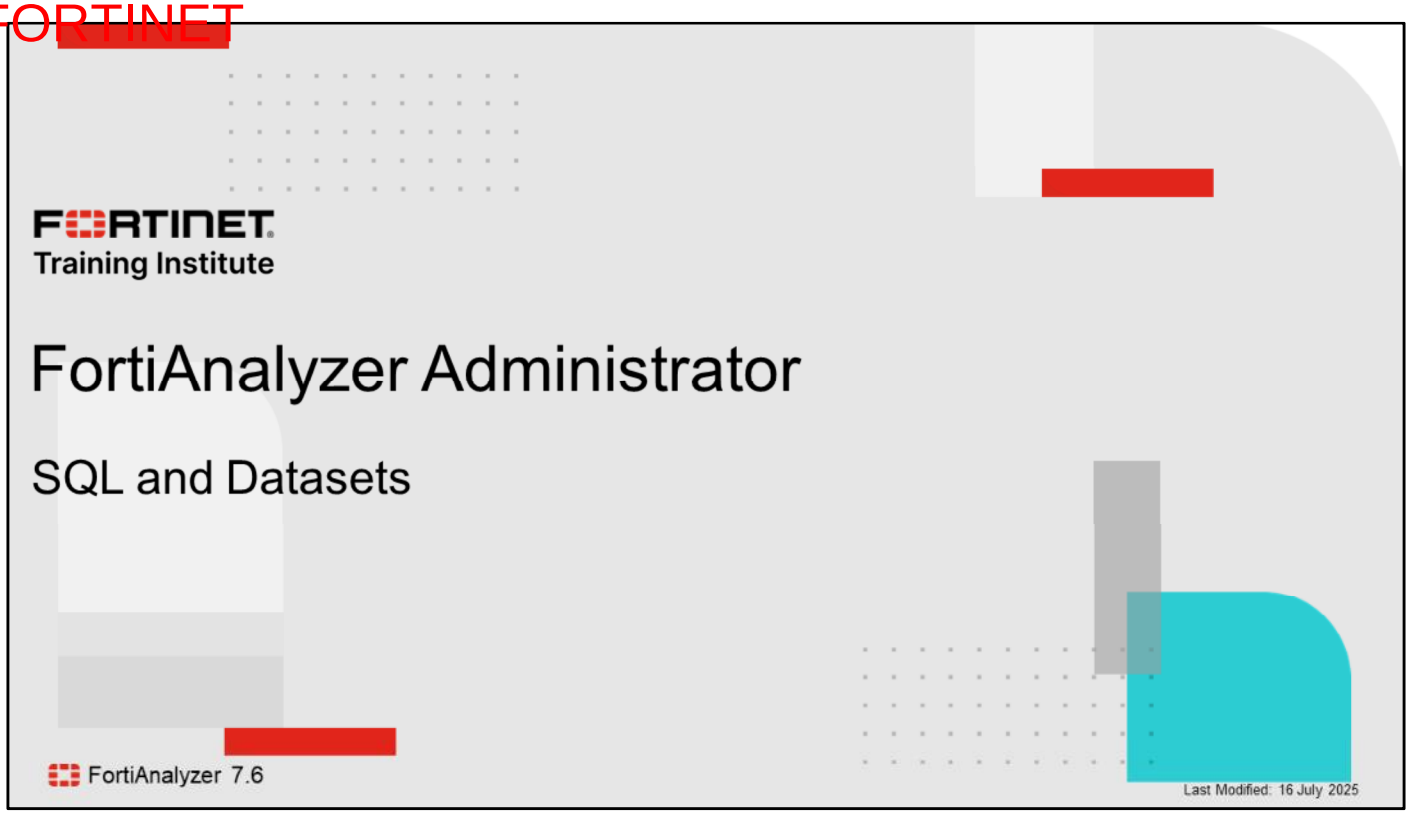
Congratulations! You have completed this lesson.

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

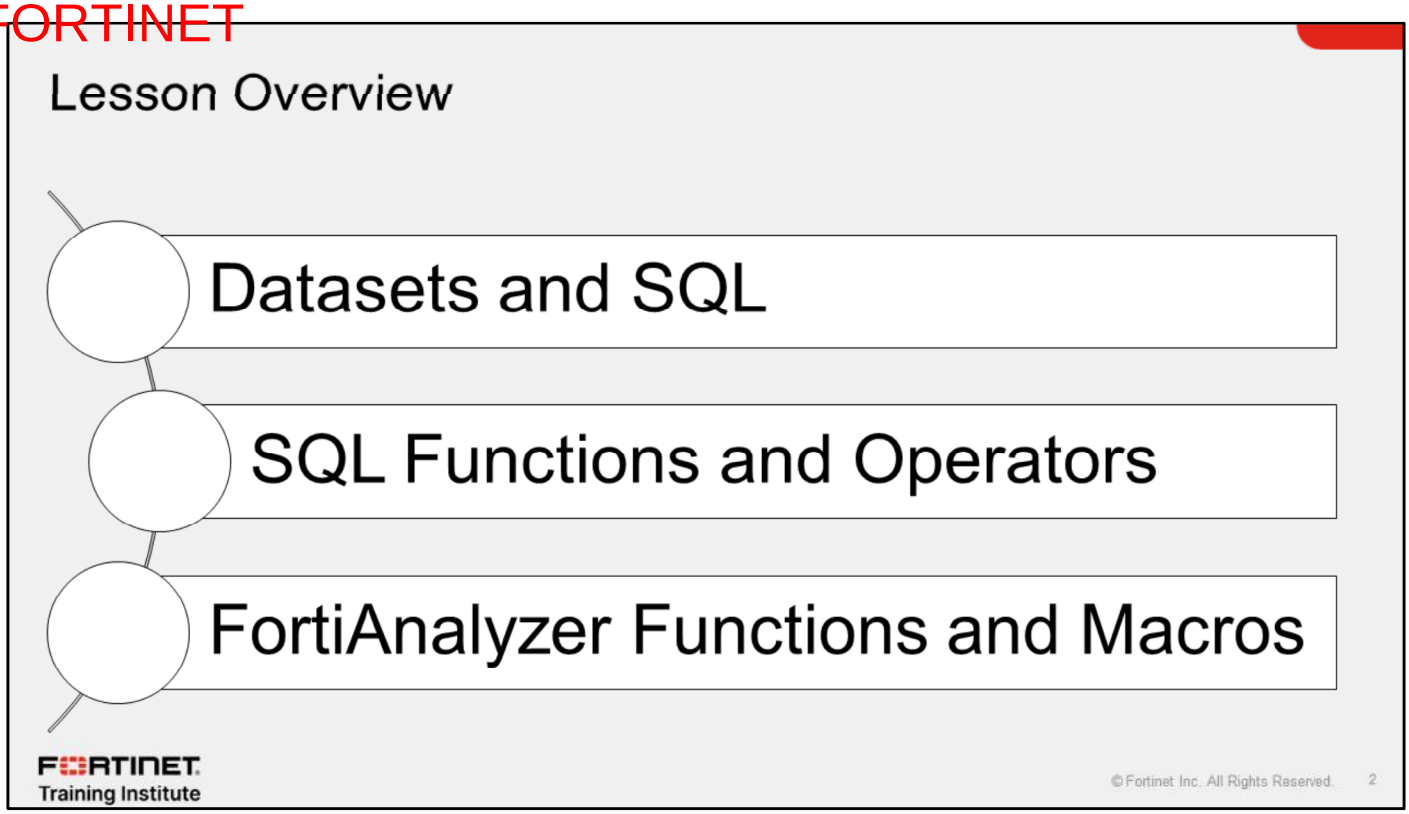


This slide shows the objectives that you covered in this lesson.

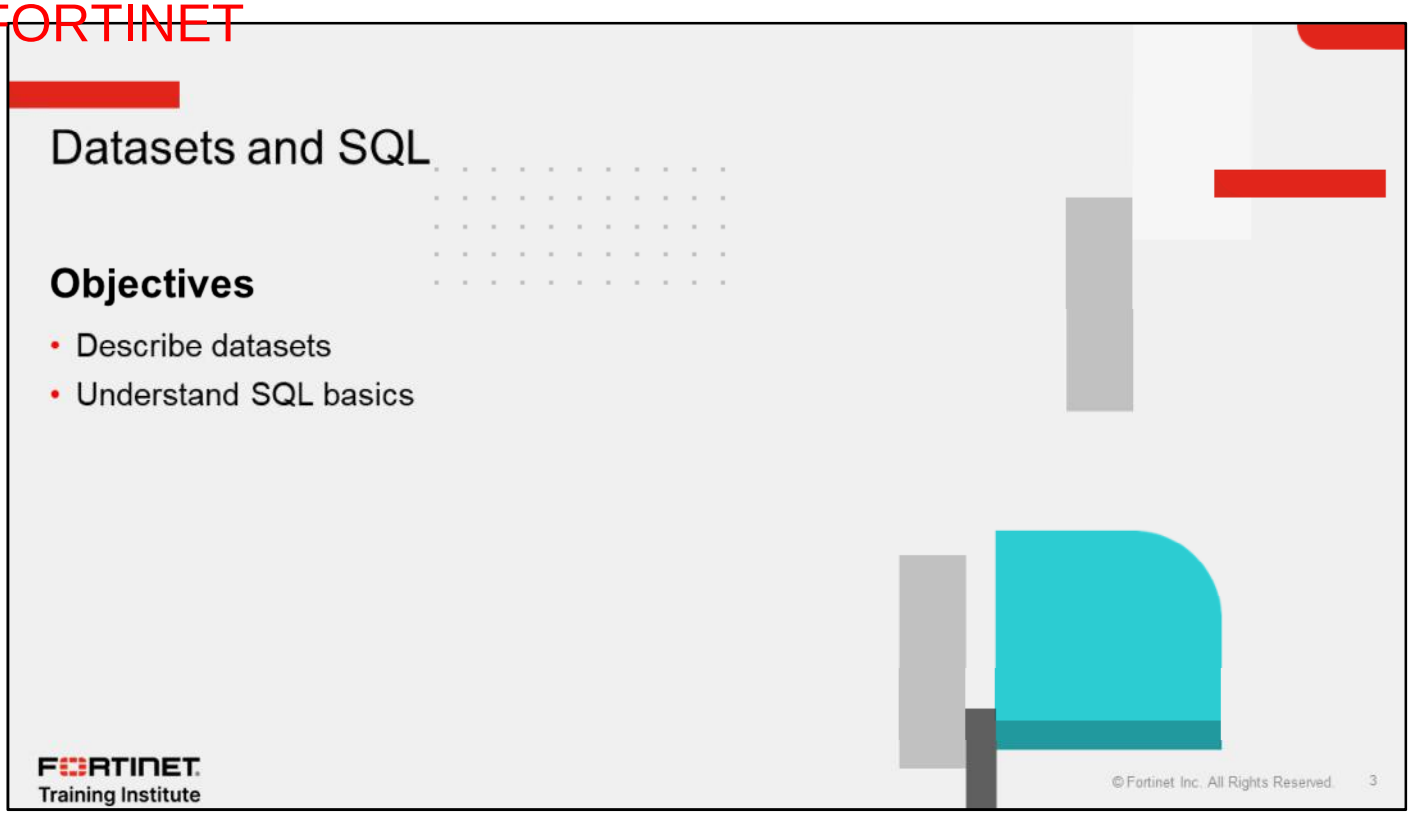
By mastering the objectives covered in this lesson, you learned how to manage the log data and reports on FortiAnalyzer.



This supplemental material provides an overview of SQL and datasets. Teaching a comprehensive lesson on SQL is out of scope for FortiAnalyzer training, so the goal of this material is to provide you with the information you need to modify or create datasets for the purpose of extracting data for reports.

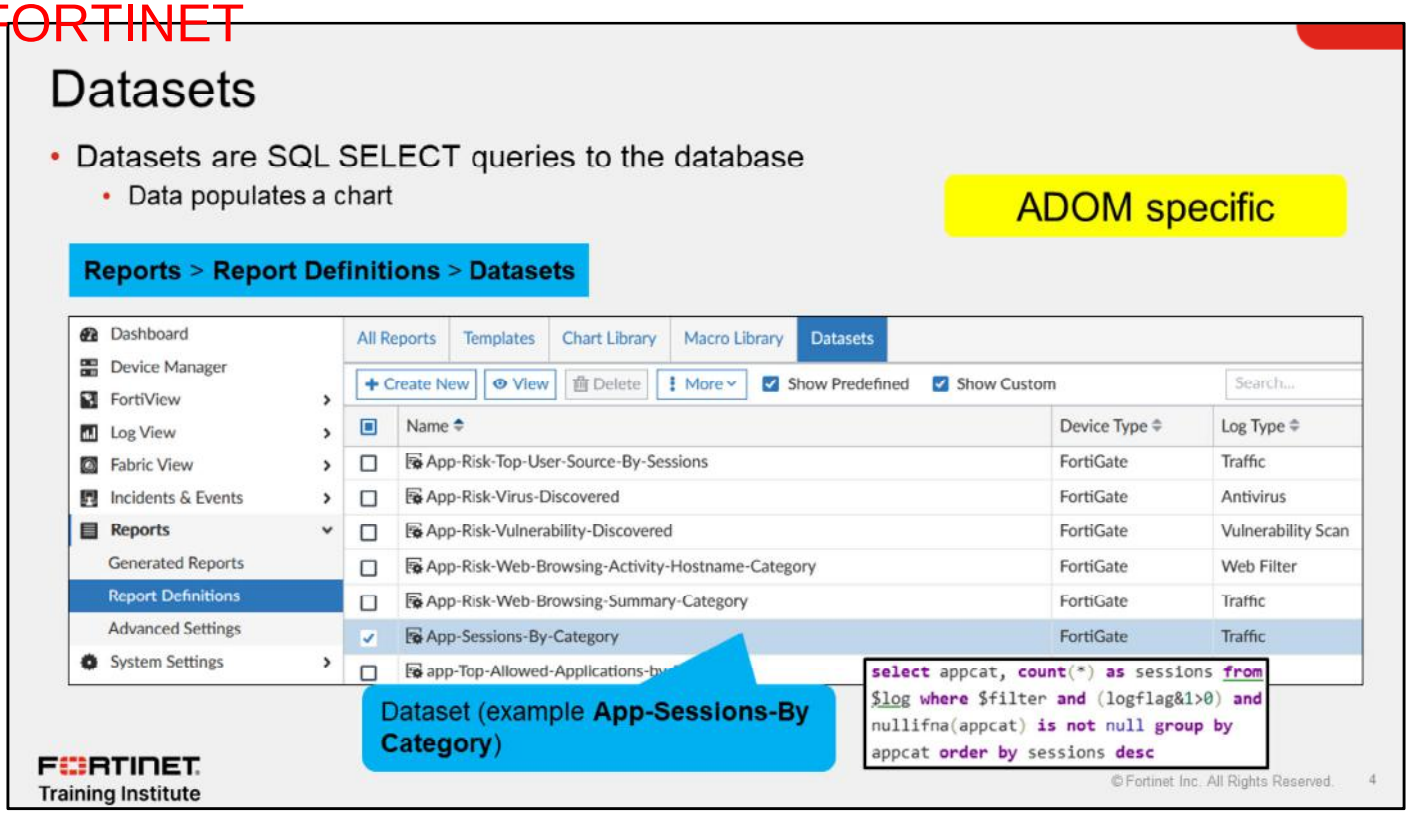


The supplemental material is covered in the topics shown on this slide.



This section covers datasets. Datasets define what data is extracted from the database and represented in the chart on a report.

