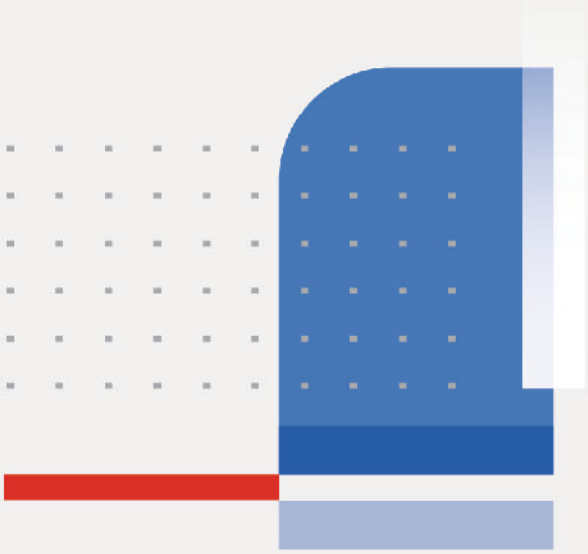
FORTINET CERTIFIED PROFESSIONAL Network Security

FortiAnalyzer Administrator Study Guide

FortiAnalyzer 7.4

FORTINET Training Institute



Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

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

Fortinet | Pearson VUE

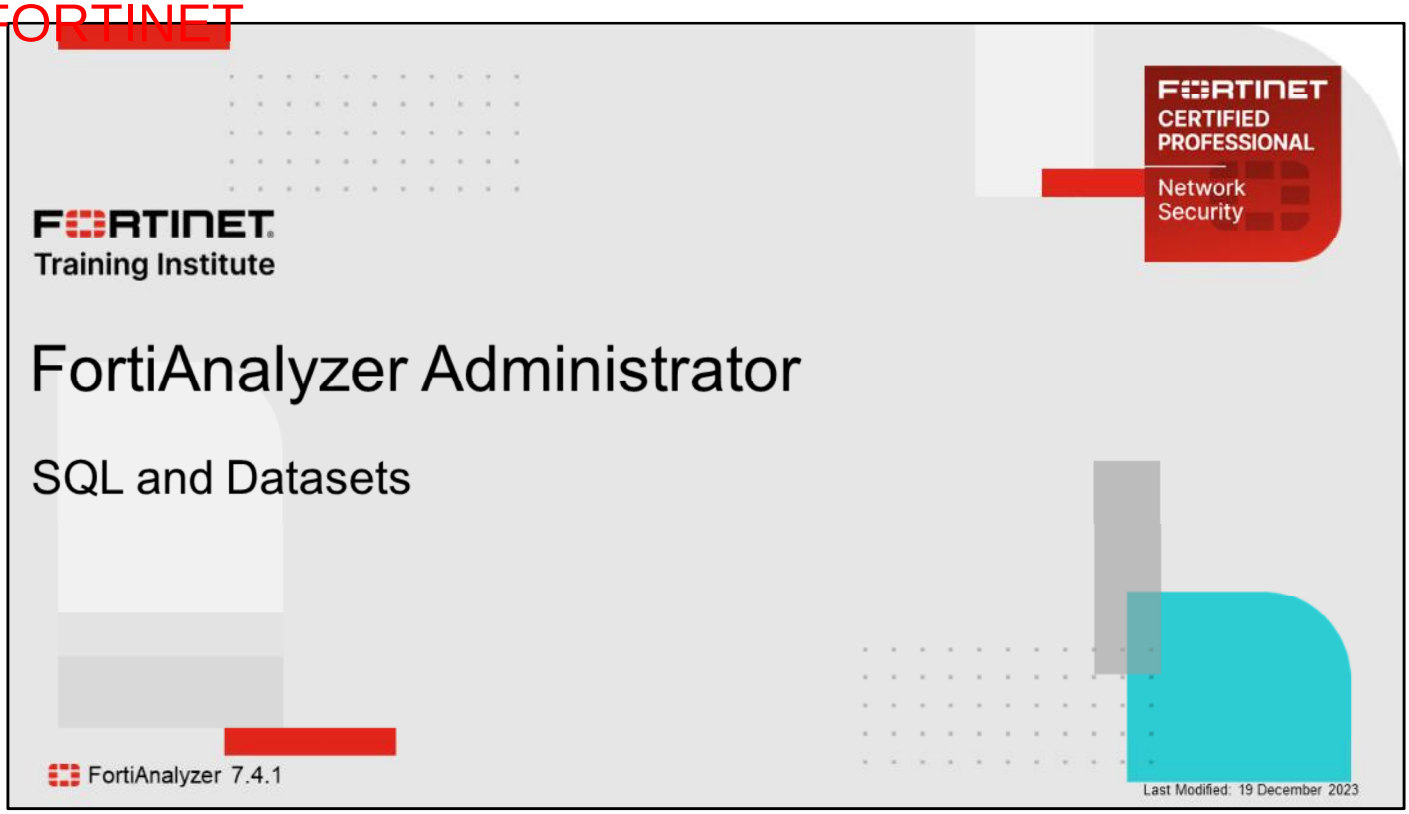
https://home.pearsonvue.com/fortinet

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

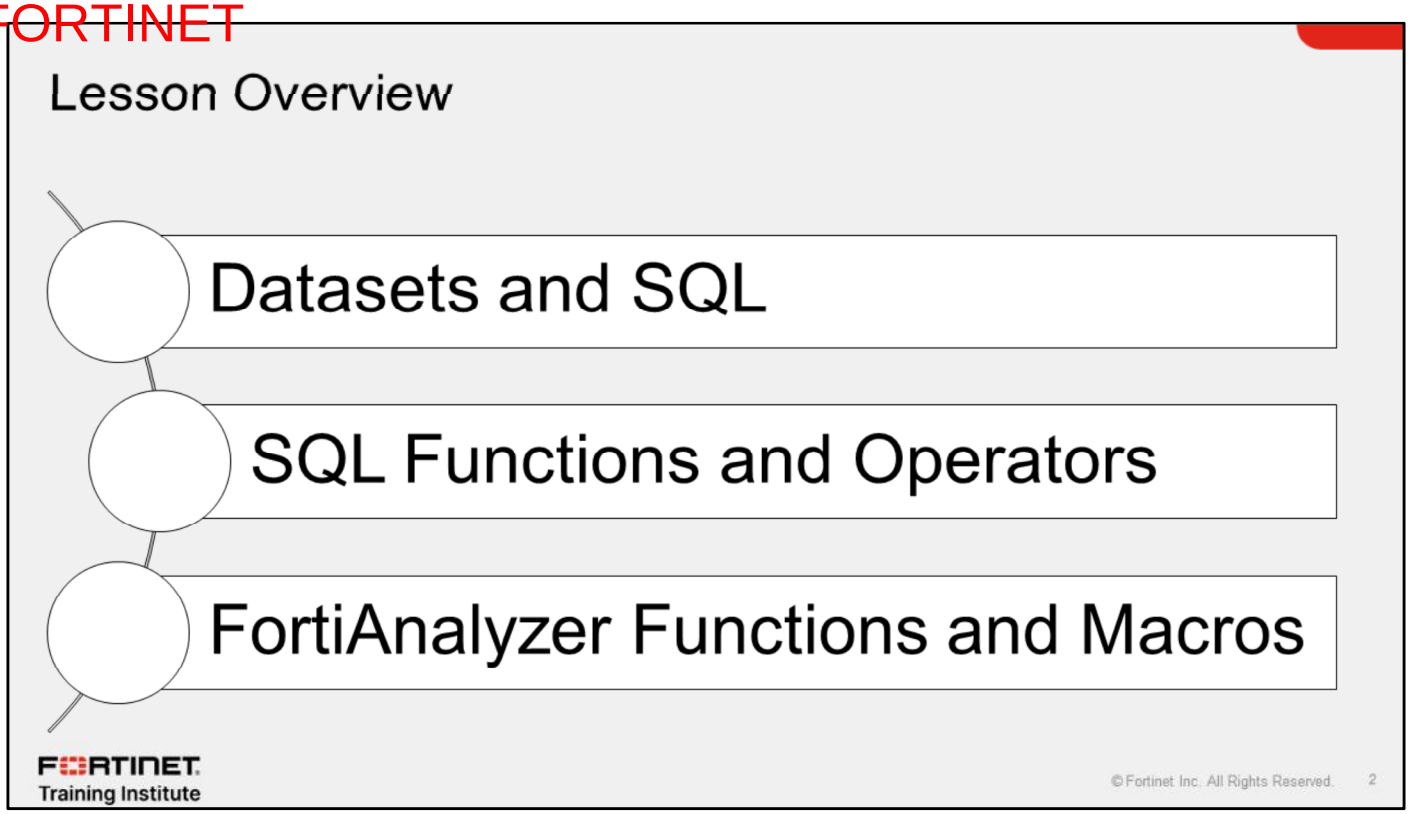
https://helpdesk.training.fortinet.com/support/home

12/19/2023

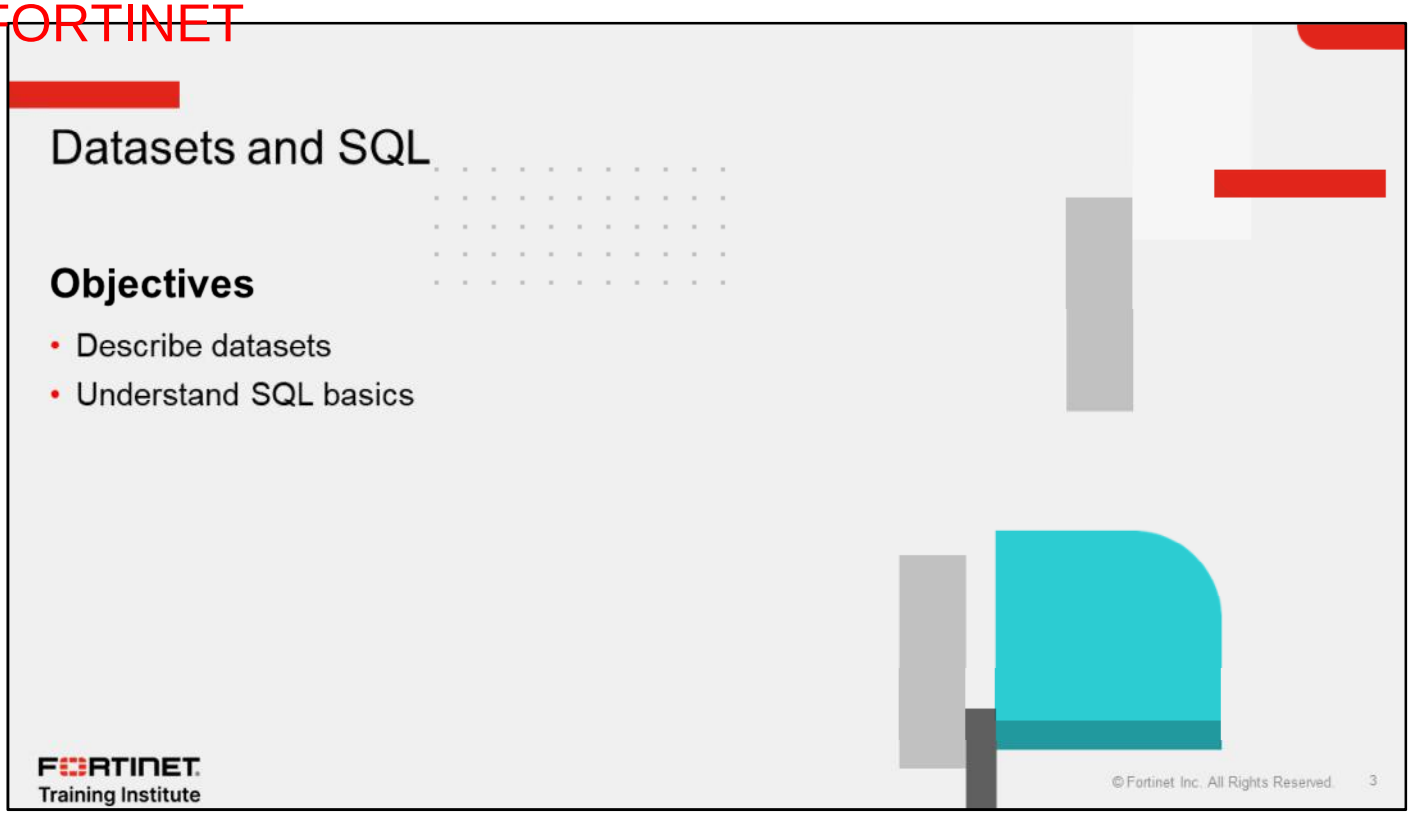
TABLE OF CONTENTS



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.

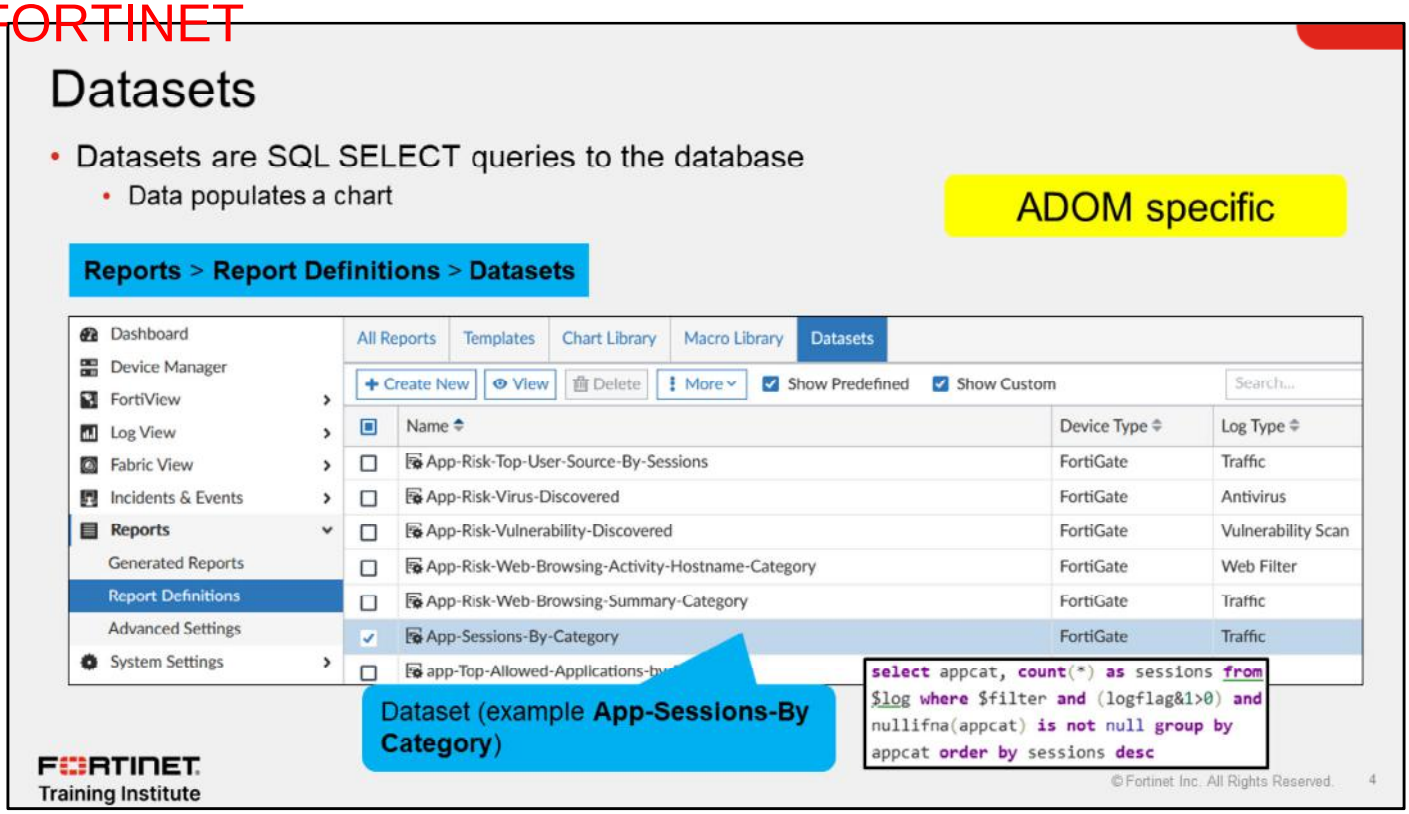


The supplemental material is covered in the topics shown on this slide.



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

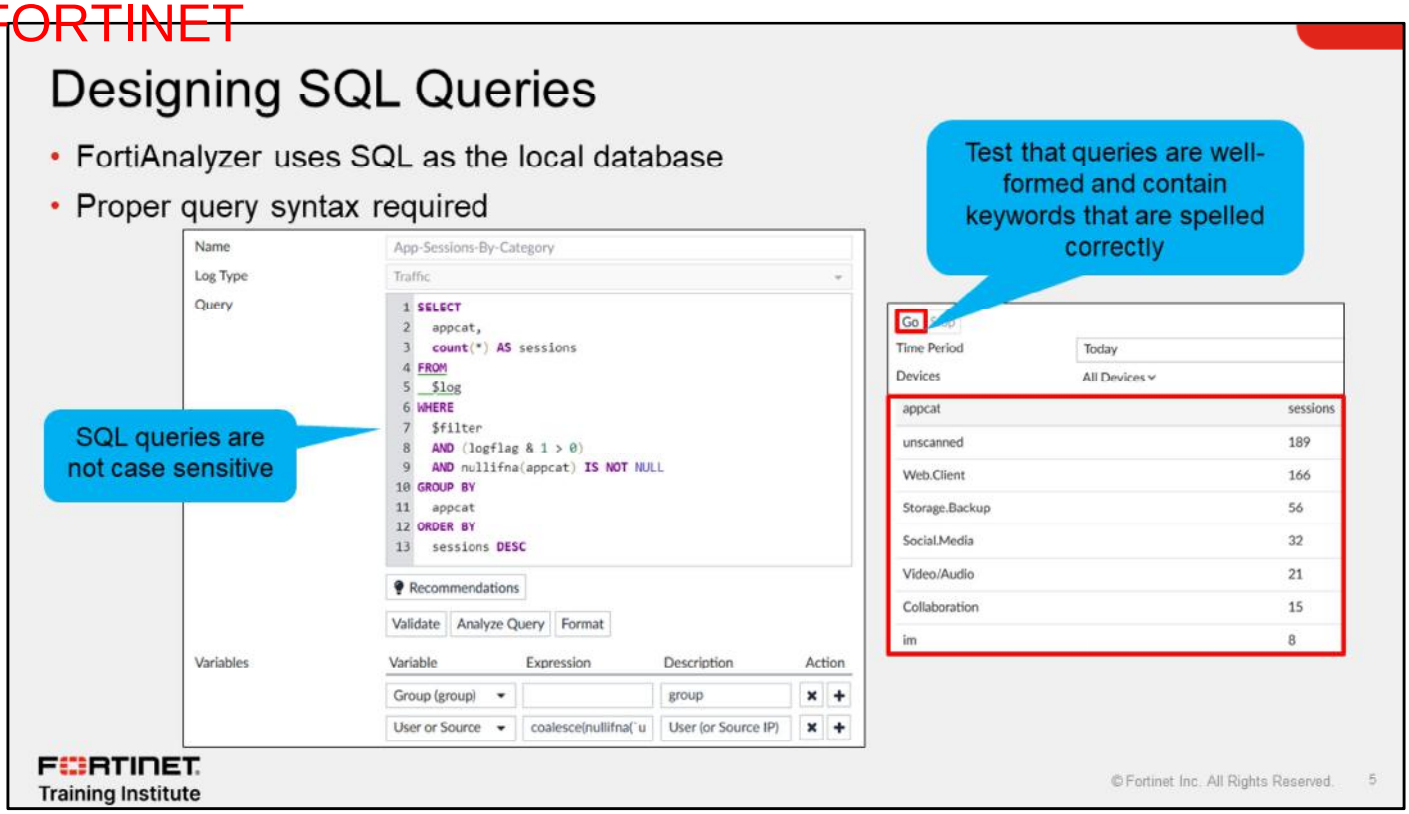
FortiAnalyzer provides predefined datasets that address the most common queries. However, if you need to modify those datasets or create your own, you need to understand SQL.



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.

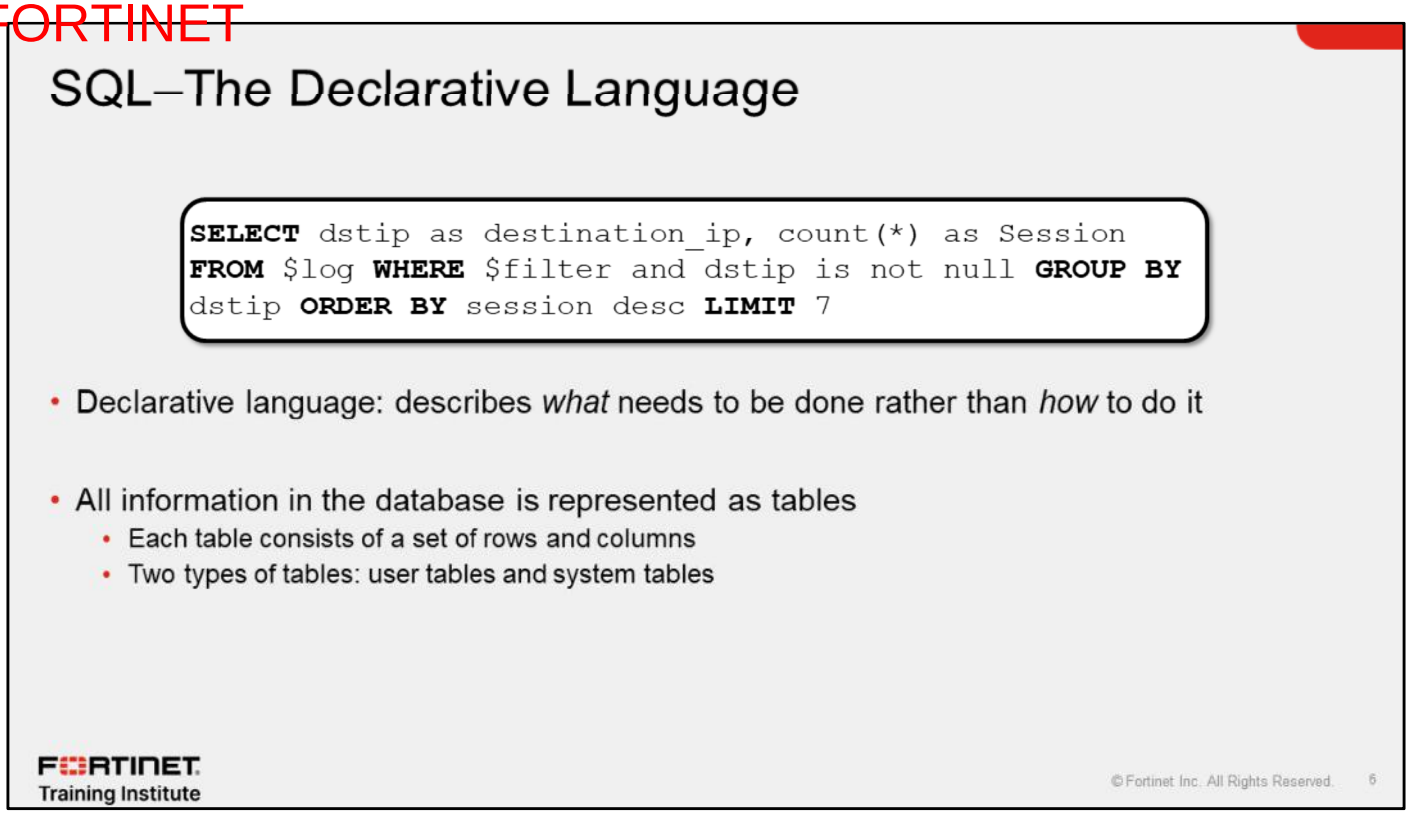
This slide shows an example of the default **App-Sessions-By-Category** dataset.



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.

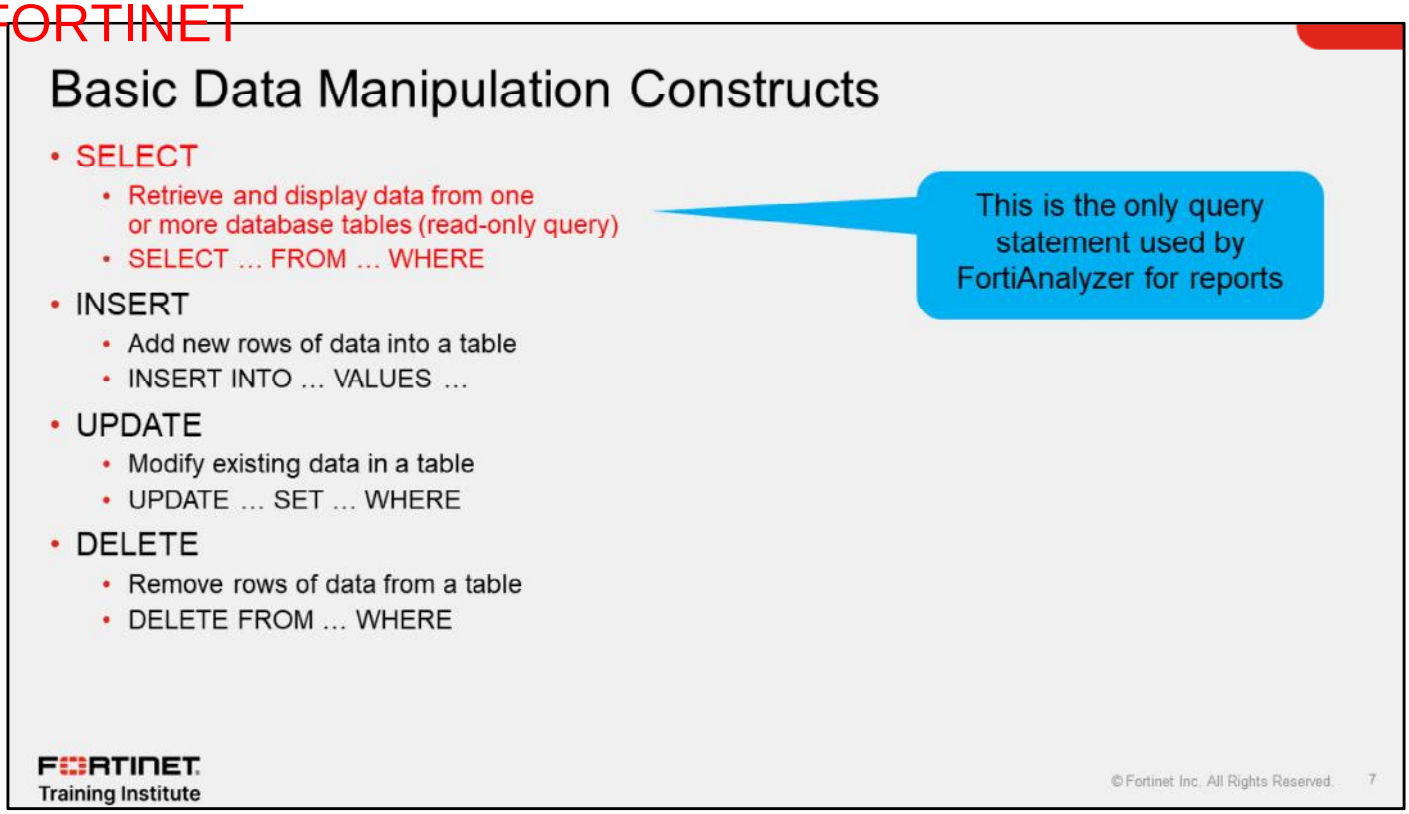
Note that SQL queries are not case sensitive.



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.

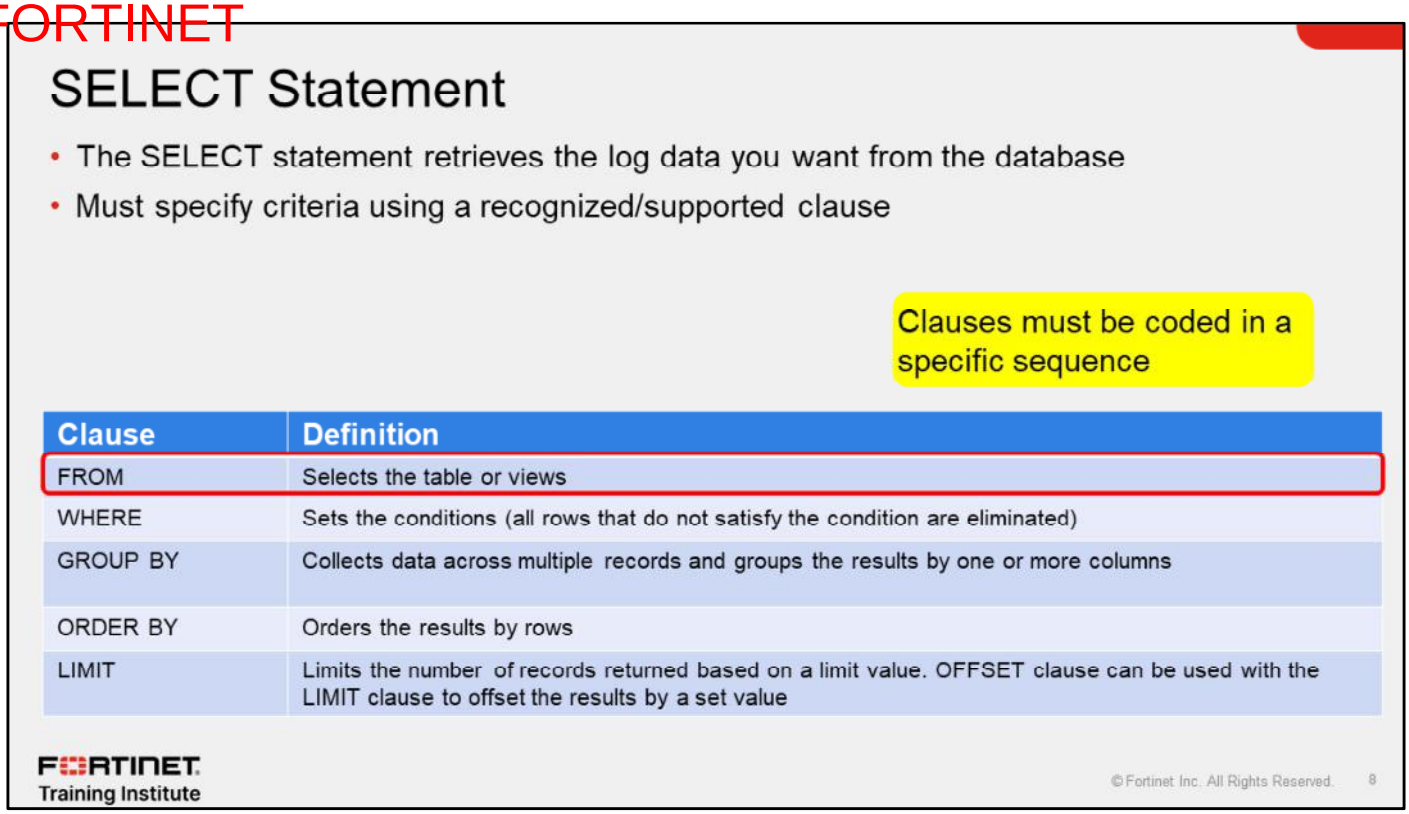
In a SQL database all information is represented as tables, and each table consists of a set of rows and columns. There are two types of tables:

- 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.

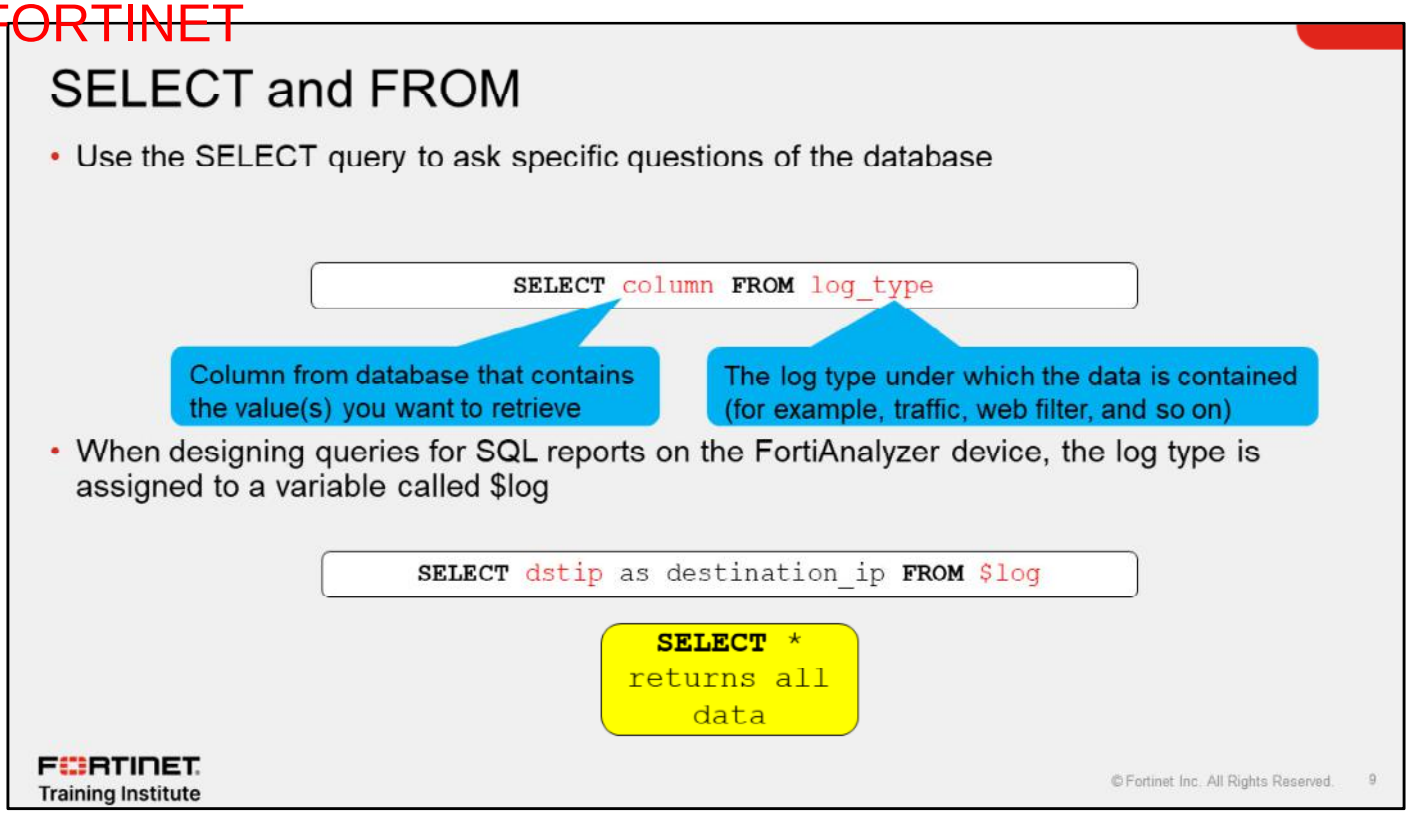


The SELECT statement is used to query the database and retrieve log data. In order to pull the data you want, you must specify the criteria. For example, let's say you want to query the database for a list of employees who work in the IT department. In order to put this criteria into a language that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

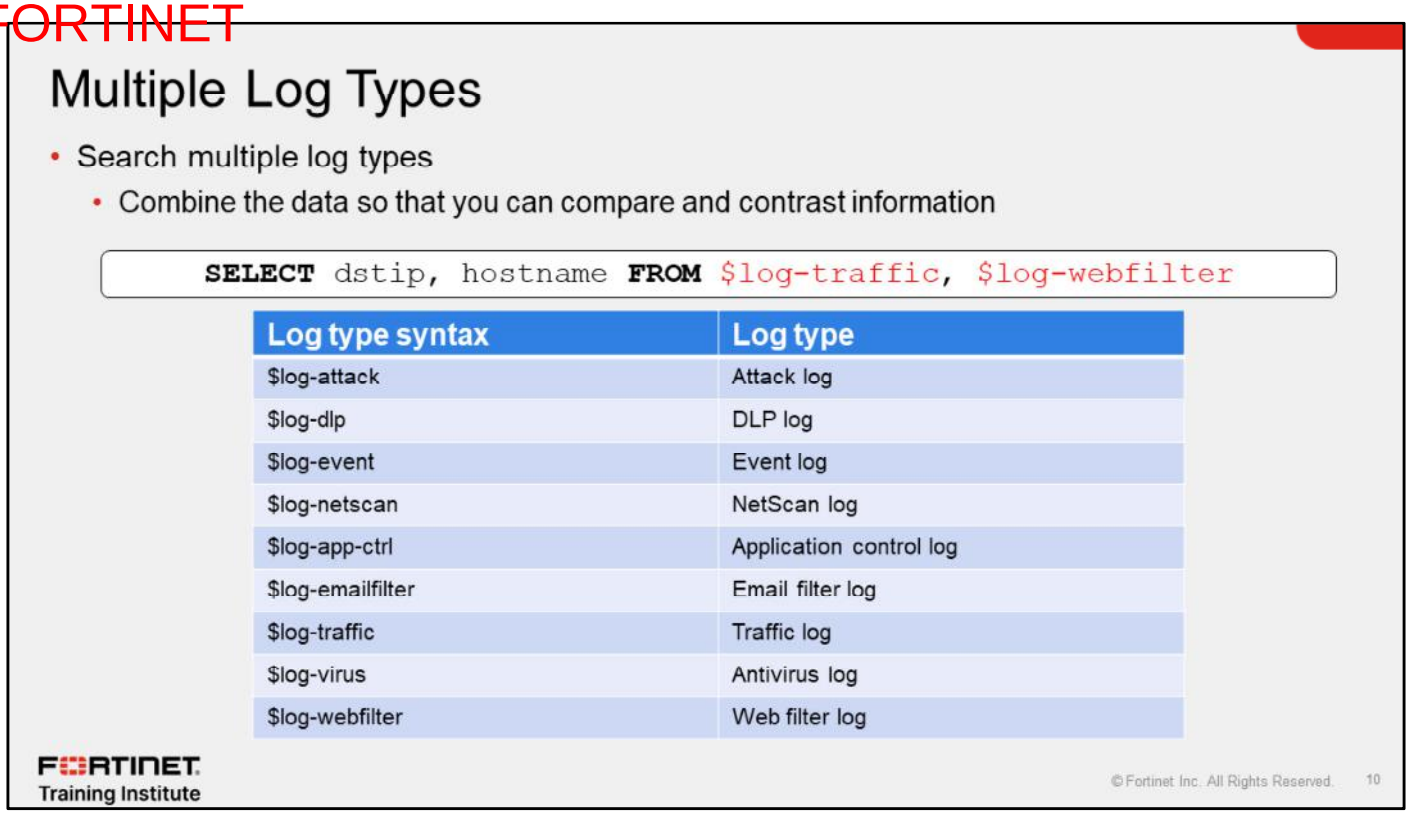
If you want to return all data, you can use the `*` symbol. For example, `SELECT *`. Though most of the time that is more information that you require.