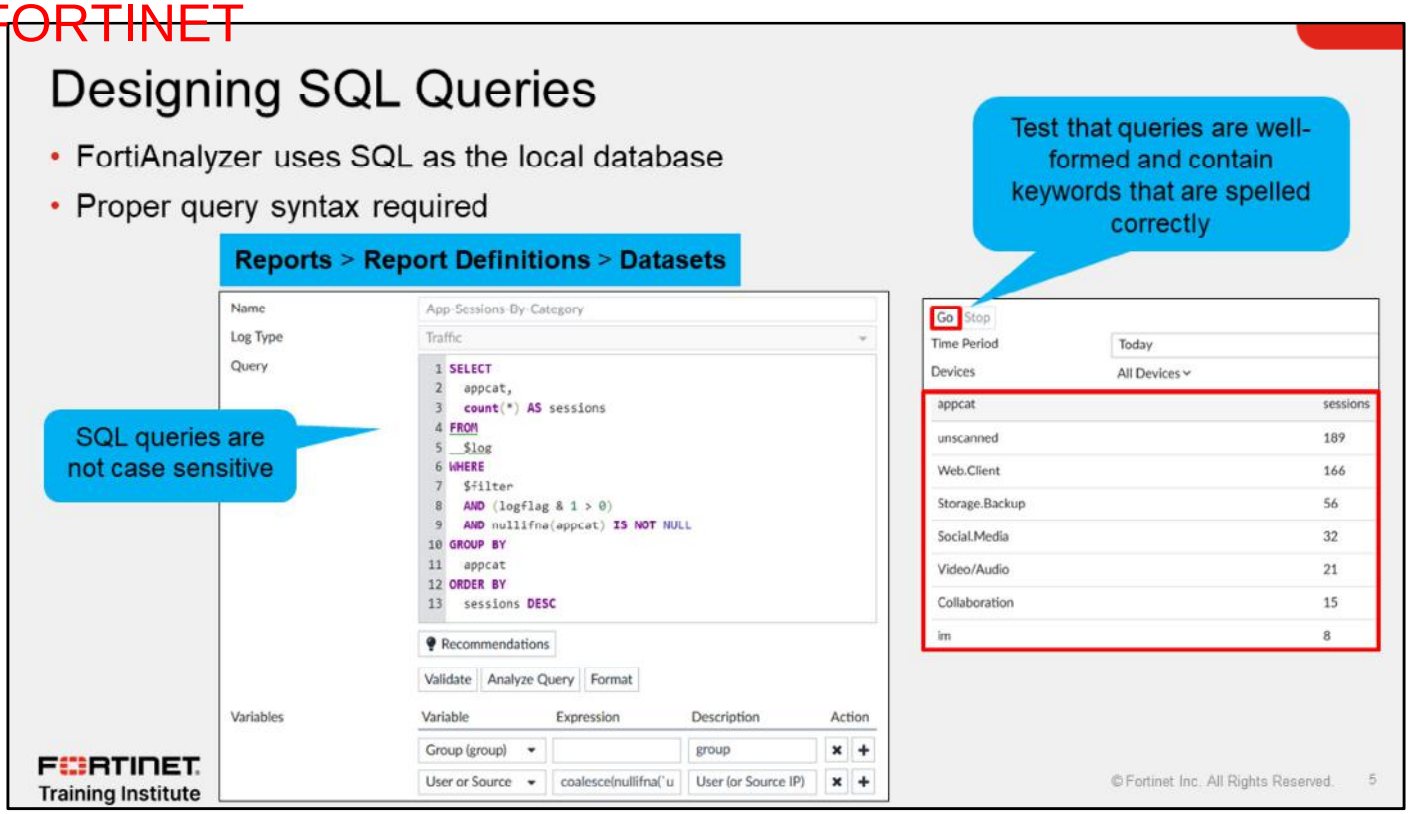
FortiAnalyzer provides predefined datasets that address the most common queries. However, if you need to modify those datasets or create your own, you need to understand SQL.



A dataset is an SQL `SELECT` query. The result of that query—the specific data polled from the database—is what populates a chart.

FortiAnalyzer includes many predefined datasets that contain some of the most common database queries. You can view the predefined datasets from the **Datasets** page.

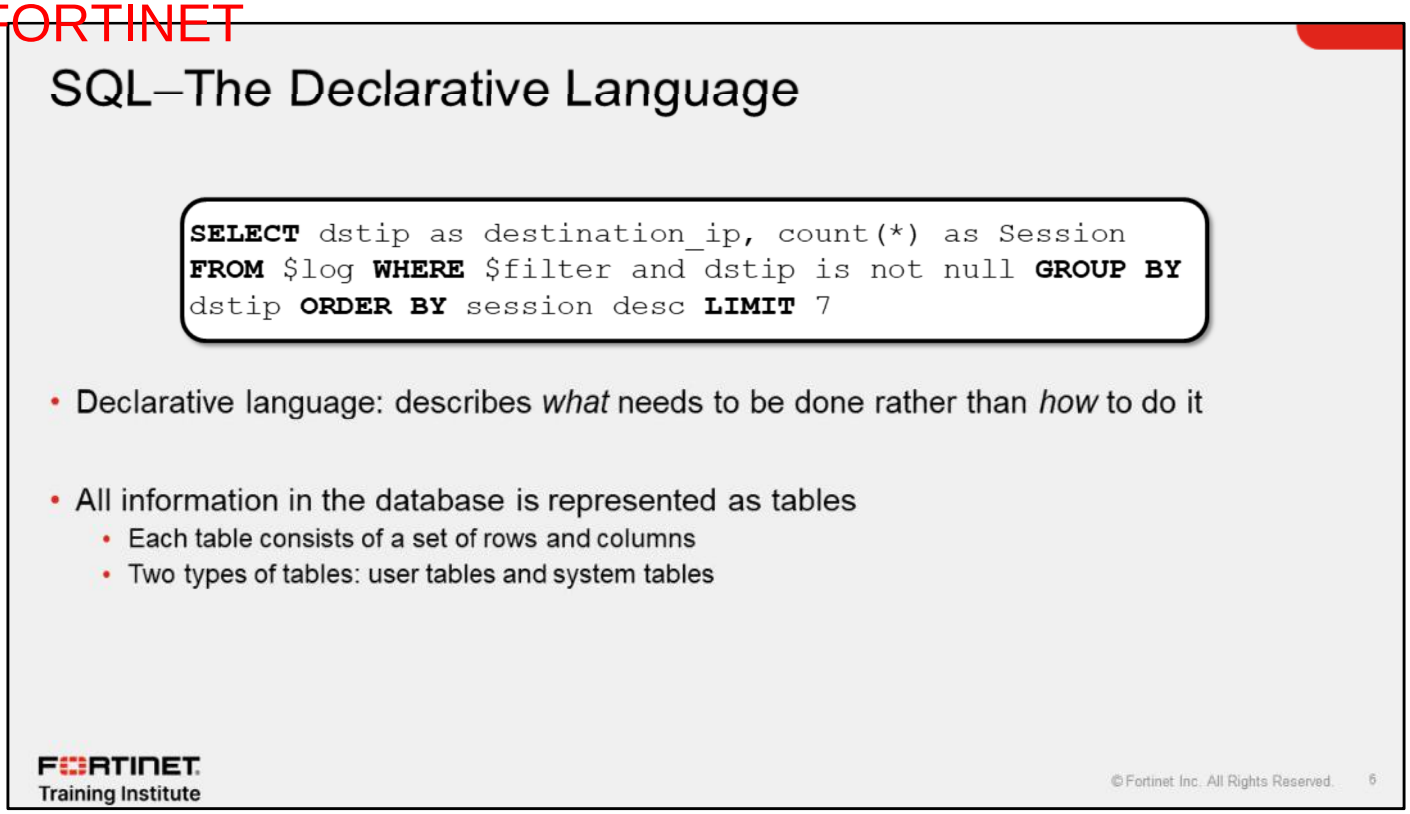
This slide shows an example of the default **App-Sessions-By-Category** dataset.



When you are building your queries, you must use SQL syntax to interface with the database. When creating or editing datasets, you can click **Validate** to check if the SQL query is valid, or see what errors are returned. You can also click **Go** to test your query. If the query is formed correctly, and the data you are querying is available in the database, the results appear. If the query is not formed correctly, you will see an error message.

You can also click **Format** to format the entered SQL query, making it easier to read, update, and detect errors. The screenshot on this slide shows a formatted SQL query.

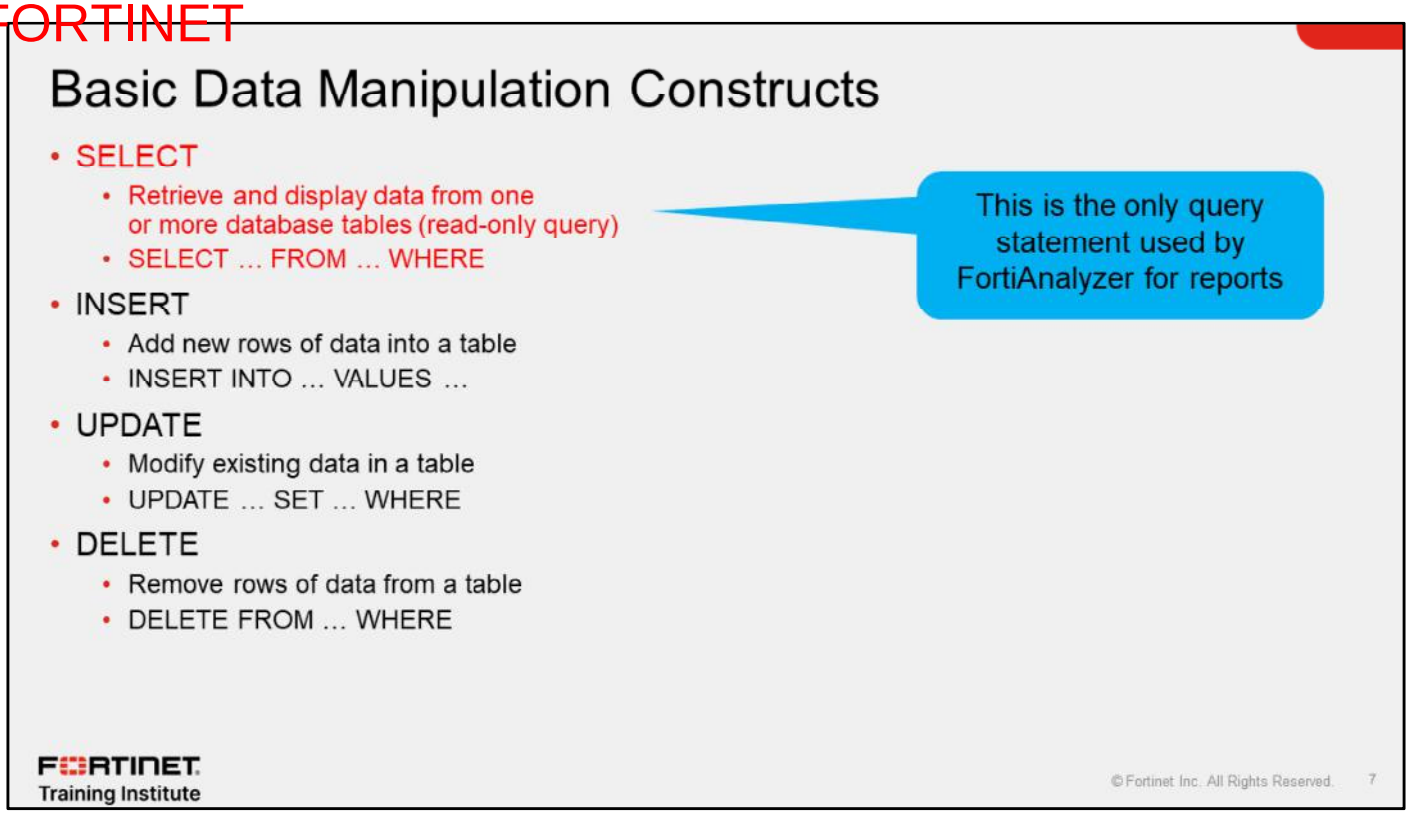
Note that SQL queries are not case sensitive.



Now take a closer look at the query itself. In order to understand this example dataset, and more specifically, what it is querying, you need to understand SQL. SQL is what is known as a declarative language—it describes *what* needs to be done rather than *how* to do it.

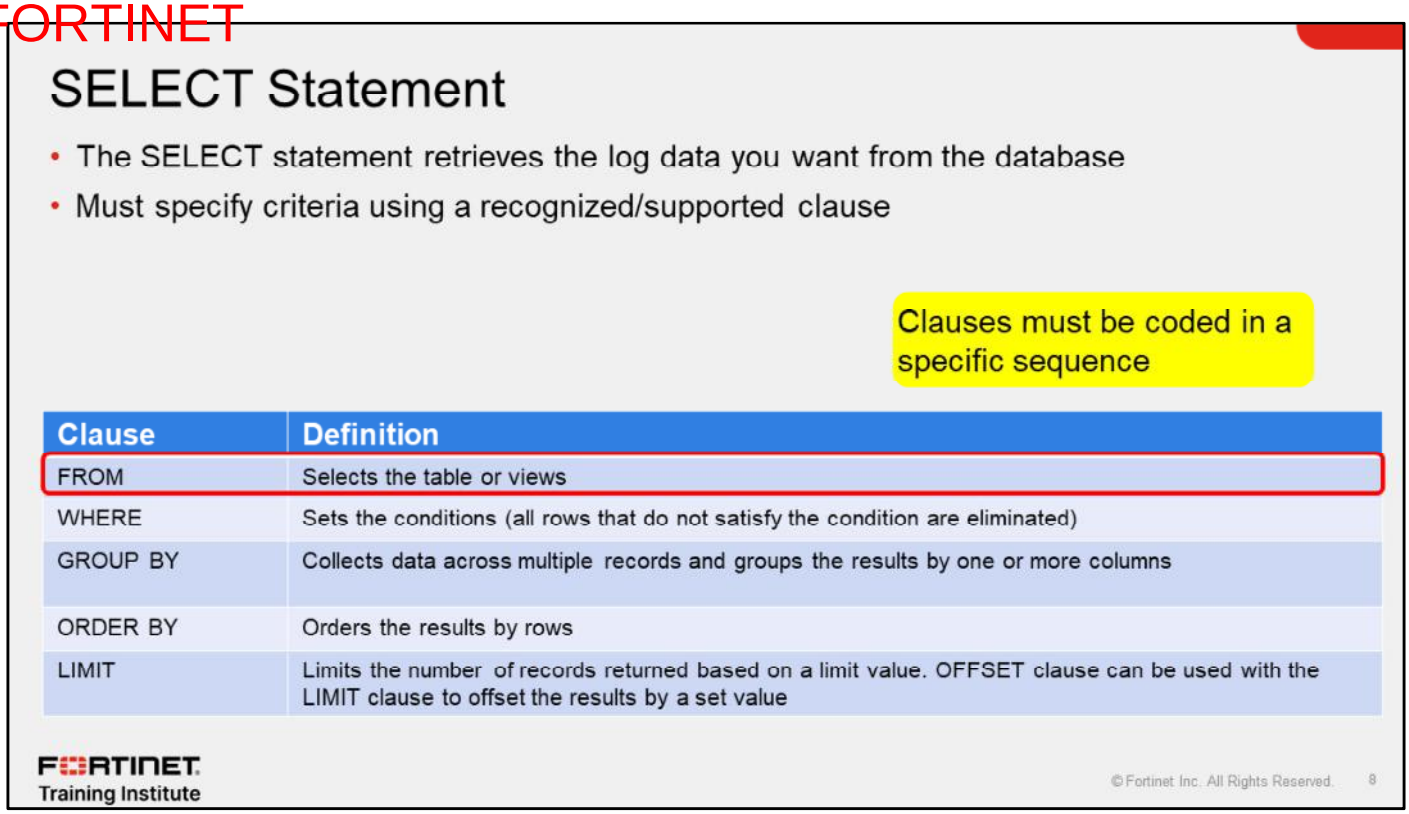
In a SQL database all information is represented as tables, and each table consists of a set of rows and columns. There are two types of tables:

- User tables, which contain information that is in the database
- System tables, which contain the database description



In order to retrieve and manipulate data in the database, you need to use data manipulation language, which is a family of syntax elements used by SQL. These syntax elements are SELECT, INSERT, UPDATE, and DELETE. These are the first words used in a query—they are the declarative verbs describing what you want done.

As far as FortiAnalyzer reports are concerned, only the SELECT statement is used. It is purely a read-only query statement that is used to retrieve data from the database.