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

For example:

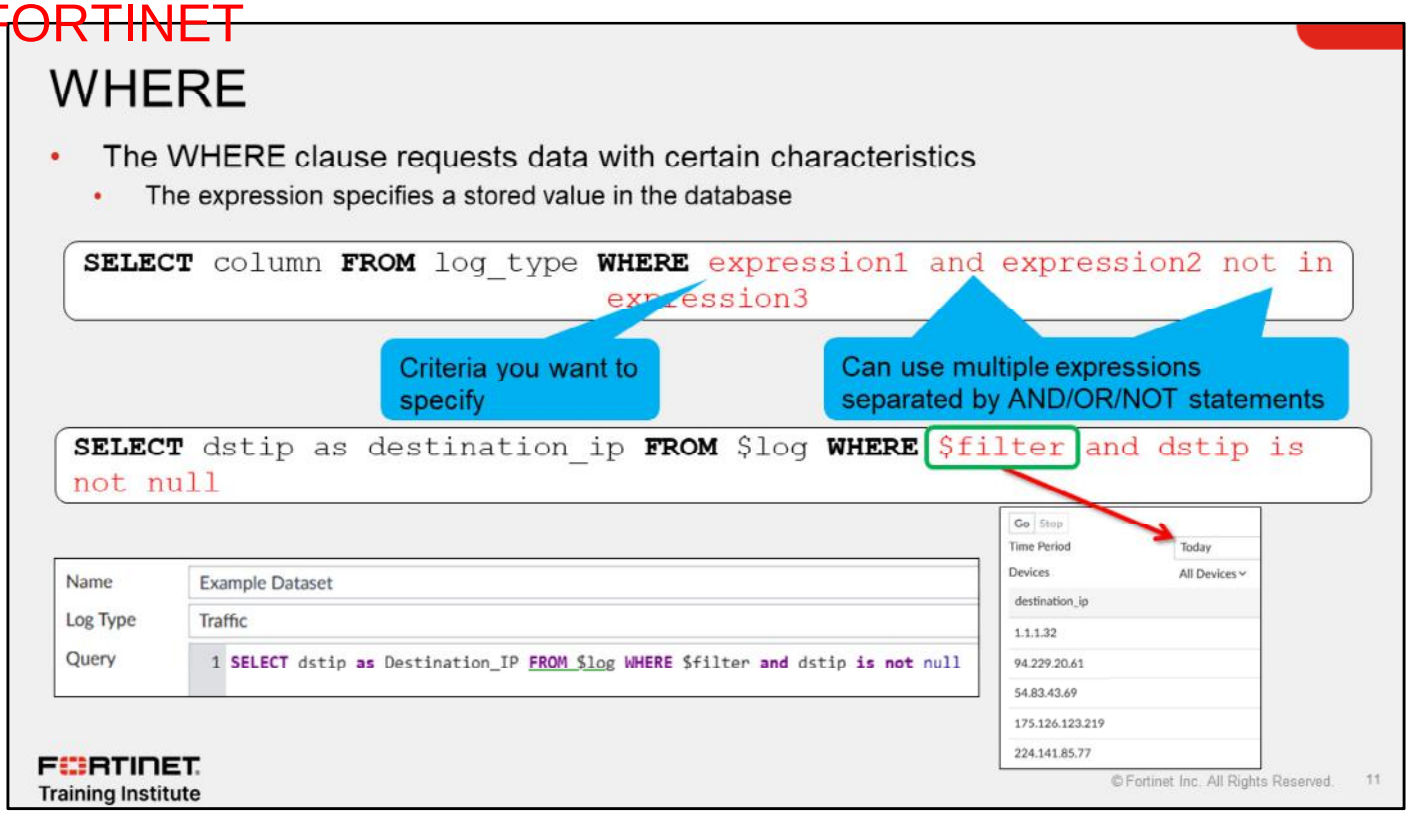
```
FROM $log
```

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
```



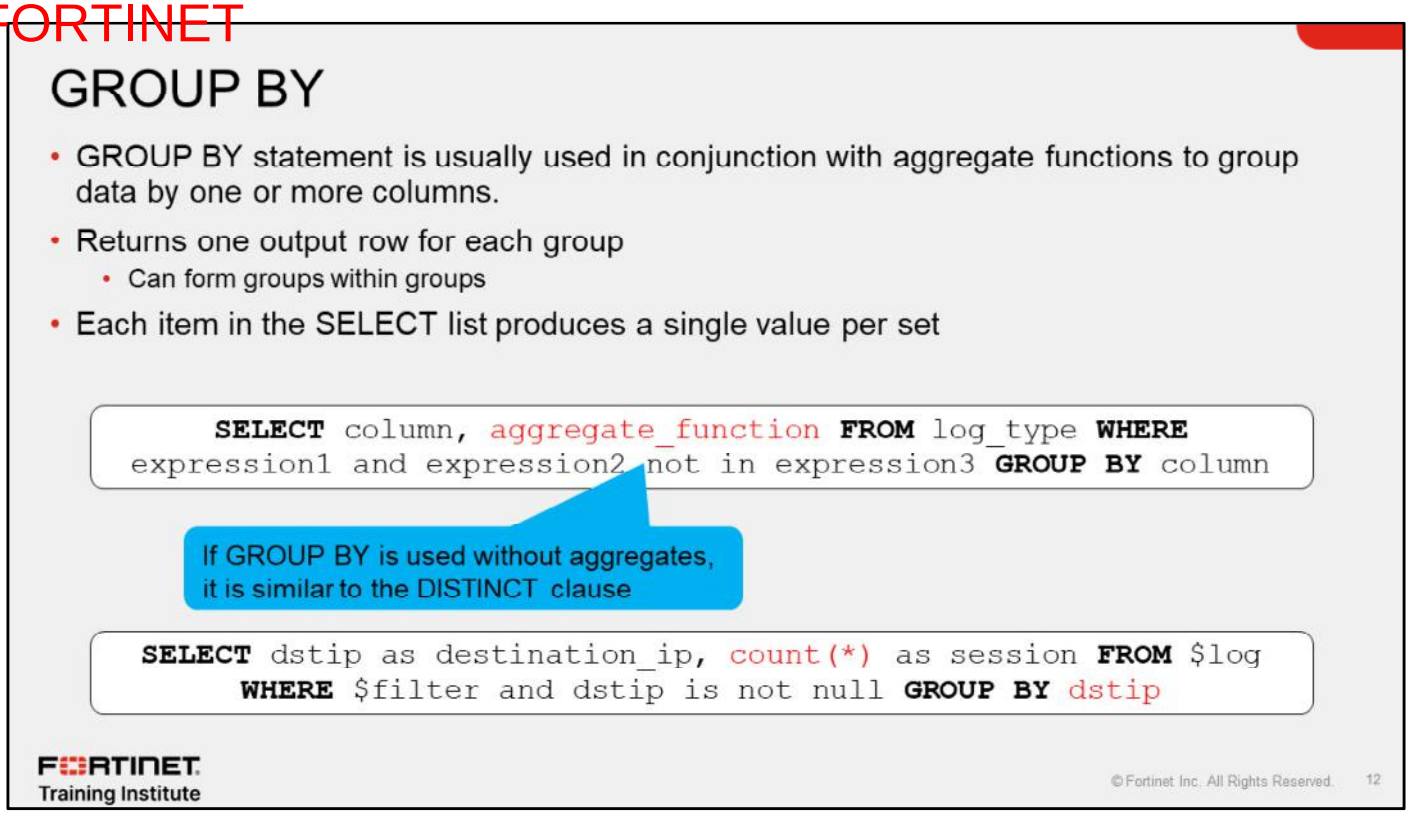
Out of all the optional clauses, the WHERE statement is really the heart of the query, because this is where you specify the criteria.

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.

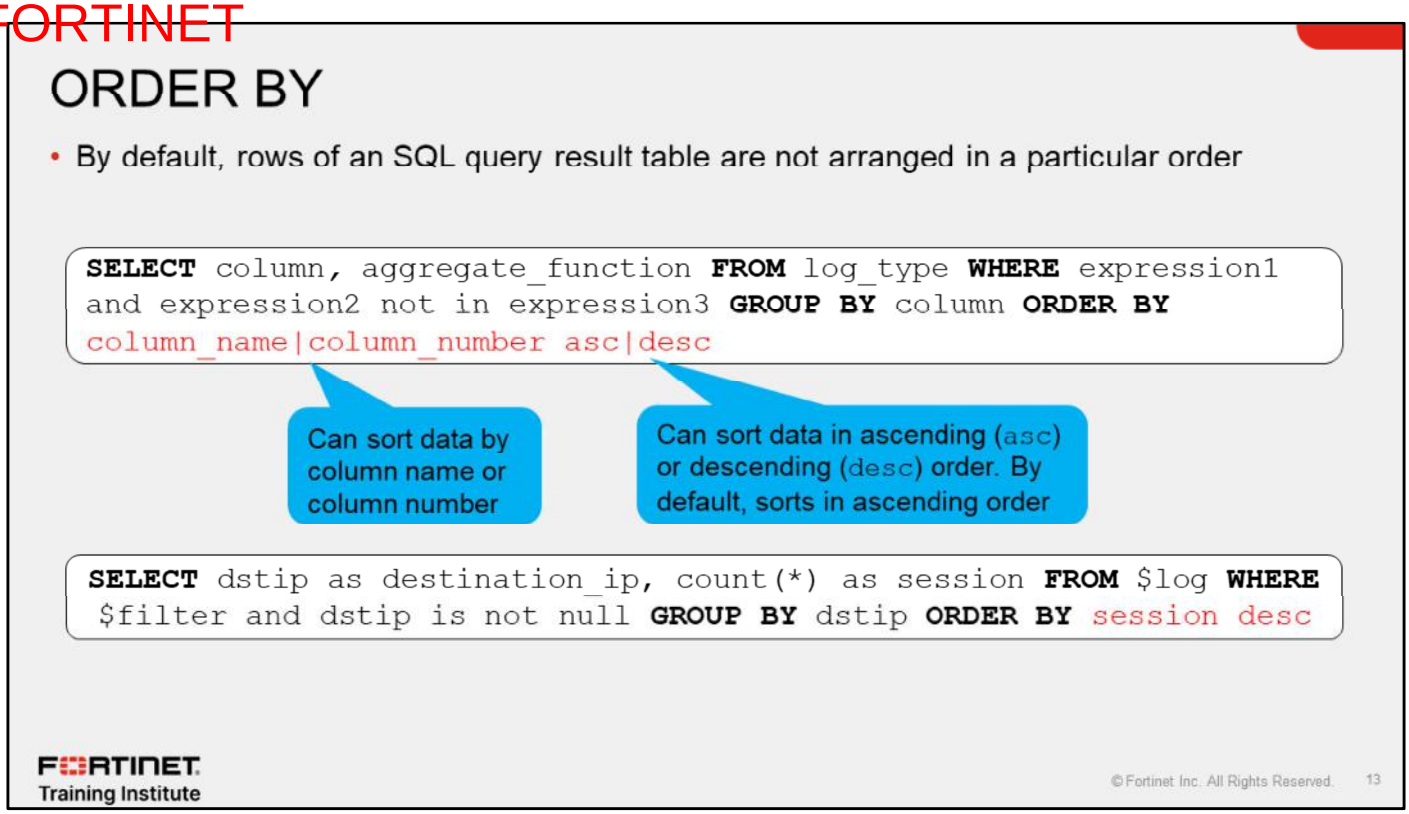
SQL supports logic operators as well, so you can use AND/OR/NOT statements in order to build out the query. Operators are also covered in this material.



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.

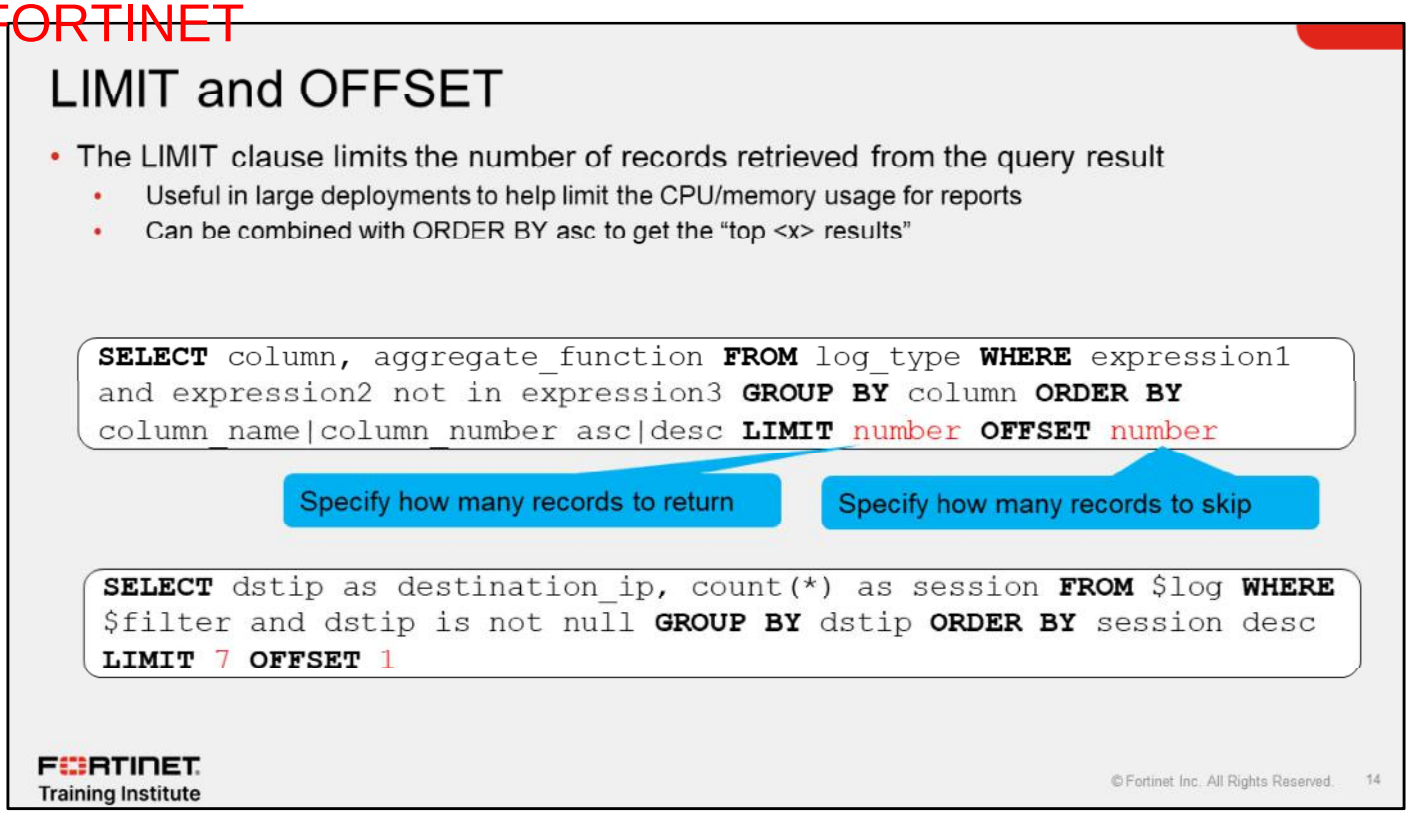
In this example, we are grouping by `dstip` (destination IP).



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.

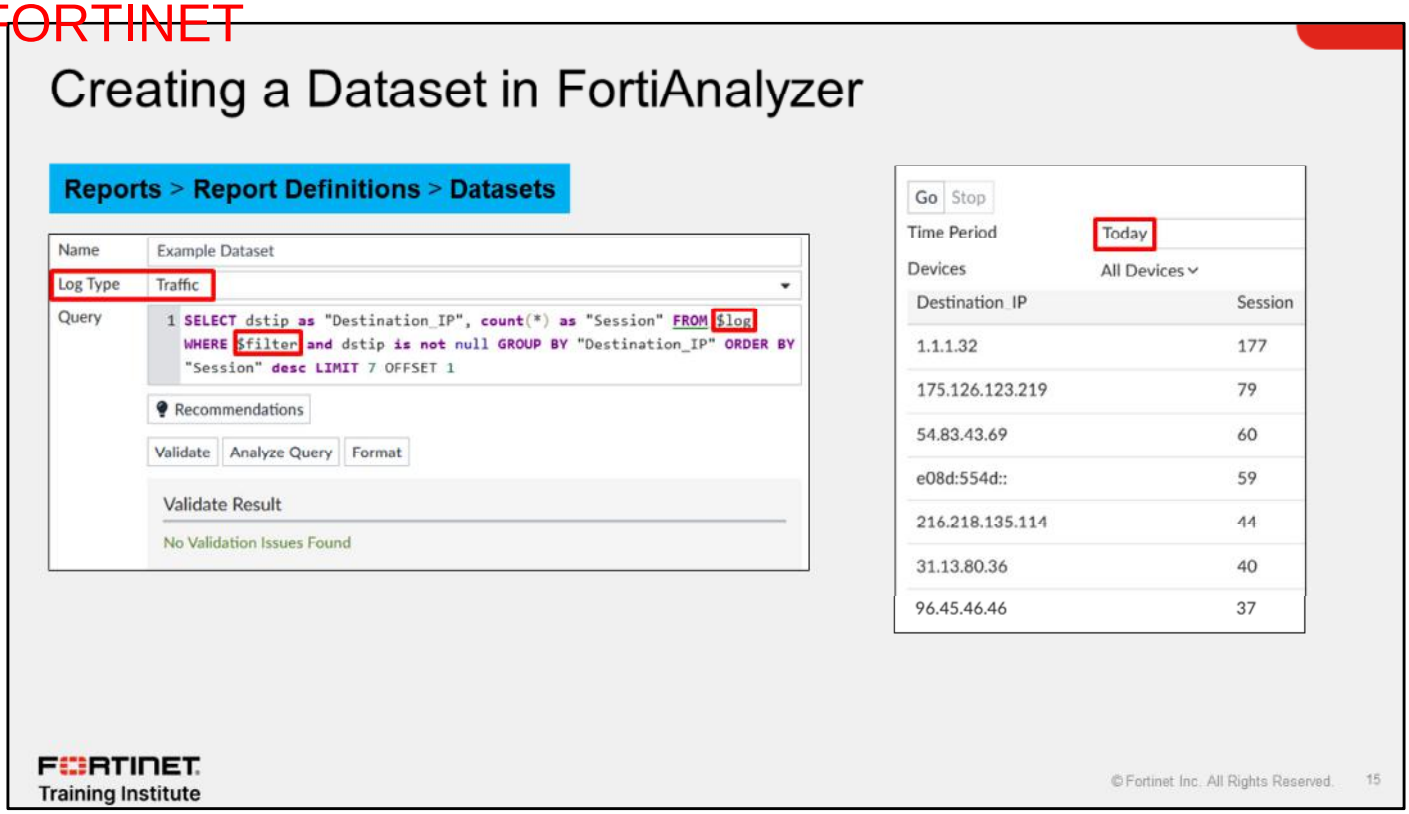
You can order multiple columns and specify different sort orders for each. For example, you can sort one column in ascending order and another column in descending order.

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.

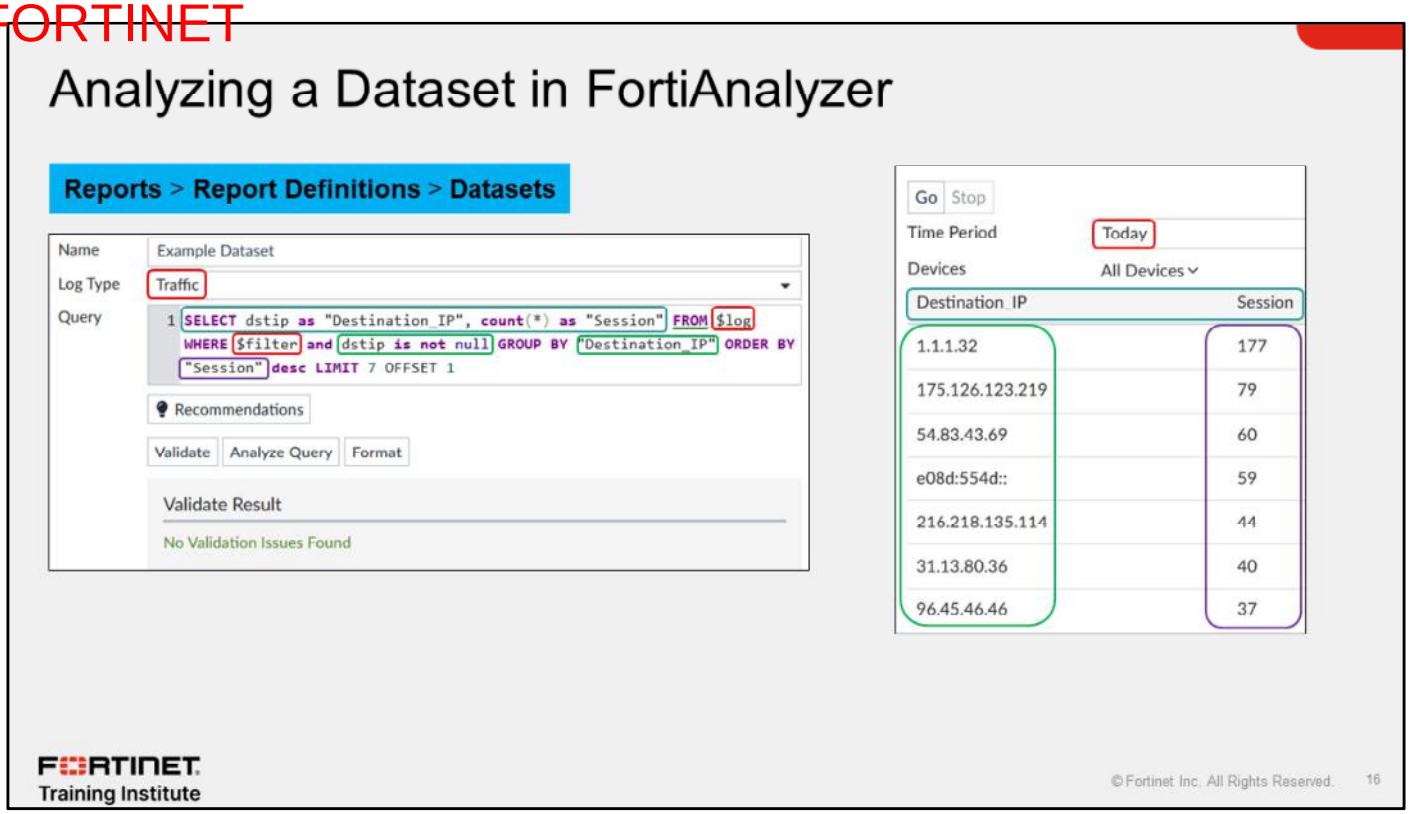


As you have been learning about the main SQL clauses, you have also been forming a full dataset query along the way. To see a visual of the query, you can use the dataset **Go** feature in the GUI. The feature is intended to test or modify a query in order to get the specific output you want.

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.

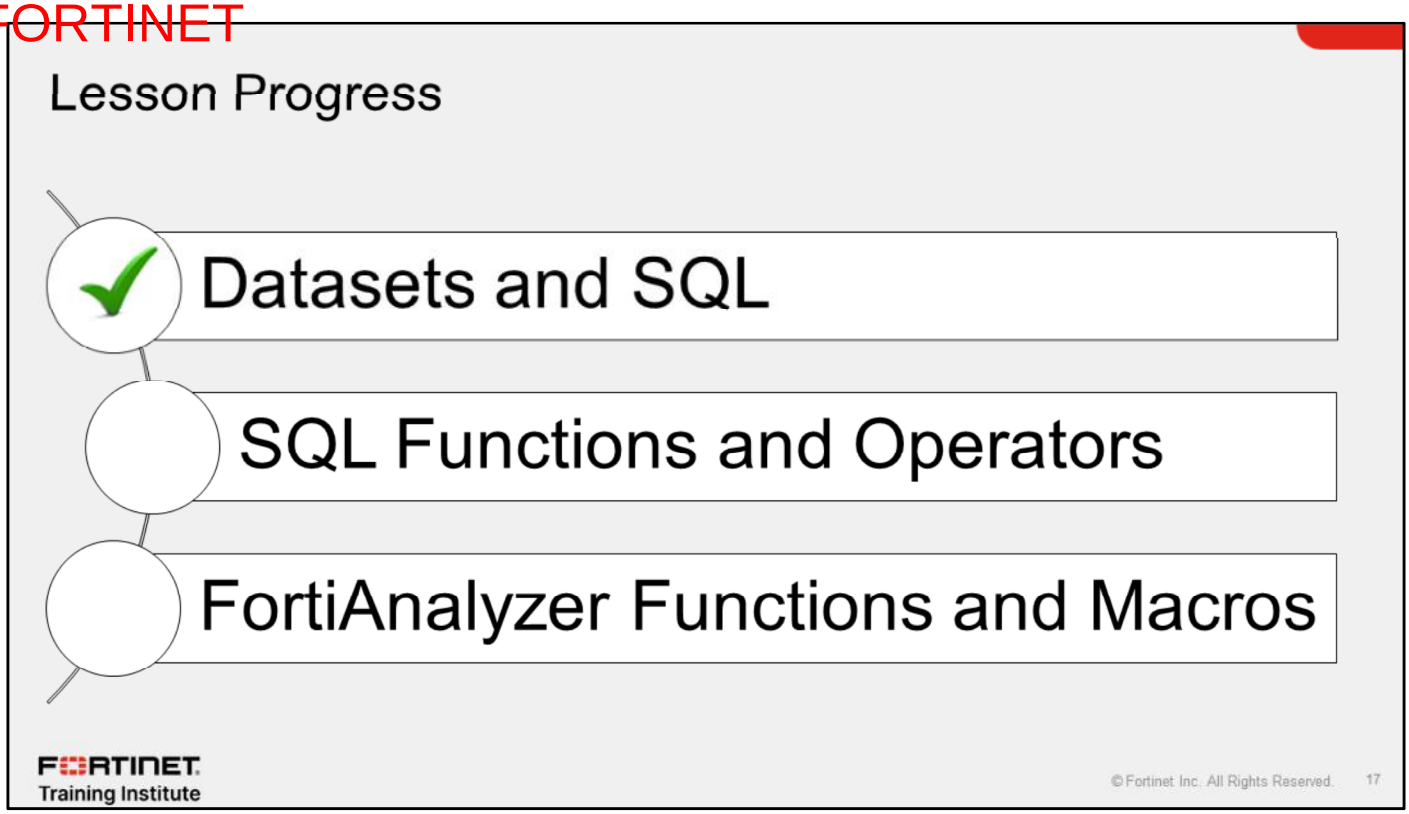
`WHERE $filter and dstip is not null`: This says, limit the results to the time period specified, which is **Today**, according to the selection in the **Time Period** field, and provide only the destination IP addresses that are not null. Note that "null" represents unknown data—it does not represent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

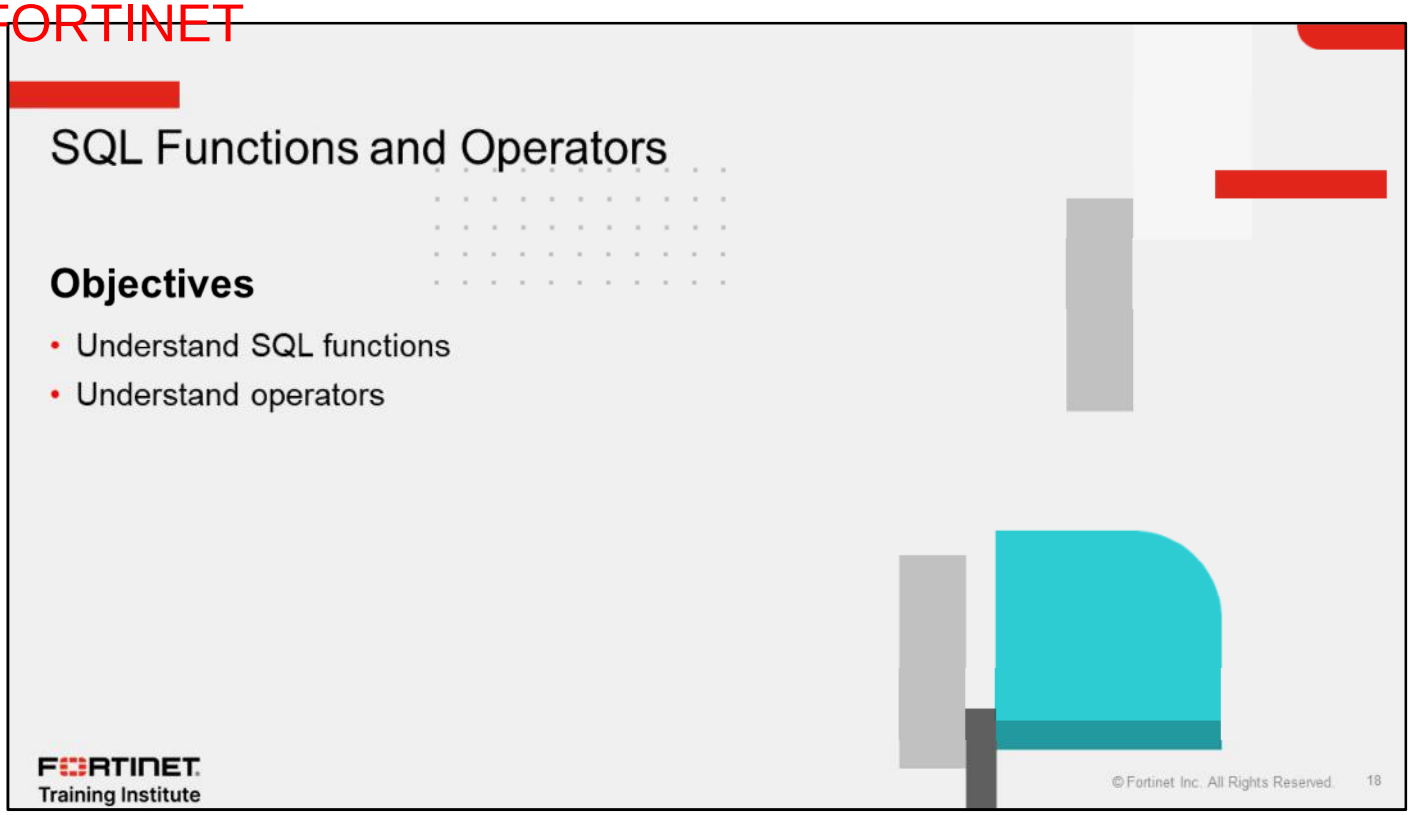
`LIMIT 7`: This says, provide only the first seven results.

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

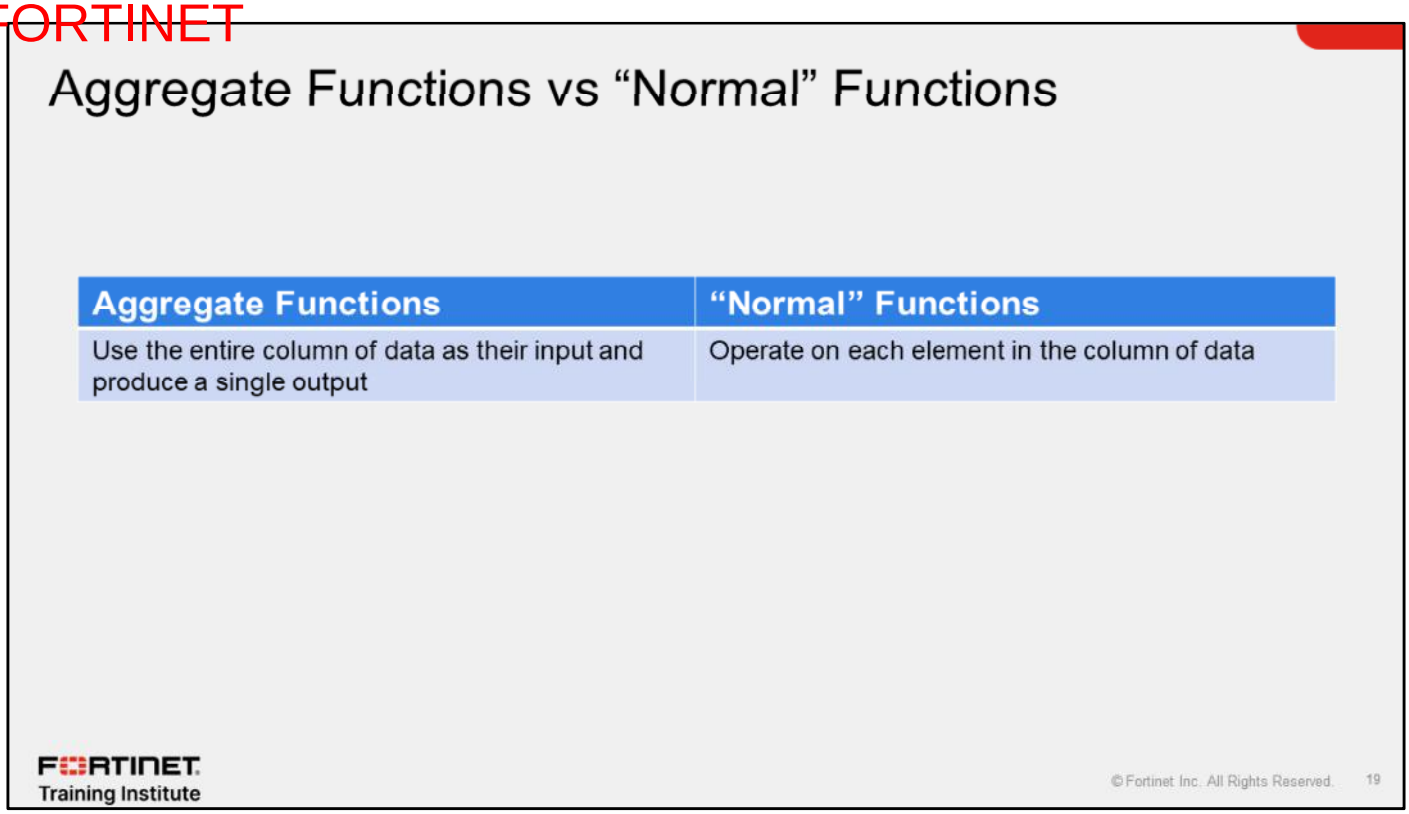


Good job! You now understand datasets and SQL.

Now, you will learn about SQL functions and operators.

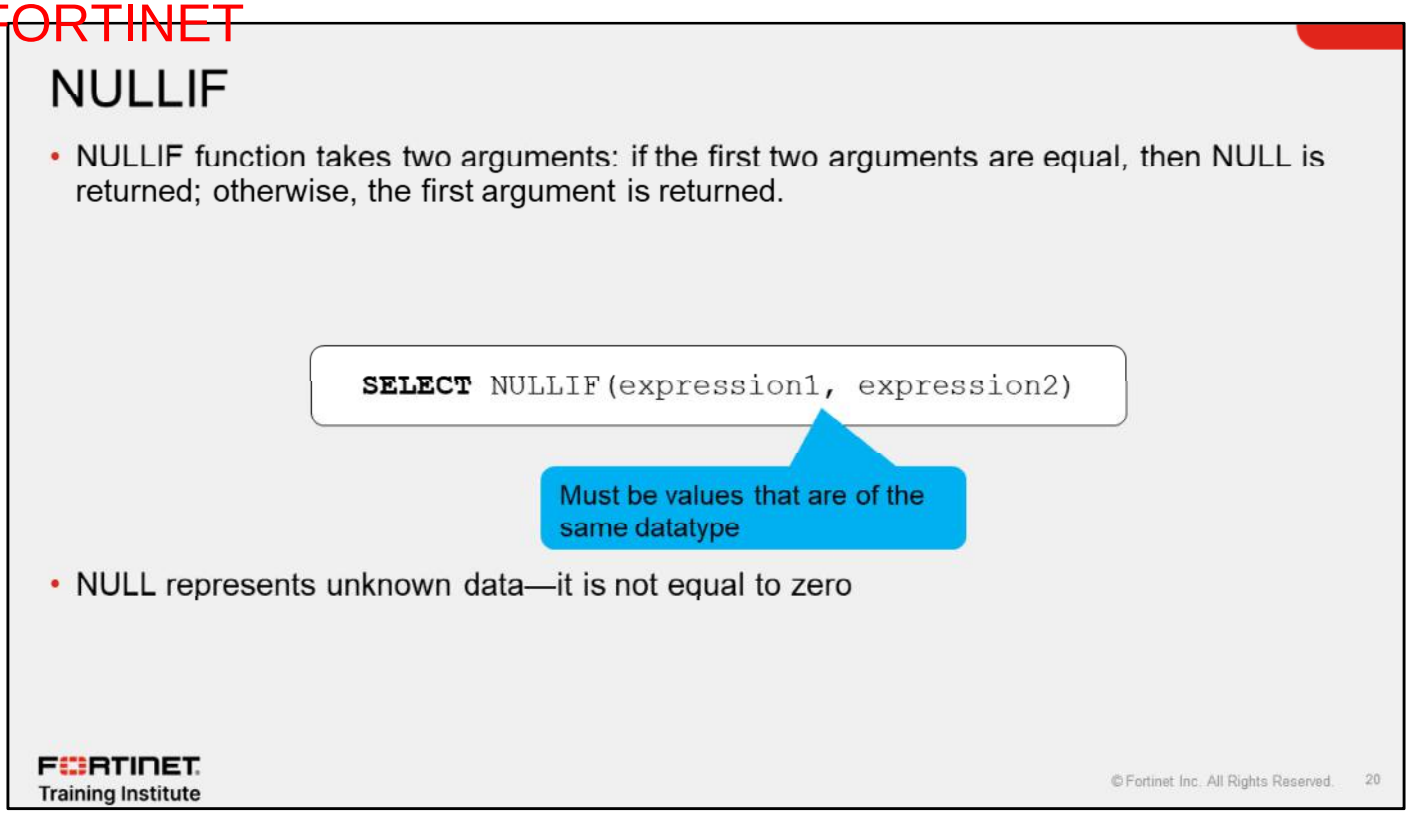


This section covers a few of the most common functions and operators used in FortiAnalyzer datasets—it is not intended as a complete and exhaustive list.

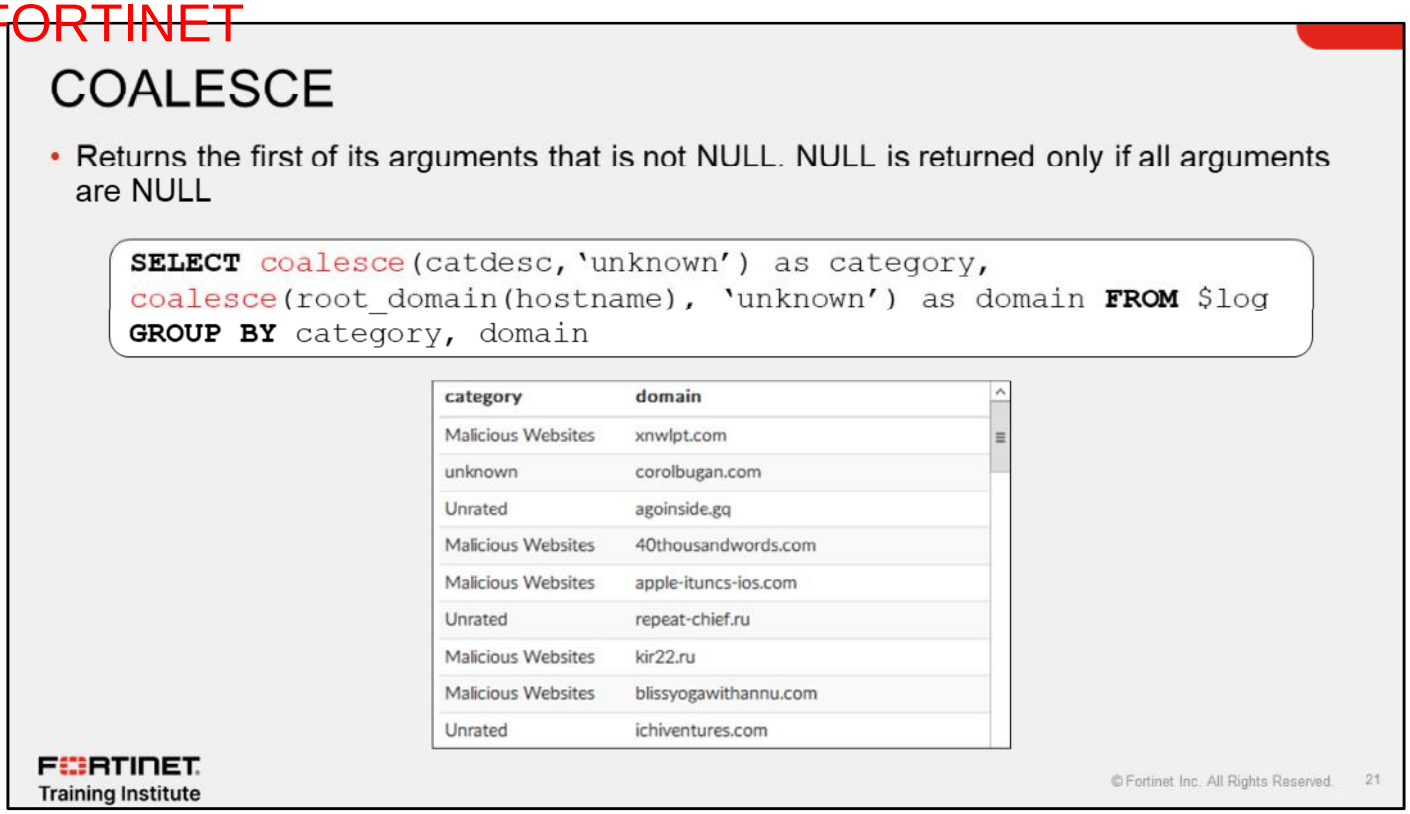


SQL has two types of functions: aggregate functions and “normal” functions.

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.



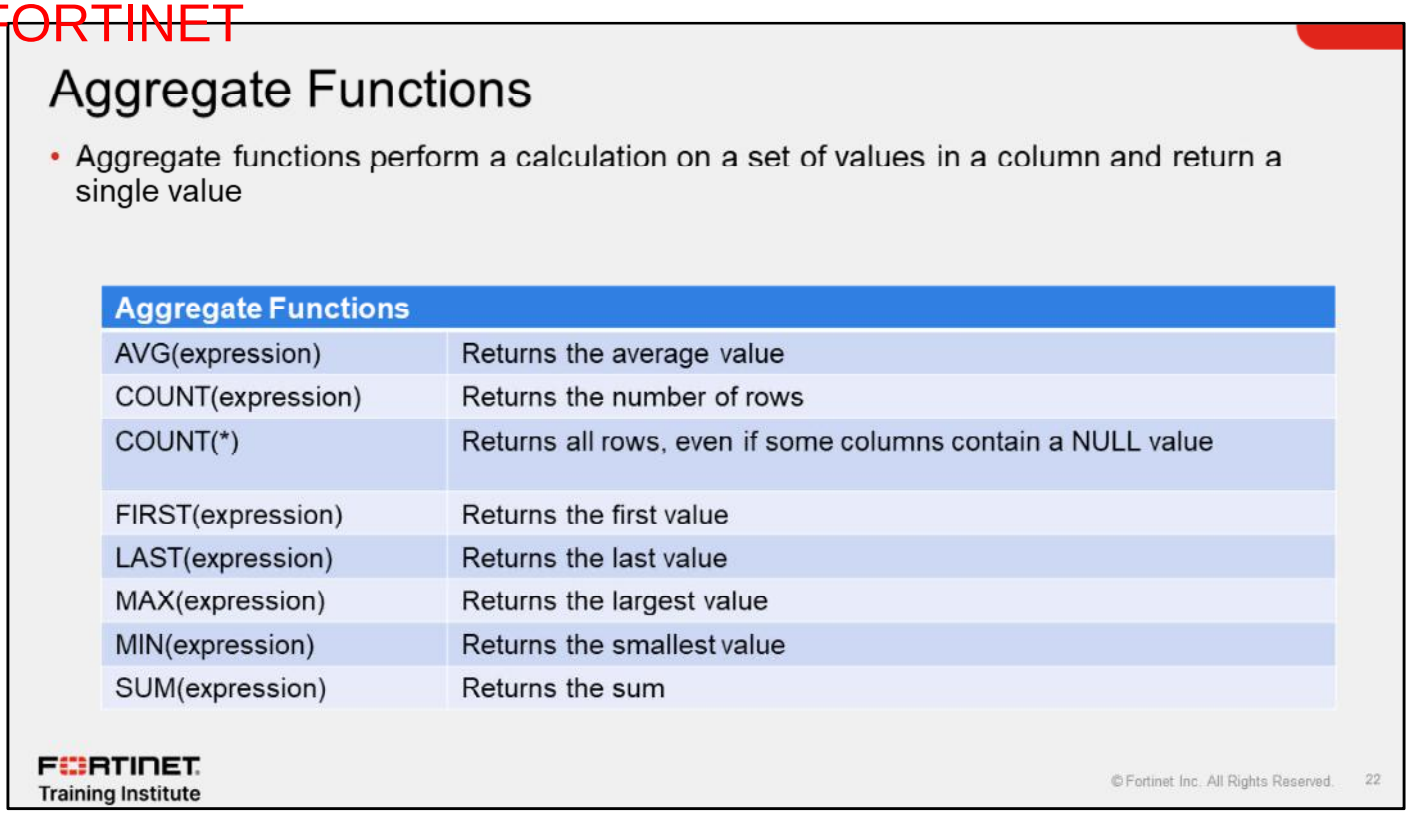
One common function used in FortiAnalyzer datasets is NULLIF. The NULLIF function takes two arguments. If the first two arguments are equal, then NULL is returned; otherwise, the first argument is returned. Note that NULL represents unknown data—it does not represent zero.



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:

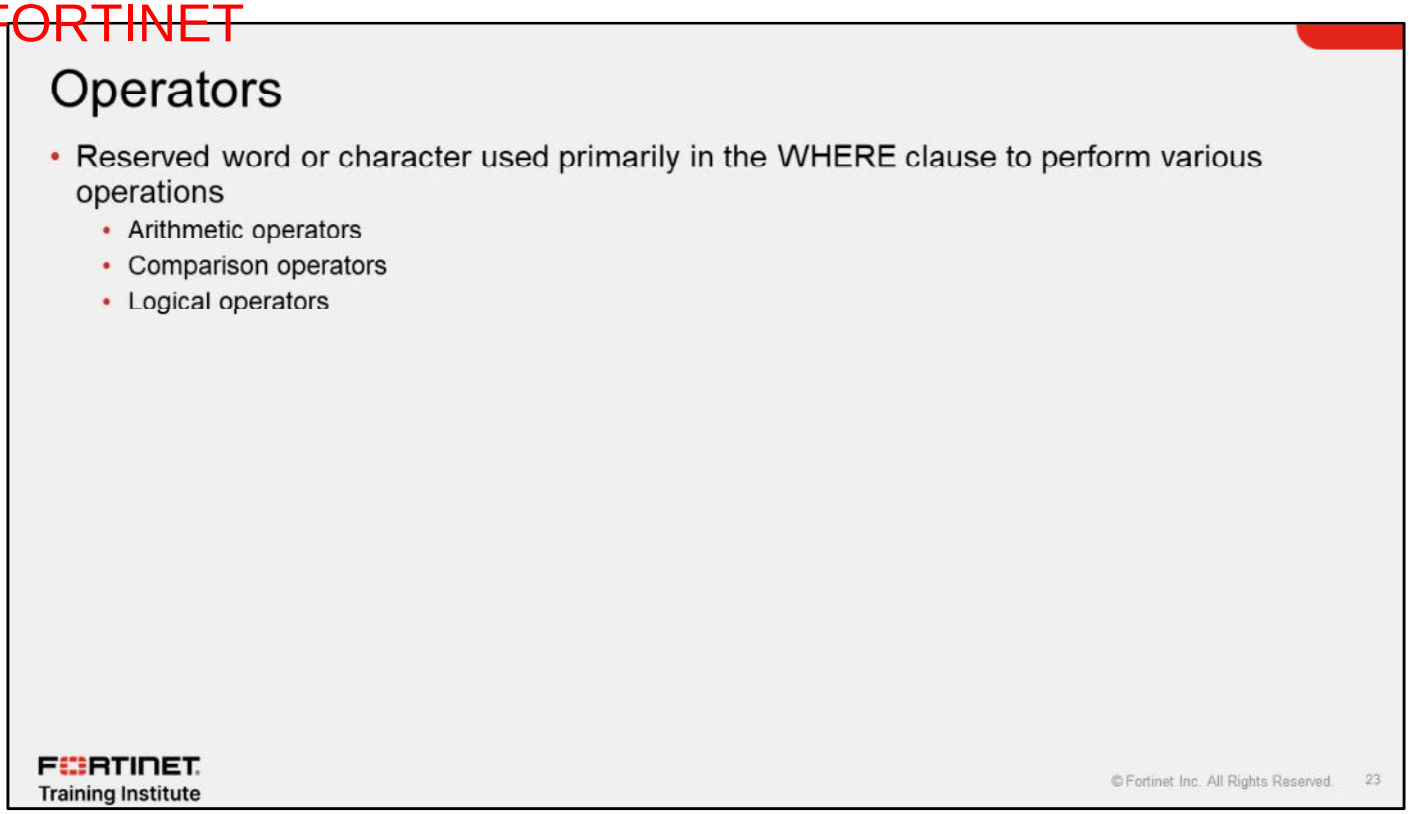
```
COALESCE (expression 1, expression 2, …)
```



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.

Comparison Operators

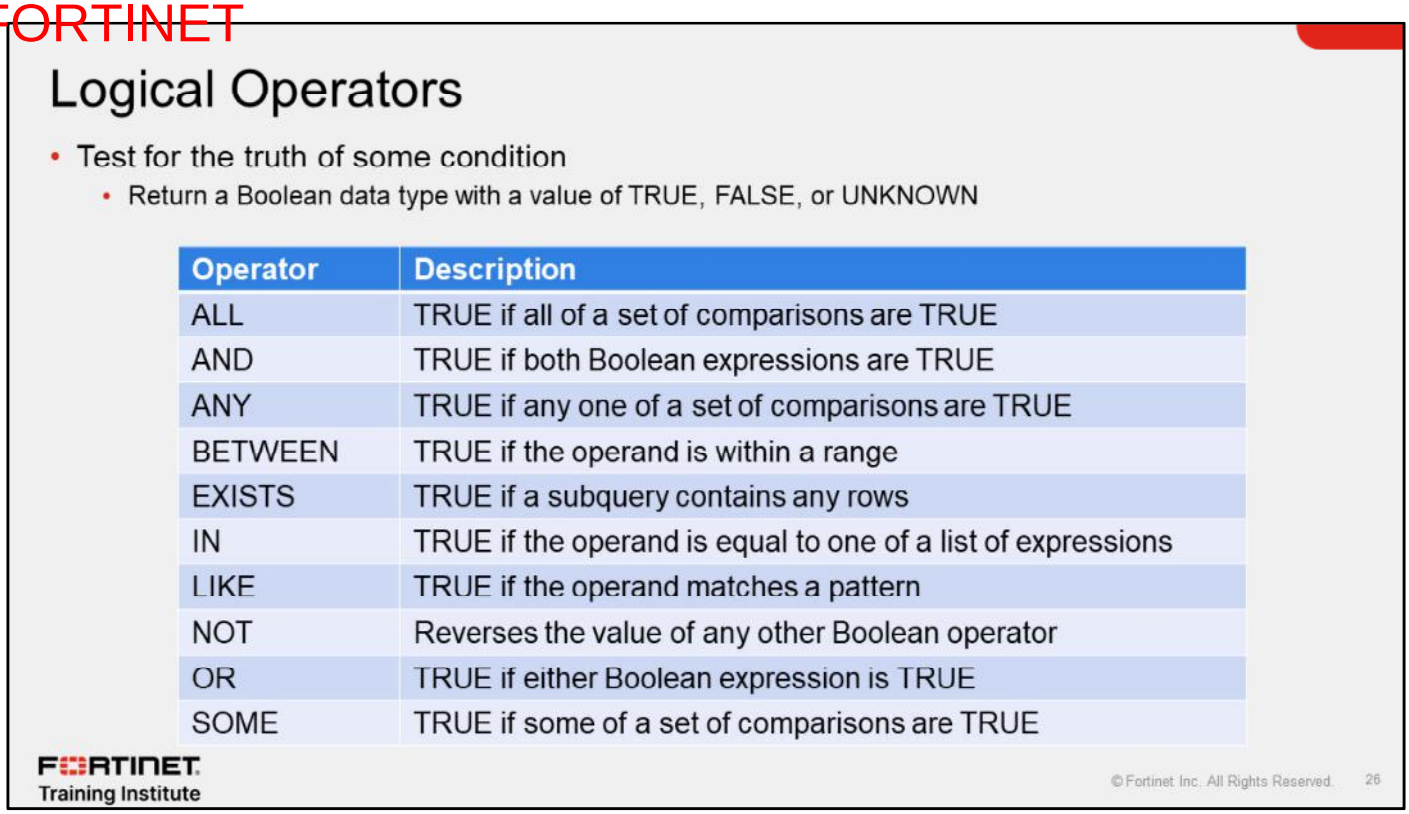
- Test whether two expressions are the same
  - Can be used on all expressions except text, ntext, or image data types

Operator	Description
=	Equal to
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to
<>	Not equal to
!=	Not equal to (not ISO standard)
!<	Not less than (not ISO standard)
!>	Not greater than (not ISO standard)

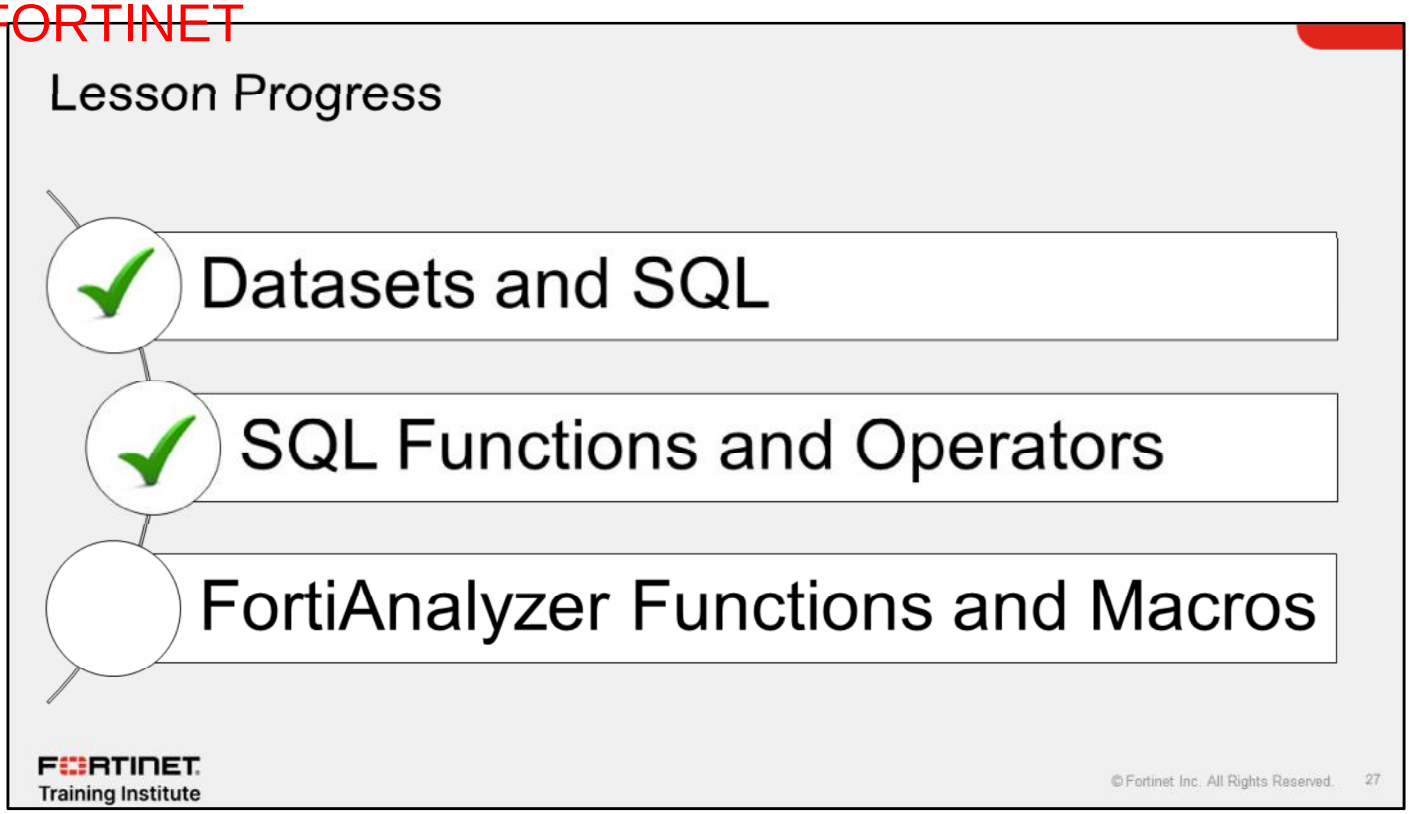
FORTINET Training Institute

 25

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.

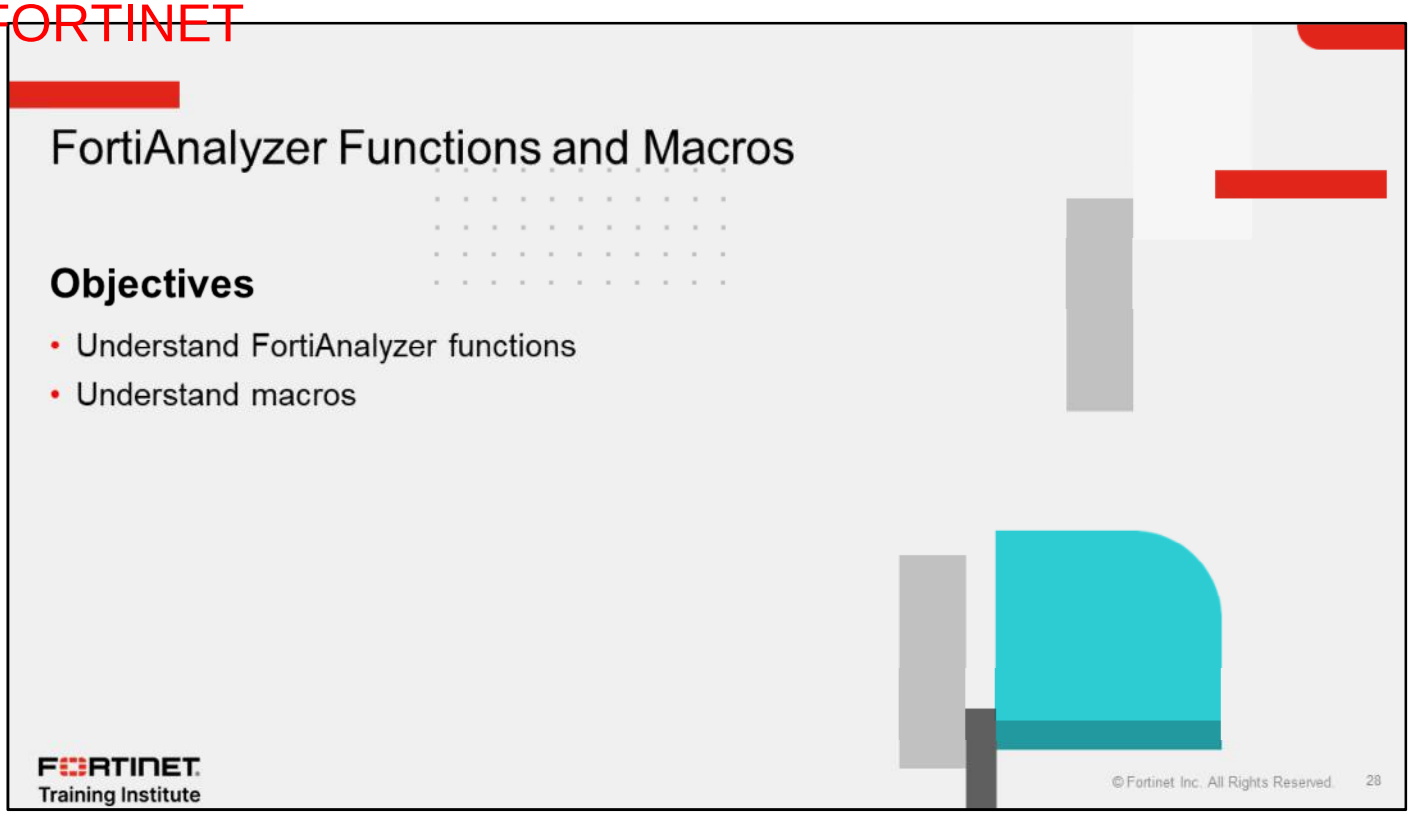


Here are some examples of logical operators. Logical operators test for the truth of a condition. Like comparison operators, they return a Boolean data type with a value of TRUE, FALSE, or UNKNOWN.



Good job! You now understand SQL functions and operators.

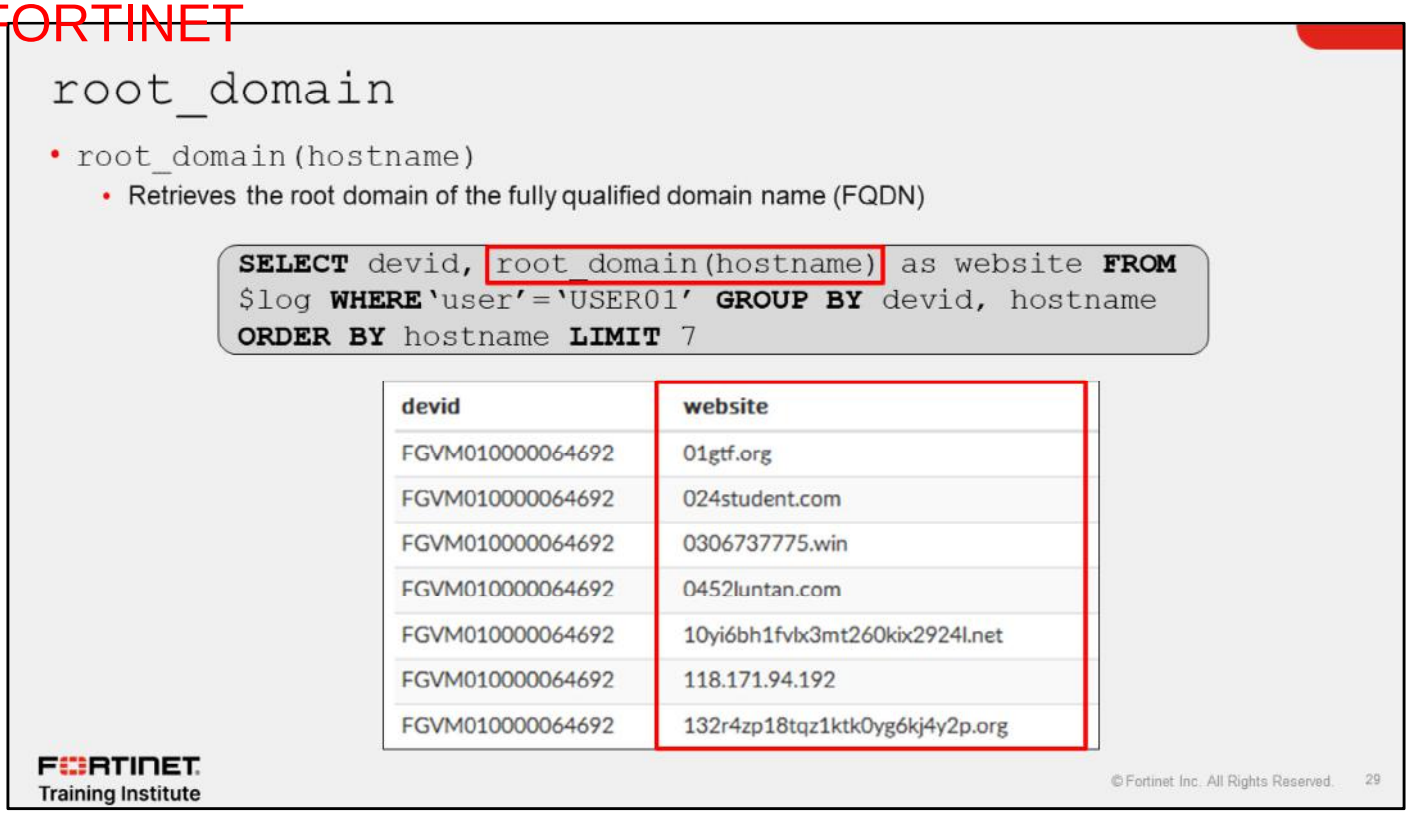