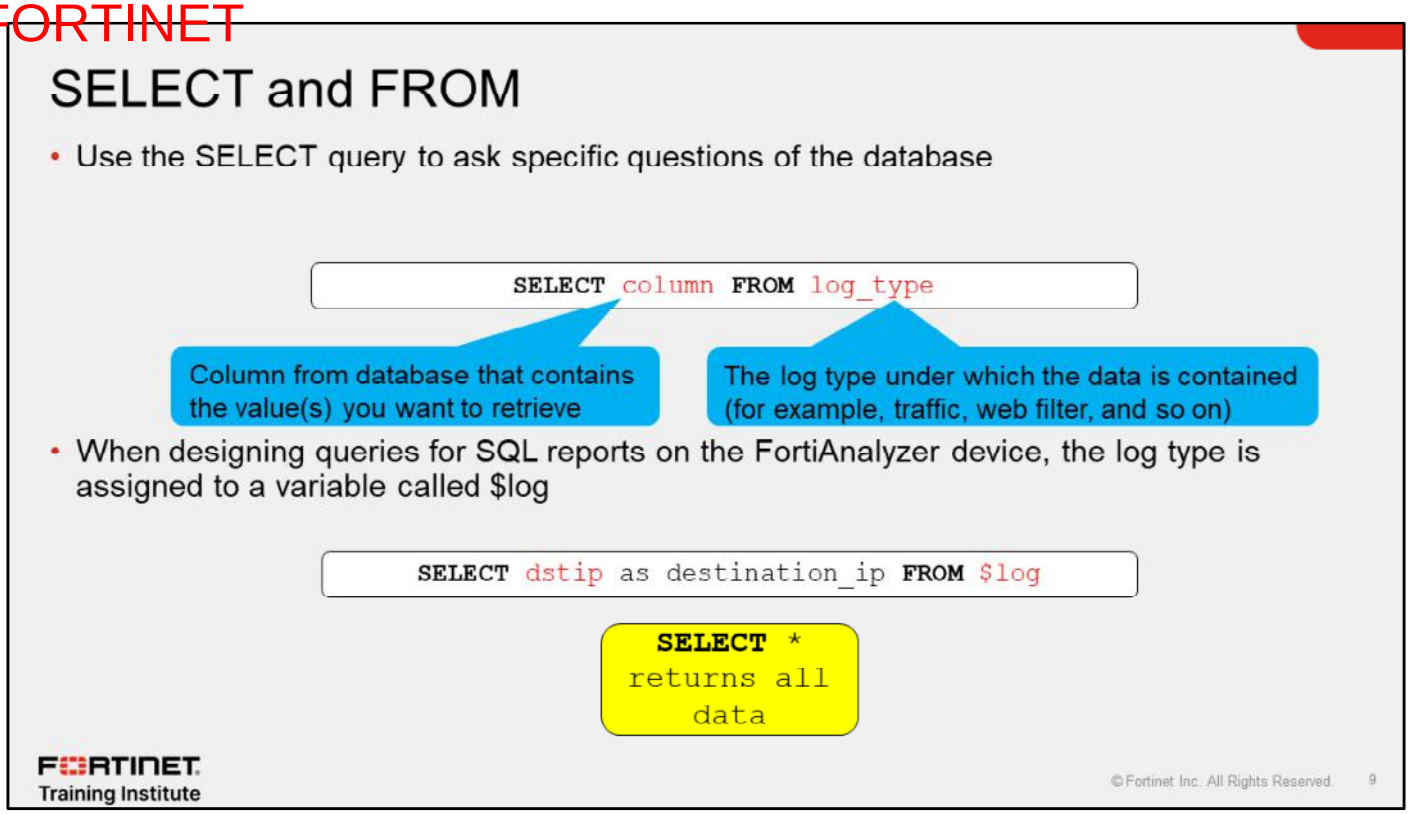


The SELECT statement is used to query the database and retrieve log data. In order to pull the data you want, you must specify the criteria. For example, let's say you want to query the database for a list of employees who work in the IT department. In order to put this criteria into a language that SQL understands, you must use a clause recognized by the SELECT statement.

The main clauses FortiAnalyzer reports use are:

- FROM, which specifies the table.
- WHERE, which specifies the conditions. All rows that do not satisfy the condition are eliminated from the output.
- GROUP BY, which collects data across multiple records and groups the results by one or more columns.
- ORDER BY, which orders the results by rows. If ORDER BY is not given, the rows are returned in whatever order the system finds the fastest to produce. And finally,
- LIMIT, which limits the number of records returned based on a specified value. OFFSET is another clause often used along with LIMIT, which offset the results by the number specified. For example, if you place a limit of three records and an offset of one, the first record that would normally be returned is skipped and instead the second, third, and fourth records (three in total) are returned.

FROM is the only mandatory clause required to form a SELECT statement; the rest of the clauses are optional and serve to filter or limit, aggregate or combine, and control the sort. It is also important to note that the clauses must be coded in a specific sequence. This is to say that following the SELECT keyword, the statement must be followed by one or more clauses in the order they appear in this table provided. For example, you cannot use the WHERE clause before the FROM clause. You do not have to use all optional clauses, but the ones you do use must be in the correct sequence.



SELECT is the first word used in any SQL query that involves FortiAnalyzer reports. This is a declarative statement that instructs the program to query the column in the database for the information you want returned. For example:

```
SELECT dstip
```

`Dstip` is the column name for destination IP in the SQL schema. Note that you can select more than one column name and you can also have the column name appear under a more user friendly name in the results table by appending the command with "`as <friendly_name_of_column>`. For example, `SELECT dstip as destination_ip`. In the results table, the values for `dstip` will appear under a column named **destination_ip**.

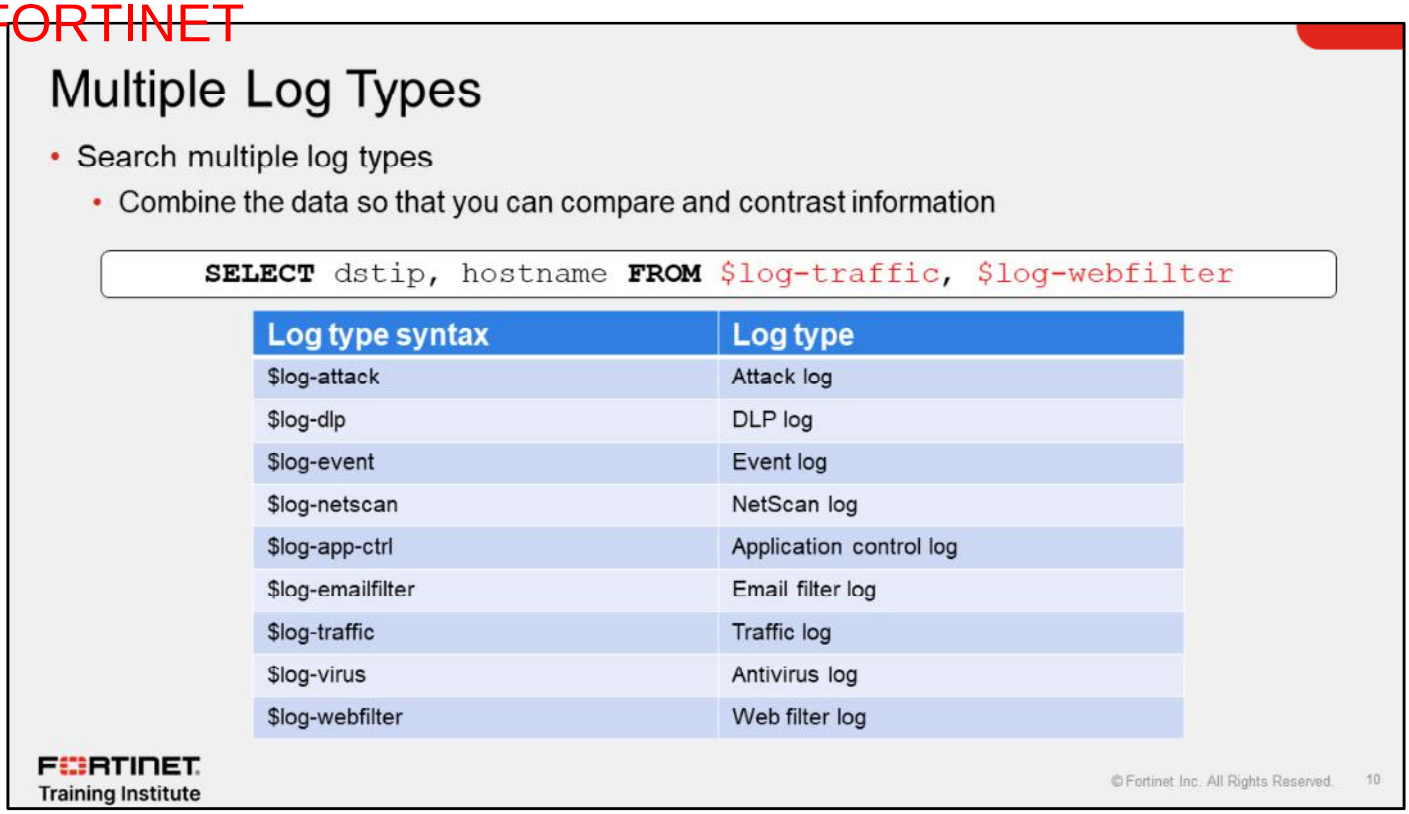
If you want to return all data, you can use the `*` symbol. For example, `SELECT *`. Though most of the time that is more information that you require.

At minimum, you must use the FROM clause with your SELECT statement. This instructs the program where the information is located.

For example:

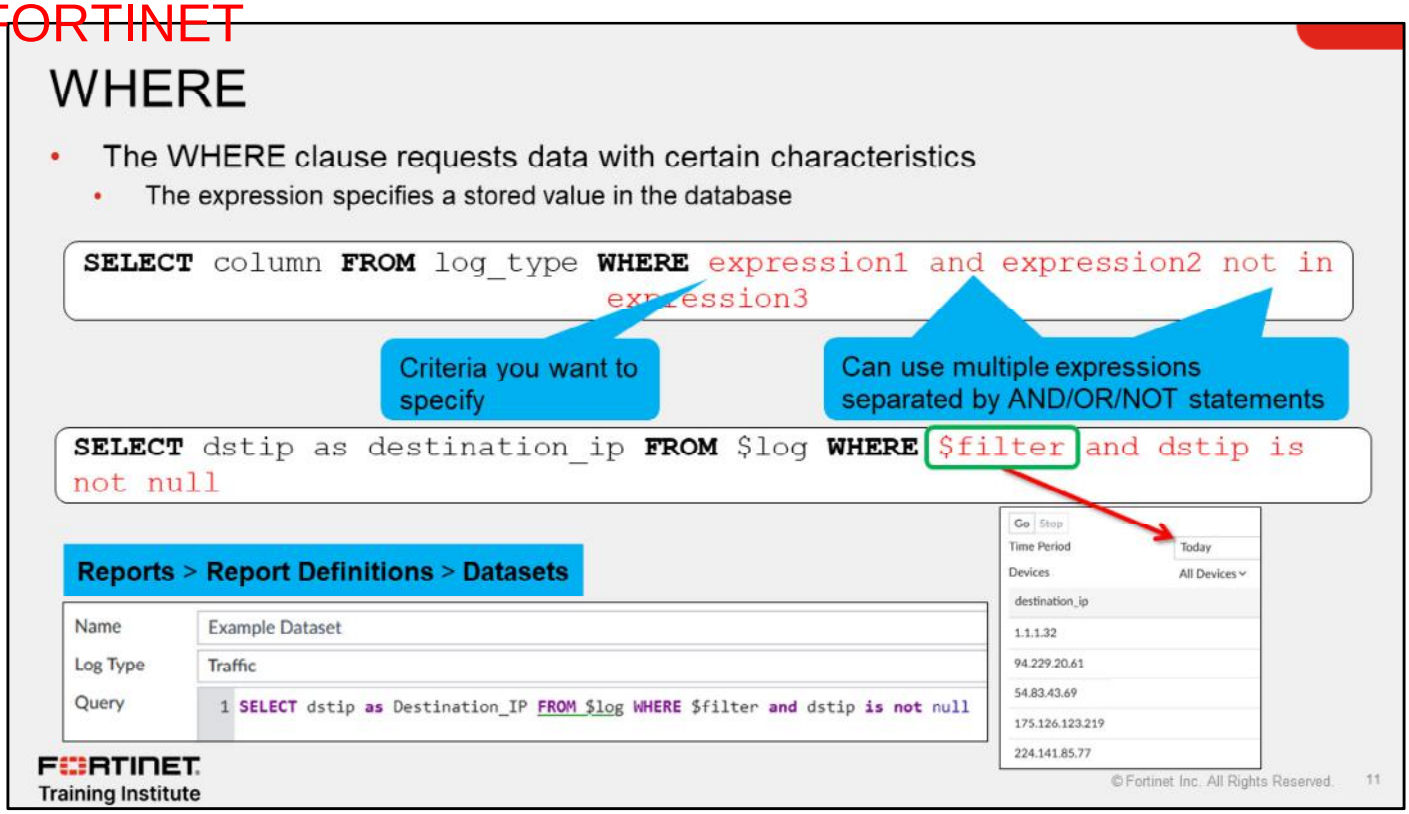
```
FROM $log
```

Here `$log` refers to the logs in the log type selected for the dataset, such as traffic logs or web filter logs.



You can search multiple log types in order to combine the data so that you can compare and contrast information. To do this, use the log type syntax associated with the specific log type. For example, if you want to search both the traffic logs and web filter logs, use:

```
FROM $log-traffic, $log-webfilter
```



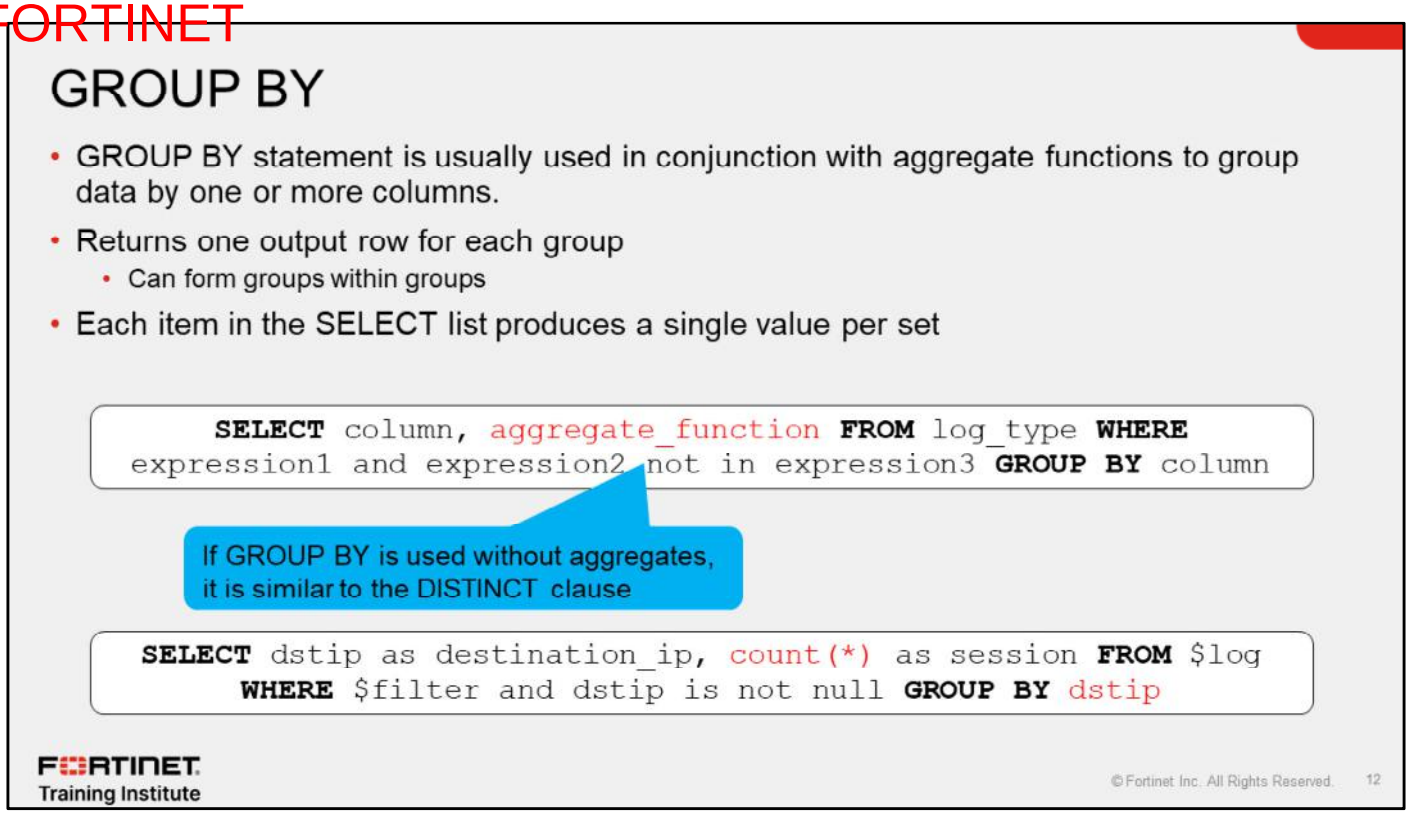
Out of all the optional clauses, the WHERE statement is really the heart of the query, because this is where you specify the criteria.

The WHERE statement must always come after the FROM statement.

In this example, the first expression is `$filter`, which is used to restrict the results to the time period you select. While the time period is not added to the query itself, it is specified by way of a drop-down box when creating the dataset through the FortiAnalyzer GUI.

The second expression is `dstip`, which is the destination IP, while the third expression is NULL.