Now, you will learn about FortiAnalyzer functions and macros.



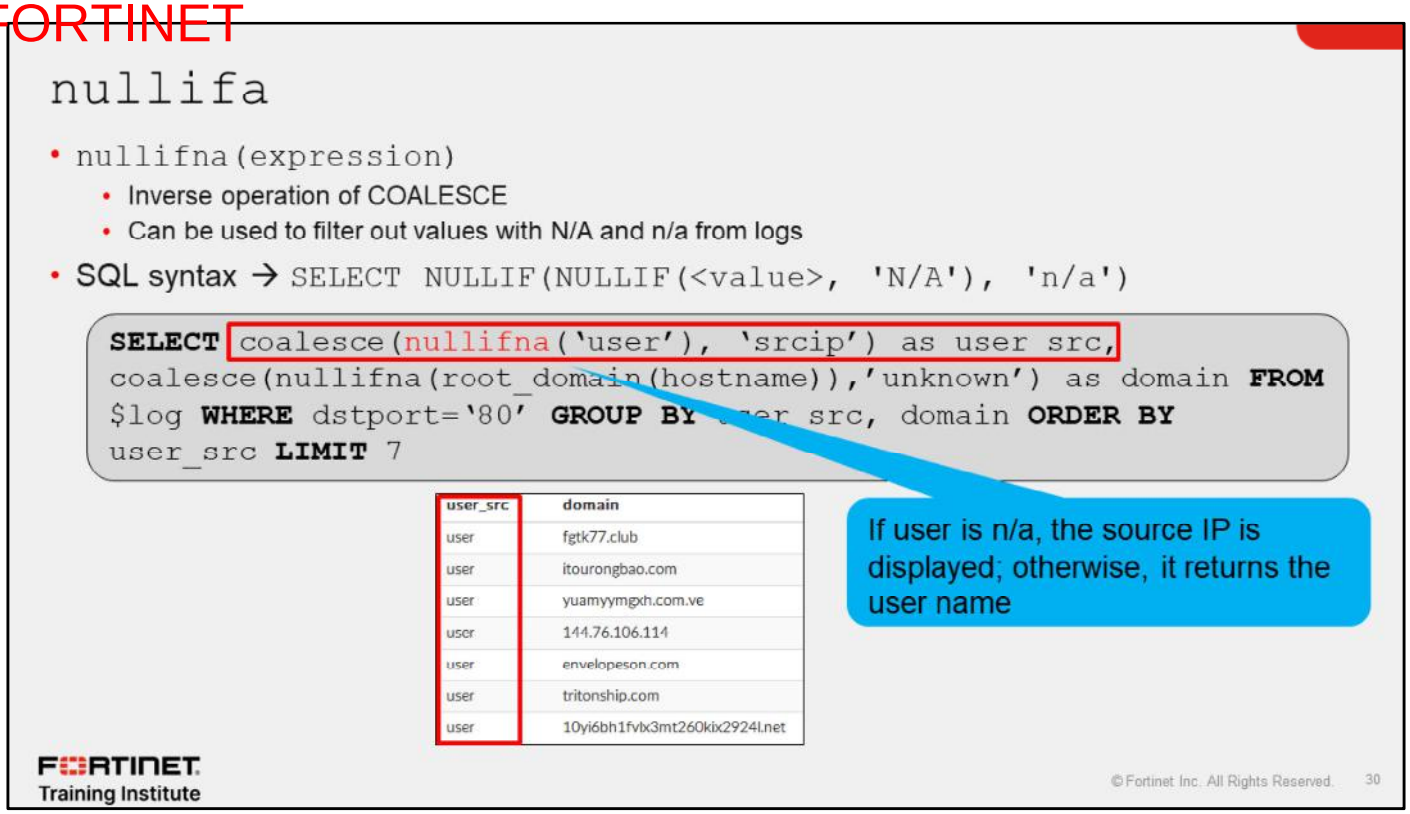
This section covers FortiAnalyzer functions and macros.

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.

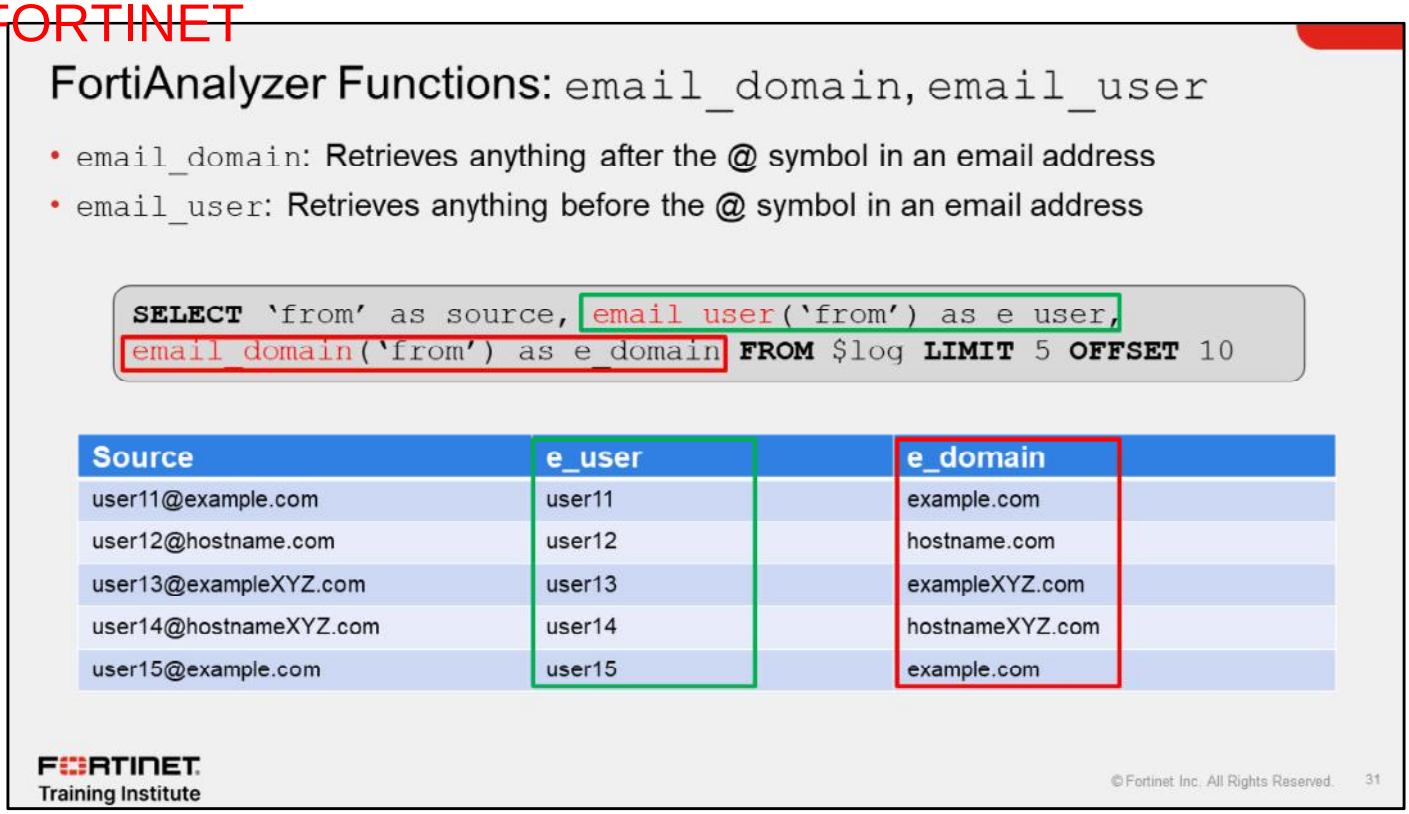


One FortiAnalyzer-specific function is `root_domain(hostname)`. This provides the root domain of the fully qualified domain name. As specified by the query, in this example `root_domain(hostname)` is listed under the **website** column in ascending order. Unless otherwise specified, ascending order is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



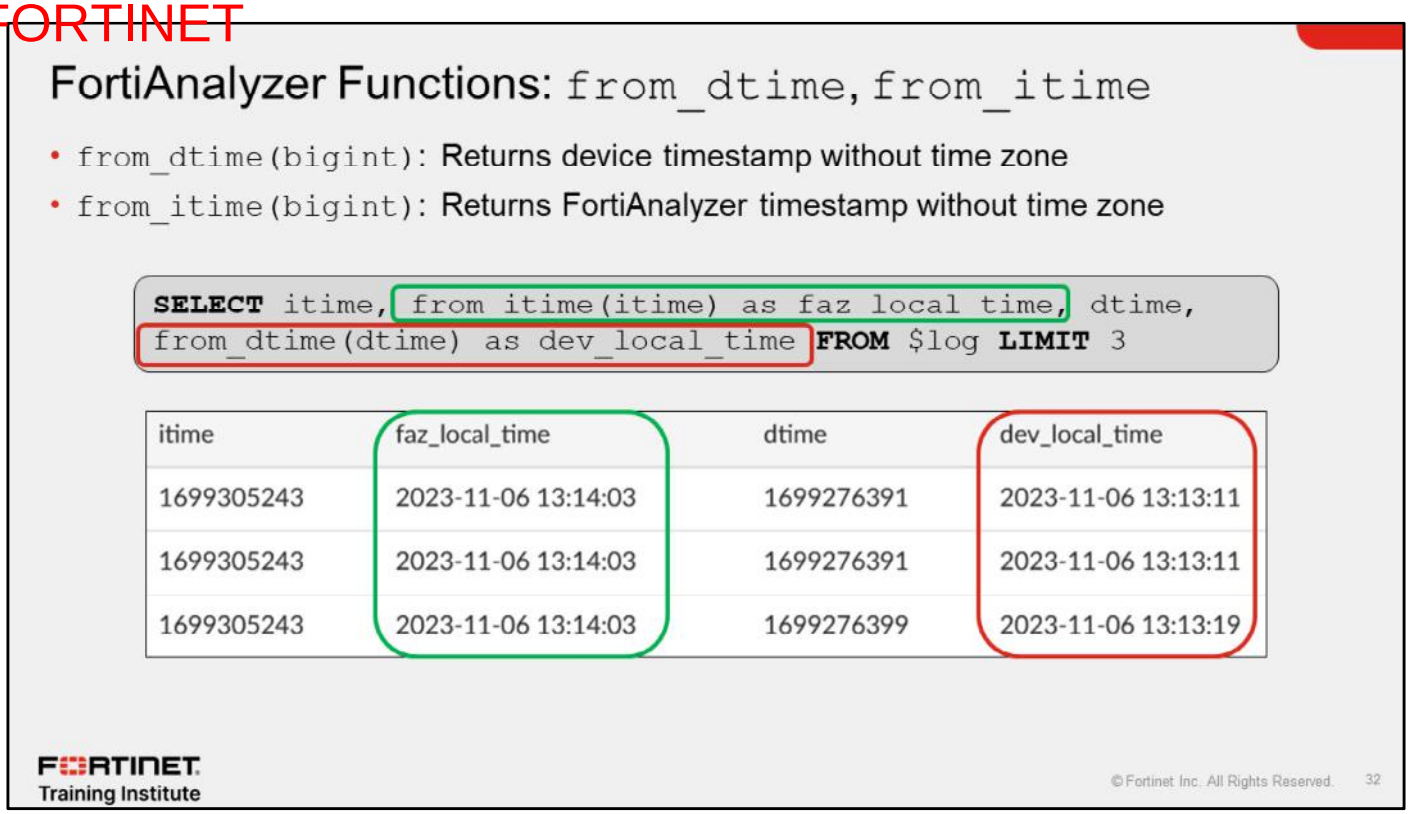
Another FortiAnalyzer-specific function is nullifna, which takes an expression as an argument. The actual SQL syntax this is based on is SELECT NULLIF(NULLIF(expression, 'N/A'), 'n/a').

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.



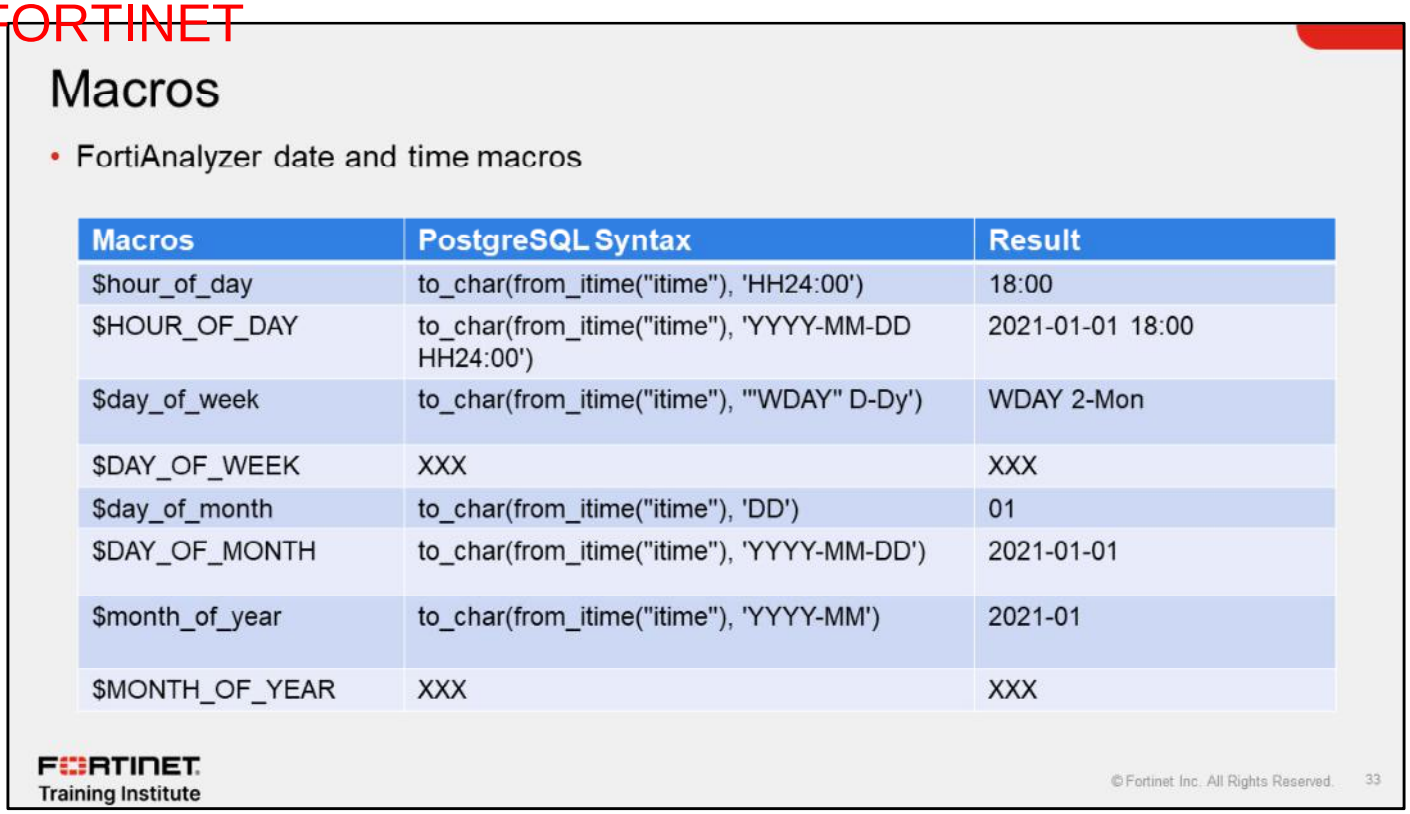
`email_domain` and `email_user` are other FortiAnalyzer-specific functions. `email_domain` retrieves anything that comes after the @ symbol in an email address—the domain. `email_user` retrieves anything that comes before the @ symbol in an email address.

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**.

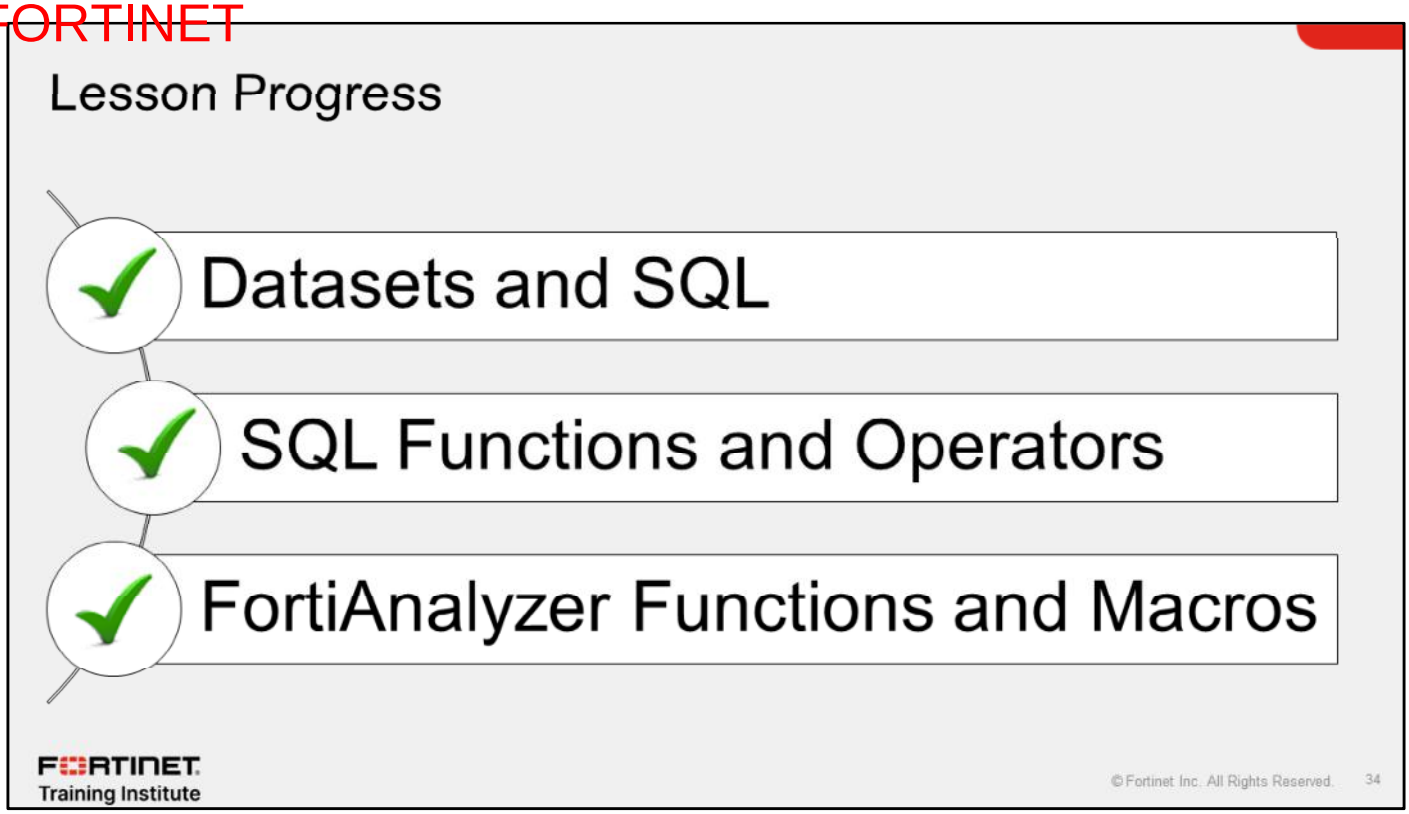


from_dtime and from_itime are other FortiAnalyzer-specific functions. from_dtime returns the device timestamp without the time zone, while from_itime returns the FortiAnalyzer's timestamp without the time zone.

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



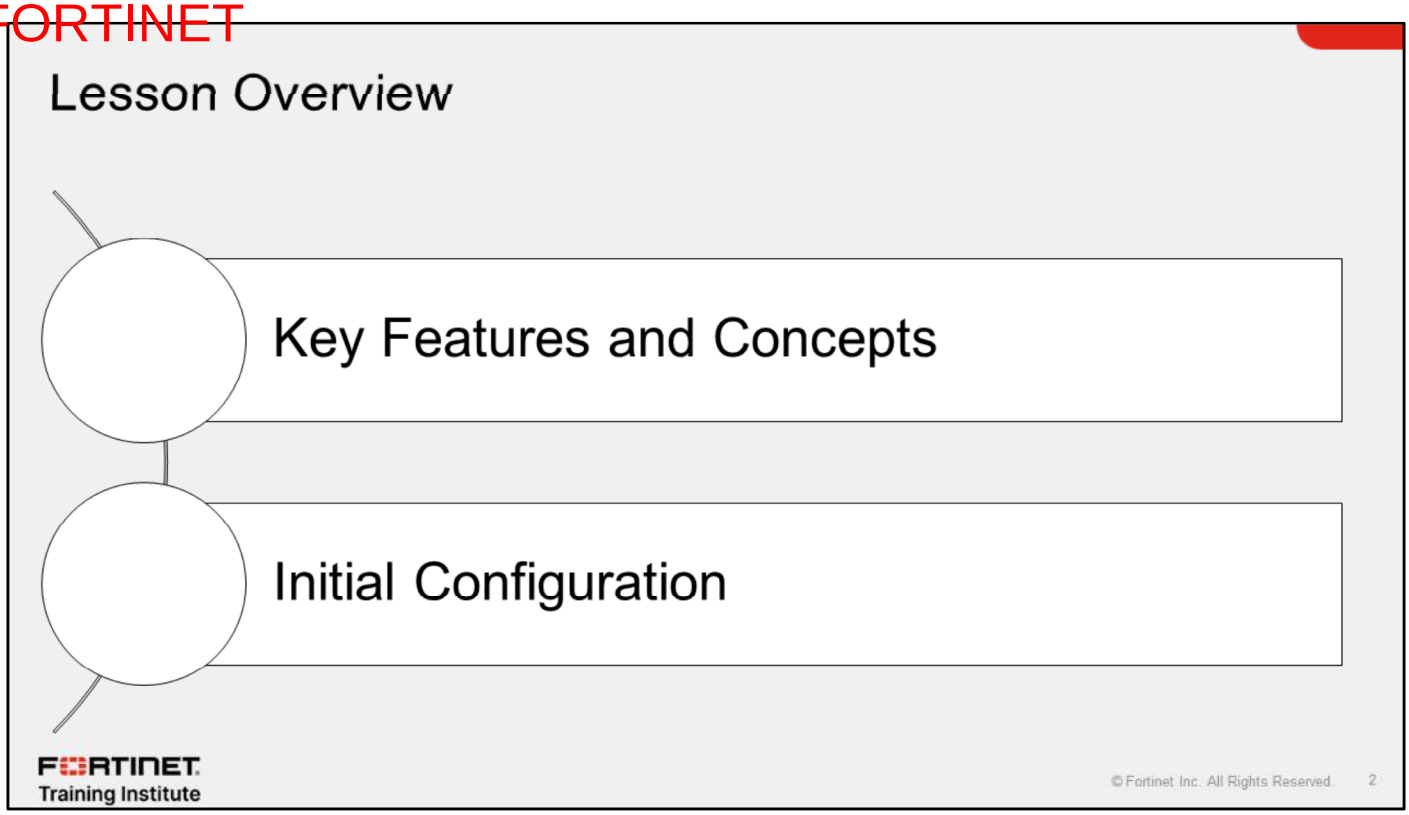
Here are some common date and time macros used in FortiAnalyzer. Macros are simple substitutions for more complex SQL statements—usually created for SQL statements that are frequently used.



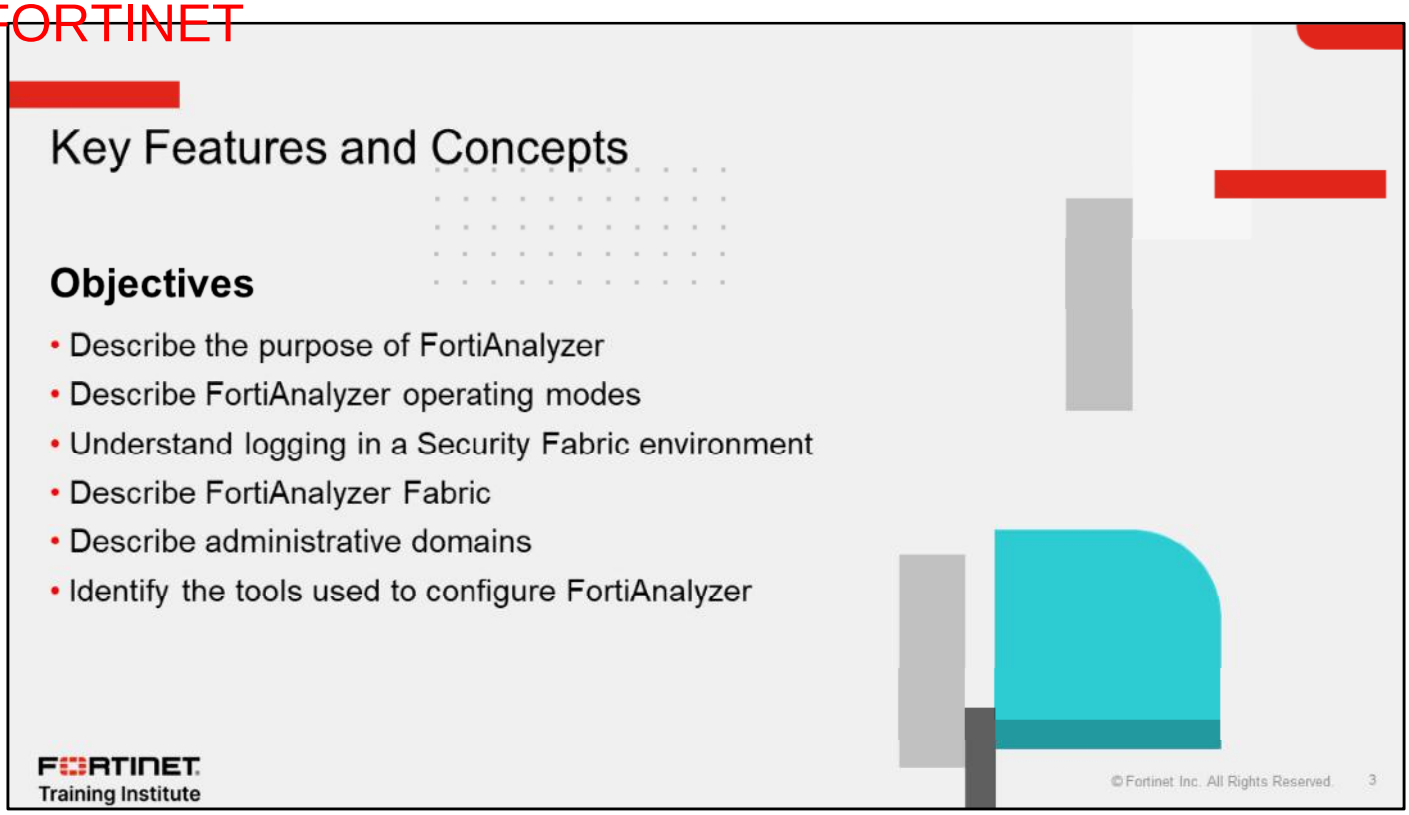
Congratulations! You have come to the end of this material.

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

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

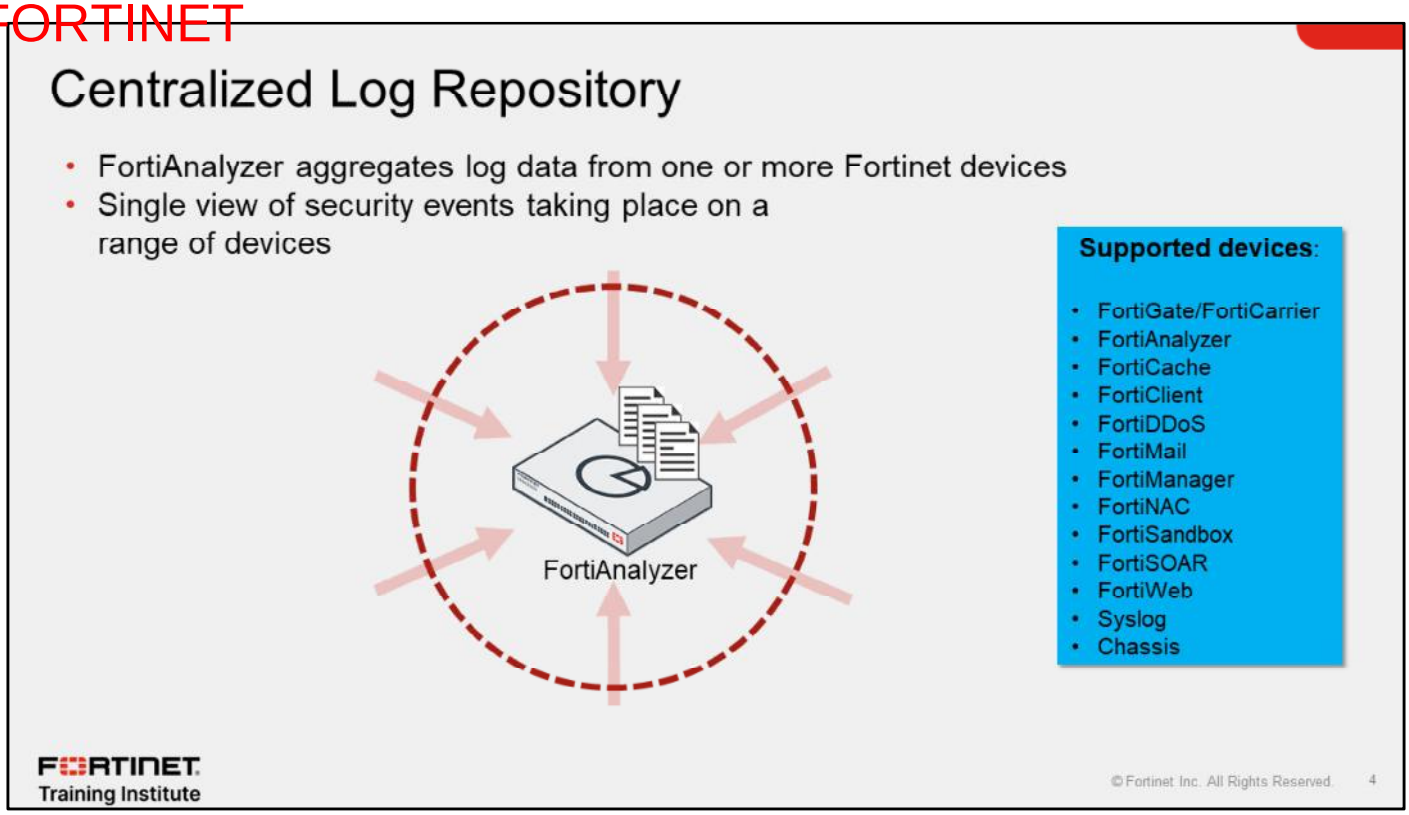


In this lesson, you will learn about the topics shown on this slide.



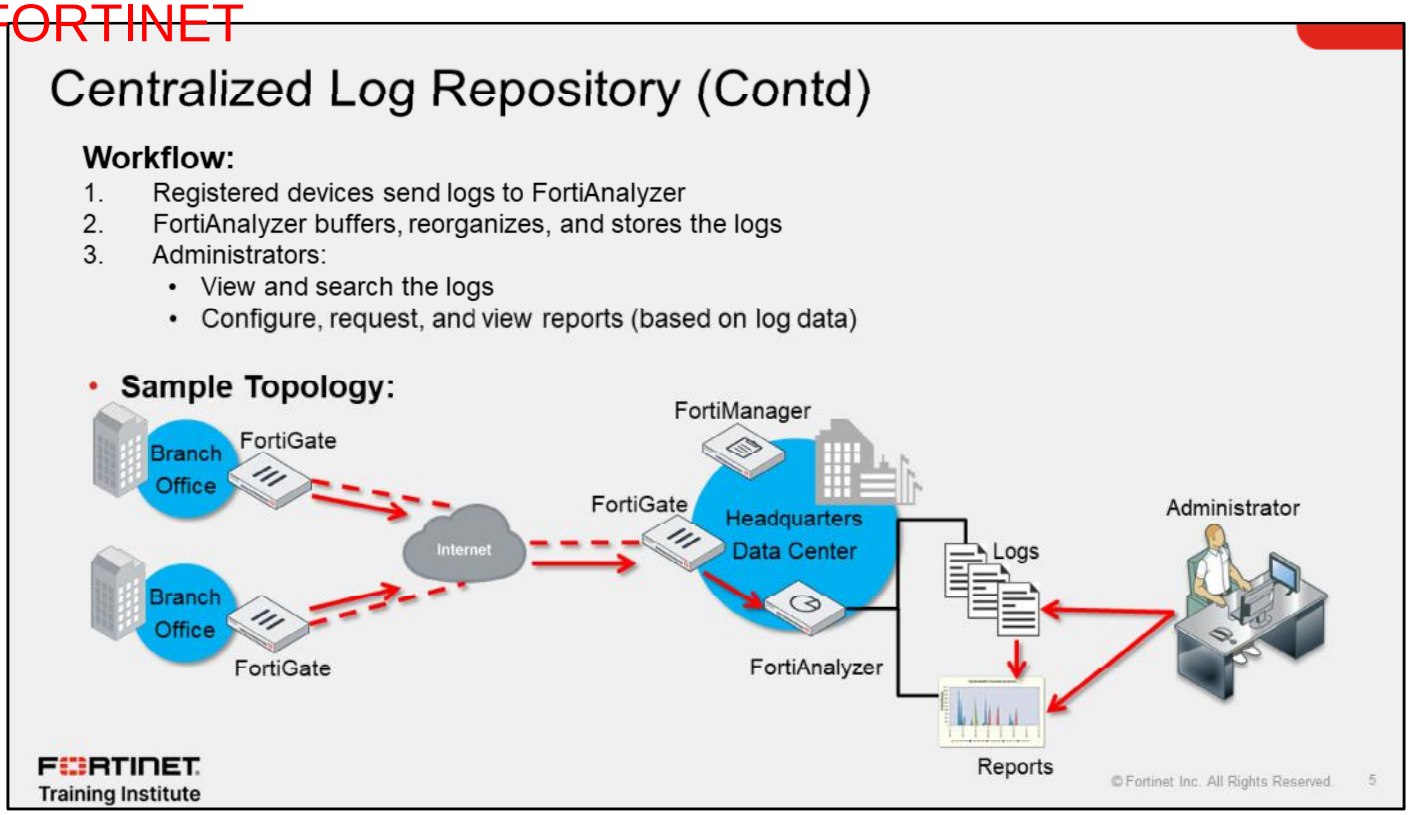
After completing this section, you should be able to achieve the objectives shown on this slide.

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

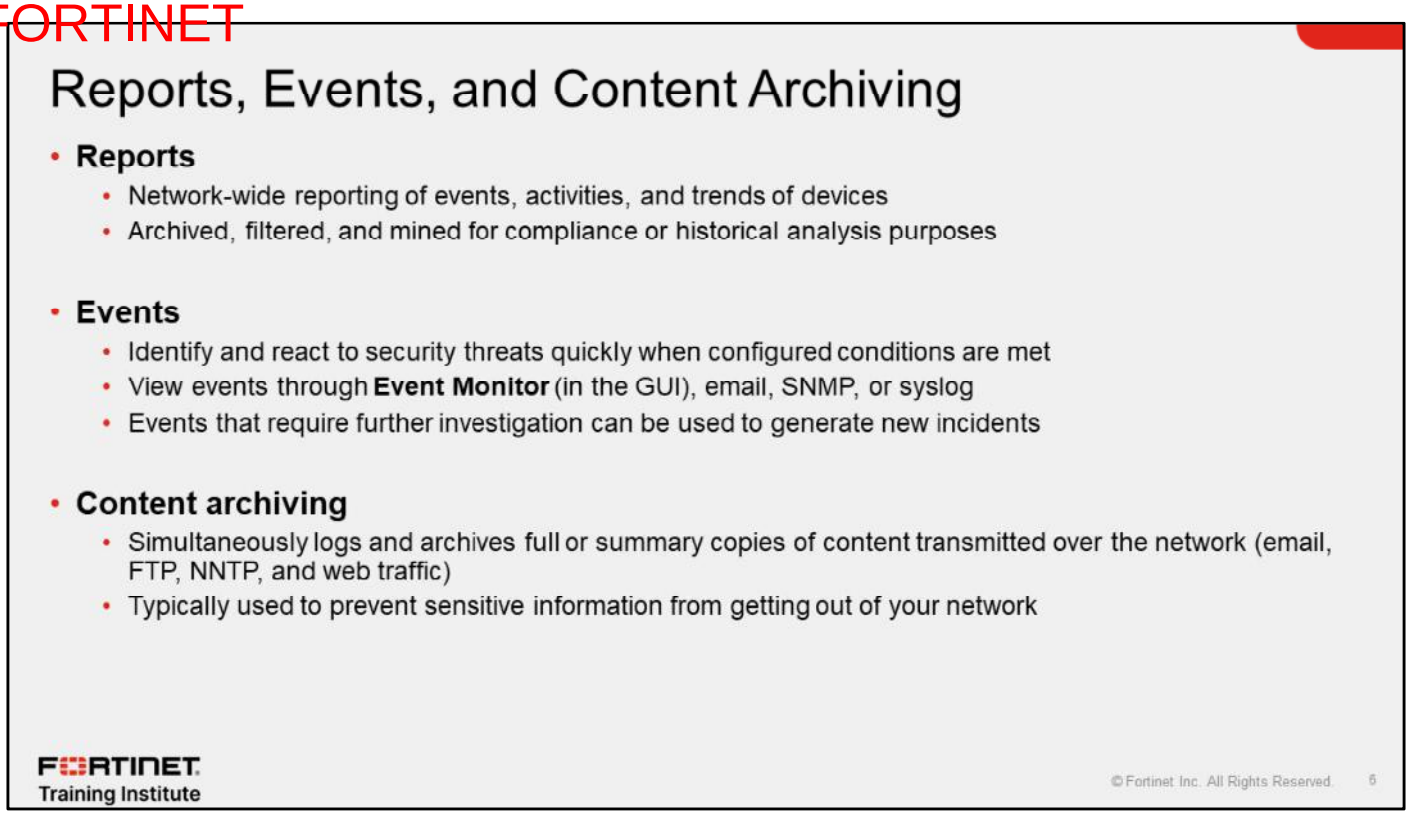
FortiAnalyzer can be integrated with many different Fortinet solutions. For a complete list, refer to the release notes at docs.fortinet.com.



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 is easy to search and run reports.
3. Administrators can connect to FortiAnalyzer using the GUI to view the logs manually, or generate reports to look at the data. You can also use the CLI to perform administrative tasks.

FortiAnalyzer can be easily integrated into a network, even if there are multiple sites. A sample topology can include multiple branches and a headquarters. Each location's firewall is added into 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 information and, if necessary, take the required actions. You can archive and filter the network knowledge you glean from these reports, as well as mine it for compliance or historical analysis purposes.

FortiAnalyzer events allow you to react quickly to threats because it’s not realistic to physically monitor your network around the clock. The system can generate events when specific conditions in the logs are met—conditions you have configured FortiAnalyzer to monitor for registered devices. You can see your events on the GUI, and you can also send them to multiple recipients by email, SNMP, or syslog. Additionally, events that required further investigation can be used 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 getting out of your organization's network. You can also use it to record network use. The data loss prevention (DLP) engine can examine email, File Transfer Protocol (FTP), Network New 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.

Database Language Support

- FortiAnalyzer supports Structured Query Language (SQL) for logging and reporting
- FortiAnalyzer inserts log data into the SQL database for log view and report generation
- FortiAnalyzer uses a PostgreSQL database
- *Advanced reporting capabilities require some knowledge of SQL and databases*

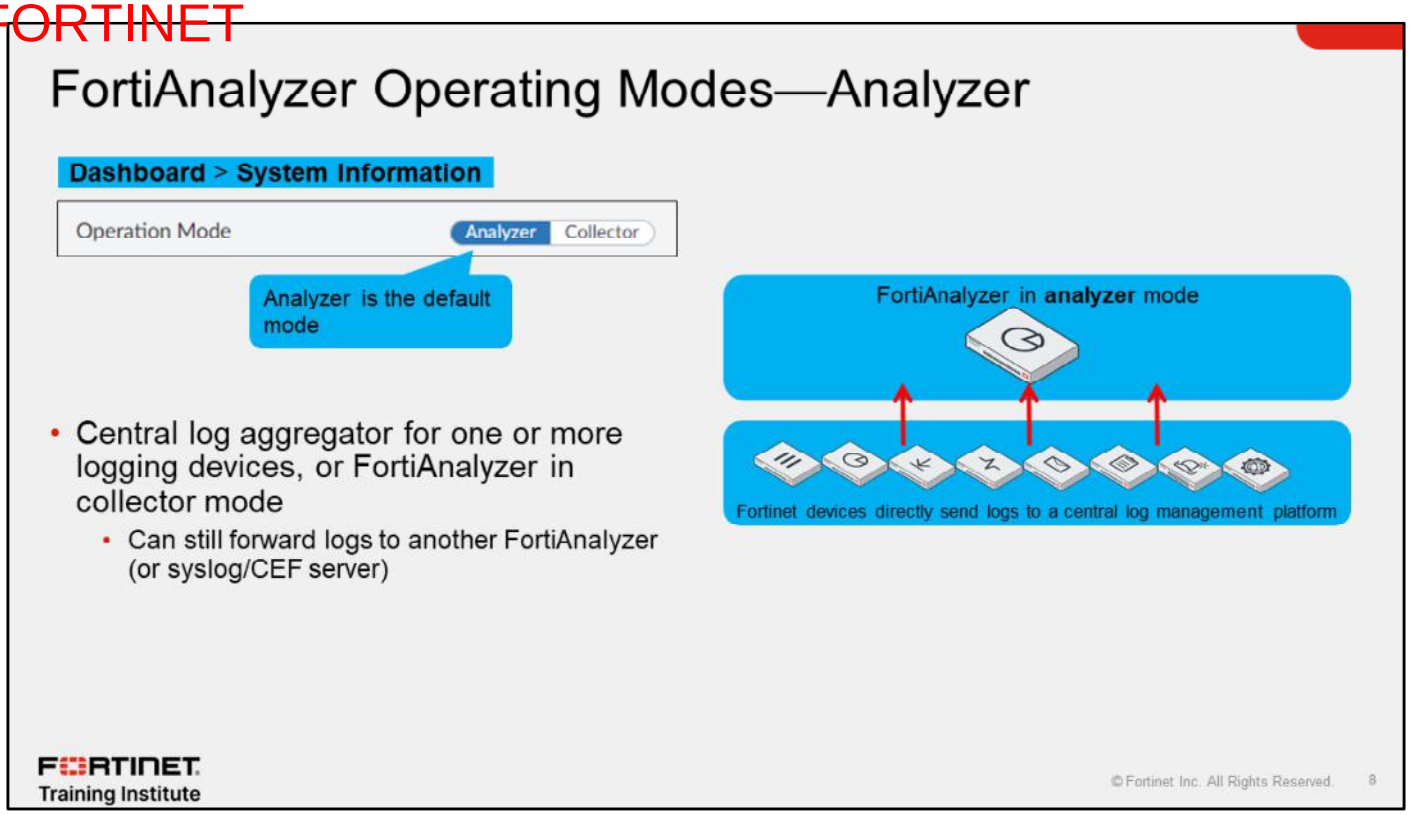
FORTINET Training Institute

 7

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

Advanced reporting capabilities require some knowledge of SQL and databases. For example, you may need to compose custom SQL queries, known as datasets, to extract the data you require from the database.

For more information on SQL and FortiAnalyzer, refer to the supplementary lesson *SQL Datasets*.



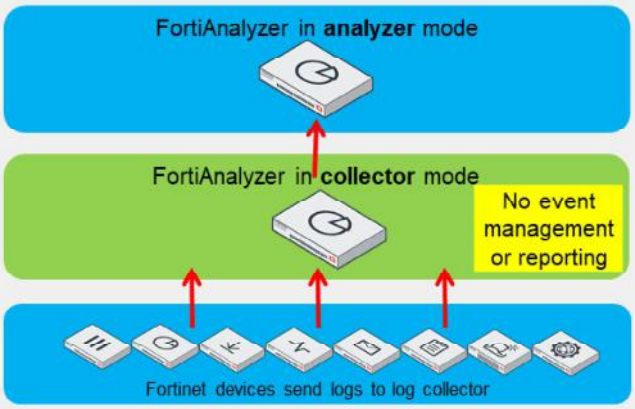
FortiAnalyzer has two modes of operation: analyzer and collector. The mode of operation you choose depends on your network topology and individual requirements.

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

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

FortiAnalyzer Operating Modes—Collector

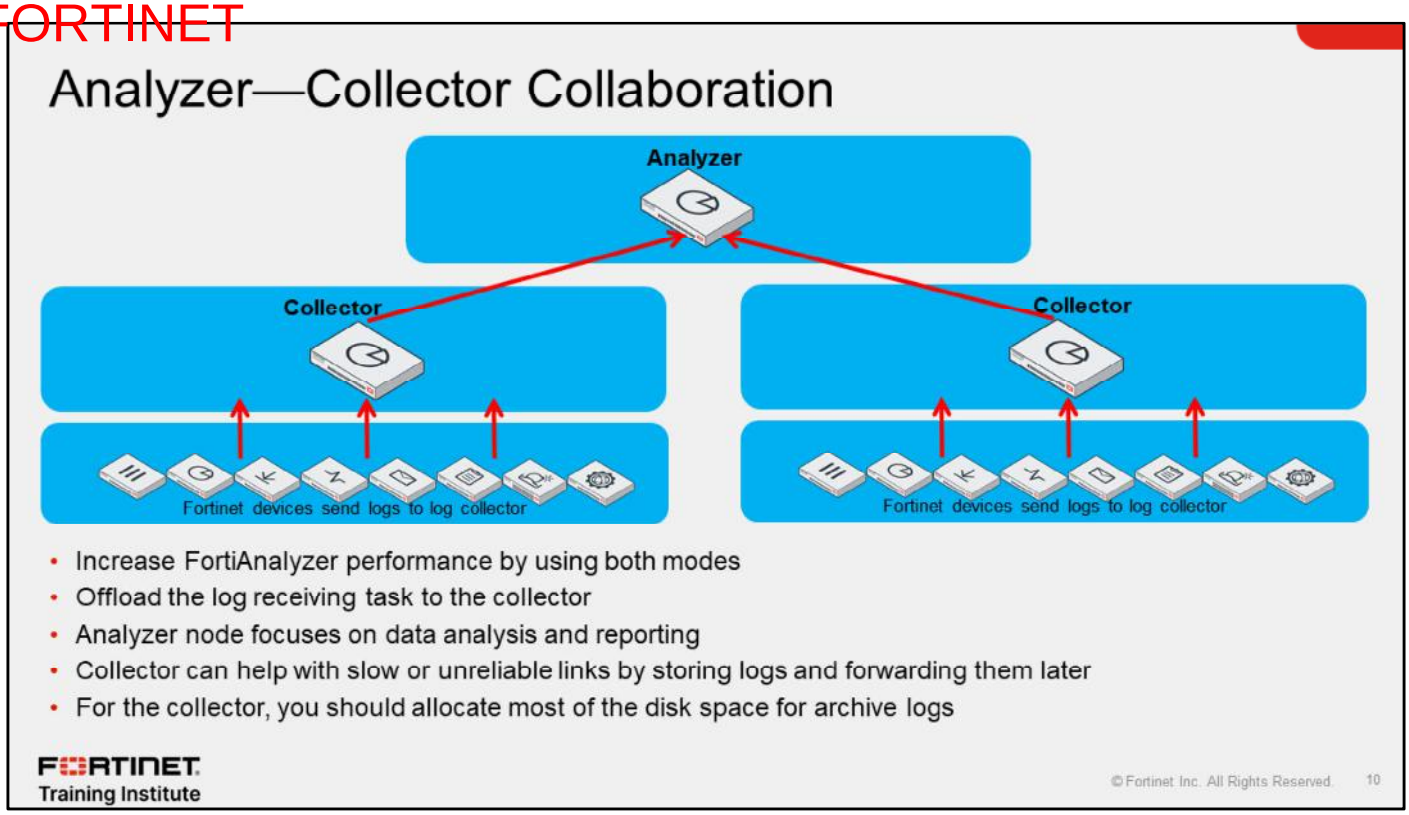
- Collects logs from multiple devices and forwards them to FortiAnalyzer in analyzer mode
  - Can aggregate logs to another FortiAnalyzer
  - However, can forward to syslog/CEF server in real-time forwarding mode only
- Not used for analytics—archiving only



FORTINET Training Institute

 9

When operating in collector mode, the device collects logs from multiple devices and then forwards those logs, in their original binary format, to another device, such as a FortiAnalyzer operating in analyzer mode. It can also send them to a syslog server or a common event format (CEF) server, depending on the forwarding mode. 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.



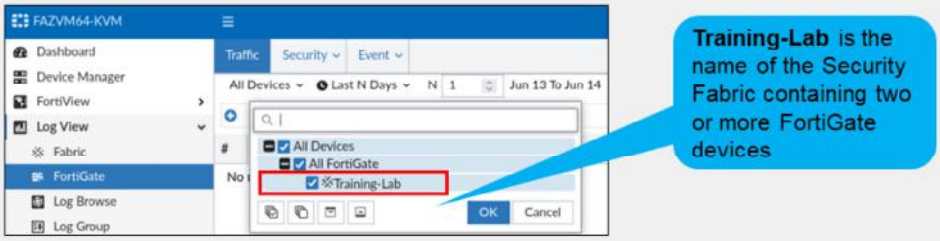
By using both analyzer and collector modes, you increase FortiAnalyzer performance: Collectors offload the task of receiving logs from multiple devices from the analyzer. This allows the analyzer to focus on data analysis and reporting tasks.

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 does not perform any analytics tasks, it should have most of the disk space allocated 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:
    - If an upstream FortiGate performs NAT
    - Upstream FortiGate devices still log UTM events
- UTM and traffic logs are correlated so session details, UTM events, reporting and automation in the Security Fabric work correctly



FORTINET Training Institute

 11

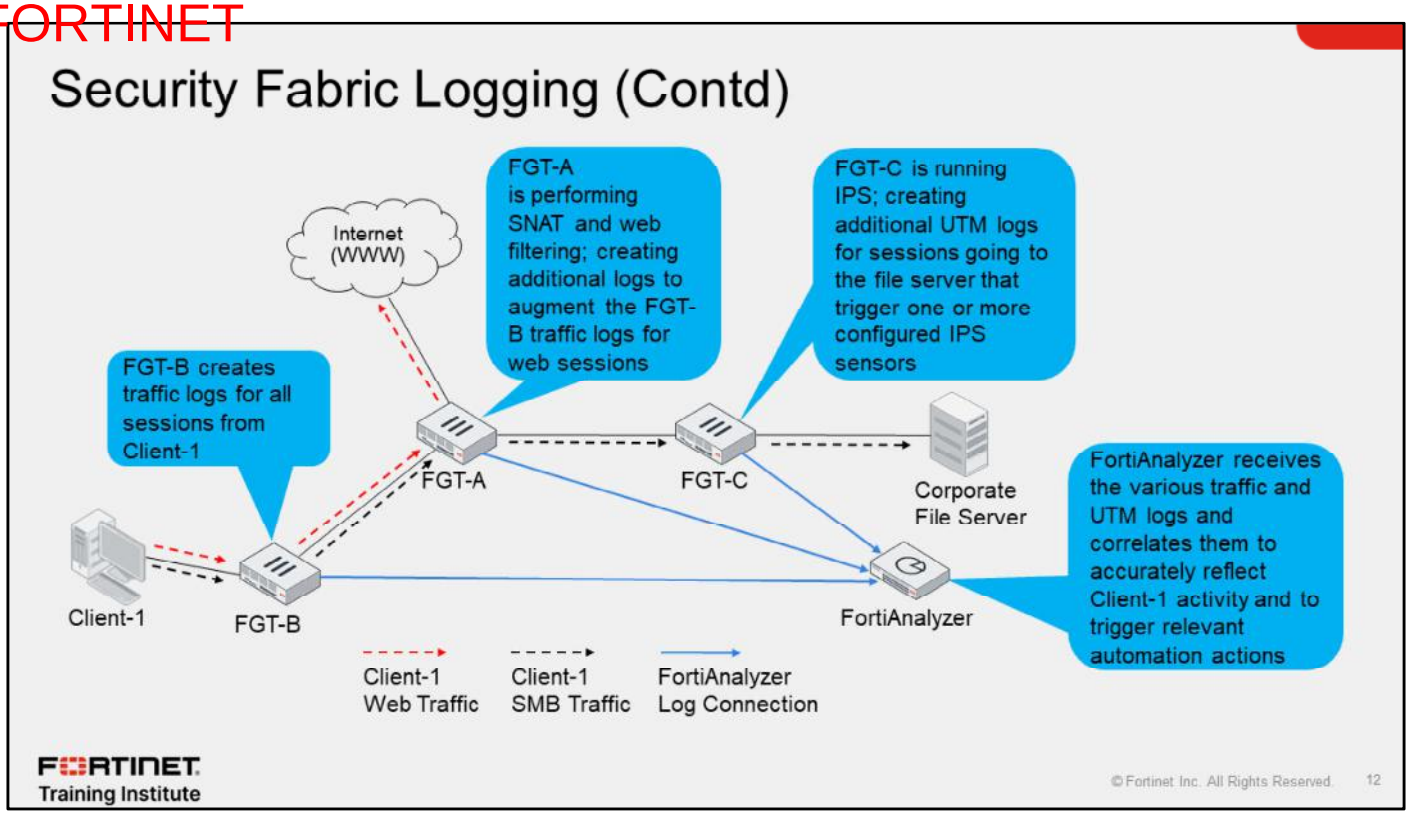
FortiAnalyzer supports the Security Fabric by storing and analyzing the logs from the devices in a Security Fabric group as if the logs are from a single device. FortiAnalyzer correlates traffic logs to corresponding UTM logs so that it can report sessions and bandwidth together with its unified traffic management (UTM) threats.

A session's traffic logging is always done by the first FortiGate that handled it in the Security 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 Security Fabric, it does not generate a new traffic log for that session. This helps to eliminate the repeated logging of a session by multiple FortiGate devices.

One exception to this behavior is that if the upstream FortiGate performs network address translation (NAT), then another log is generated. The additional log is needed to record NAT details, such as translated ports and addresses.

Upstream devices complete UTM logging, if configured, and FortiAnalyzer performs UTM and traffic log correlation for the Security Fabric, in order to provide a concise and accurate record of any UTM events that may occur. No additional configuration is required for this to take place because FortiAnalyzer performs this function automatically.