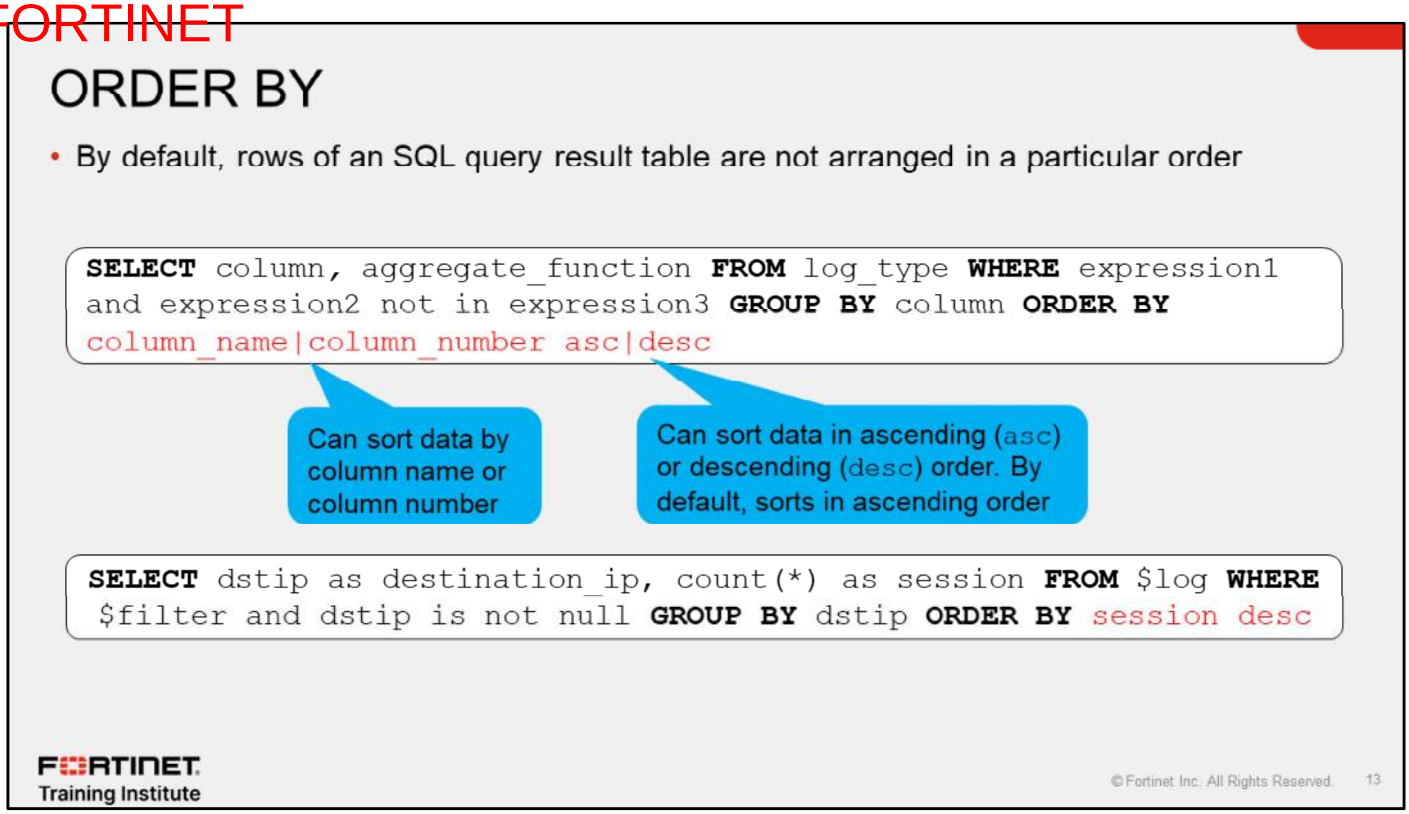
SQL supports logic operators as well, so you can use AND/OR/NOT statements in order to build out the query. Operators are also covered in this material.



The GROUP BY clause is used to create one output row for each group. It is usually used with an aggregate function within the SELECT statement. We will cover aggregate functions later, but essentially they perform a calculation on a set of values and return a single value. If it is not used with an aggregate function, it is similar to the DISTINCT clause, in that it removes duplicates from the result set of a SELECT statement.

In this example, the GROUP BY clause is use with an aggregate function. The aggregate function is `count(*)`, which selects all rows in a table, even if some columns contain a NULL value.

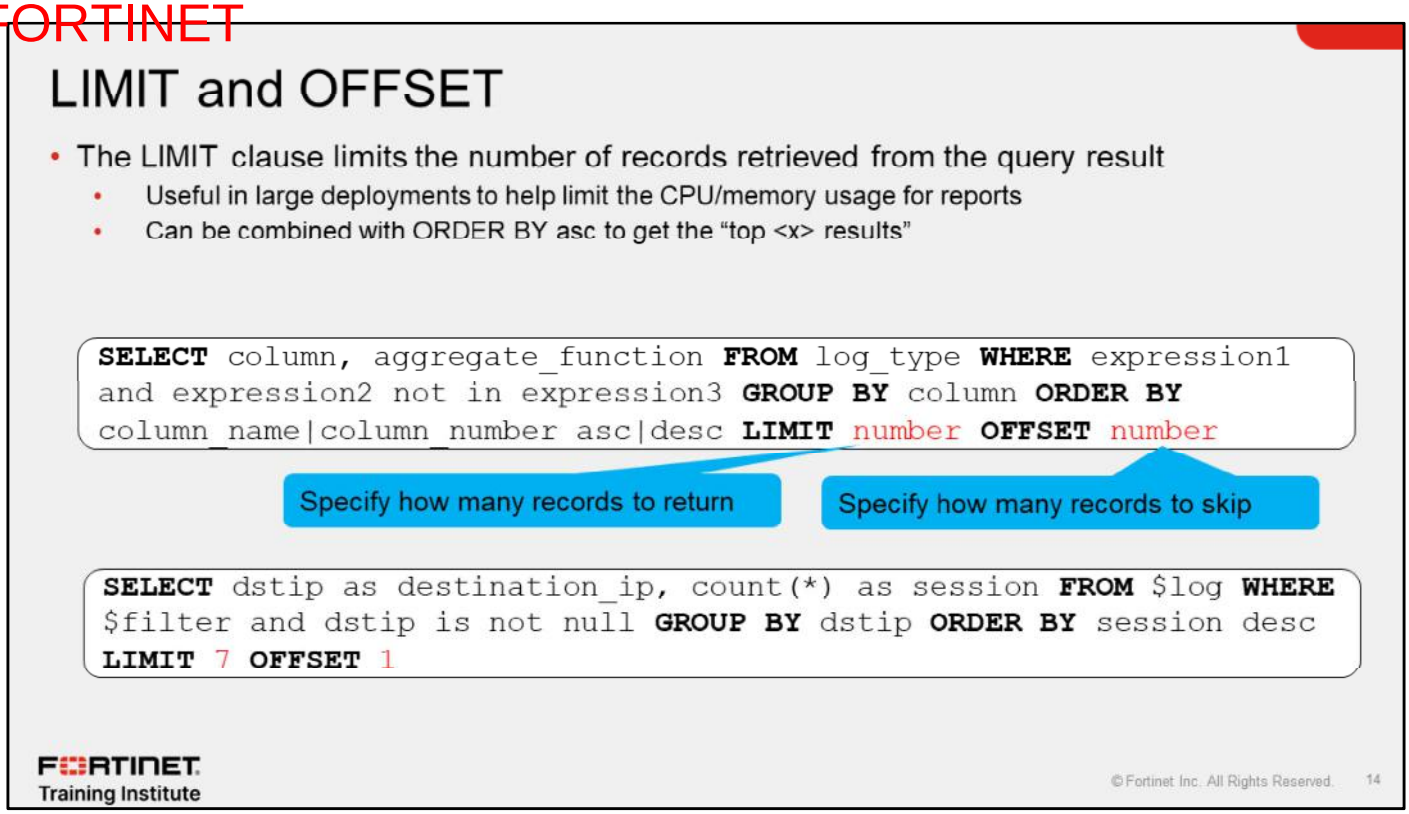
In this example, we are grouping by `dstip` (destination IP).



ORDER BY is a clause that allows you to sort queries by column name or column number. By default, rows of an SQL query result table are not arranged in a particular order, so you can use the ORDER BY clause to sort column values in either ascending (`asc`) or descending (`desc`) order. If you use this clause and do not specify ascending or descending, the default is ascending.

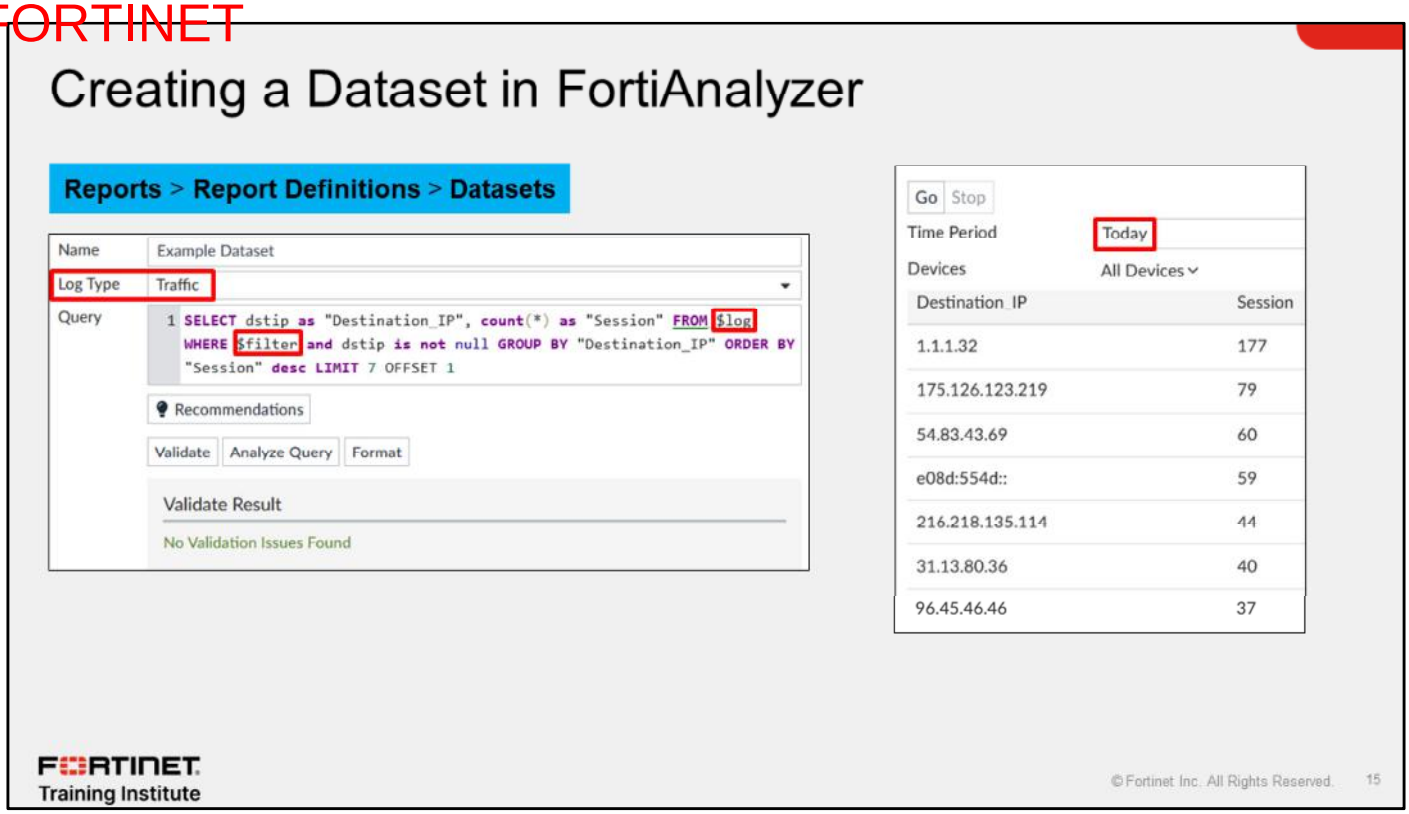
You can order multiple columns and specify different sort orders for each. For example, you can sort one column in ascending order and another column in descending order.

In this example, we are ordering by session in descending order.



By default, all results that satisfy the conditions specified in the query are returned. However, if you want to retrieve only a subset of records, you can place a limit on the number of records returned. To do this, use the LIMIT clause and specify the number of results you want. For example, `LIMIT 7`. Applying limits can ensure that the query doesn't use unnecessary CPU or memory, especially if you have a large-scale deployment with lots of devices logging to FortiAnalyzer. You can also combine LIMIT with ORDER BY asc to get the "top <x> results" (or desc for the "bottom <x> results").

In conjunction with the LIMIT clause, you can use the OFFSET clause. This offsets the results by a set value. For example, if you place a limit of seven records and an offset of one, the first record that would normally be returned is skipped and two through eight are returned instead.

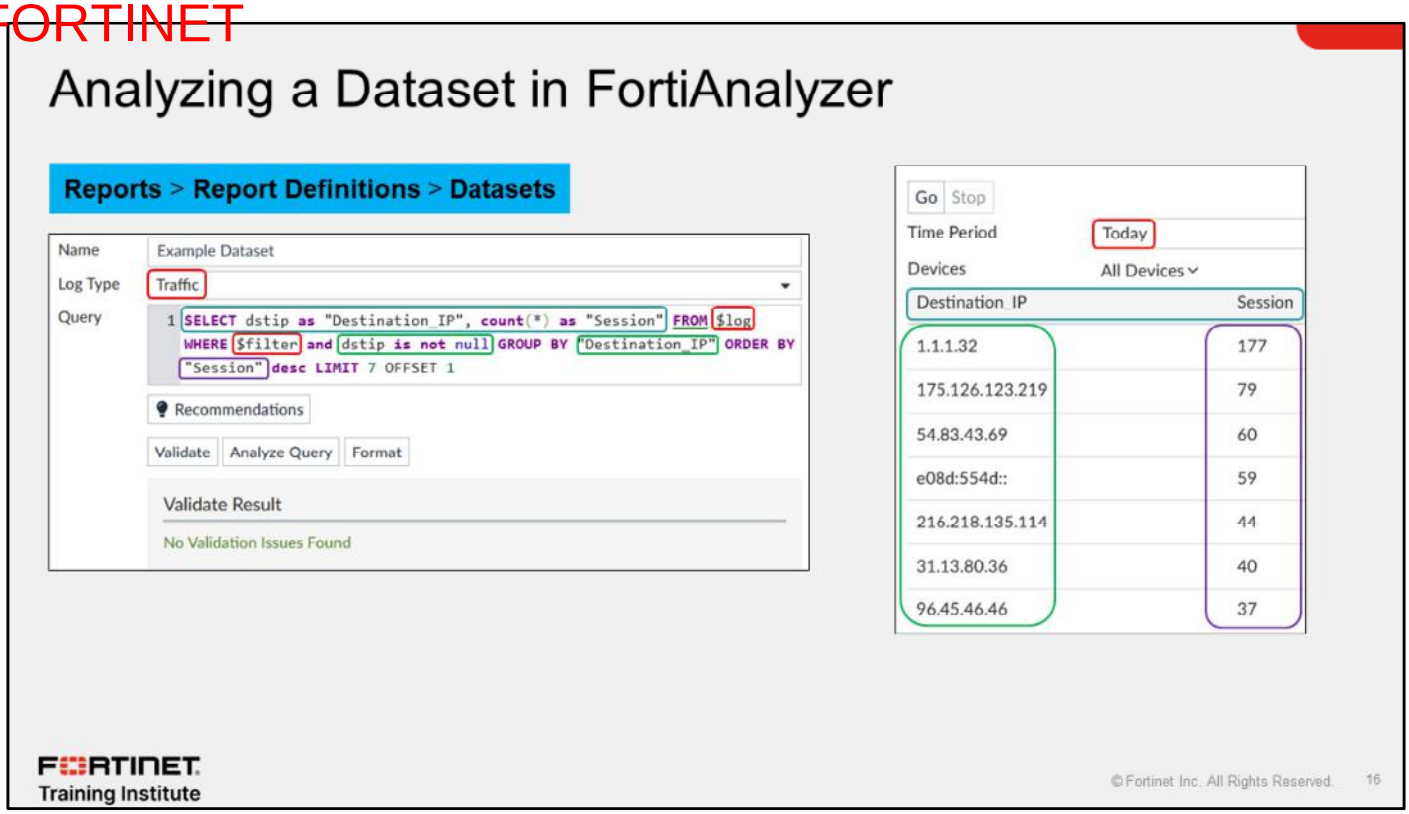


As you have been learning about the main SQL clauses, you have also been forming a full dataset query along the way. To see a visual of the query, you can use the dataset **Go** feature in the GUI. The feature is intended to test or modify a query in order to get the specific output you want.

Ensure you select the log type for the query. The query uses the generic `$log`, but it references the log type specified in the **Log Type** field (in this example, **Traffic**). You can enter the specific log type in the query instead (for example, `$log-traffic`). If you want to view this query on a different log type later, it's less risky and easier to change your selection in the **Log Type** field than in the actual dataset query itself.

You must also specify the device or devices on which to use this query. In this example, **All Devices** is specified.

You must also specify a time period for this query. You can use the `$filter` expression with the WHERE clause to limit the results to the time period that you specify in the **Time Period** field.



Now align the written query with the visual results to fully understand how the query is interpreted by FortiAnalyzer.

`SELECT dstip as "Destination_IP", count(*) as "Session"`: This says, select the destination IP address and call the column "`Destination_IP`". Select the count (all data) and call the column "`Session`".

`FROM $log`: This says, query the traffic log for the data, which is specified in the **Log Type** field.

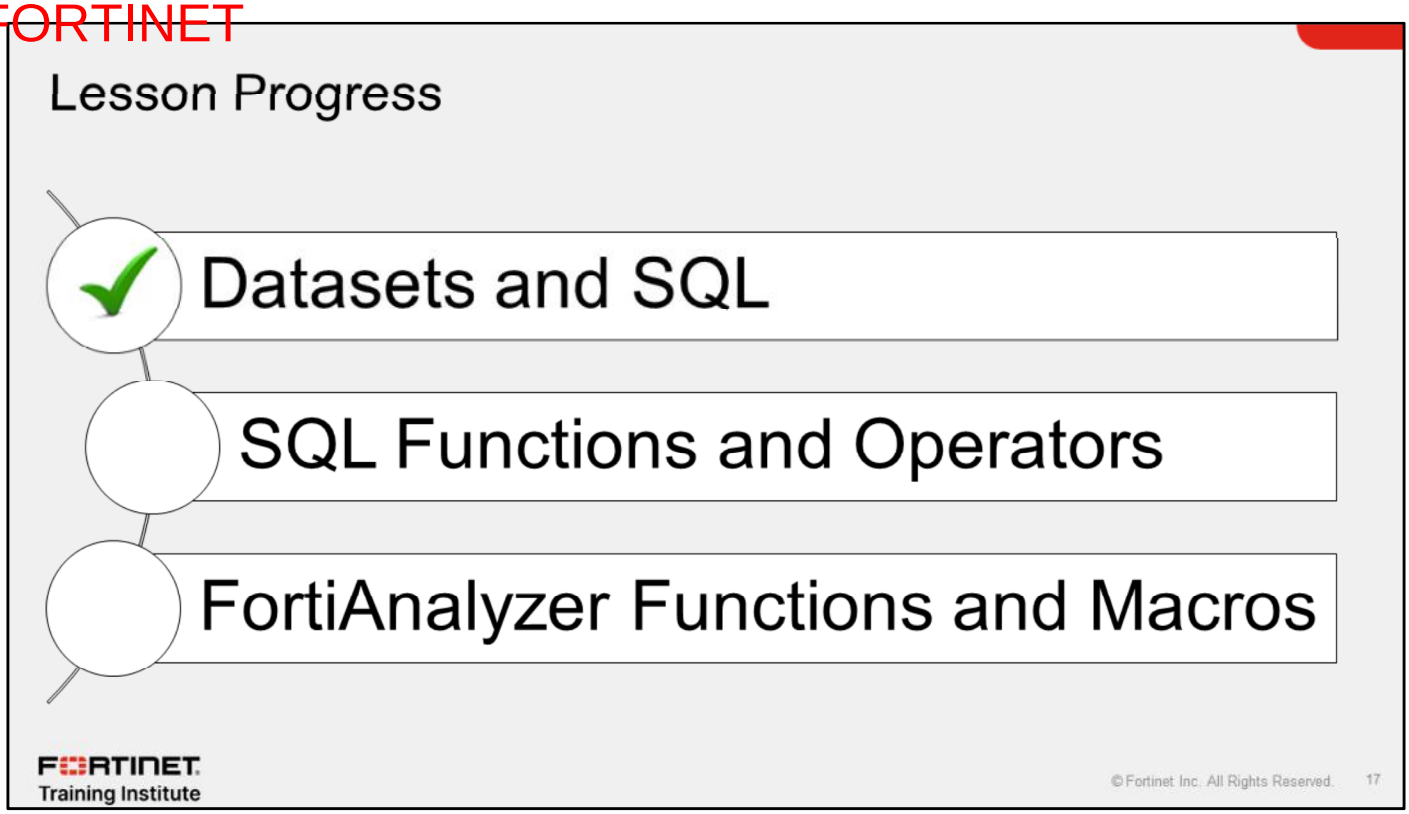
`WHERE $filter and dstip is not null`: This says, limit the results to the time period specified, which is **Today**, according to the selection in the **Time Period** field, and provide only the destination IP addresses that are not null. Note that "null" represents unknown data—it does not represent zero.

`GROUP BY dstip`: This says, group the results by destination IP. You previously specified that the destination IP should be put in a column called "`Destination_IP`".

`ORDER BY session desc`: This says, order the results by session in descending order. Note that the results go from high (177) to low (37).

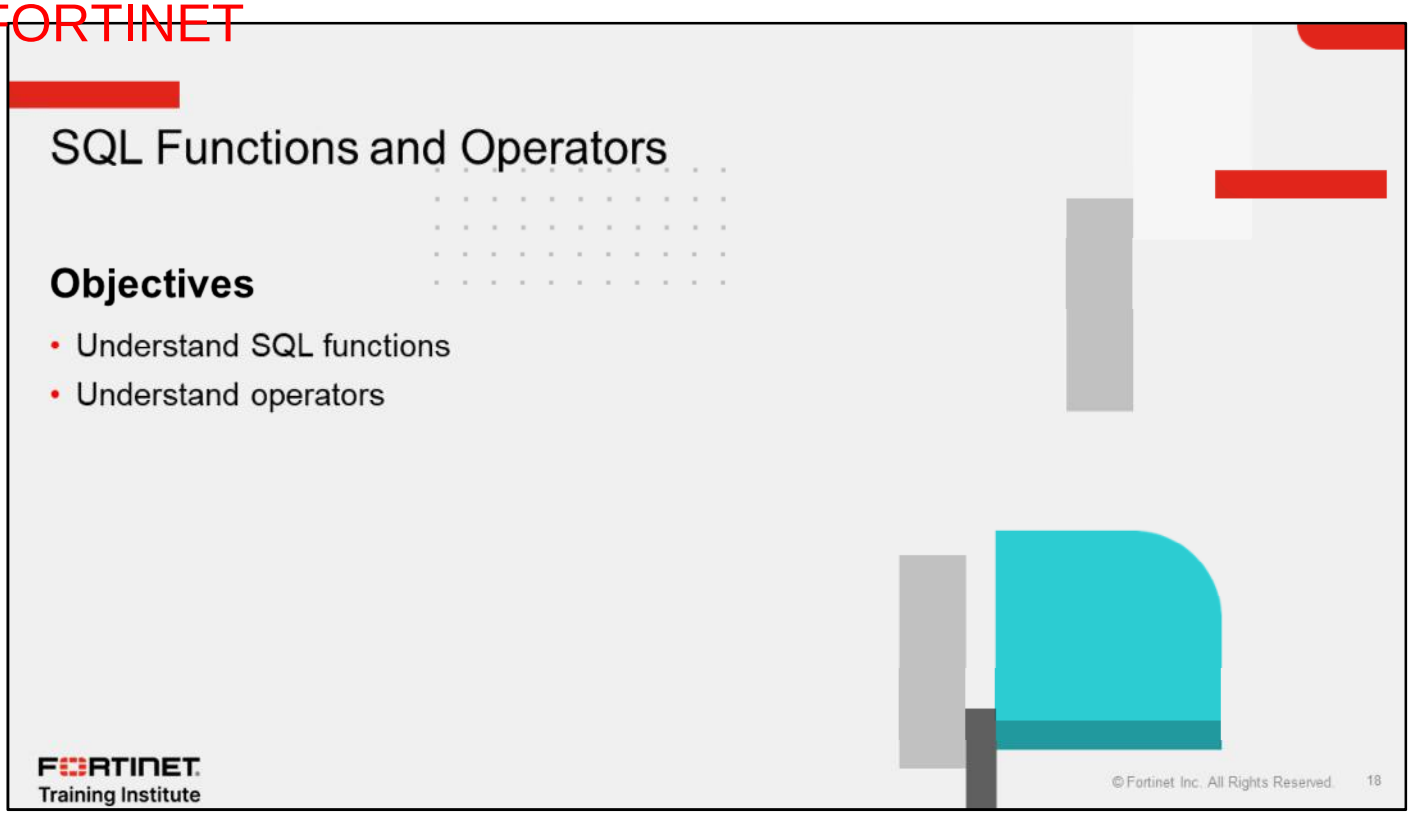
`LIMIT 7`: This says, provide only the first seven results.

`OFFSET 1`: This says, skip the first result, but still limit the results to the next seven (that is, two through eight).

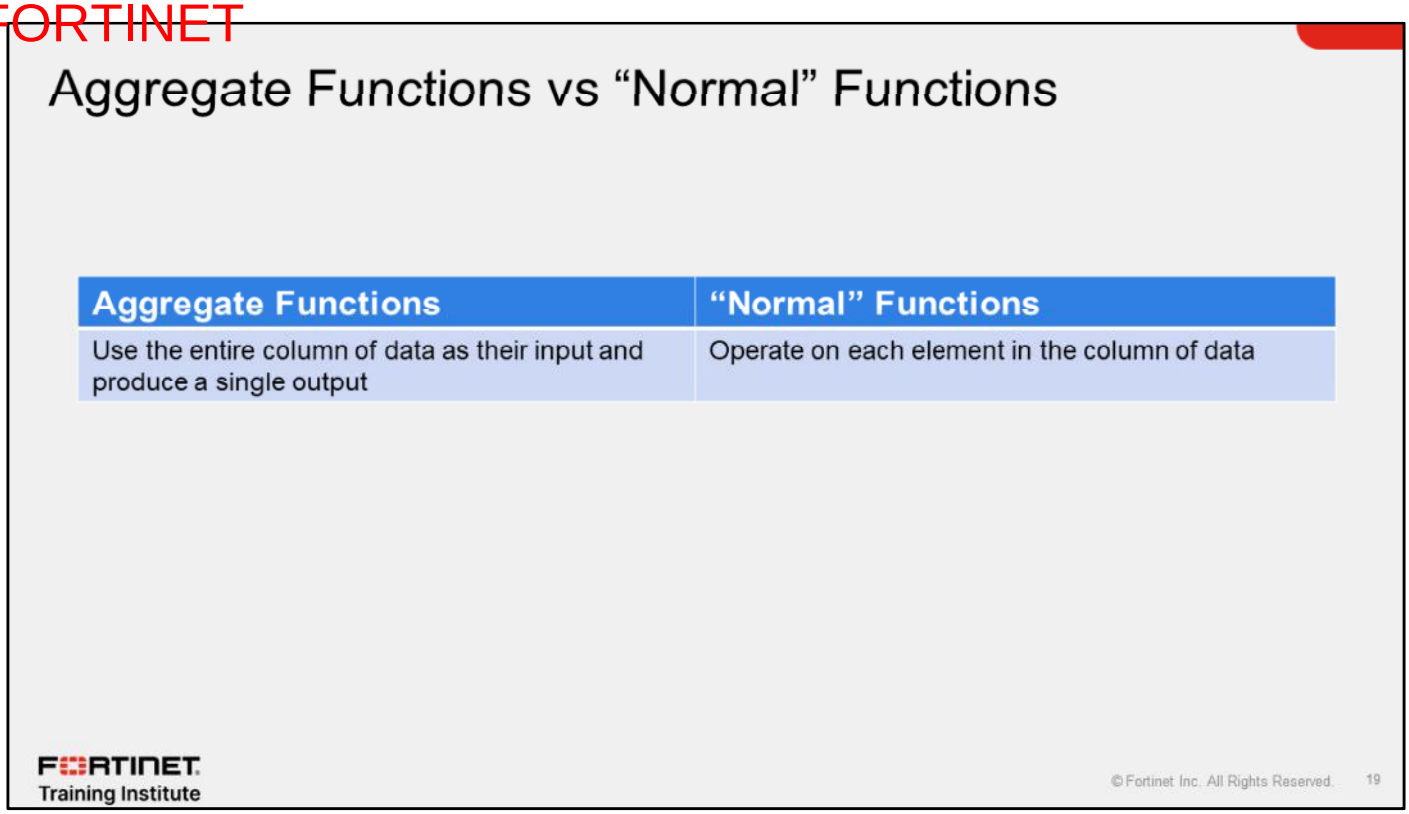


Good job! You now understand datasets and SQL.

Now, you will learn about SQL functions and operators.

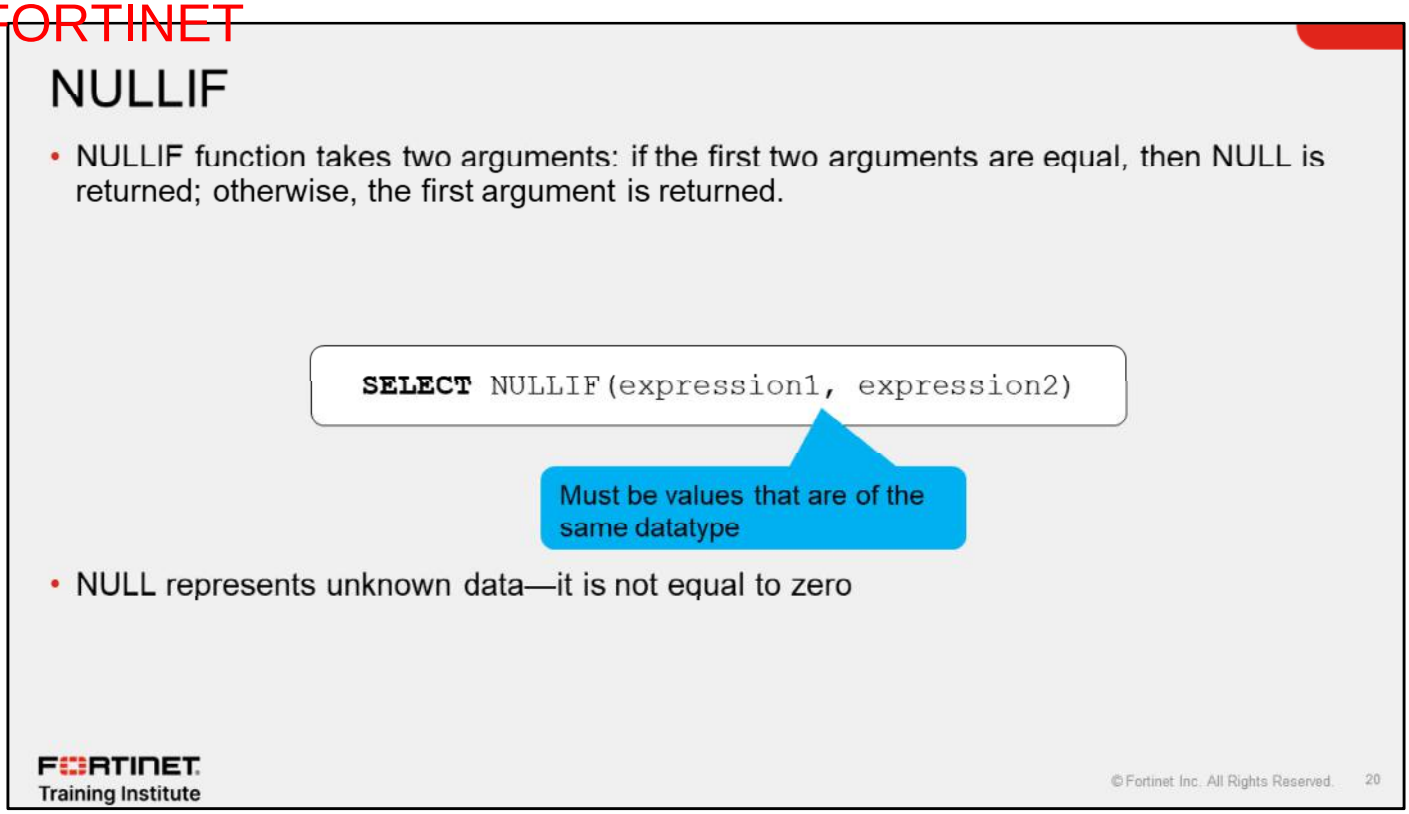


This section covers a few of the most common functions and operators used in FortiAnalyzer datasets—it is not intended as a complete and exhaustive list.