Note that each FortiGate in the Security 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 shows how logging functions in the Security Fabric to give full visibility while eliminating duplicate logs throughout the environment. There are three FortiGate devices configured in a Security Fabric along with a FortiAnalyzer device:

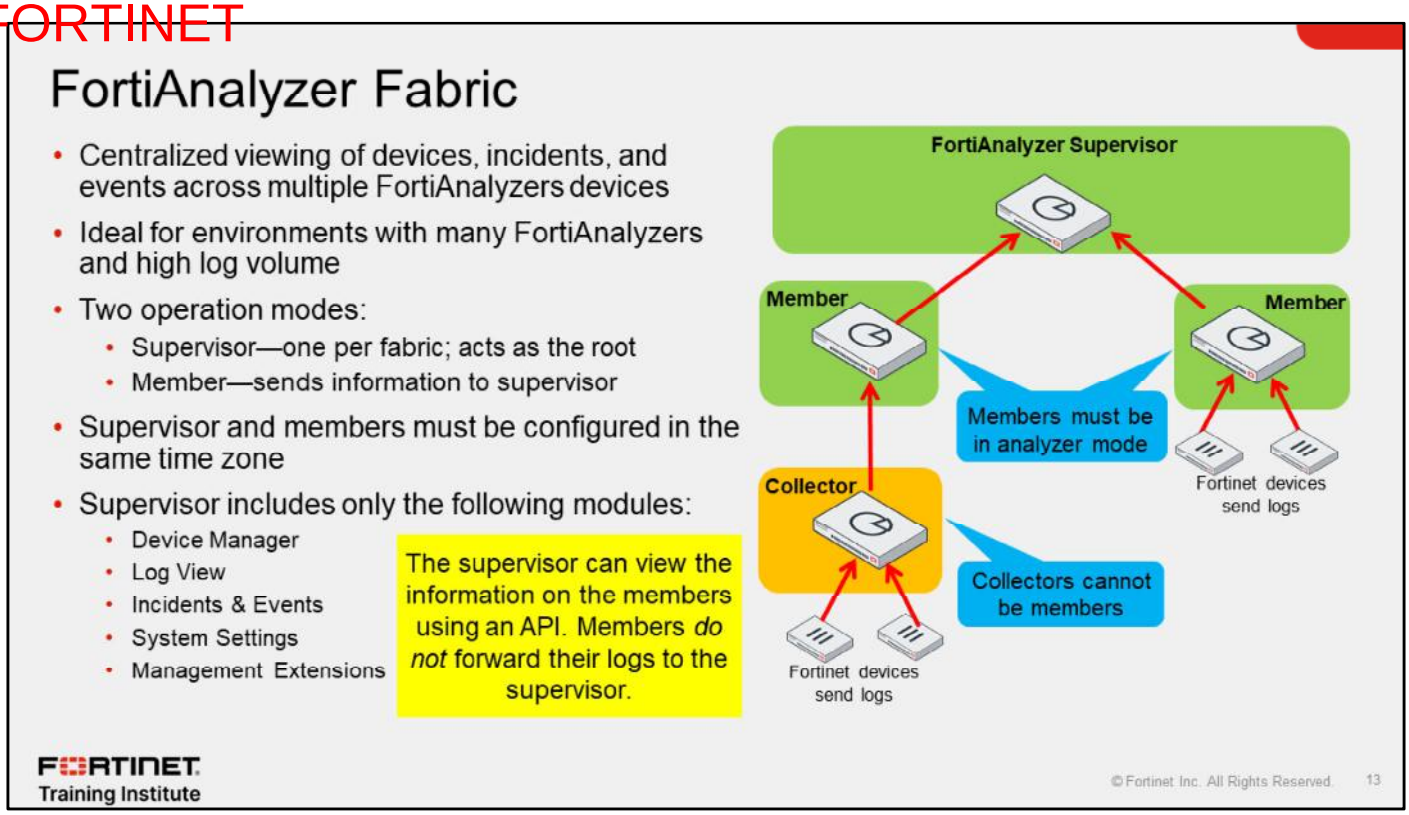
- FGT-A is installed between the corporate network and its internet service provider, where it performs SNAT on outbound communications for RFC-1918 hosts, as well as web filtering for HTTP/HTTPS sessions.
- FGT-B is installed in the access layer, providing device detection, breach isolation, and basic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

All traffic from Client-1 is received by FGT-B, which creates traffic logs for the initial session.

The web session is forwarded to FGT-A, which doesn't duplicate the initial traffic log, but does generate a traffic log as a result of source network address translation (SNAT) being applied to the session. Additionally, FGT-A applies a web filtering policy to this session and generates the relevant UTM logs, if appropriate.

The server message block (SMB) session is forwarded 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 and, should a signature match be triggered that results in an action generating a log, logs the event.

FortiAnalyzer receives the various traffic and UTM logs and correlates them automatically so that they are linked for proper viewing, reporting, and automation actions.



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

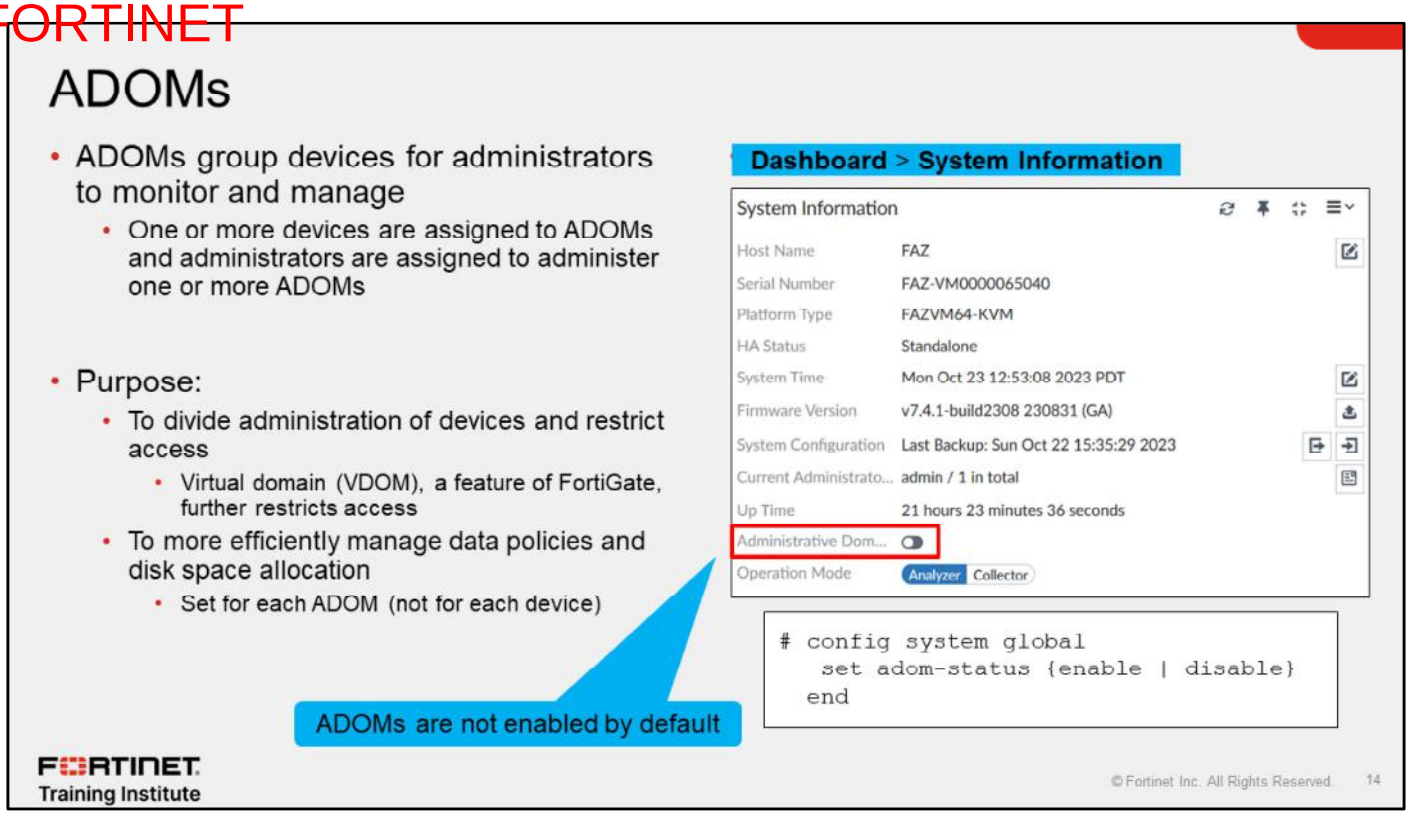
FortiAnalyzer Fabric includes two operation modes: supervisor and member.

Supervisors act as the root device in the FortiAnalyzer Fabric. Security operations center (SOC) administrators can use the supervisor to view member devices and their administrative domains (ADOMs), authorized logging devices, as well as incidents and events created on members. Incident and event information is synced from members to the supervisor using the API.

Members are devices in the FortiAnalyzer Fabric that send information to the supervisor for centralized viewing. When configured as a member, FortiAnalyzer devices continue to have access to the FortiAnalyzer features identified in the *FortiAnalyzer Administration Guide*. Incidents and events are created or raised from each member.

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

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



ADOMs allow you to group devices to monitor and manage. For example, administrators can manage devices that are grouped based on their geographical location or business division.

The purpose of ADOMs is to:

- Divide administration of devices by ADOM and to control (restrict) administrator access. If your network uses virtual domains (VDOMs), ADOMs can further restrict access to data that comes from the VDOM of a specific device.
- More efficiently manage data policies and disk space allocation, which are set per ADOM.

ADOMs are not enabled by default and can be configured only by the default **admin** administrator (or an administrator who has the Super_User profile).

All Fortinet devices included in a Security Fabric can be placed into an ADOM of the *Fabric* type, allowing for fast data processing and log correlation.

You will learn more about ADOMs in this course.

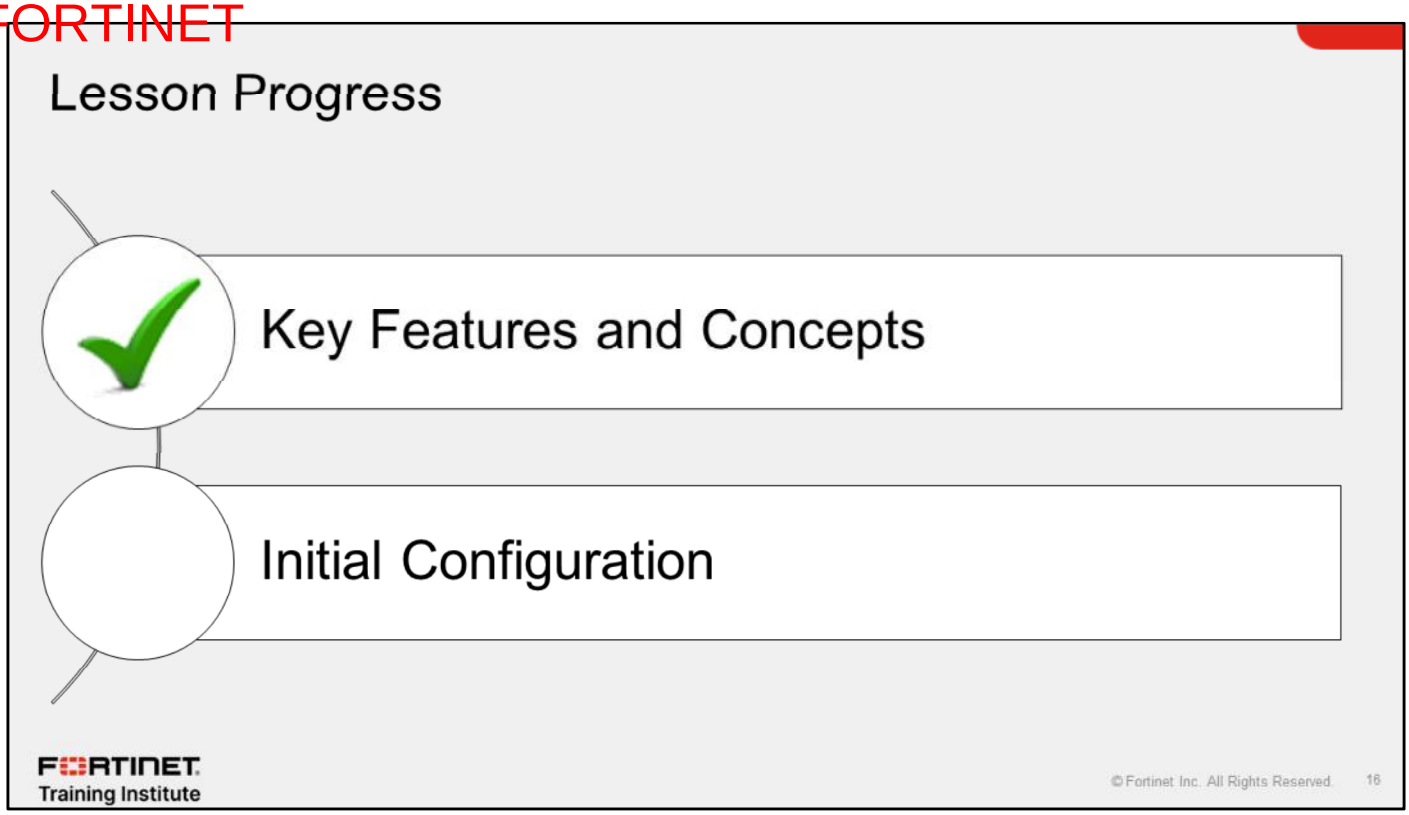
Knowledge Check

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

2. Which FortiAnalyzer operating mode do you use to collect logs from multiple devices and then forward those logs to another device?
   - A. Analyzer
   - ✓ B. Collector

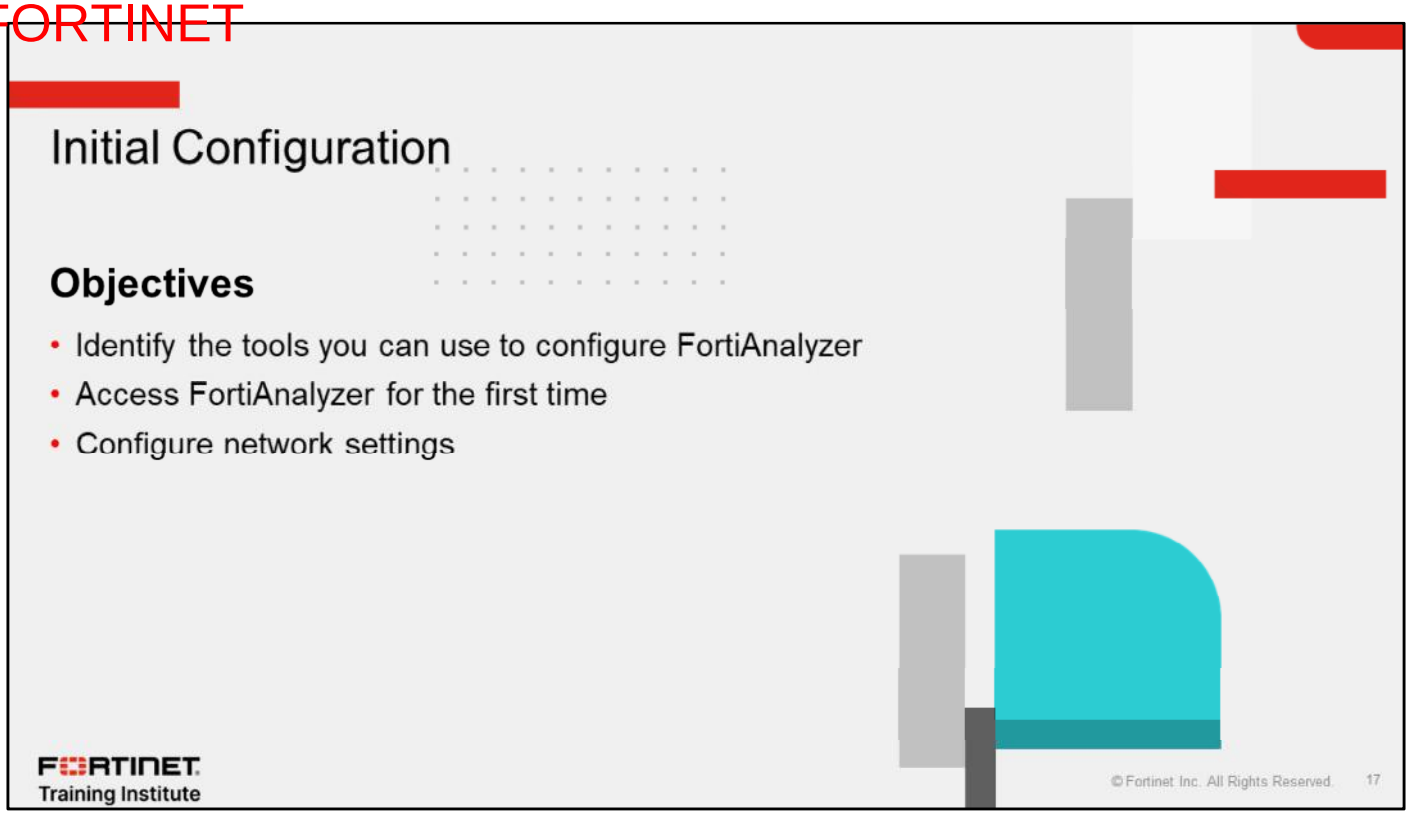
FORTINET Training Institute

 15



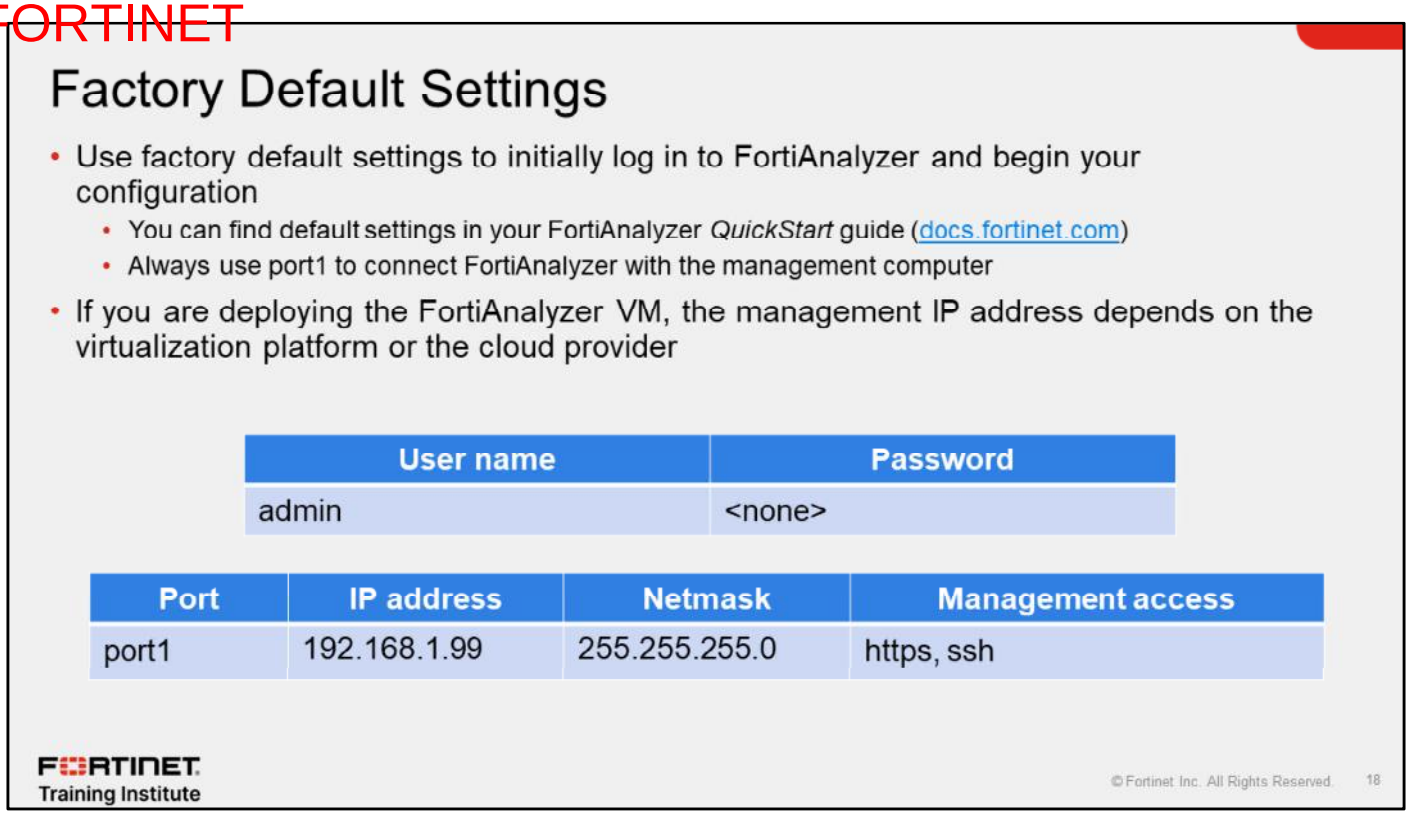
Good job! You now understand FortiAnalyzer key features and concepts.

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.

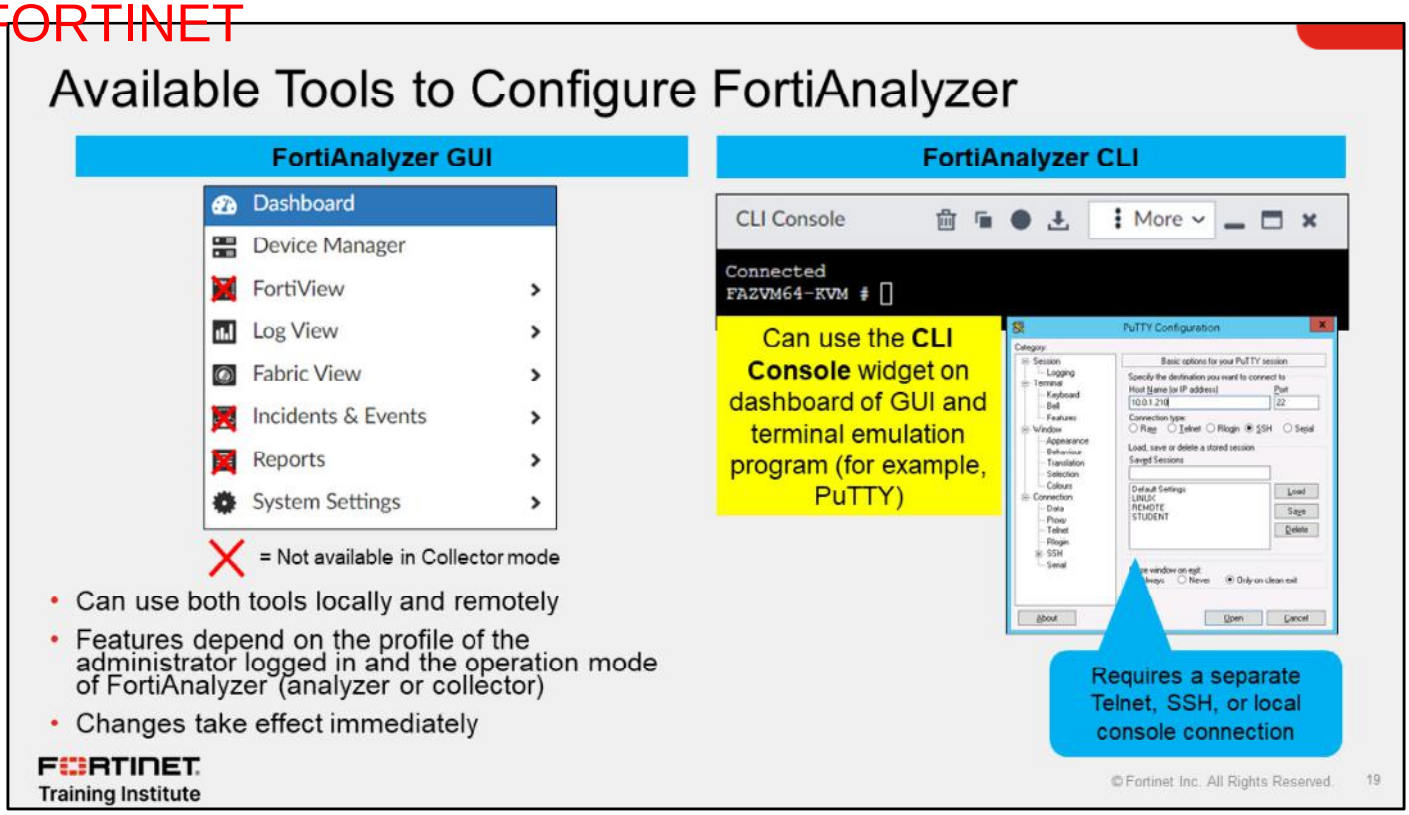


It is important to know the factory default settings, such as the default username and password, the port1 IP address, the netmask, and the default supported management access protocols, so you can initially connect to the management interface and configure FortiAnalyzer for your network.