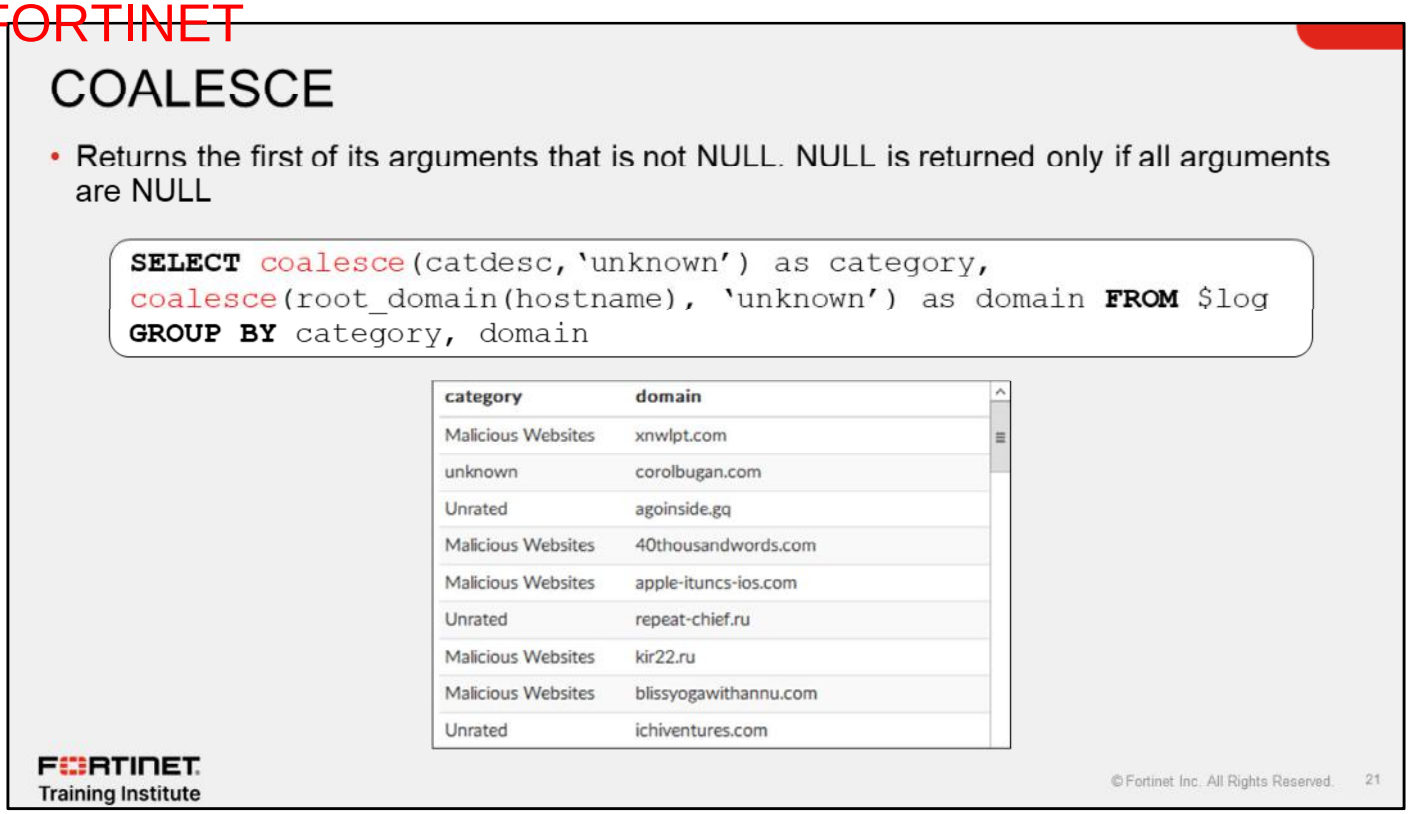


SQL has two types of functions: aggregate functions and “normal” functions.

Aggregate functions use the entire column of data as their input and produce a single output. “Normal” functions operate on each element in the column of data.



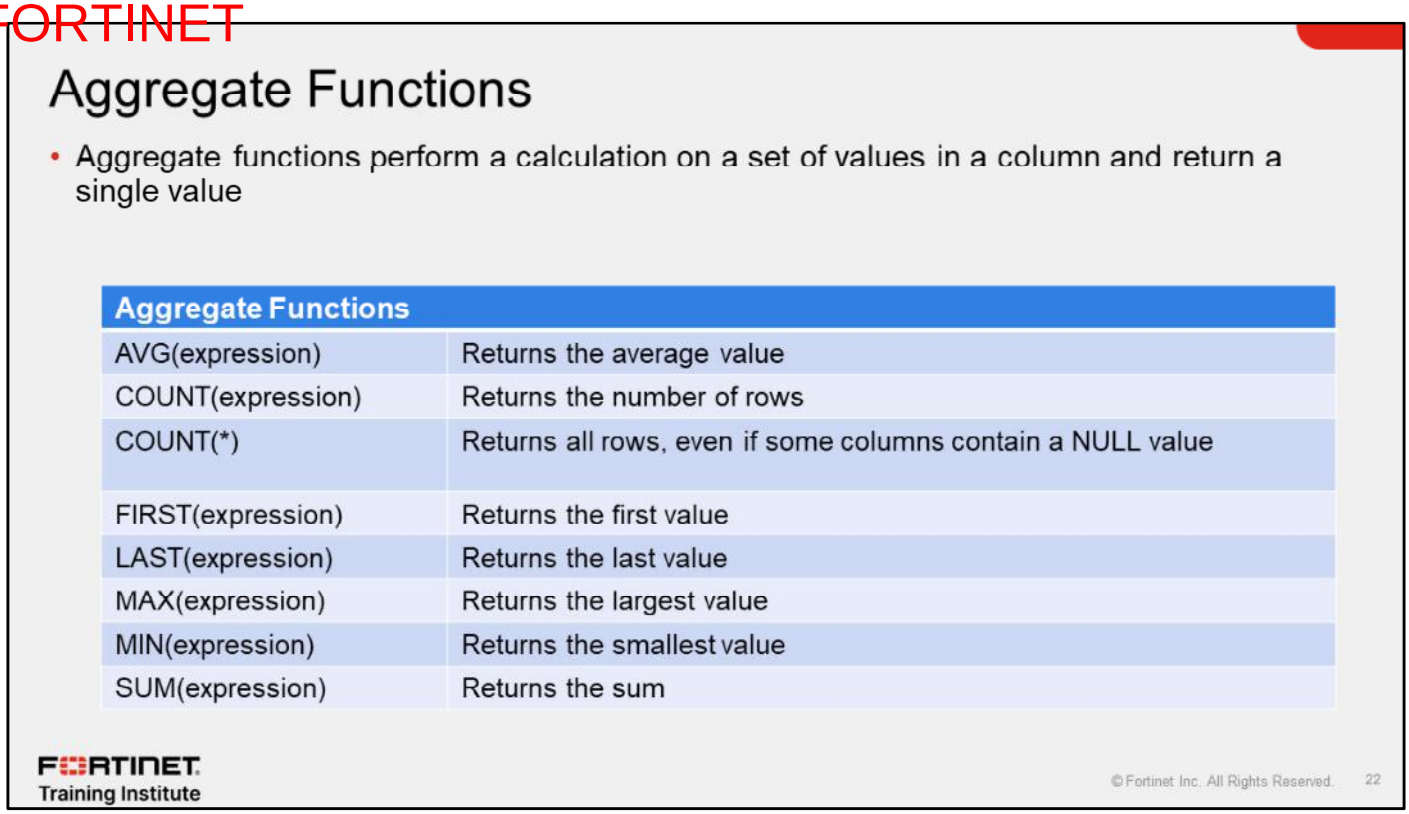
One common function used in FortiAnalyzer datasets is NULLIF. The NULLIF function takes two arguments. If the first two arguments are equal, then NULL is returned; otherwise, the first argument is returned. Note that NULL represents unknown data—it does not represent zero.



Another common function used in FortiAnalyzer datasets is COALSECE. The COALESCE function returns the first non-NULL expression among its arguments. Null is returned only if all arguments are null. It is often used to substitute a default value for null values when data is retrieved for display.

COALESCE is used with the SELECT statement. It takes one or more expressions as an argument. The values do not have to be string data types—they can be any data type (and also different data types). The syntax is:

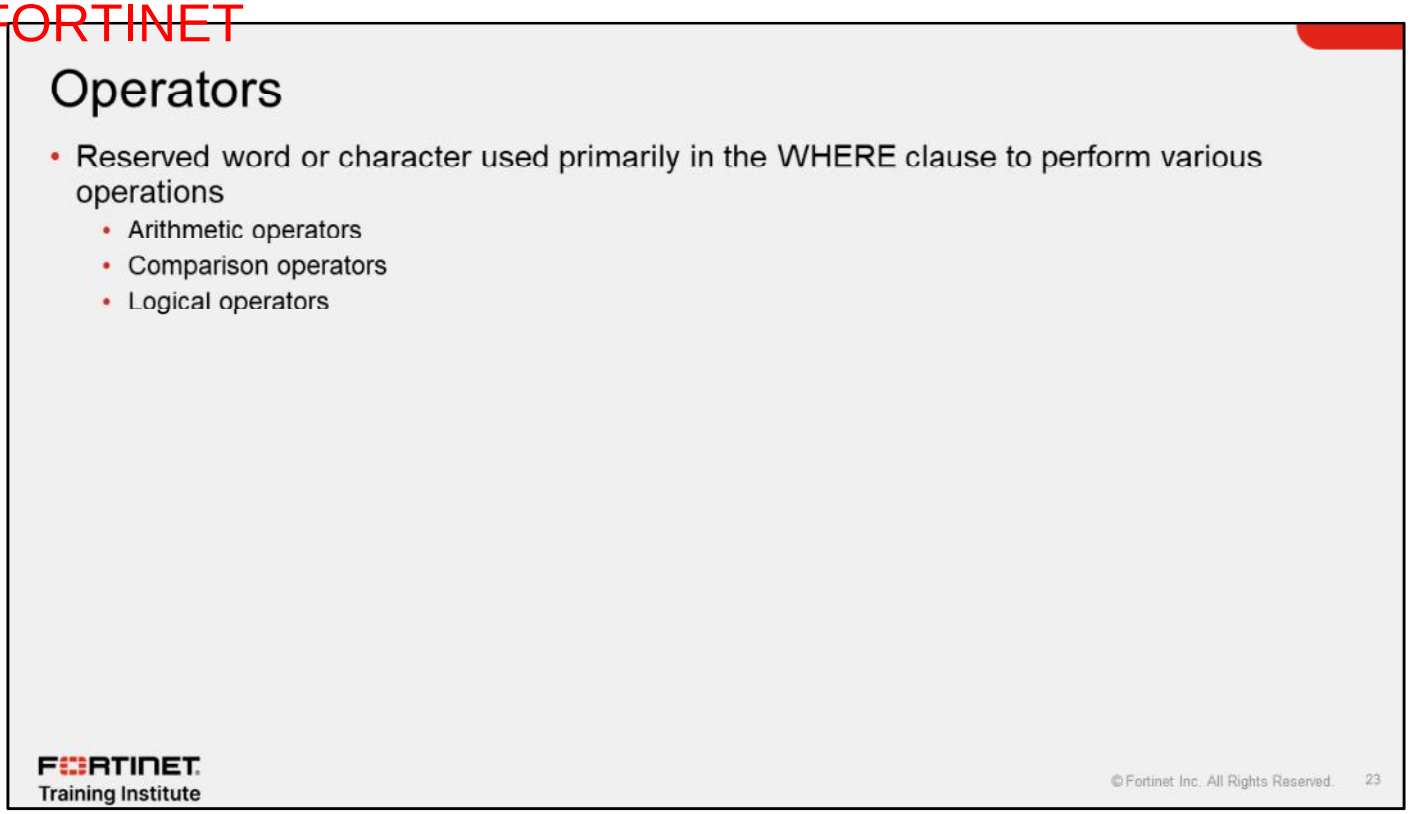
```
COALESCE (expression 1, expression 2, …)
```



Aggregate functions are a special category with different rules, as they operate on entire columns of data instead of discrete values. These functions perform a calculation on a set of values in a column and returns a single value. Although aggregate functions are usually used in conjunction with the GROUP BY clause, these functions can be used on their own in a SELECT statement.

This table includes a list of aggregate functions used in SQL. All can take an expression as an argument and ignore null values, except for count. Count can take an asterisk as an argument. The asterisk in this case means all rows are returned, even if some columns contain a NULL value.

An example of an expression used with an aggregate function is `SELECT count(unauthuser)`. This returns the number of unauthorized users.



An operator is a reserved word or a character used primarily in an SQL statement's WHERE clause to perform various operations.

There are three types of operators:

- Arithmetic operators
- Comparison operators
- Logical operators

Arithmetic Operators

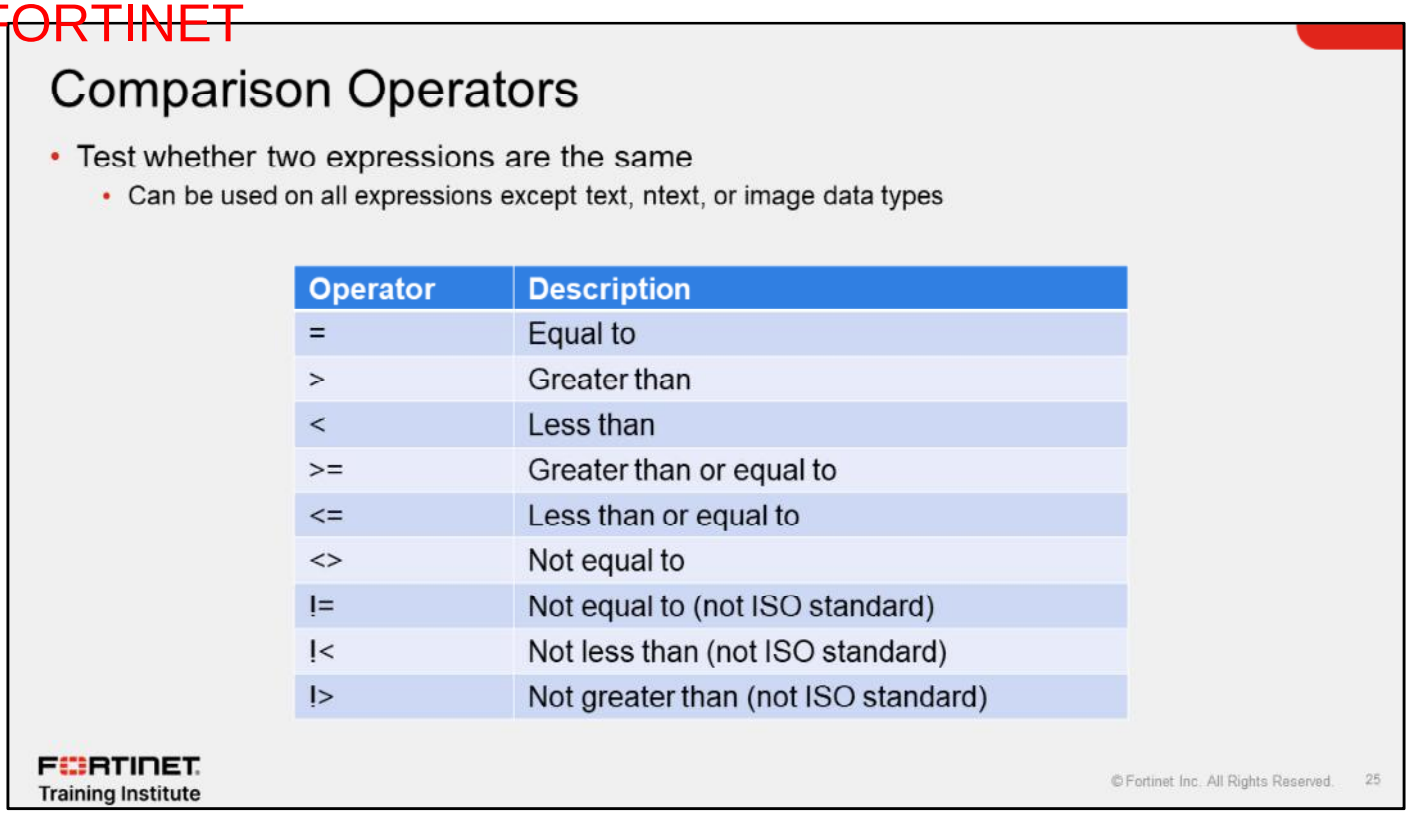
- Perform mathematical operations on two expressions of one or more of the data types of the numeric data type category

Operator	Description
+	Addition: Adds values on either side of the operator
-	Subtraction: Subtracts right hand operand from left hand operand
*	Multiplication: Multiplies values on either side of the operator
/	Division: Divides left hand operand by right hand operand
%	Modulus: Divides left hand operand by right hand operand and returns remainder

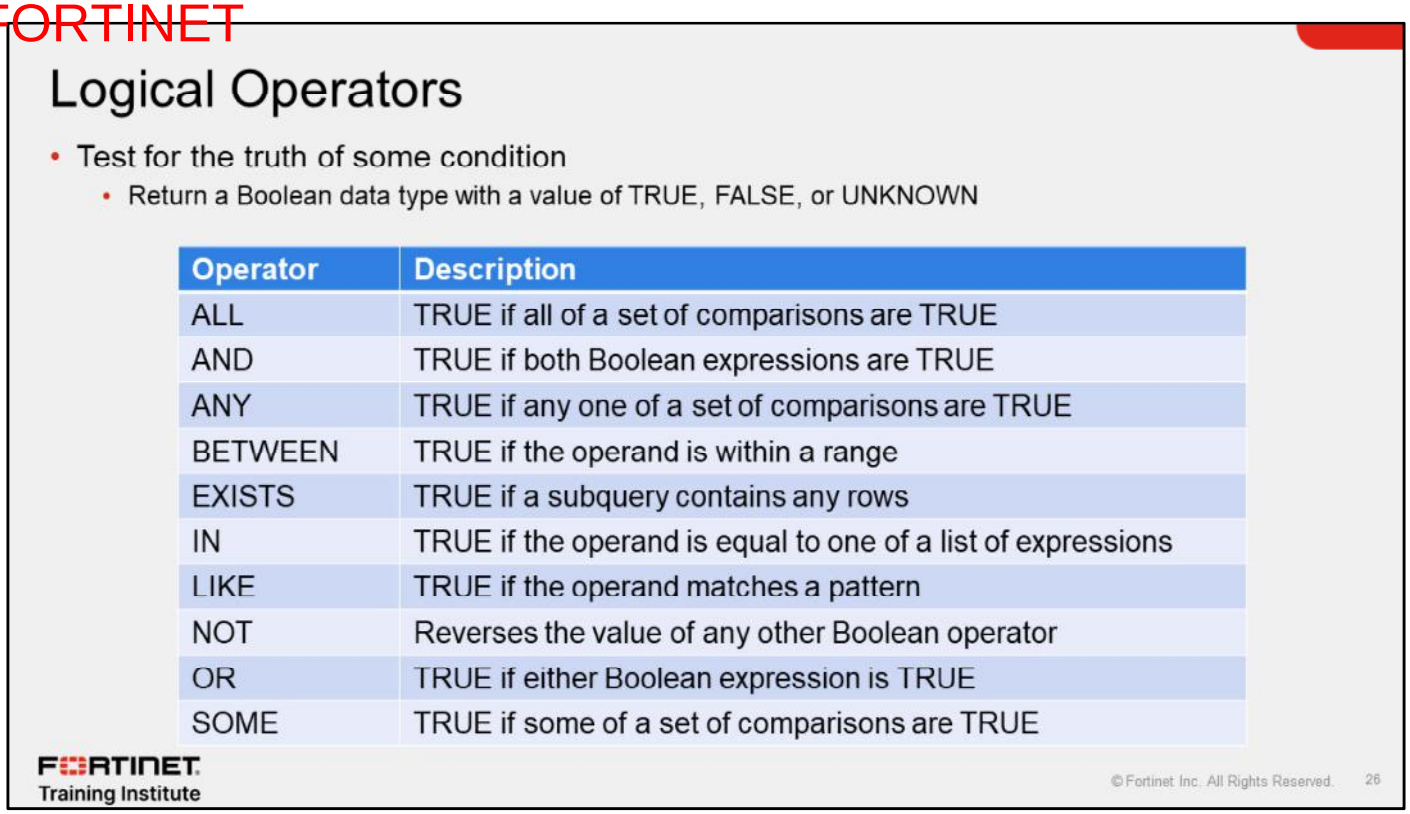
FORTINET Training Institute

 24

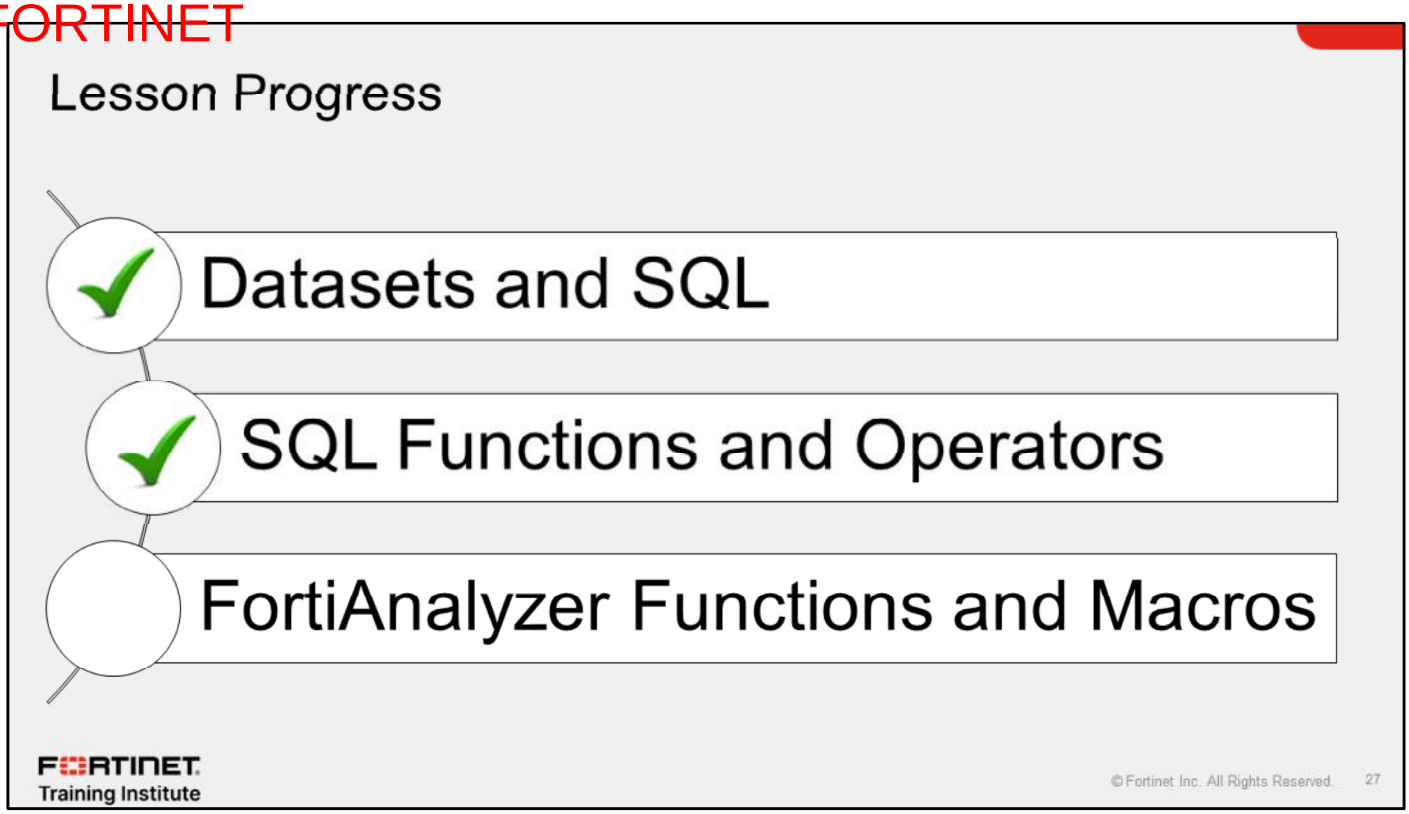
Here are some examples of arithmetic operators. Arithmetic operators perform mathematical operations on two expressions of one or more of the data types of the numeric data type category.



Here are some examples of comparison operators. Comparison operators test whether two expressions are the same and can be used on all expressions except expressions of the text, ntext, or image data types.

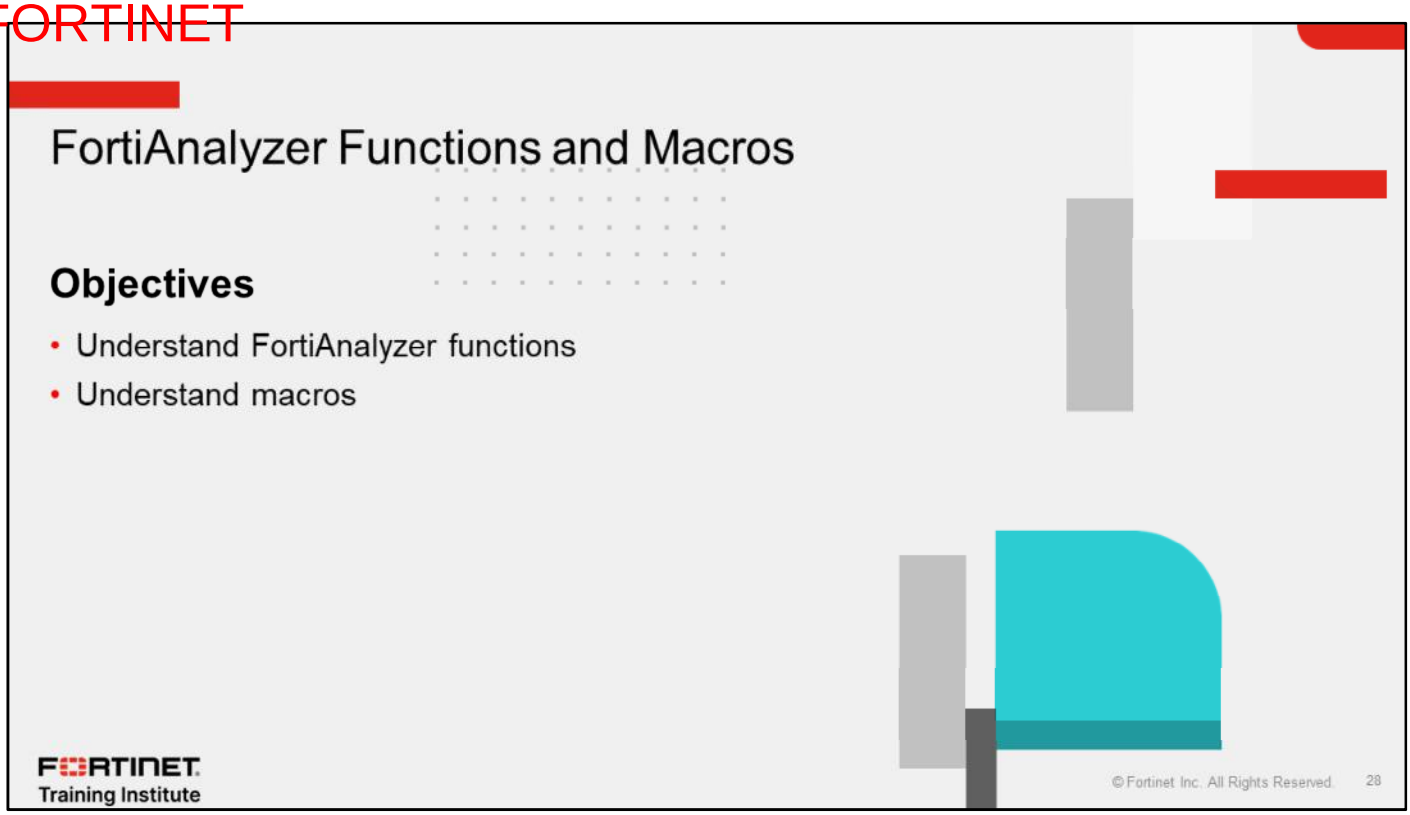


Here are some examples of logical operators. Logical operators test for the truth of a condition. Like comparison operators, they return a Boolean data type with a value of TRUE, FALSE, or UNKNOWN.



Good job! You now understand SQL functions and operators.

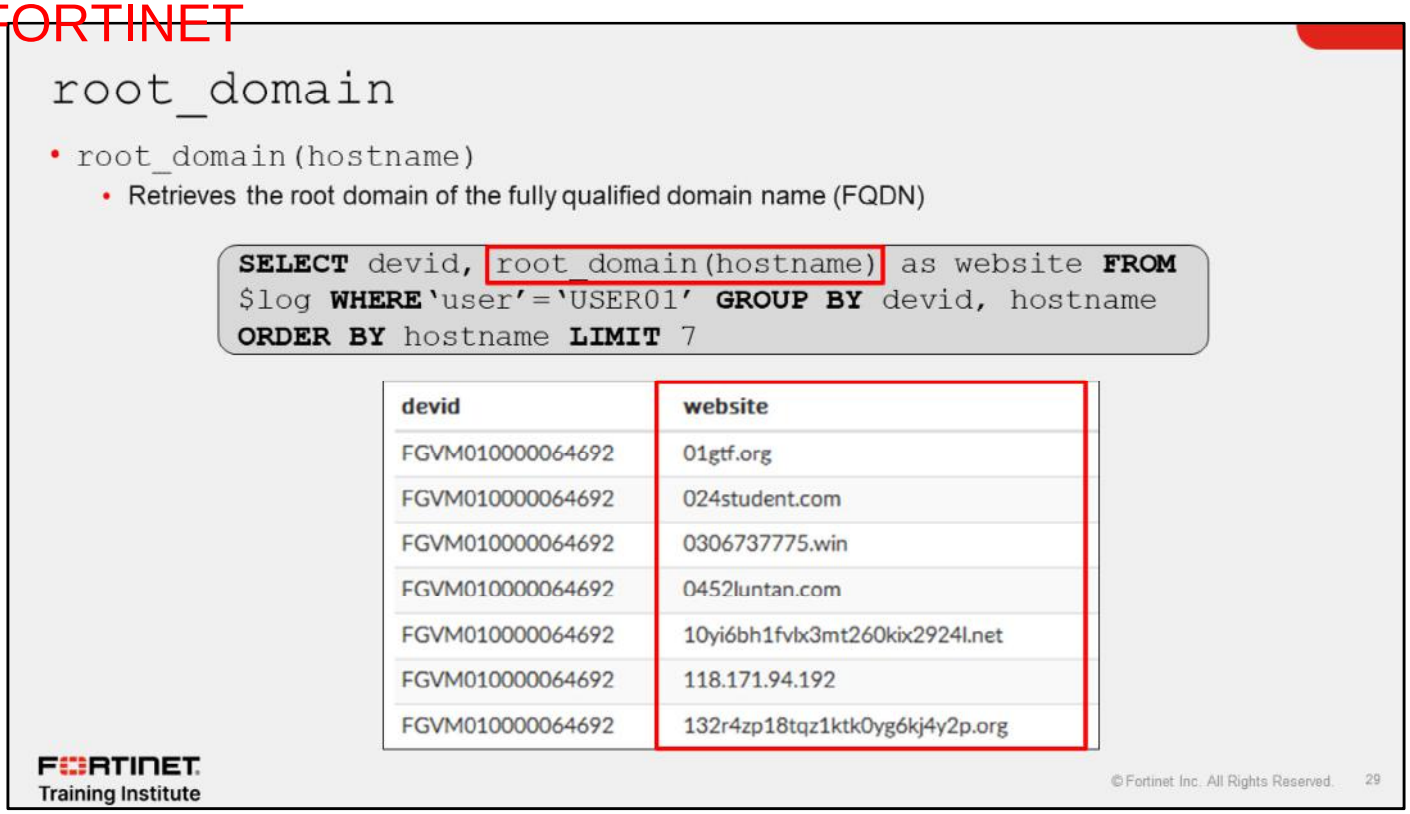
Now, you will learn about FortiAnalyzer functions and macros.