You can find the default settings in the *FortiAnalyzer QuickStart Guide* that is specific to your FortiAnalyzer model. Different FortiAnalyzer models have different numbers of ports, but port1 is the management port and always has the same default IP address.

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

You can also configure your management IP on the CLI using the `config system interface` command.



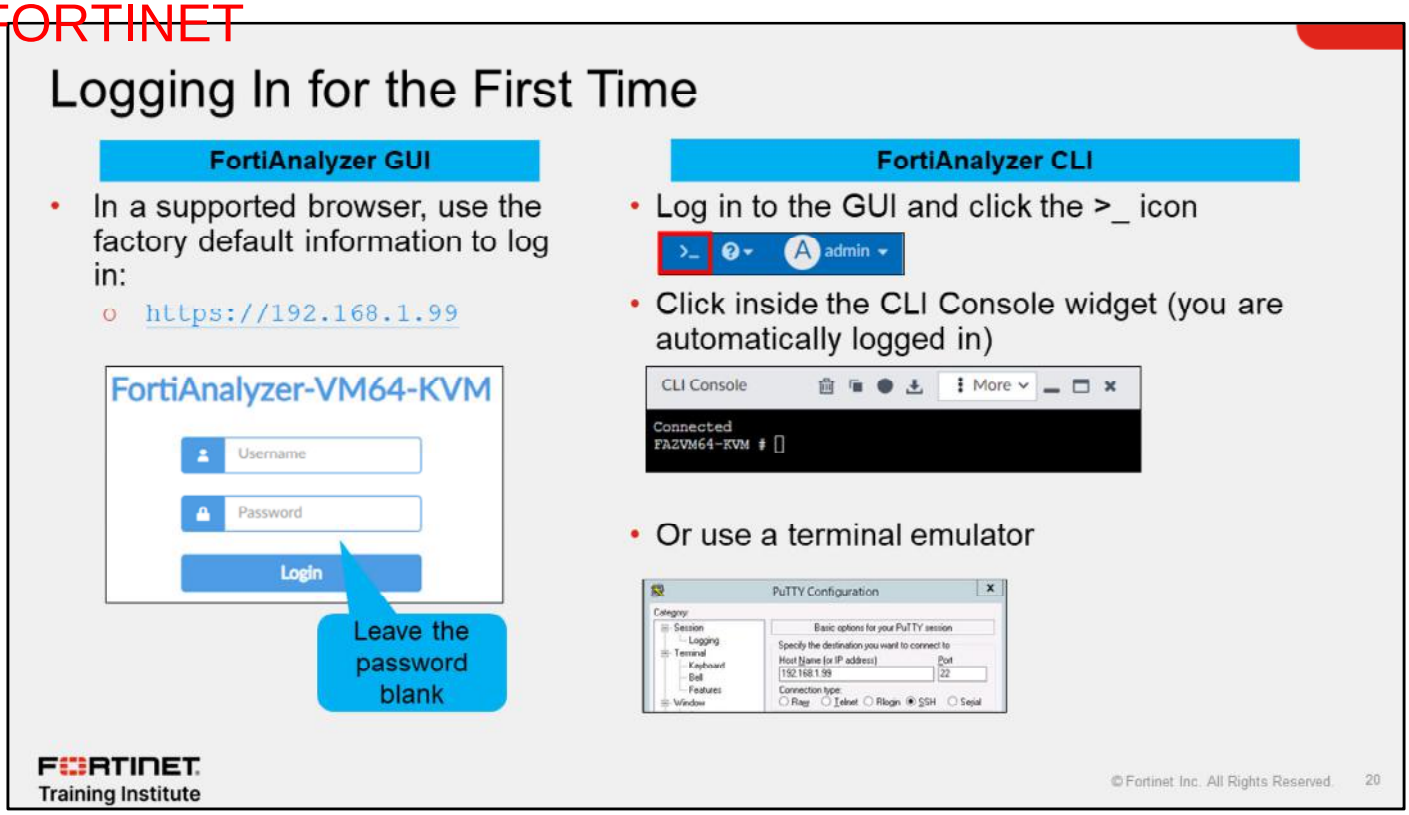
The GUI and CLI are the two configuration tools you can use to manage FortiAnalyzer. You can use both tools locally by connecting directly to FortiAnalyzer, and remotely, based on your configured settings. You can deny or permit access based on IP address.

When you use the CLI, you can run 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 FortiAnalyzer features available on the GUI and CLI depend on the profile of the administrator logged in and the operation mode of FortiAnalyzer. For example, when operating in collector mode, the GUI doesn't include **FortiView**, **Reports**, or **Incidents & Events**. Also, if you are logged in with the Standard_User or Restricted_User administrator profiles, full access privileges, like those granted to the Super_User profile, are not available. The CLI also includes some settings that are not available through the GUI.

Any configuration changes you make using the GUI and CLI take effect immediately upon applying the settings, without resetting the FortiAnalyzer system or interrupting services.

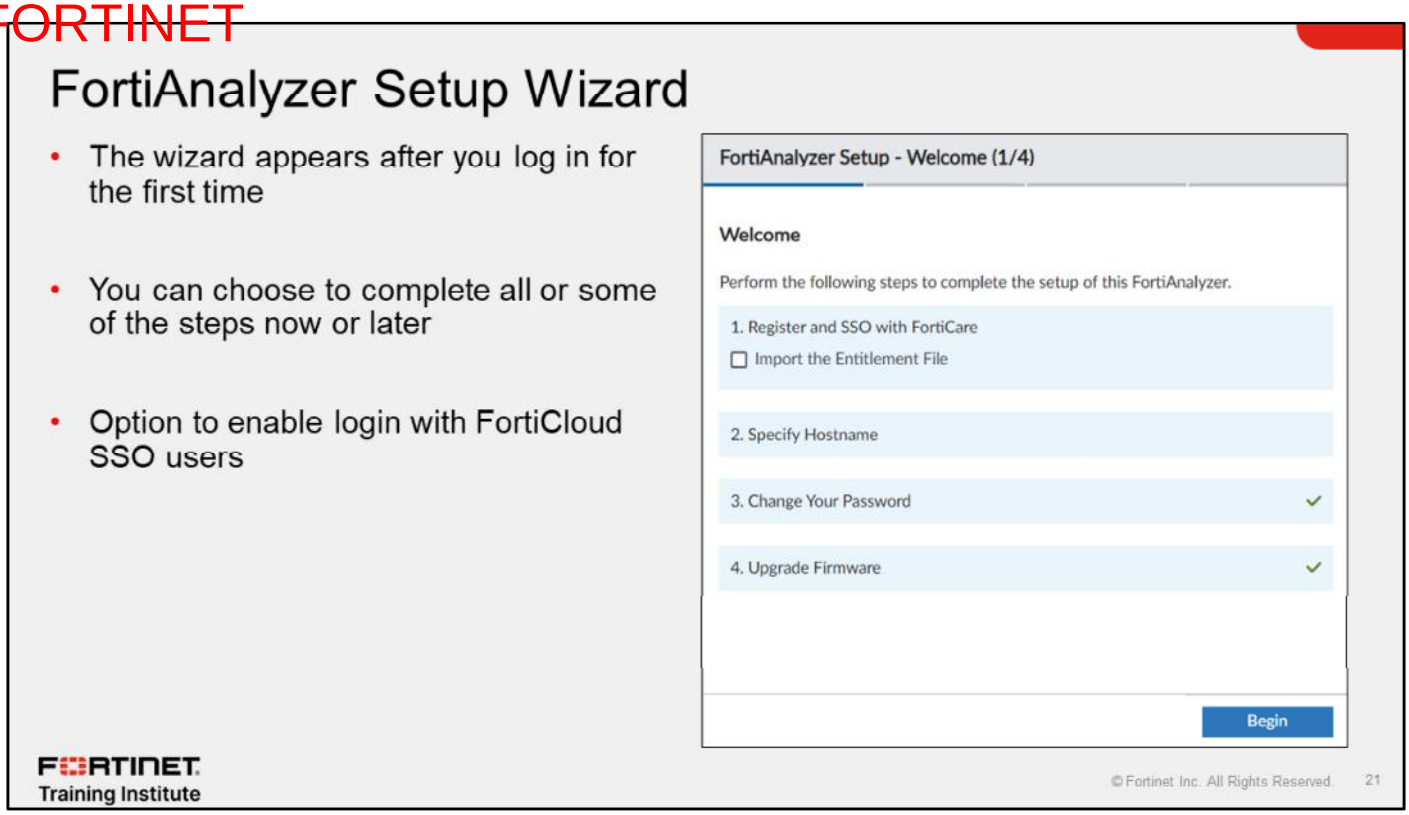
Note that the SQL database is disabled, by default, when FortiAnalyzer is in collector mode, so logs that require the SQL database are not available in collector mode unless the SQL database is enabled on the CLI.



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 lower case) 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 on the CLI icon located on 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.

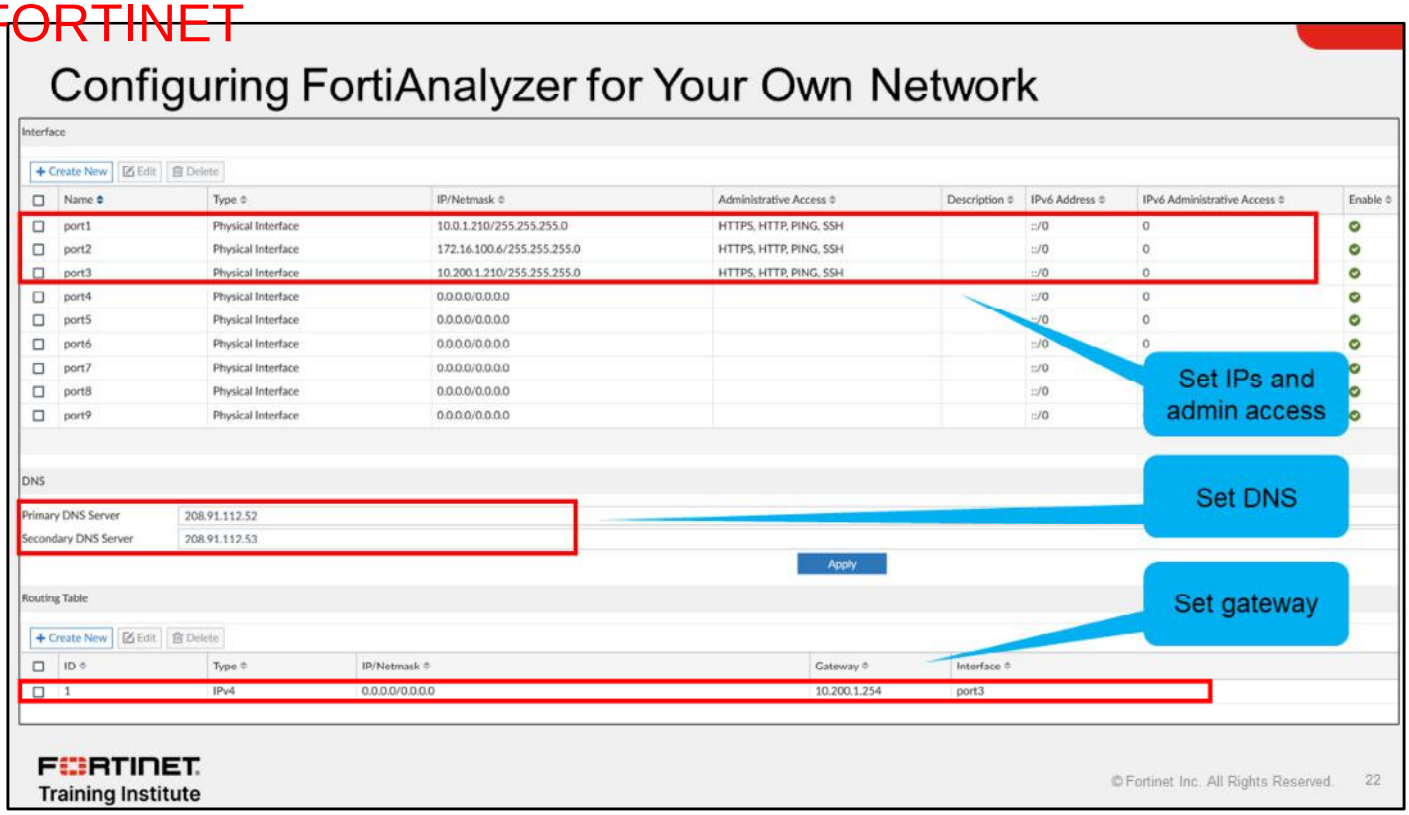


The **FortiAnalyzer Setup** wizard appears after you log in for the first time.

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.

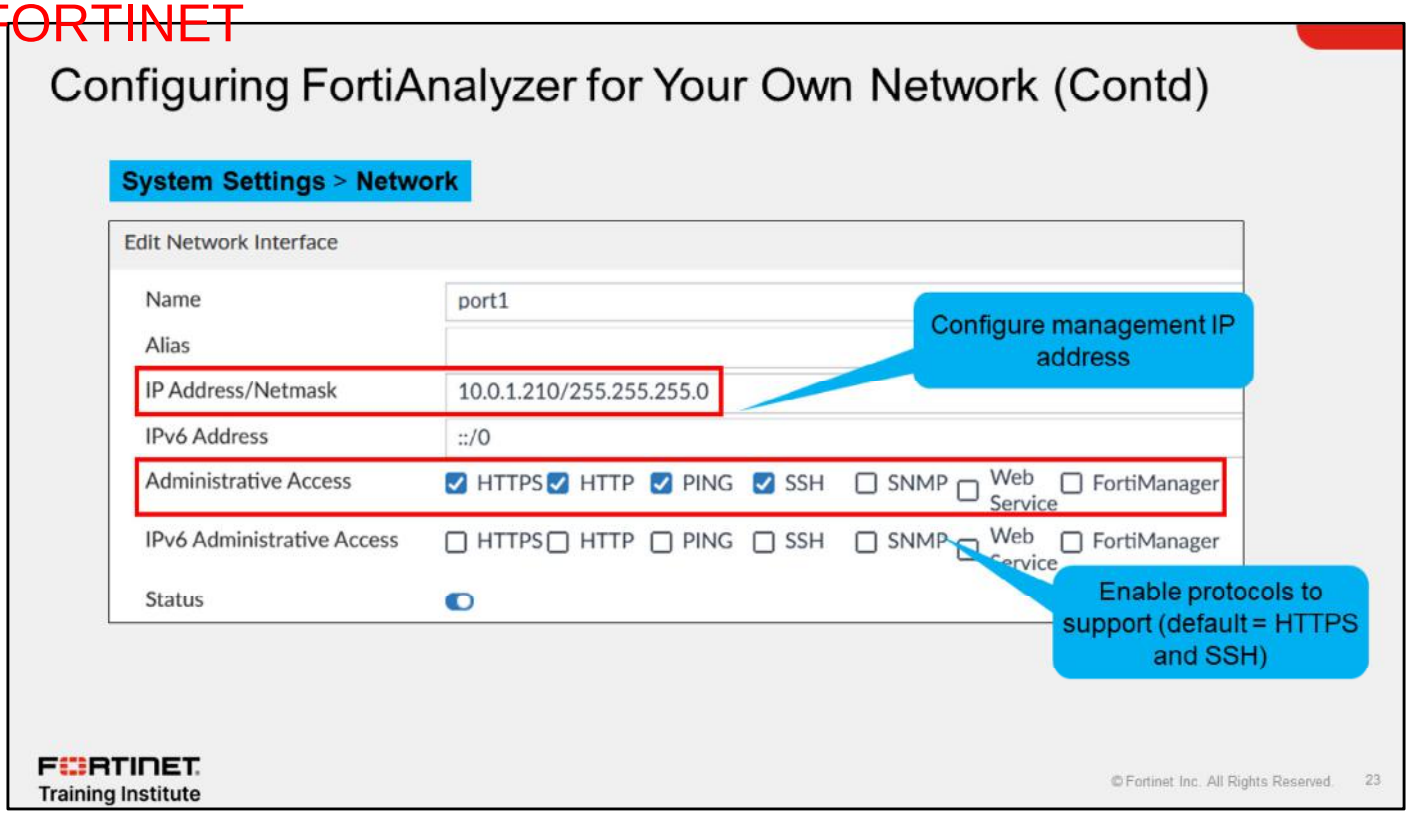
For air-gap environments where the FortiAnalyzer has no direct internet access to contact FortiGuard, you can obtain an entitlement file by contacting Fortinet Customer Service.

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



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

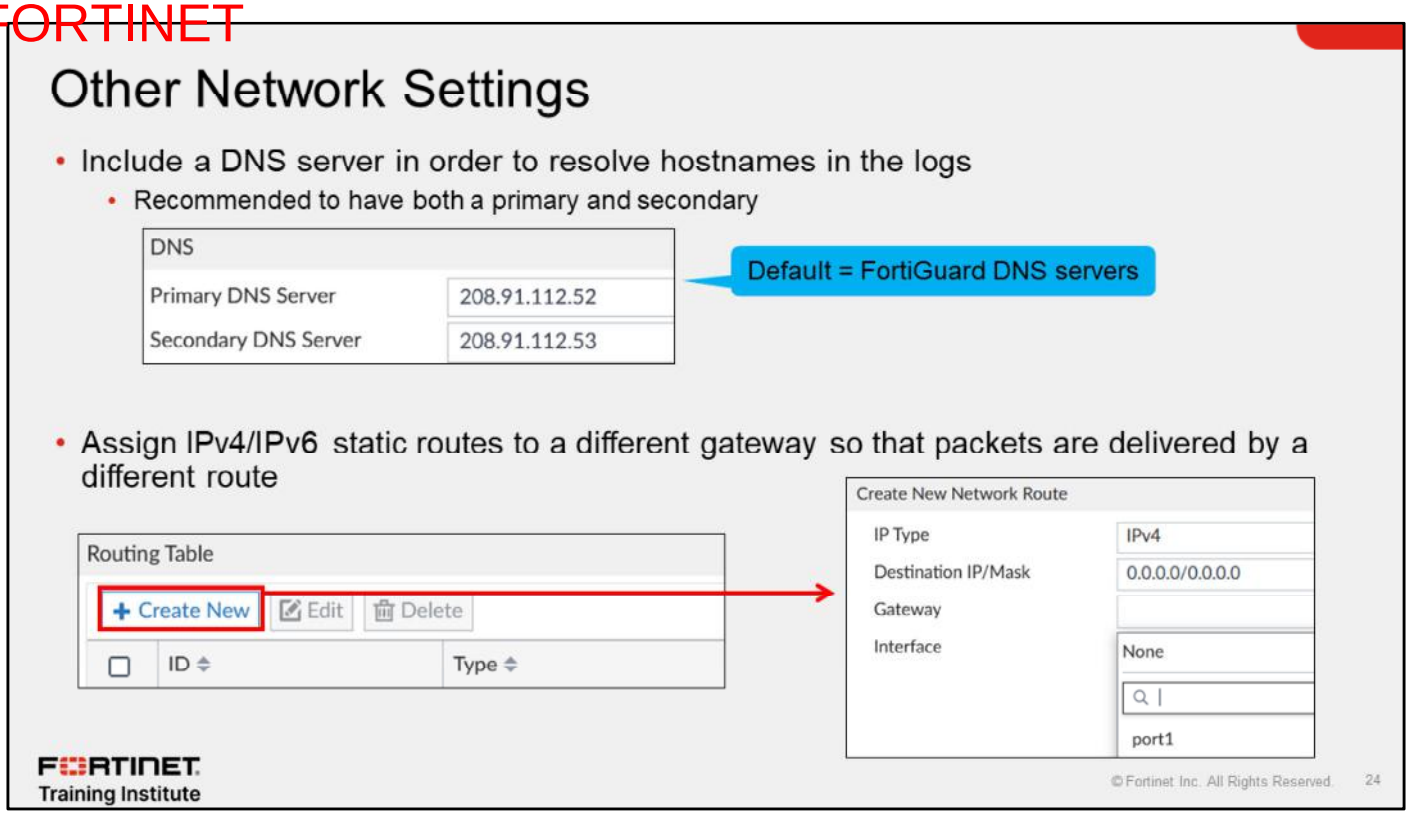
In order to configure FortiAnalyzer for your network, you must set the IP address and netmask, select supported administrative access protocols, and specify a default gateway for routing packets. You can also specify a primary and a secondary DNS server. You can do all this on the **Network** page.



Setting your own IP address and netmask provides more security than using the default address and, if more than one FortiAnalyzer 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.

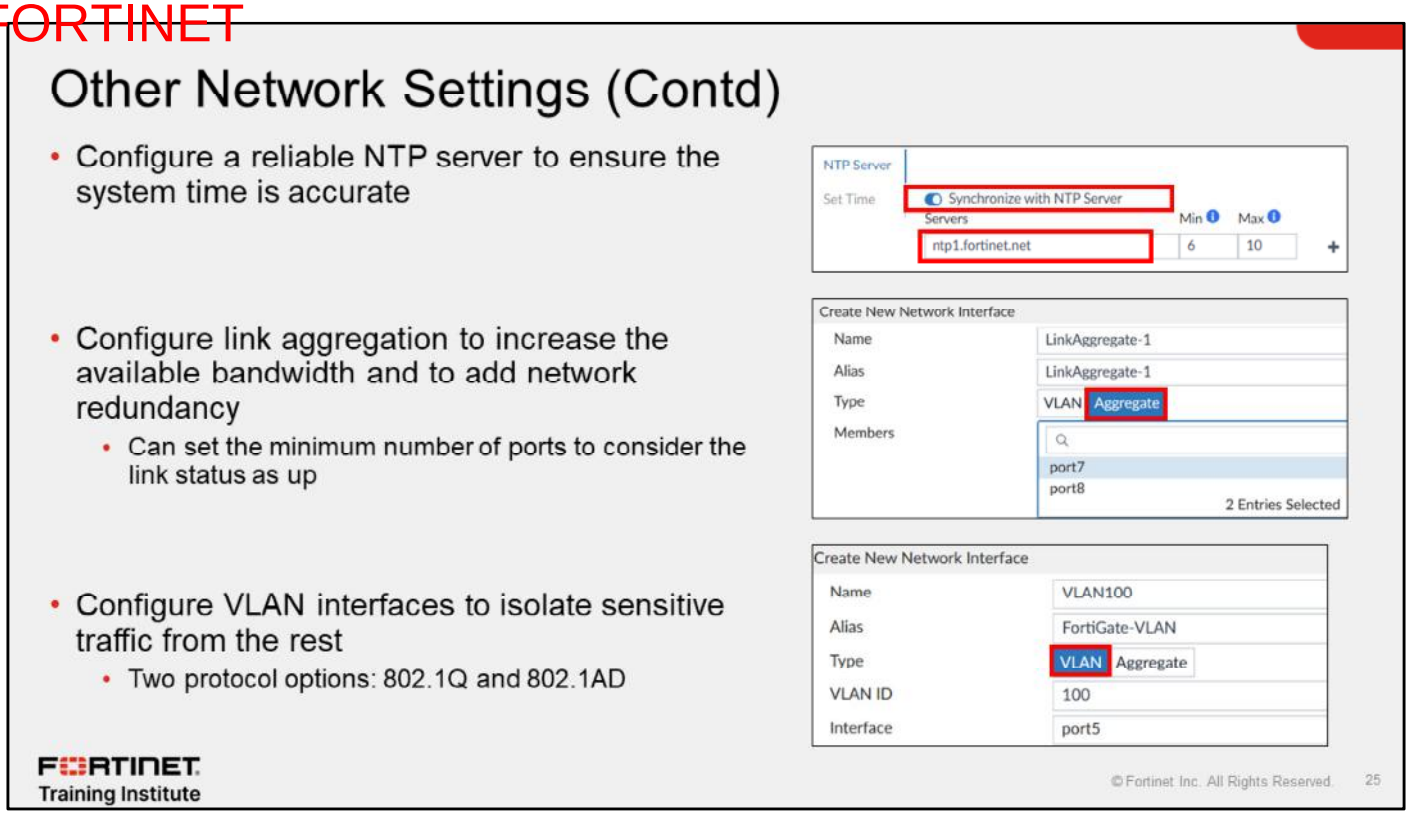
There are a few *non-standard* administrative access protocols that are worth mentioning as well:

- Web Service: Allows access to the FortiAnalyzer API using Simple Object Access Protocol (SOAP) on port 8080.
- FortiManager: Allows FortiAnalyzer to be managed by a FortiManager.



If you want to be able 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 some other servers of your preference, 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 as close as possible to your network.

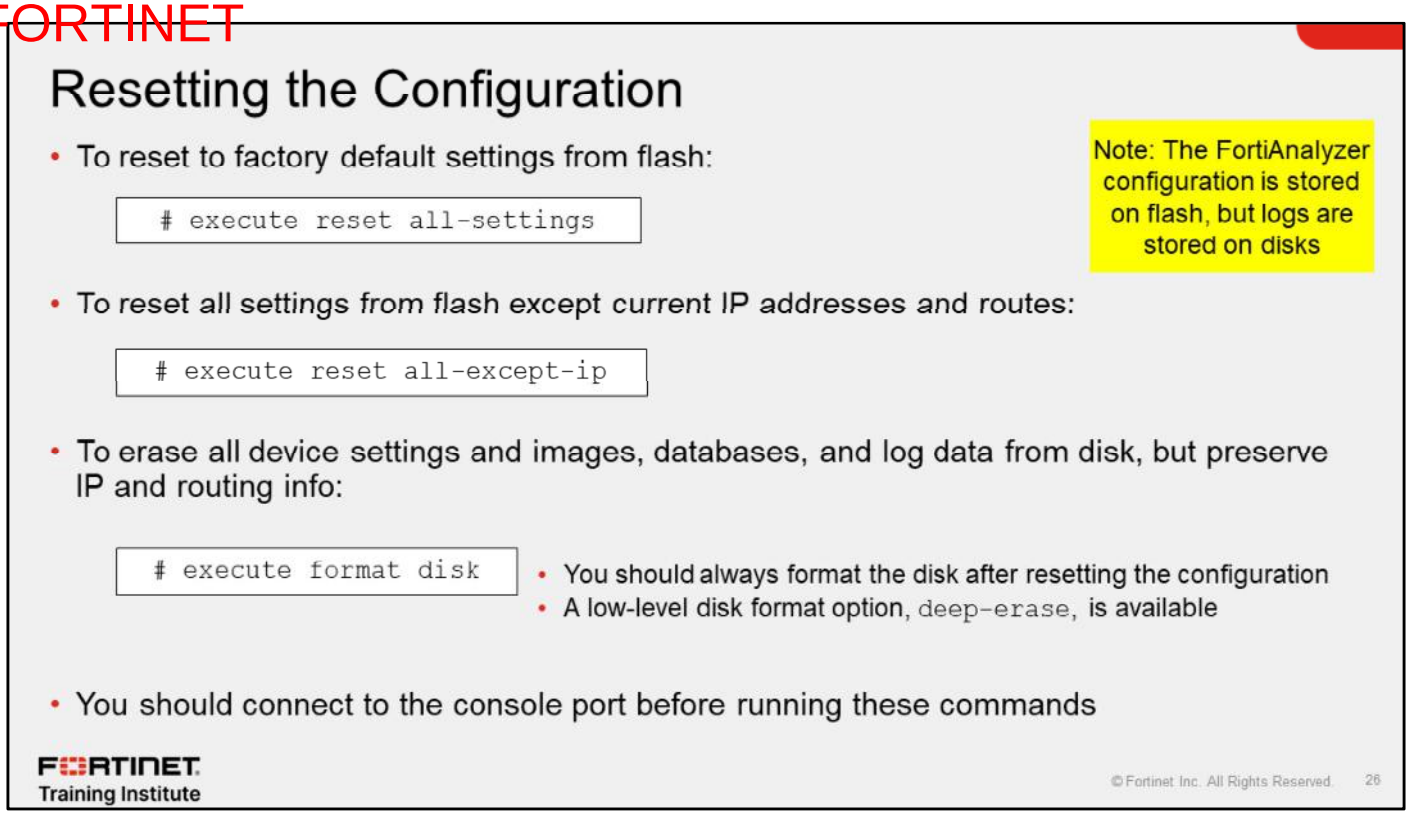
If you want to configure another port on FortiAnalyzer, you can assign specific IPv4 or IPv6 static routes to a different gateway, so that packets are delivered by a different route.



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

To increase the bandwidth available to receive logs, and to add network redundancy to FortiAnalyzer, you can configure one or more aggregate links. These are logical links that 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, hence adding network redundancy to your device.

VLANs are used to 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 in FortiAnalyzer to make use of 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 on disk, 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 data cannot be recovered. Keep in mind that this process can take a very long time, even days, depending on the size of the disk being formatted 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 the configuration is reset.

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 servers 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

 27

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 proper indentation.
- The `execute` commands allow you to perform a function in FortiAnalyzer.

You can use the `?` key to view available syntax options. You can also use the `Tab` key to auto complete 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 servers' information, such as IPs, stratum, poll time, latency
`# 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

 28

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.

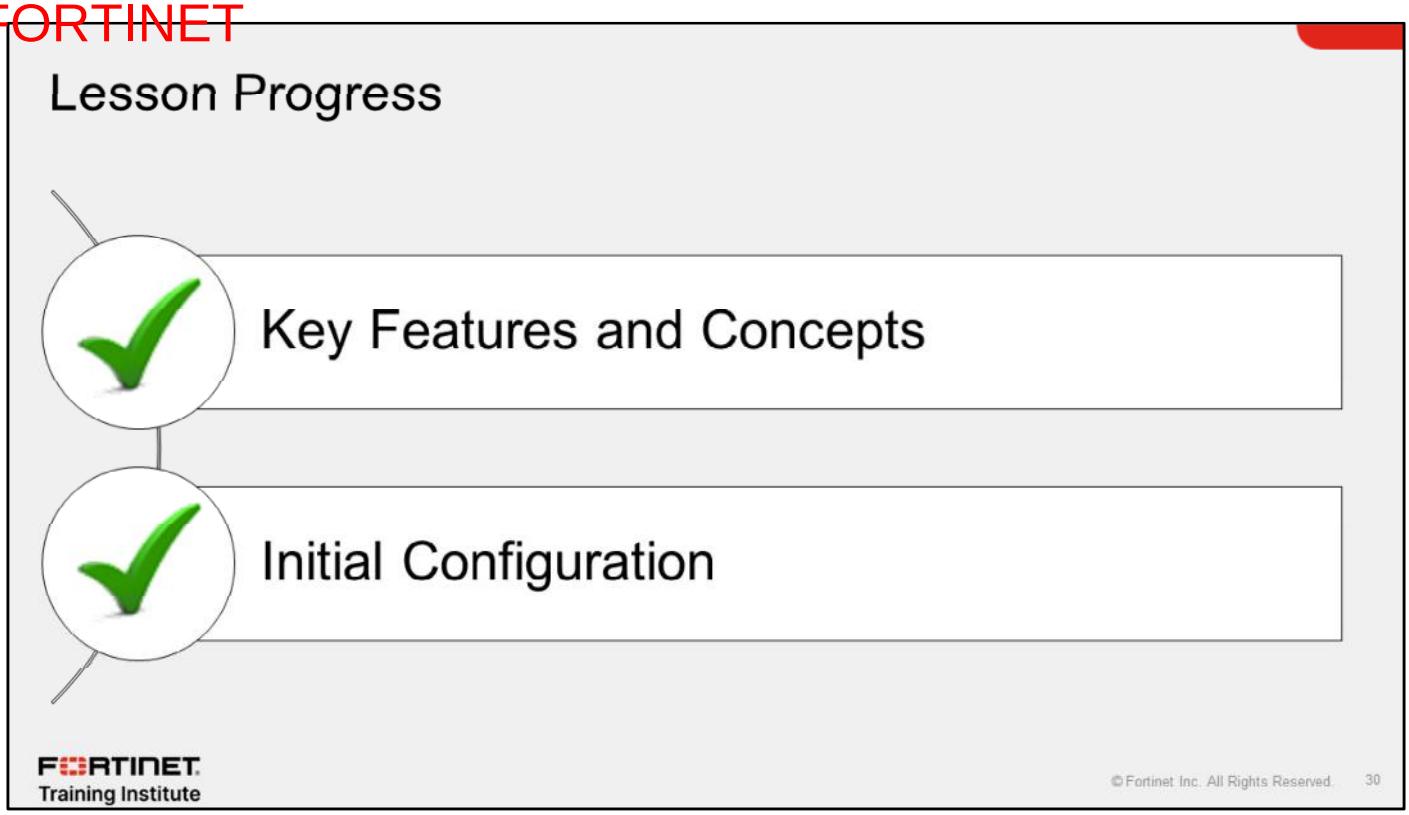
Knowledge Check

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.

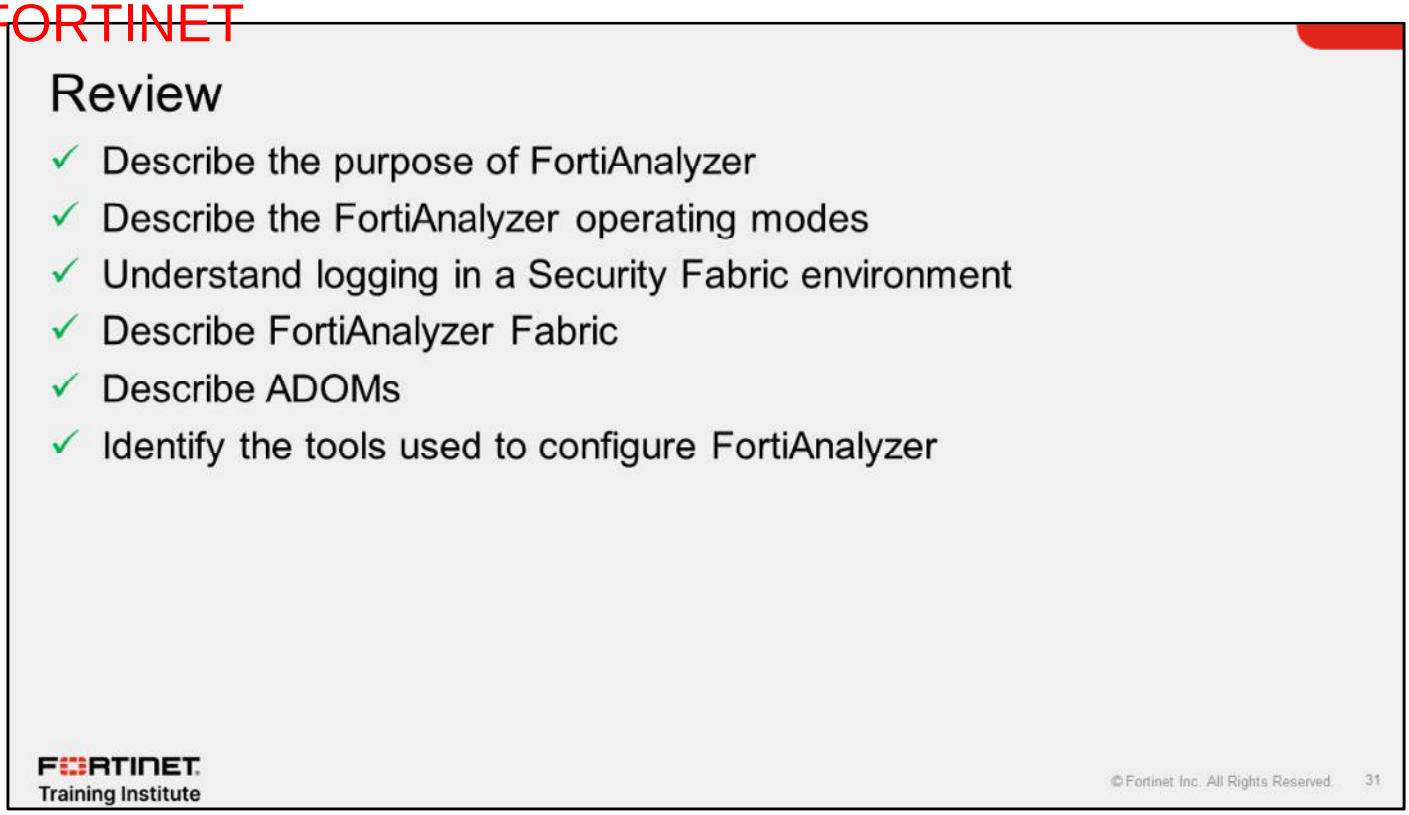
FORTINET Training Institute

 29



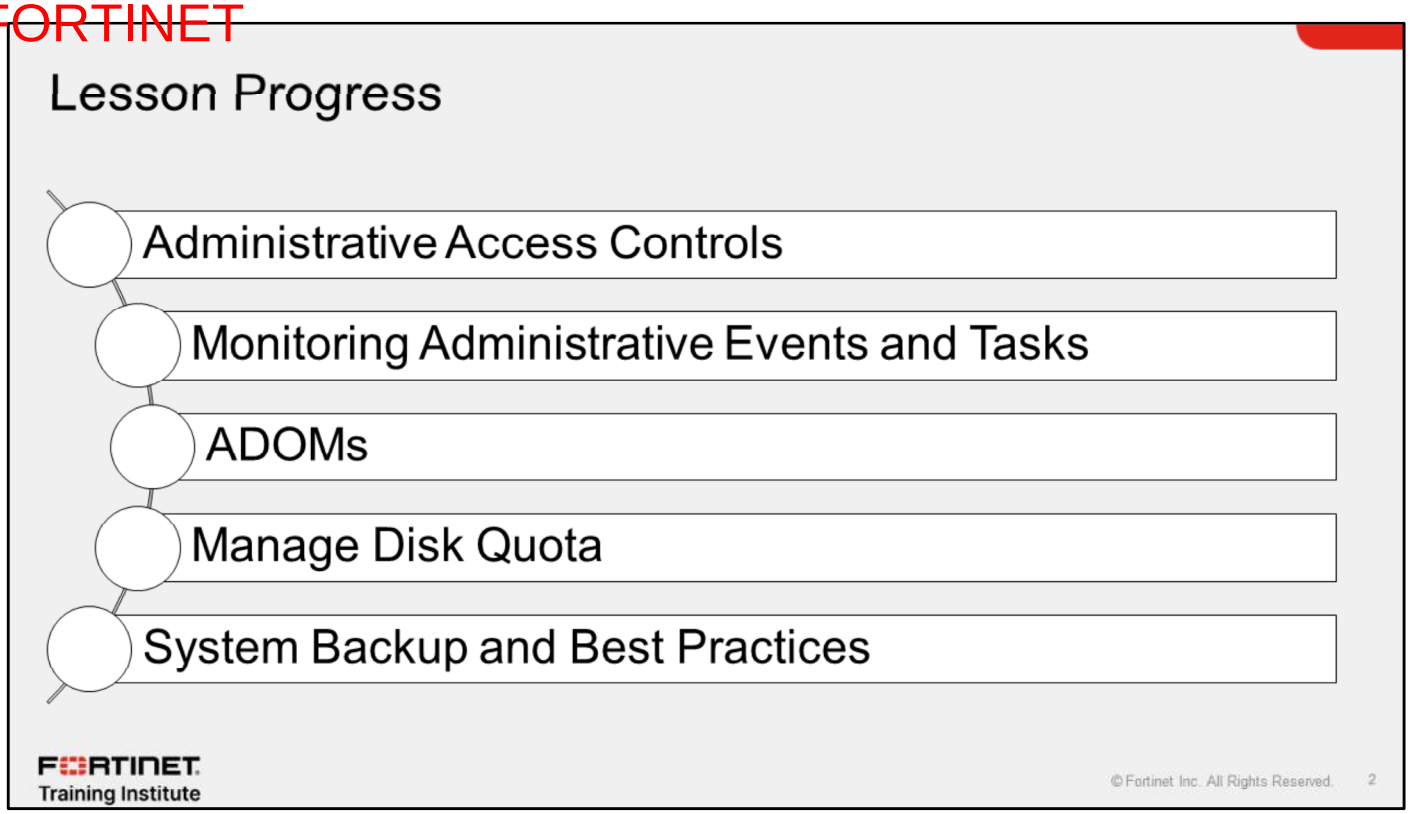
Congratulations! You have completed this lesson.

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

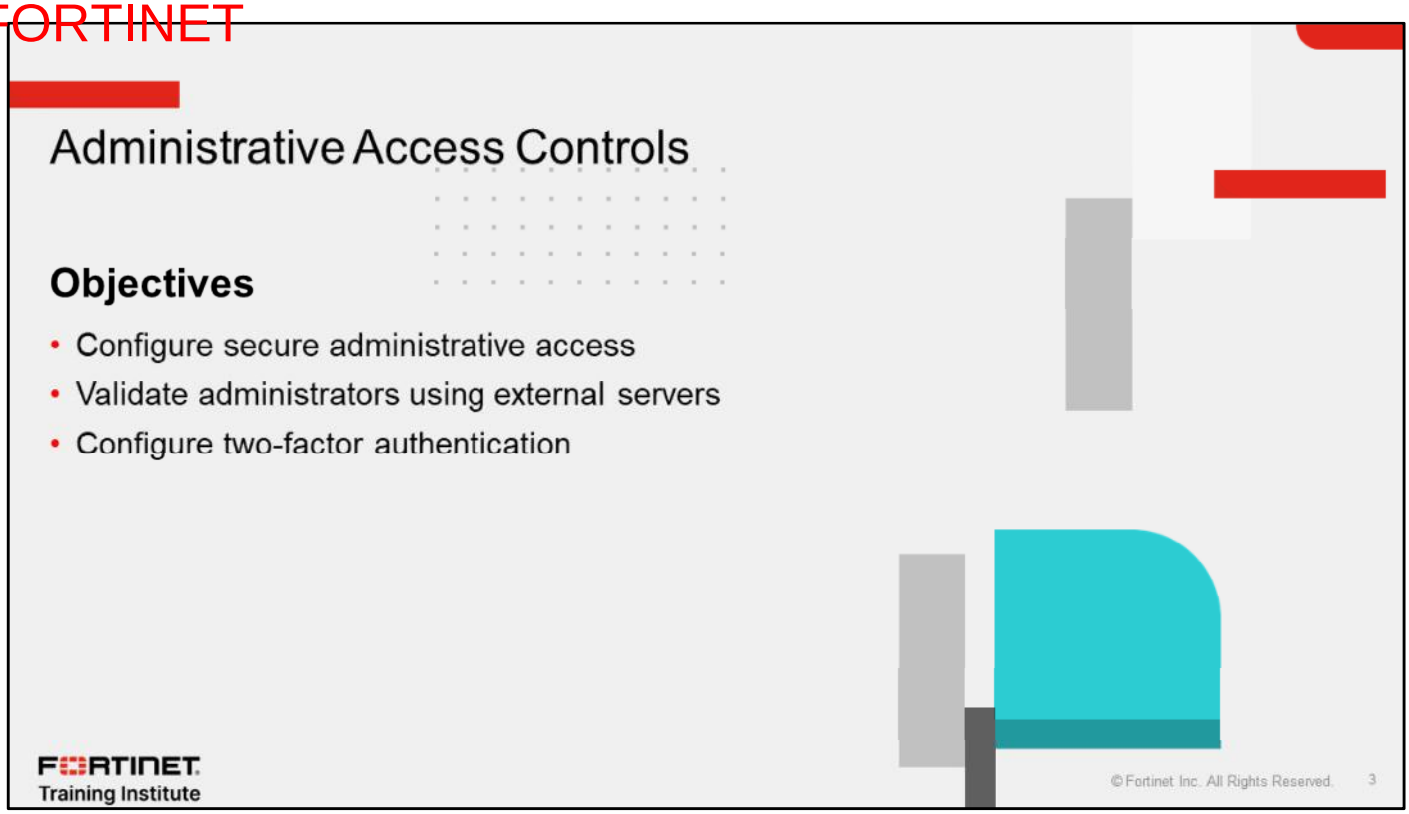


This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned about FortiAnalyzer key features and concepts and how to configure FortiAnalyzer.

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

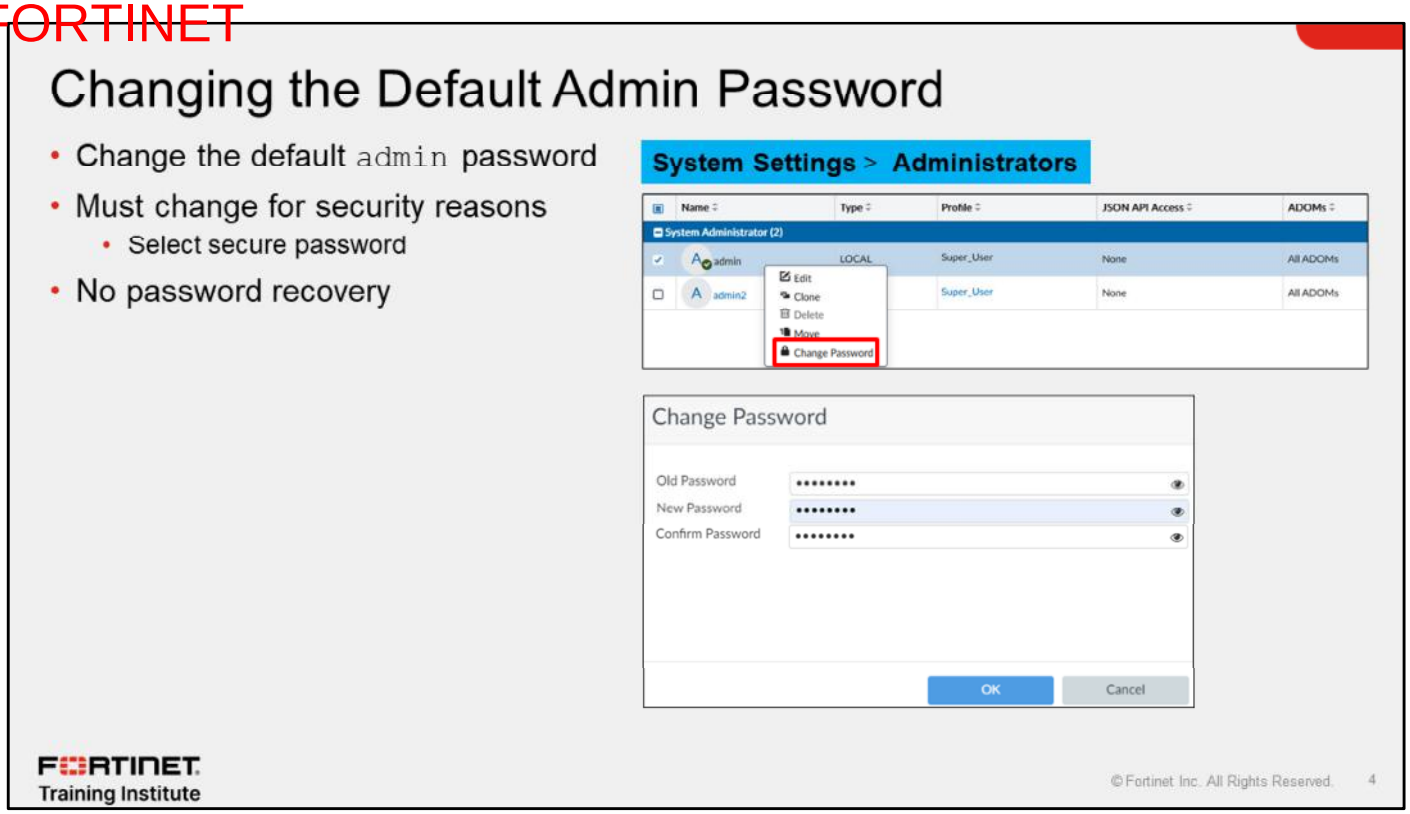


In this lesson, you will learn about the topics shown on this slide.



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 `admin` password. It is recommended that you do this during the Setup Wizard. You can also change it at any time on the **Administrators** page by right-clicking the administrator user, and then selecting **Change Password**. Make sure you enter a secure, strong password.

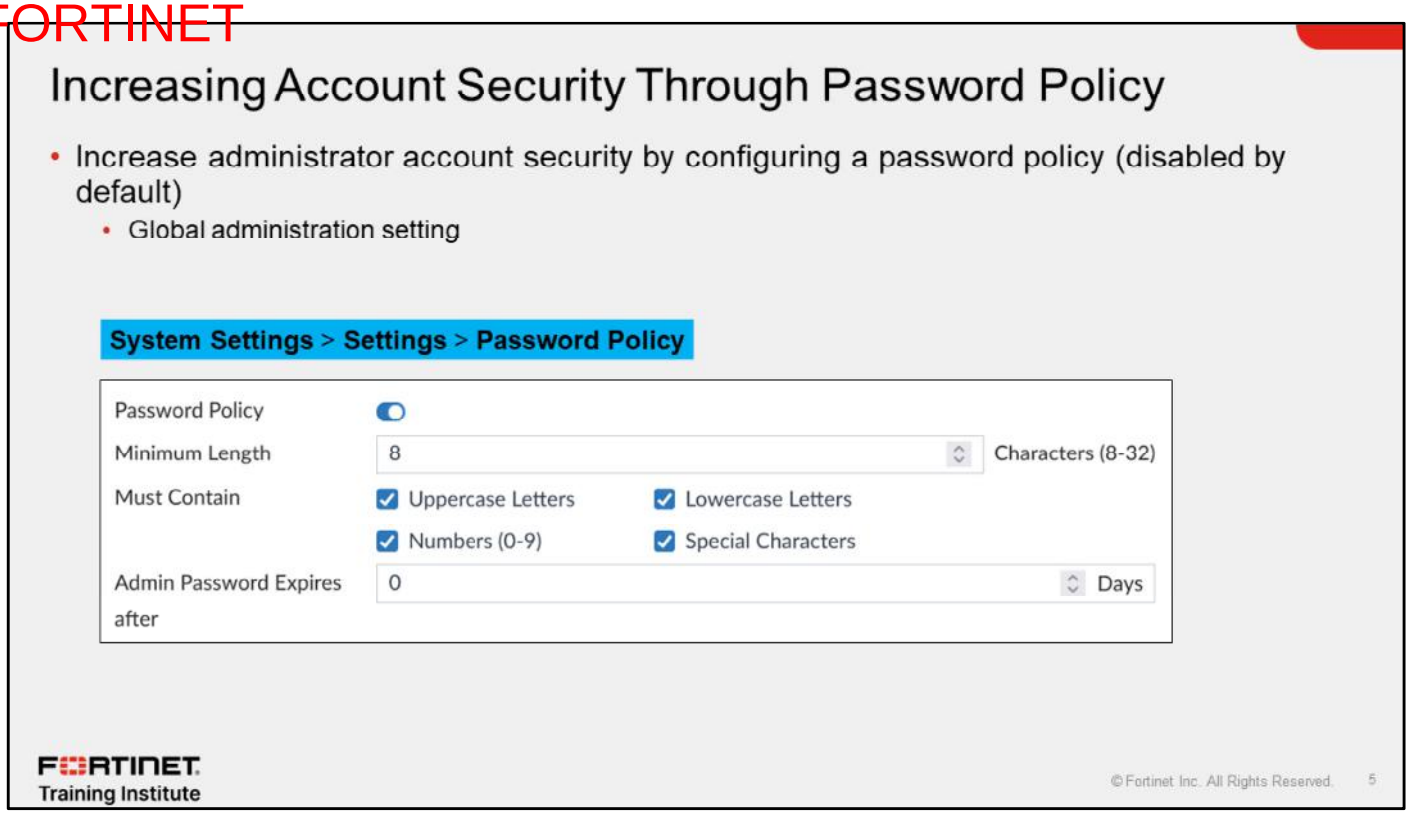
Be aware that there is no password recovery option for FortiAnalyzer!

If you forget your password and lose access to FortiAnalyzer, one option is to use the `execute migrate` command that 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 `admin` account and password (system settings are not restored).

The other option is to format the flash and reload the image (from the BIOS configuration menu). This erases the system settings, including the administrative accounts.

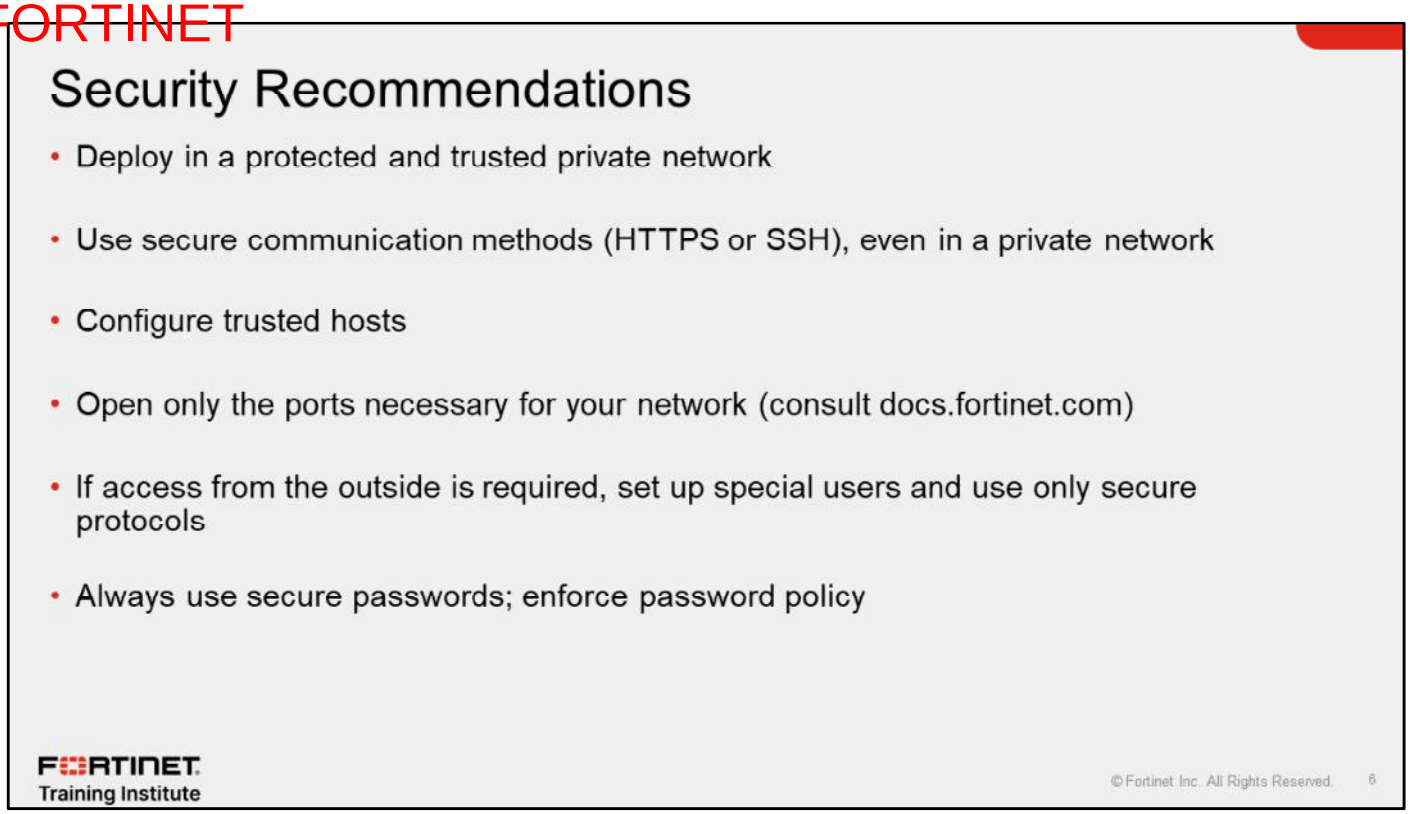
So, make sure you remember your password or store it in a secure location.



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.

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

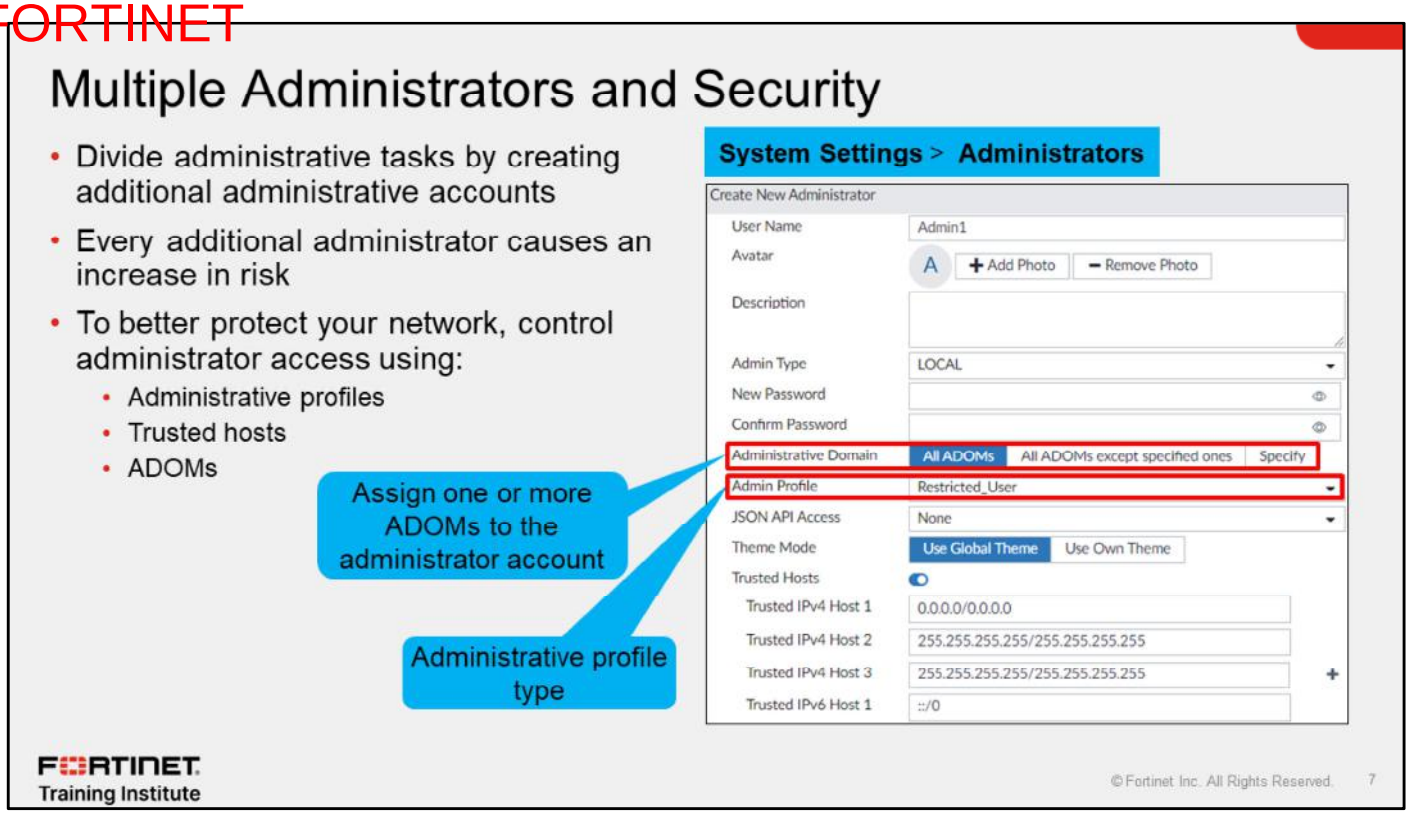
If you do set a password expiry, ensure you adhere to the policy and change the password before it expires because there is no password recovery option.



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.

Here are some security recommendations:

- Deploy FortiAnalyzer in a protected and trusted private network. You should never deploy it 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 plain text, 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 only from 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 place because FortiAnalyzer does not support password recovery.

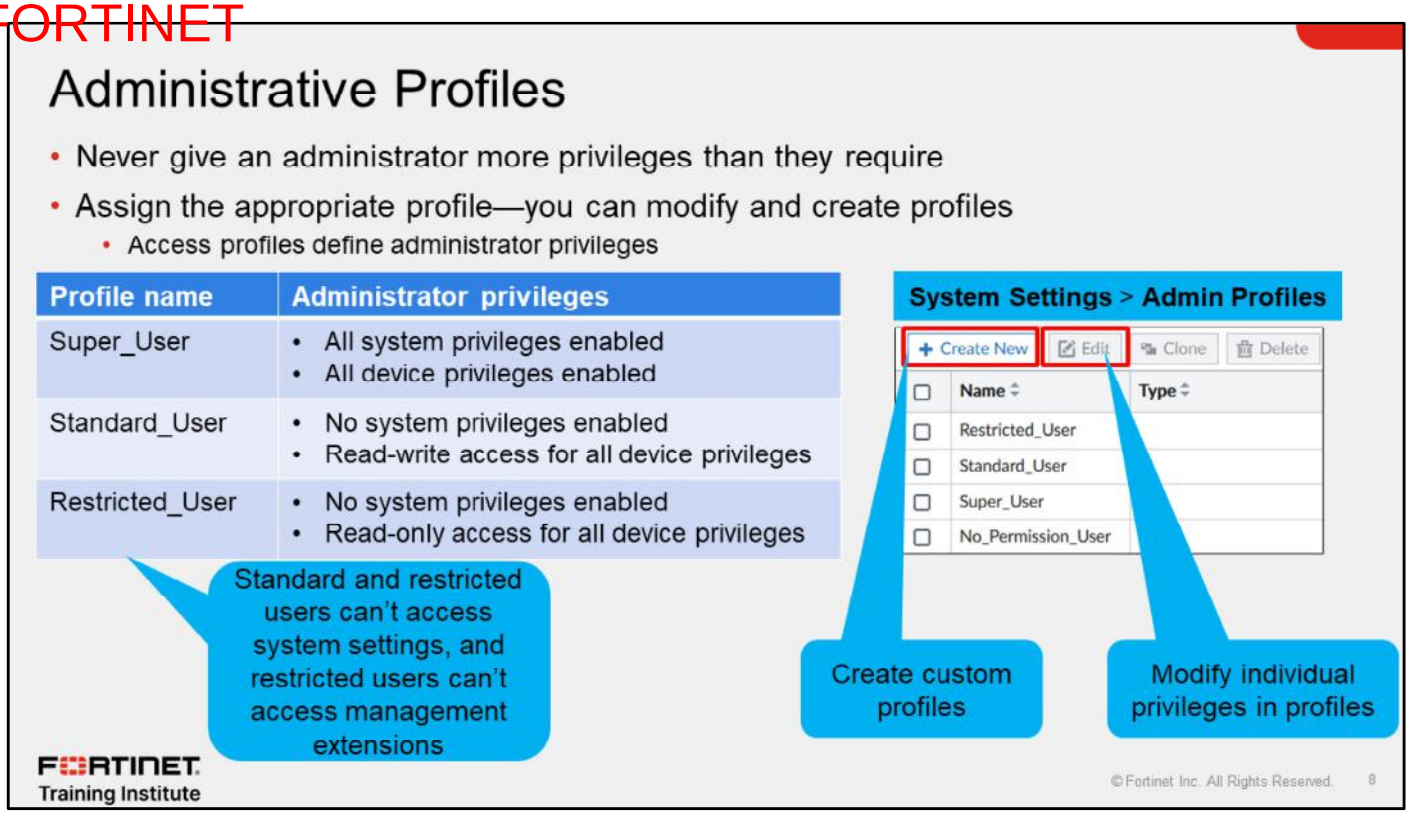


Depending on your deployment, you may want to divide FortiAnalyzer administrative tasks among multiple employees by creating additional administrative accounts. However, every additional individual to which you give administrator access causes potential growth in risk.