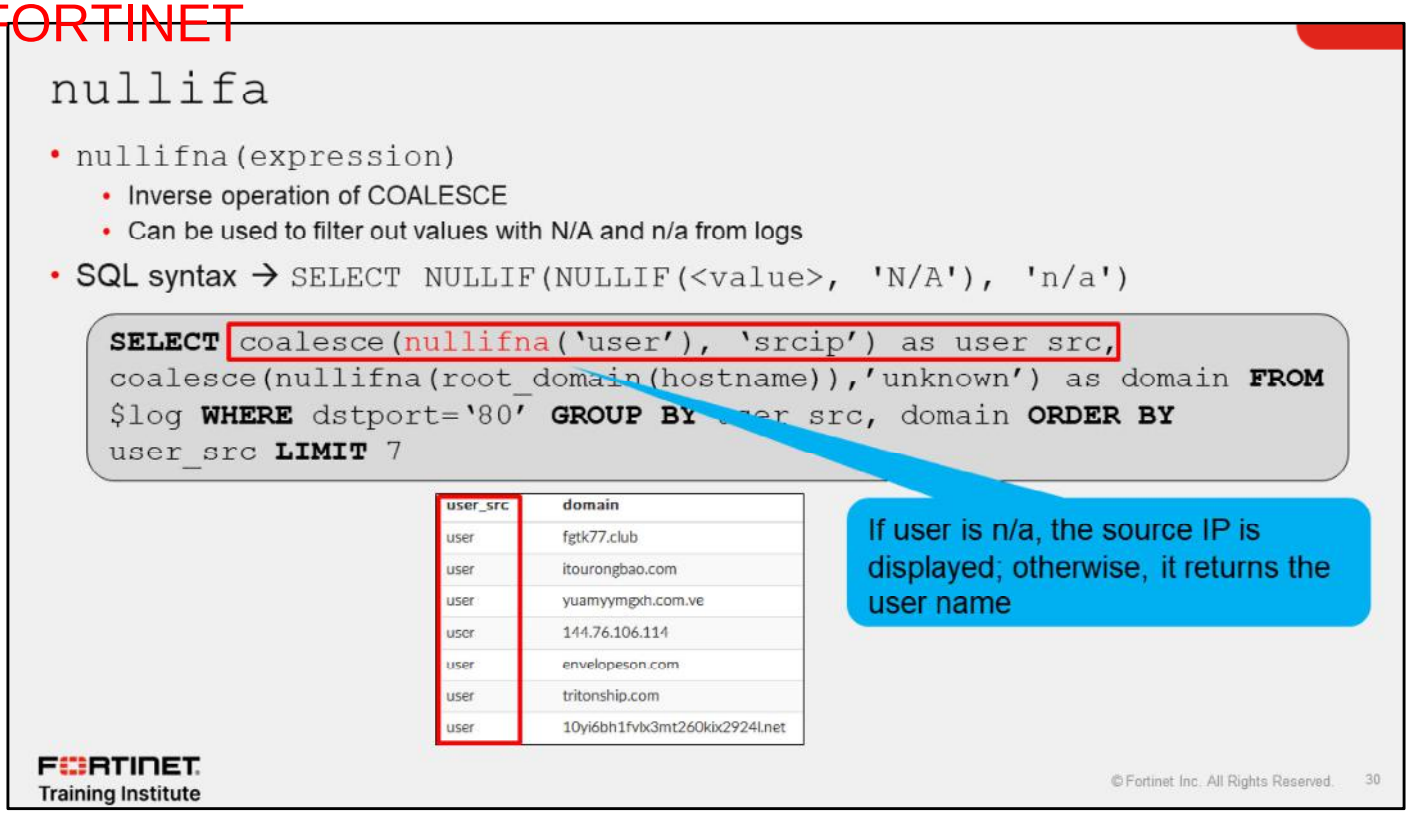
This section covers FortiAnalyzer functions and macros.

FortiAnalyzer includes some built-in functions that are based on known SQL functions, but scripted differently.

FortiAnalyzer also includes macros, which are best described as lengthy or complex SQL statements scripted more simplistically. An SQL macro can be used anywhere in a query where an ordinary SQL expression can be used.

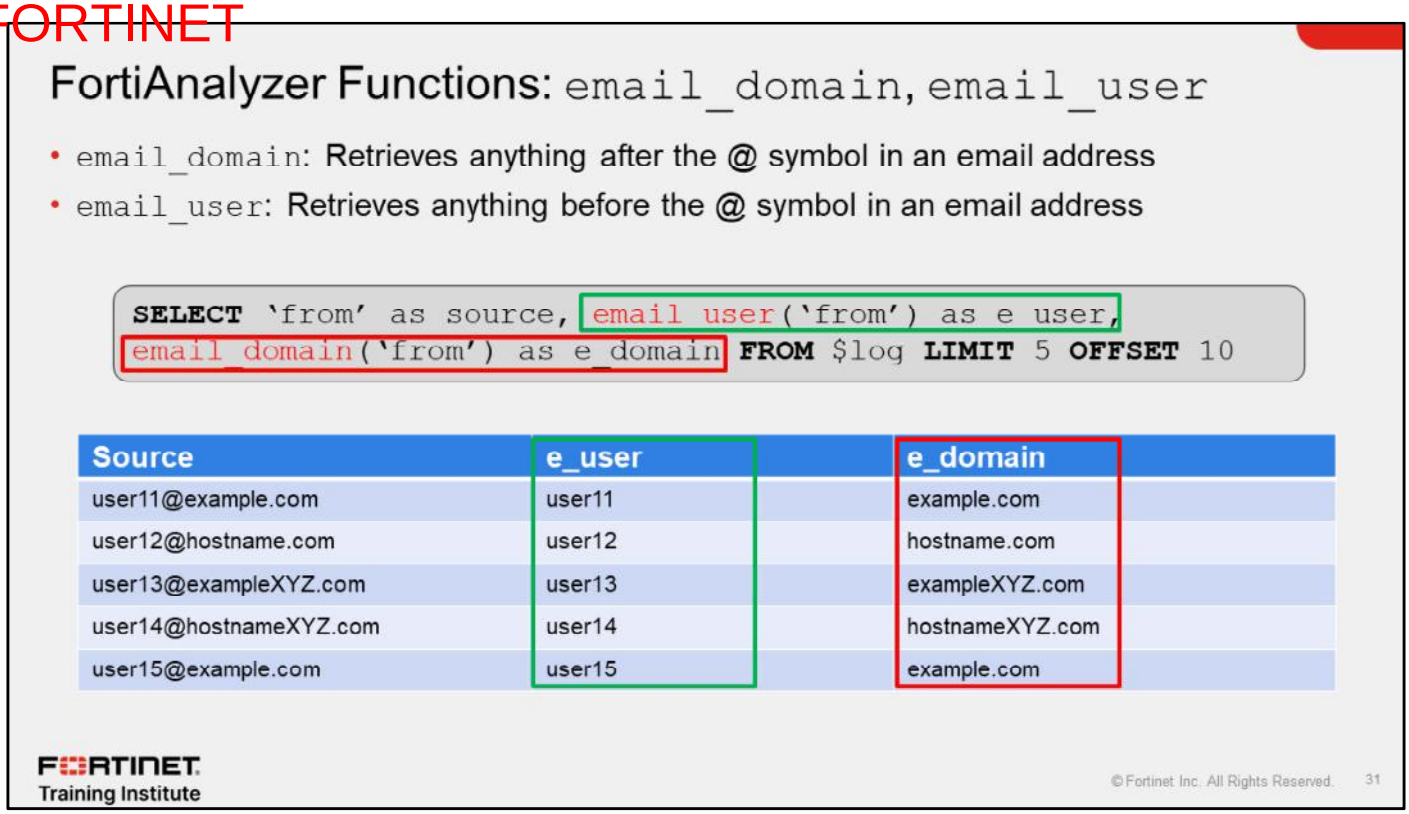


One FortiAnalyzer-specific function is `root_domain(hostname)`. This provides the root domain of the fully qualified domain name. As specified by the query, in this example `root_domain(hostname)` is listed under the **website** column in ascending order. Unless otherwise specified, ascending order is the default for the ORDER BY clause.



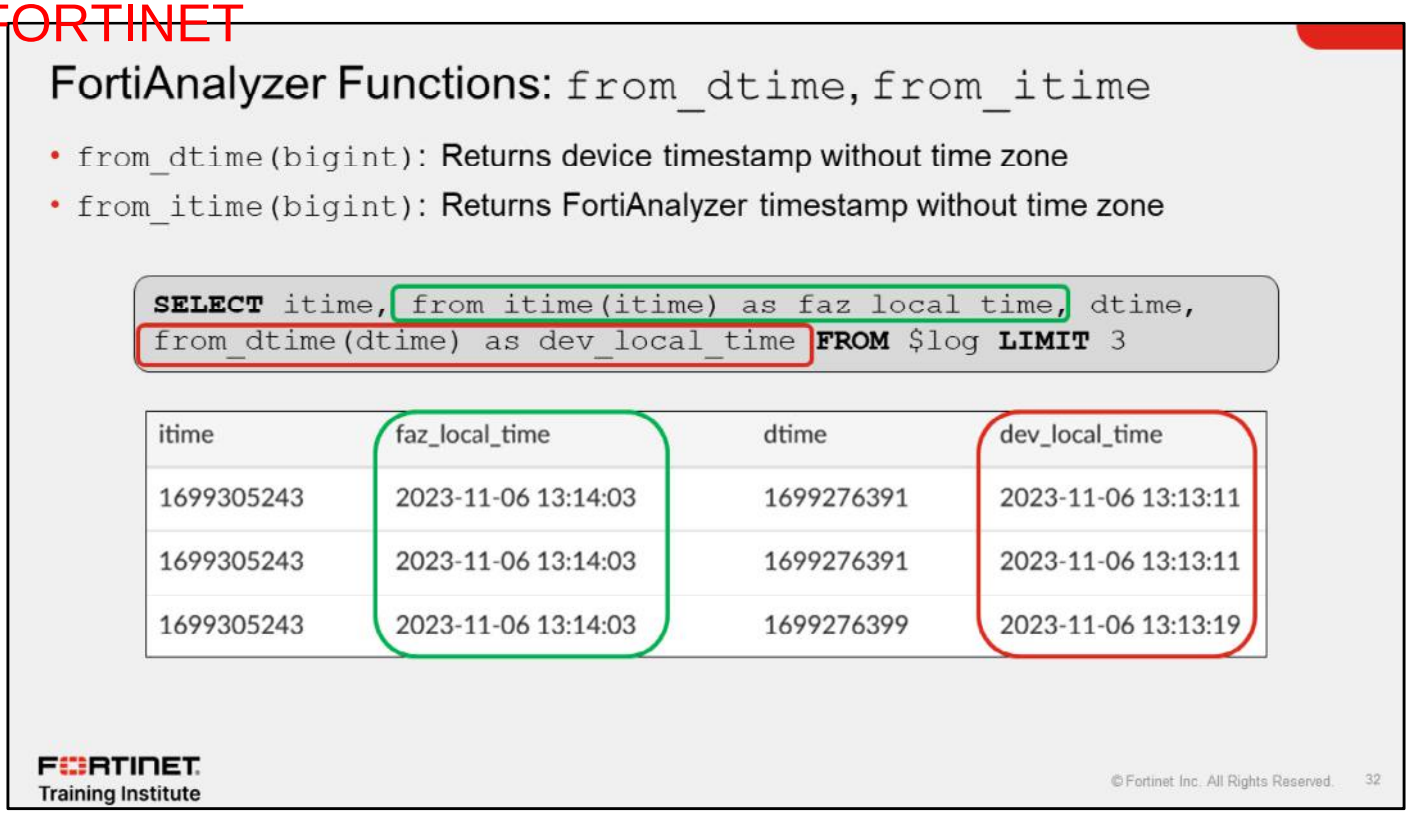
Another FortiAnalyzer-specific function is nullifna, which takes an expression as an argument. The actual SQL syntax this is based on is SELECT NULLIF(NULLIF(expression, 'N/A'), 'n/a').

In this example, if the user is n/a the source IP is displayed; otherwise, it returns the user name. It performs the inverse operation of the COALESCE function.



`email_domain` and `email_user` are other FortiAnalyzer-specific functions. `email_domain` retrieves anything that comes after the @ symbol in an email address—the domain. `email_user` retrieves anything that comes before the @ symbol in an email address.

As specified by the query, in this example `email_user` displays in the column **e_user**, while `email_domain` displays in the column **e_domain**.



from_dtime and from_itime are other FortiAnalyzer-specific functions. from_dtime returns the device timestamp without the time zone, while from_itime returns the FortiAnalyzer's timestamp without the time zone.

As specified by this query, from_itime appears in the column **faz_local_time**, while from_dtime appears in the column **dev_local_time**.

Macros

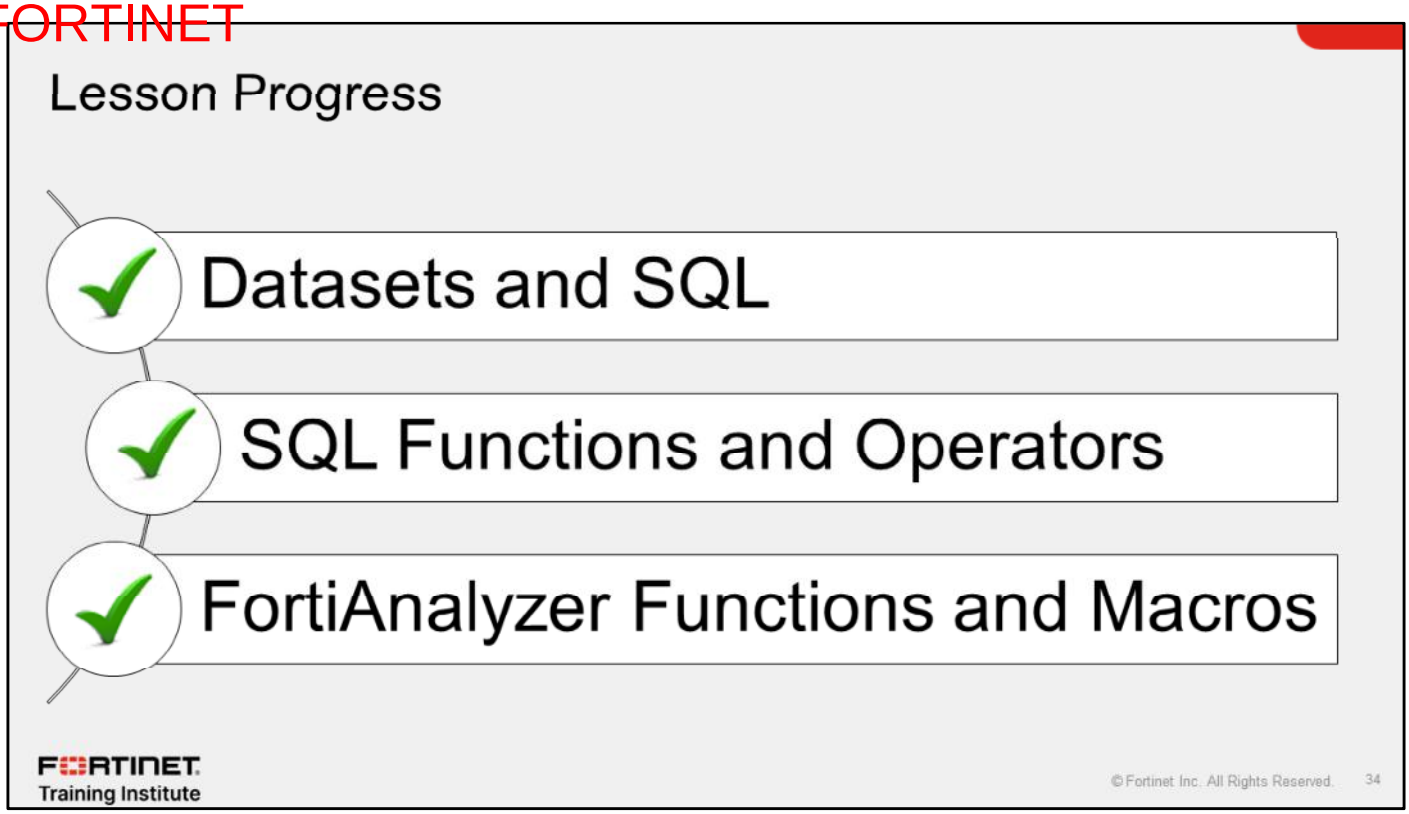
- FortiAnalyzer date and time macros

Macros	PostgreSQL Syntax	Result
$hour_of_day	to_char(from_itime("itime"), 'HH24:00')	18:00
$HOUR_OF_DAY	to_char(from_itime("itime"), 'YYYY-MM-DD HH24:00')	2021-01-01 18:00
$day_of_week	to_char(from_itime("itime"), '"WDAY" D-Dy')	WDAY 2-Mon
$DAY_OF_WEEK	XXX	XXX
$day_of_month	to_char(from_itime("itime"), 'DD')	01
$DAY_OF_MONTH	to_char(from_itime("itime"), 'YYYY-MM-DD')	2021-01-01
$month_of_year	to_char(from_itime("itime"), 'YYYY-MM')	2021-01
$MONTH_OF_YEAR	XXX	XXX

FORTINET Training Institute

 33

Here are some common date and time macros used in FortiAnalyzer. Macros are simple substitutions for more complex SQL statements—usually created for SQL statements that are frequently used.



Congratulations! You have come to the end of this material.