In order 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.

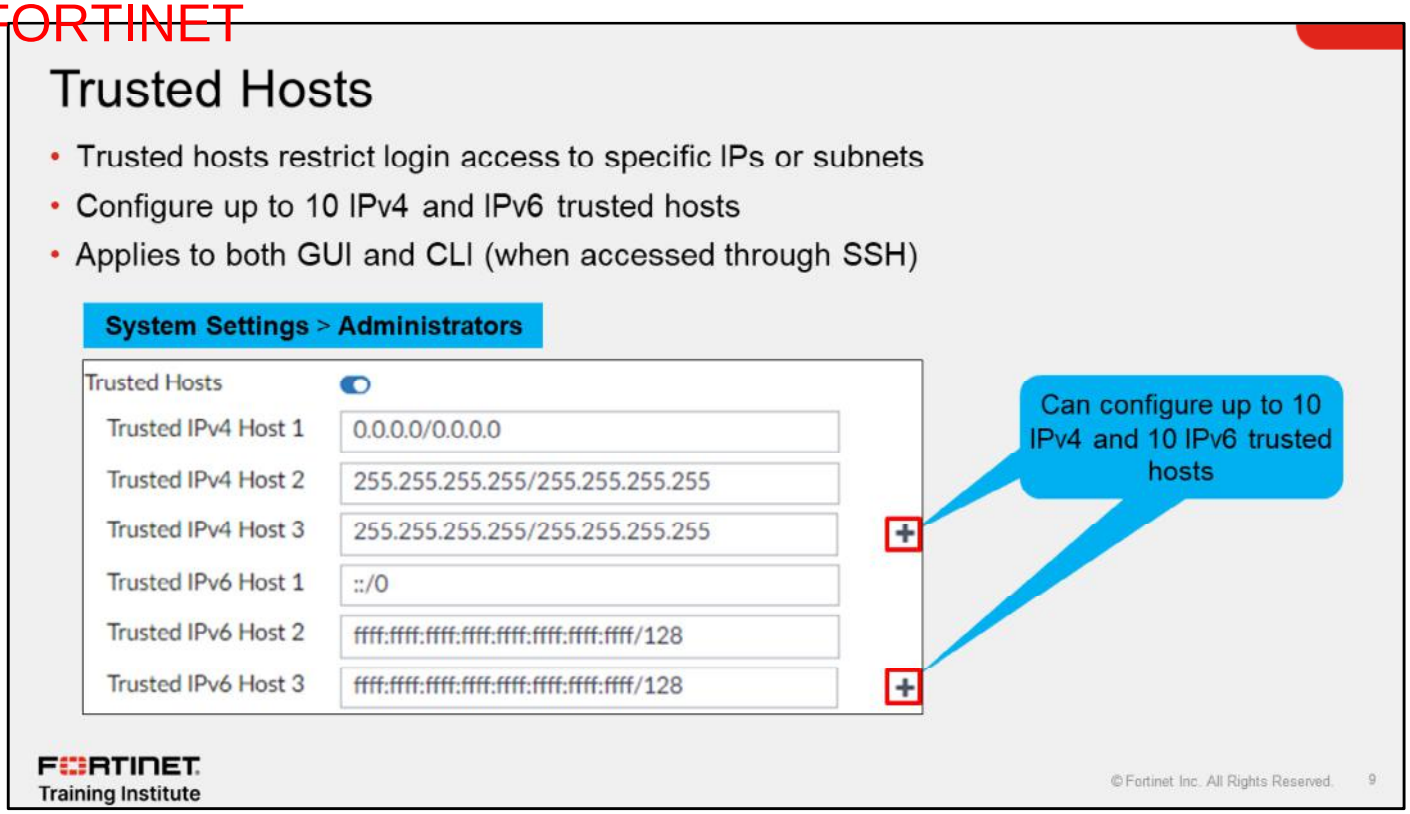
By dividing administrative access among multiple people, and employing methods of control, you can better protect your network.



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:

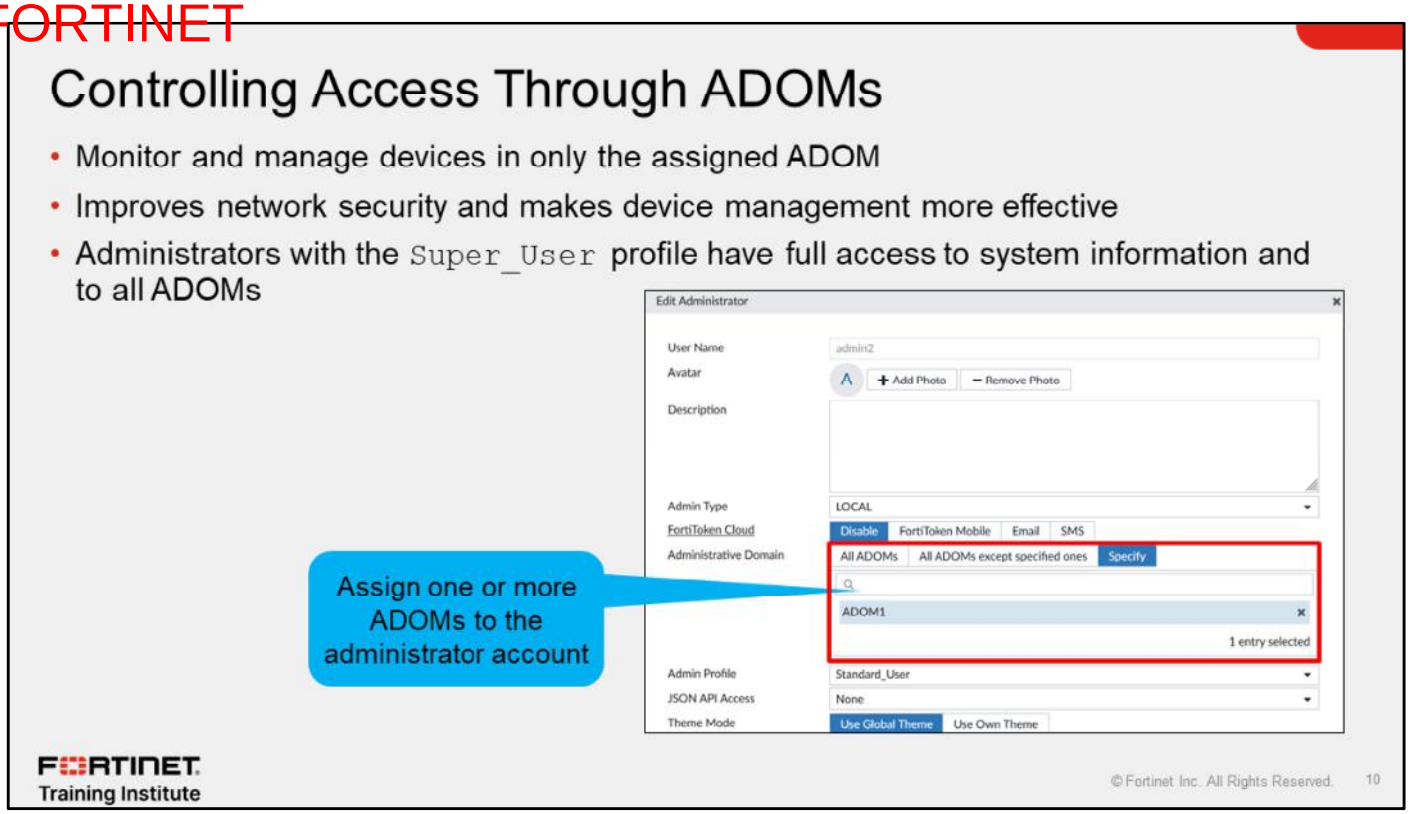
- Super_User, which provides access to all device and system privileges.
- Standard_User, which provides read and write access to device privileges, but not system privileges.
- Restricted_User, which provides read access only to device privileges, but not system privileges, and removes all access to 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.



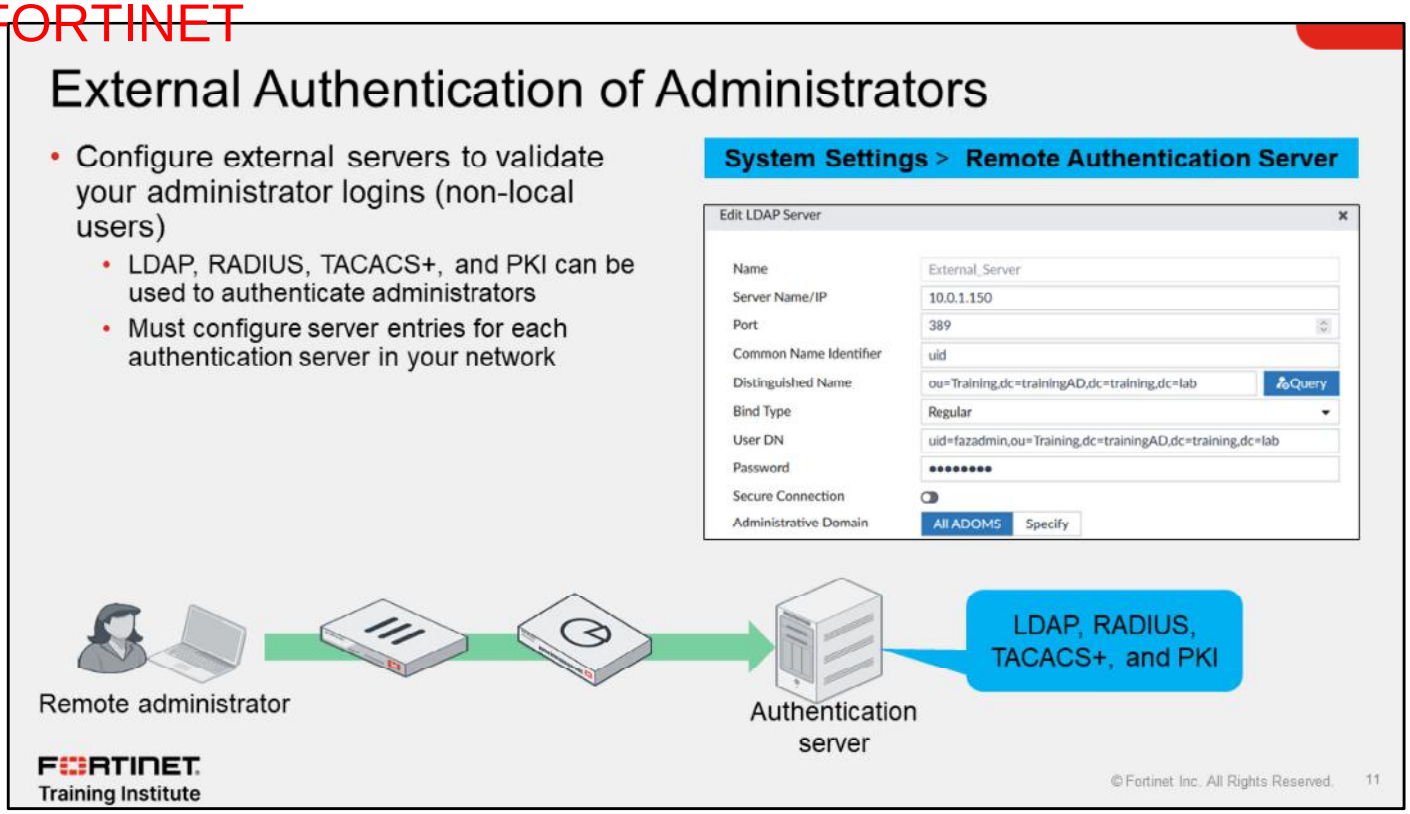
In addition to controlling administrative access through administrator profiles, you can further control access by setting up trusted hosts for each administrative user. This restricts administrators to logins from only specific IPs or subnets. You can even restrict an administrator to a single IP address, if you define only one trusted host IP.

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



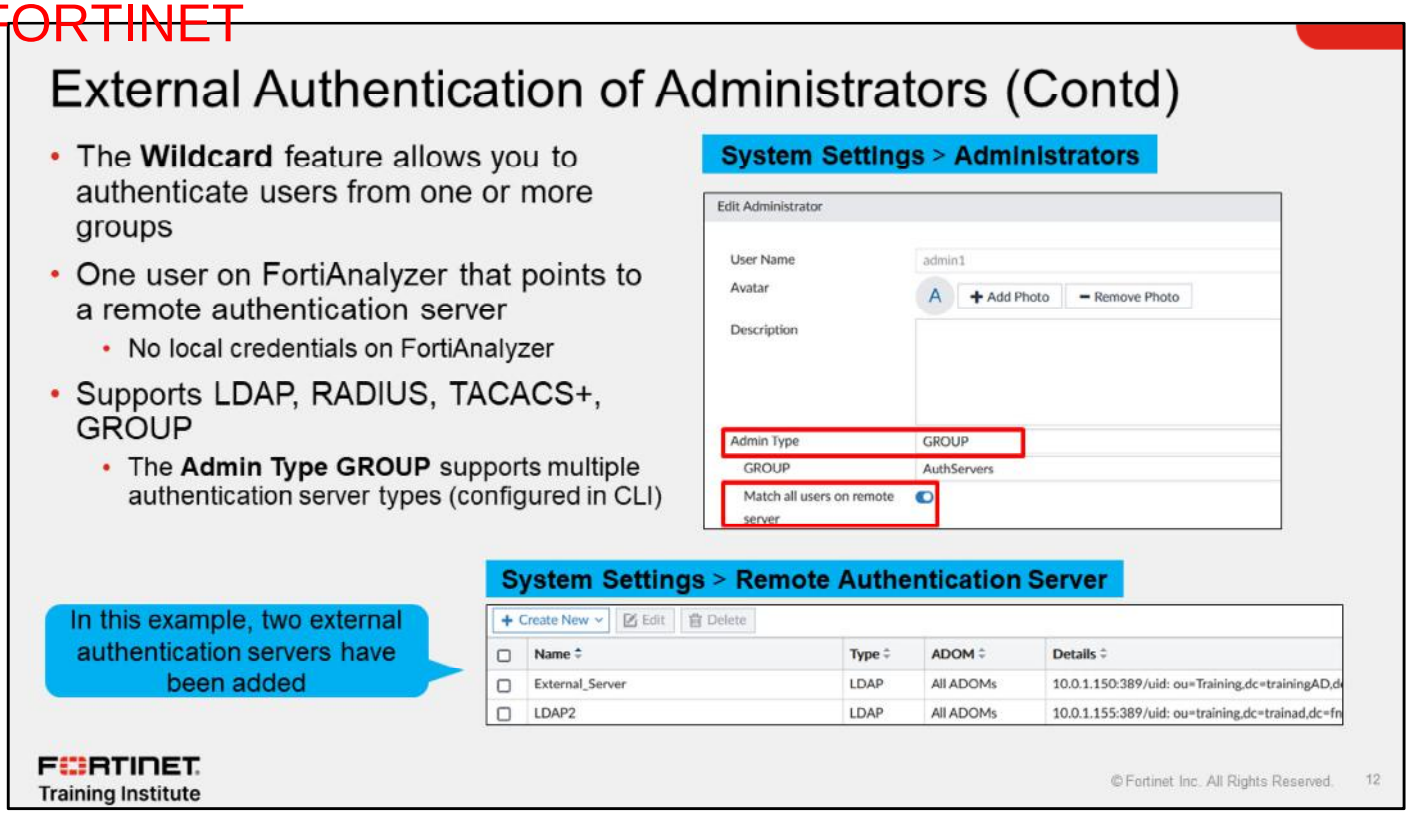
Another way you can control administrative access is through ADOMs. Using ADOMs makes device management more effective because administrators need to monitor and manage only devices in their assigned ADOMs. It also makes the network more secure because administrators are restricted to only those devices 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 logins are validated by FortiAnalyzer, you can configure external servers to validate your administrator logins. RADIUS, LDAP, TACACS+, and PKI can all be used to authenticate administrators.

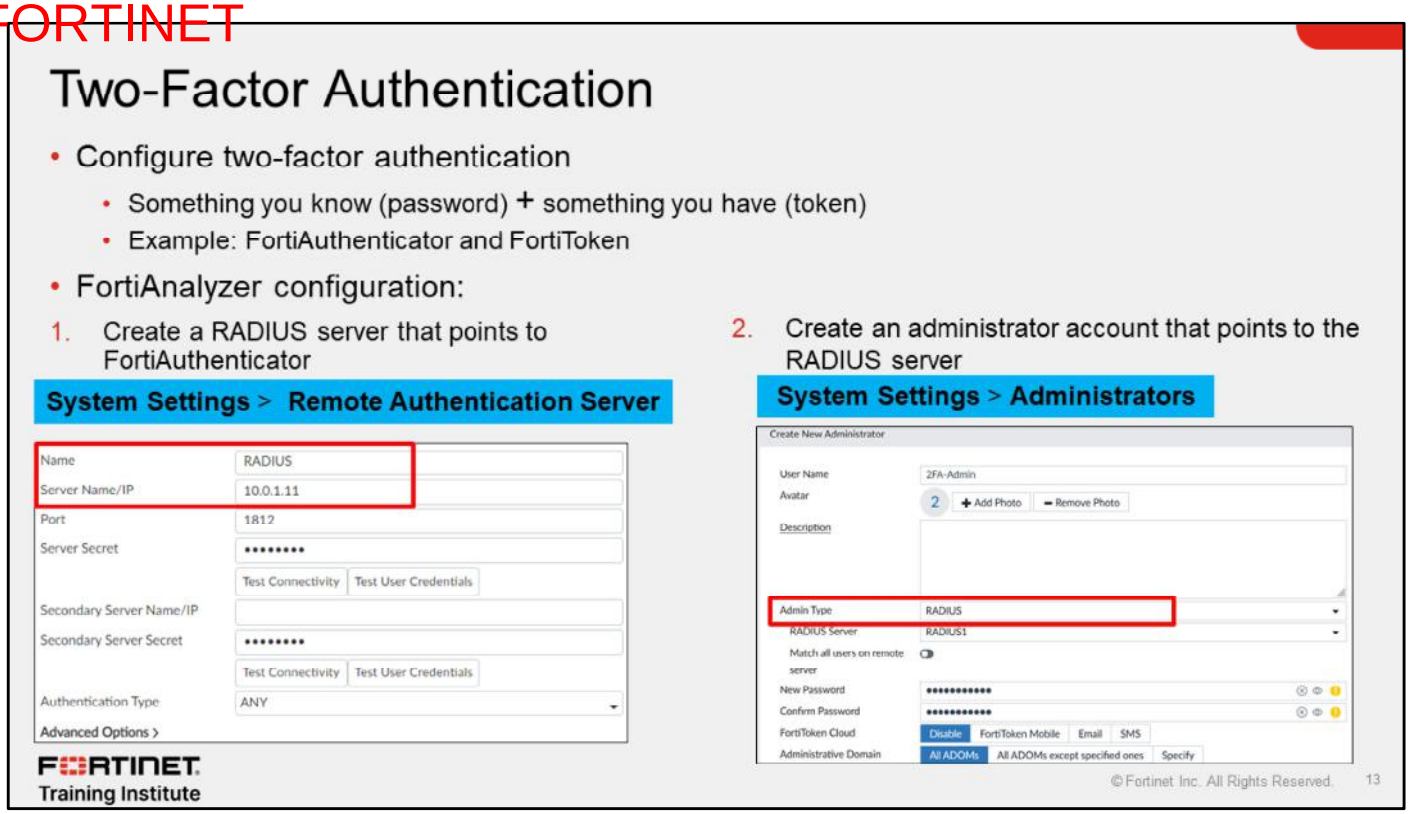
The image on this slide shows an example of an LDAP server configuration.



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.

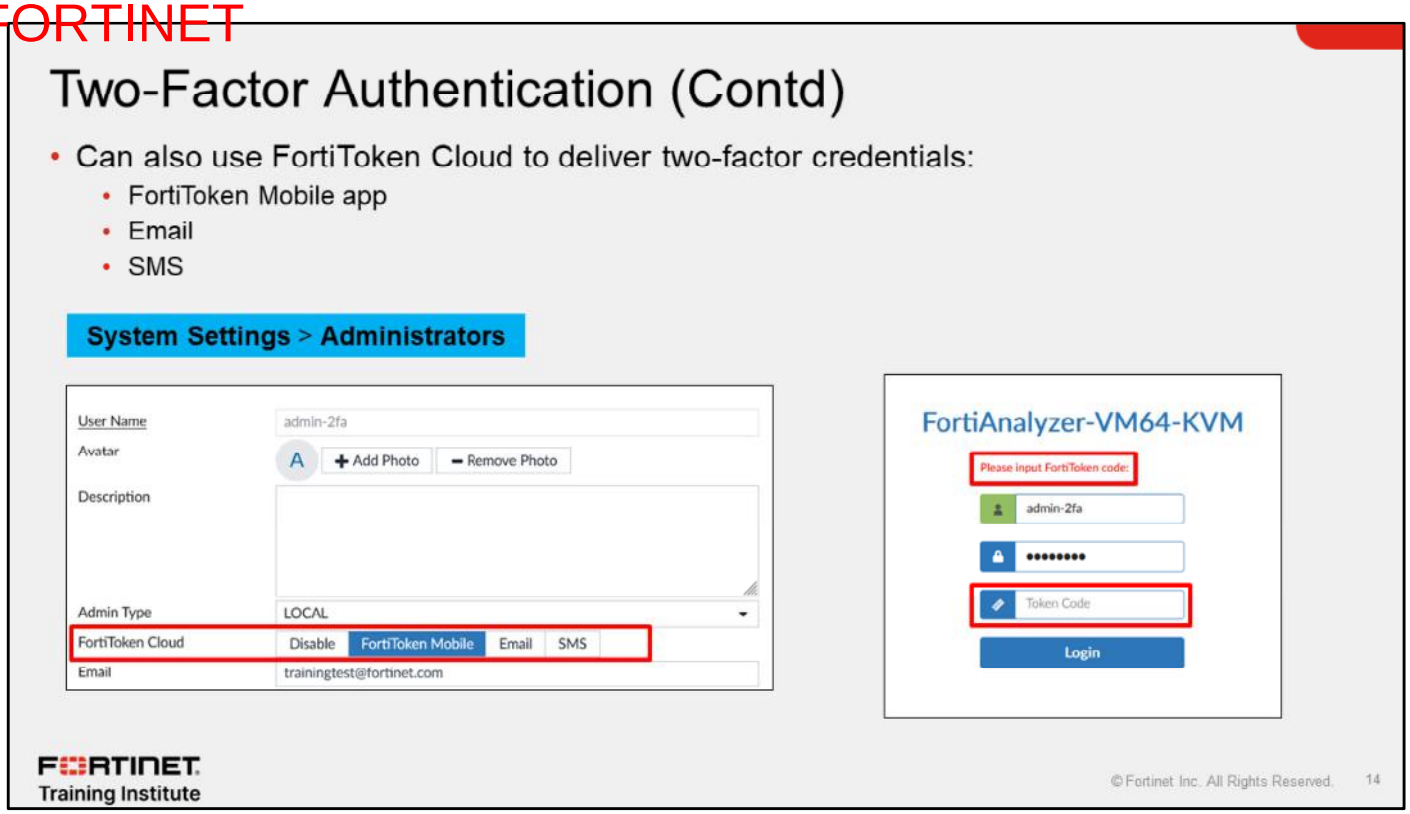
You can group multiple servers of the same type to act as backup—if one server fails, the administrator can still be authenticated by another server in the group. You can add remote authentication server groups using the CLI only. In the example shown on the slide, two existing LDAP servers were added. 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.



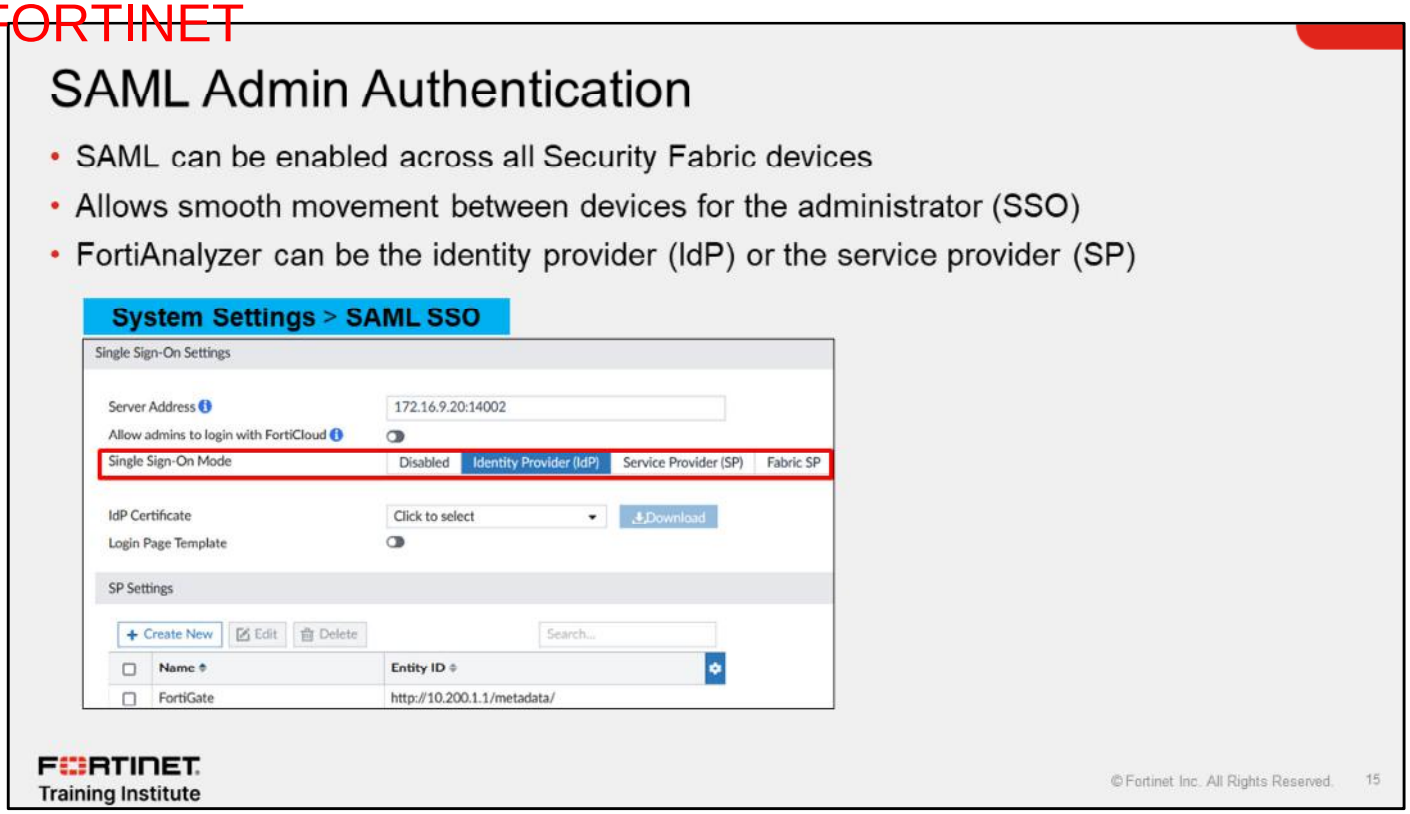
To add additional security to external administrators, you can configure two-factor authentication. To do this, you can use FortiAuthenticator and FortiToken.

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, see 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 smart phone, receive the verification code through email, or get the verification code through SMS.



FortiAnalyzer supports single-sign on (SSO) in multiple ways. It can play the role of the identity provider (IdP), the service provider (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. If the IdP leverages a remote authentication server, such as LDAP, this drastically reduces configuration requirements. If you don't enable the **Match all users on remote server** wildcard option, then you must create all those users in 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.

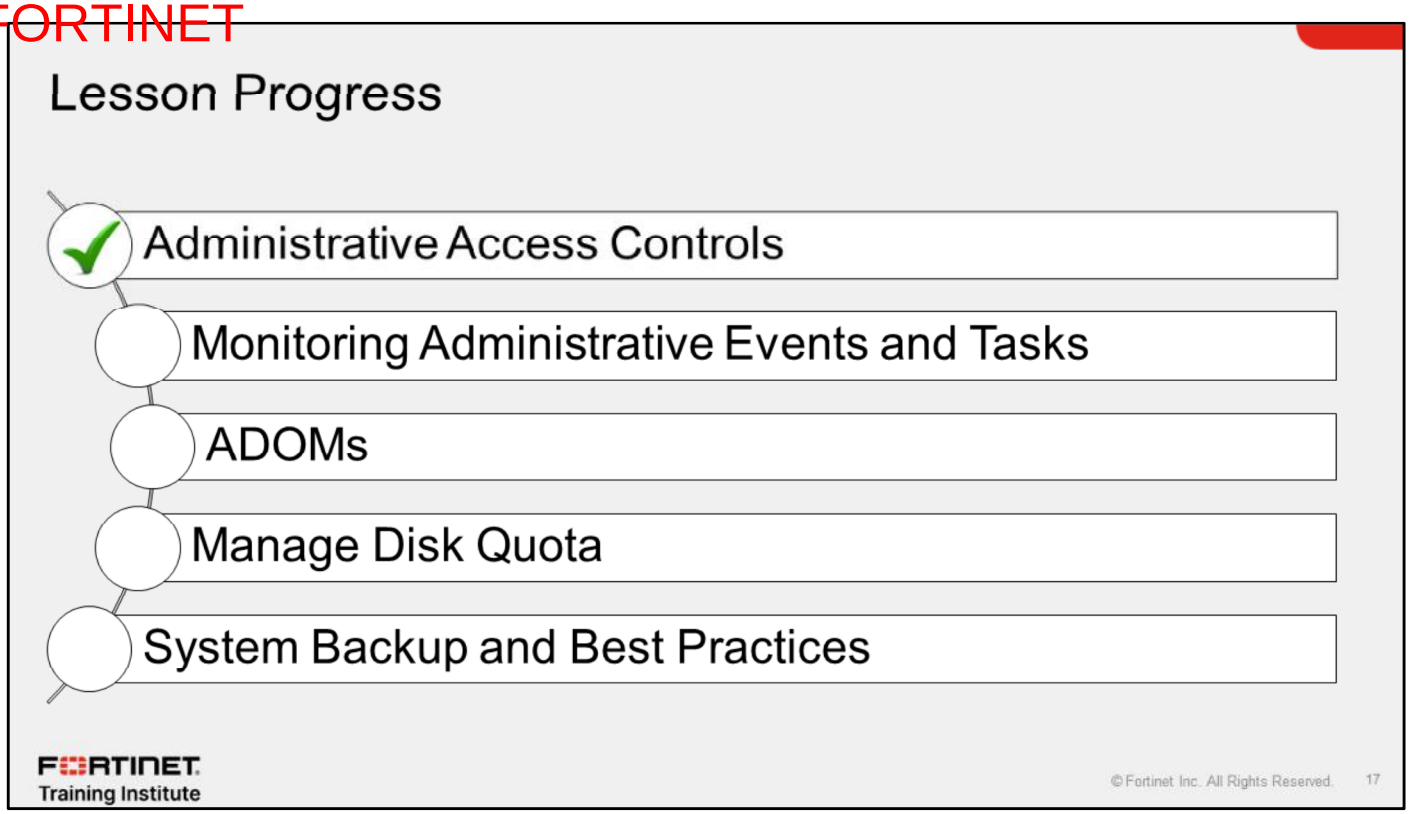
Knowledge Check

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 a wildcard administrator?
   - A. Allows administrators to log in with credentials stored locally on FortiAnalyzer
   - ✓B. Allows administrators to log in with credentials stored on a remote authentication server

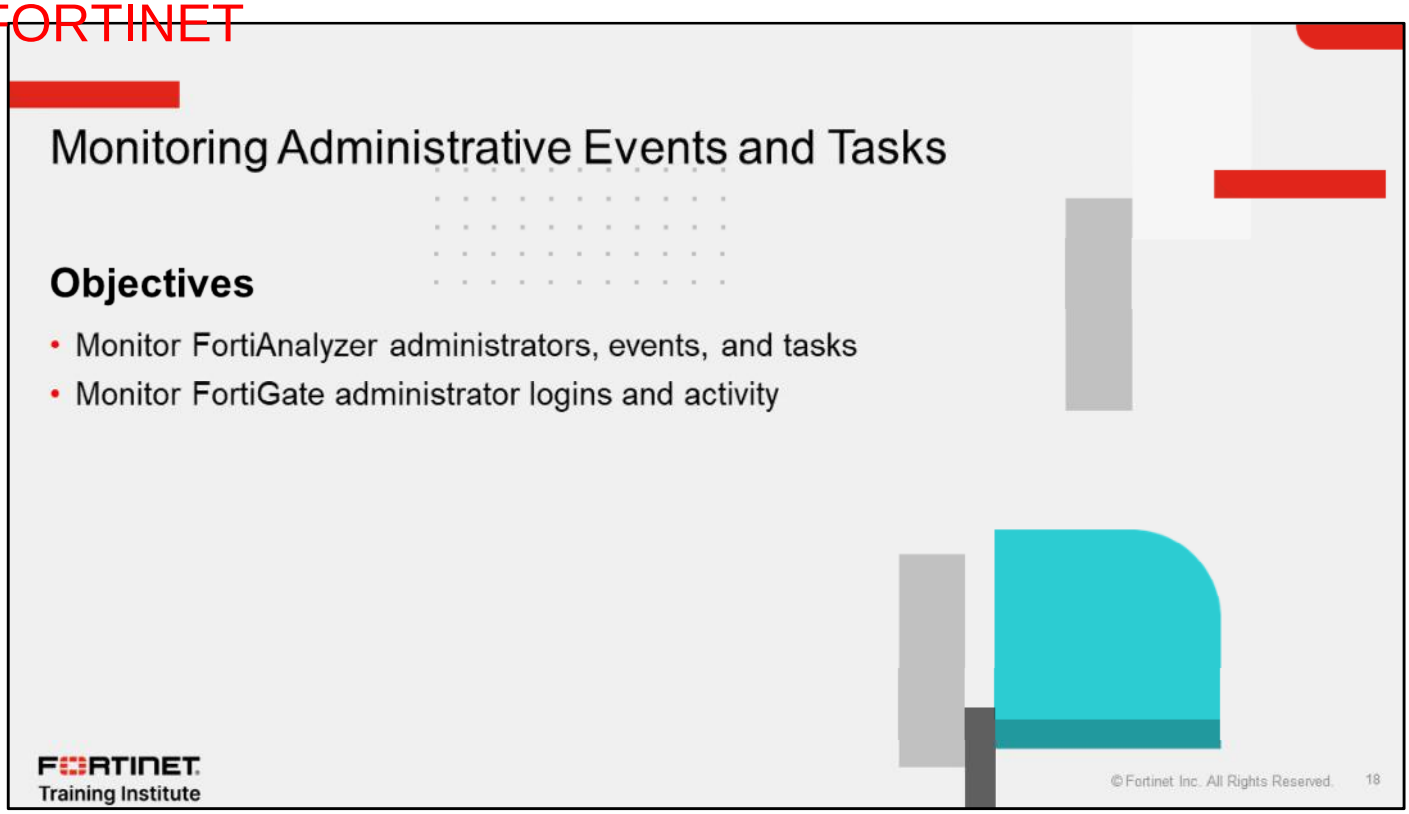
FORTINET Training Institute

 16



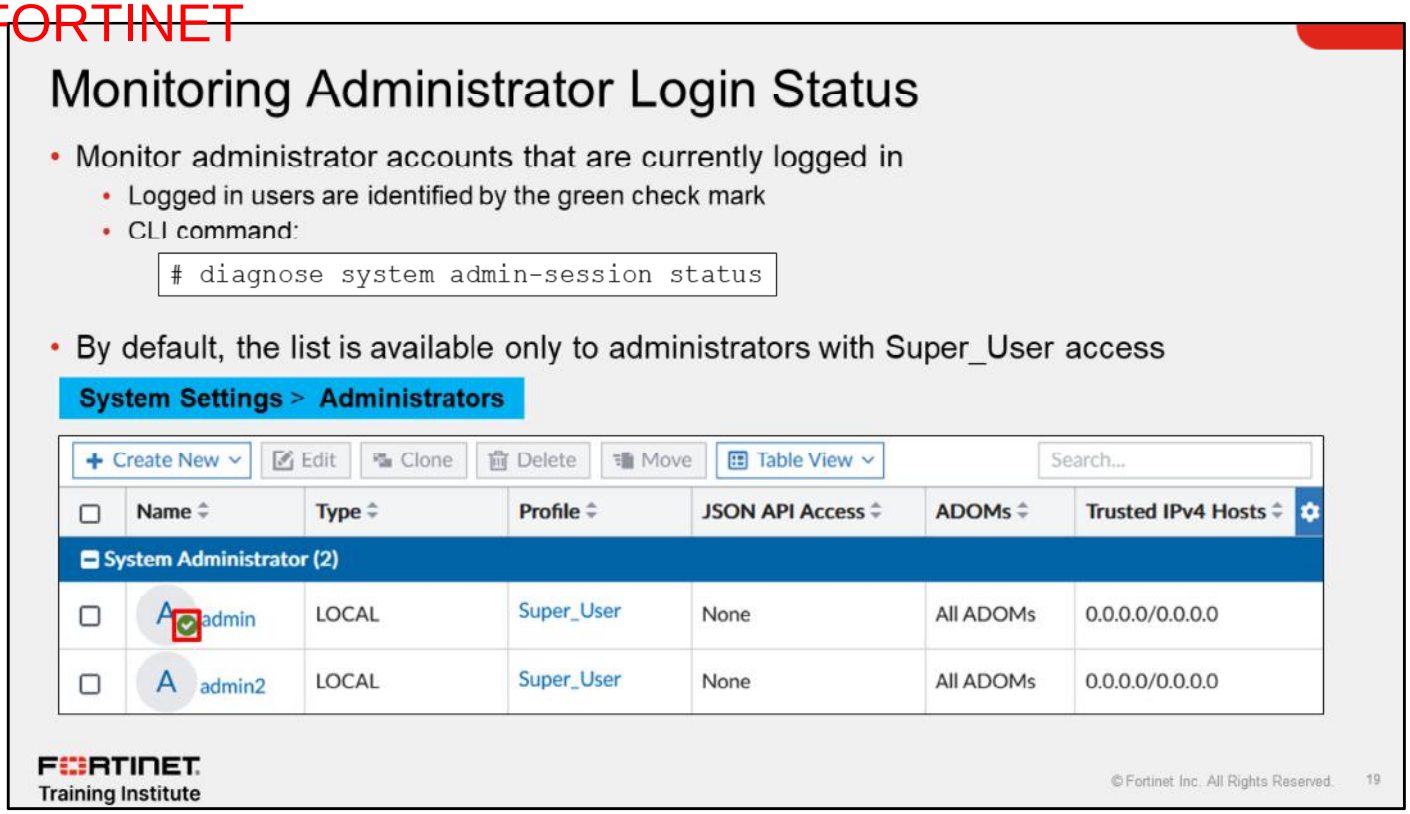
Good job! You now understand administrative access controls.

Now, you will learn how to monitor administrative events.



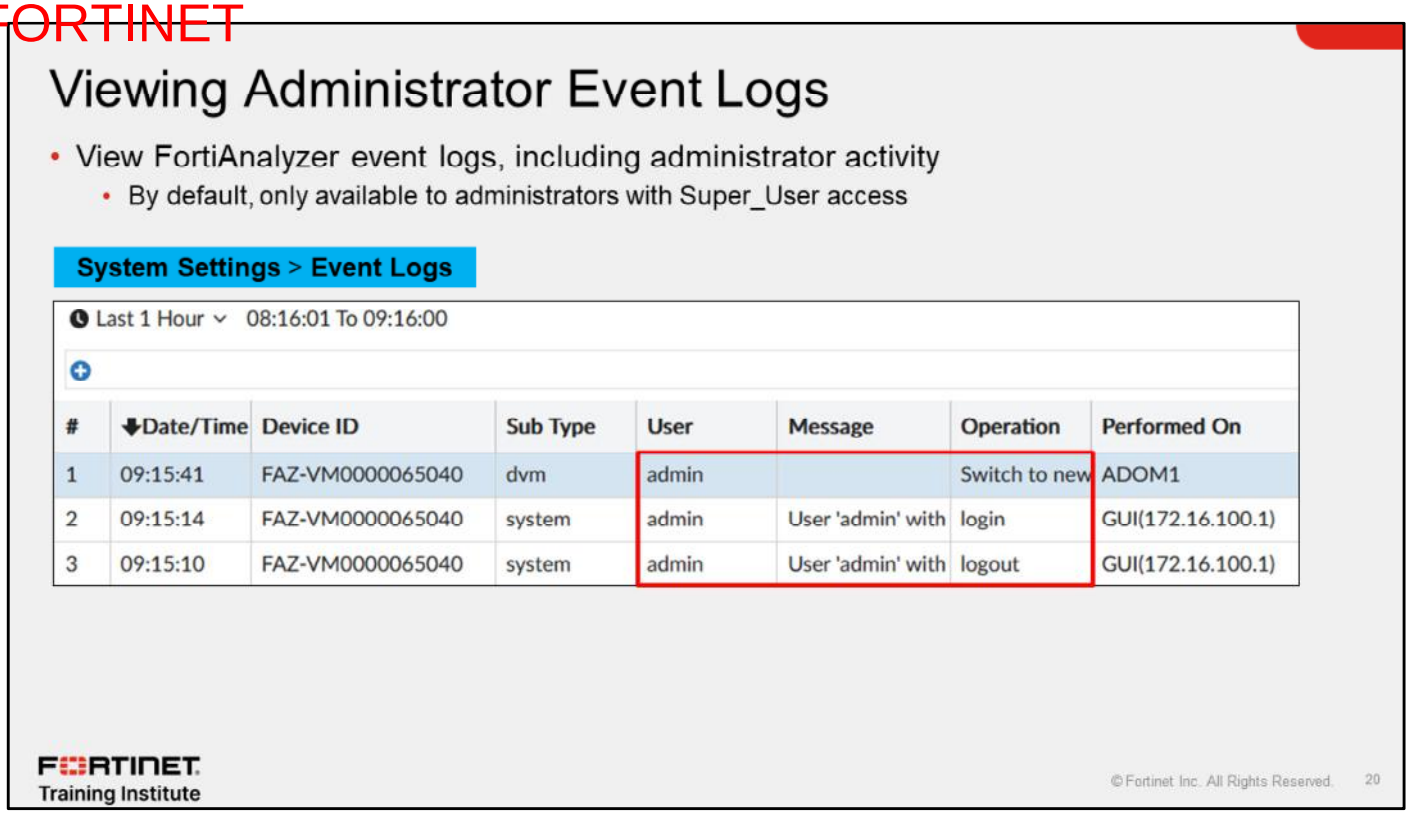
After completing this section, you should be able to achieve the objectives shown on this slide.

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.



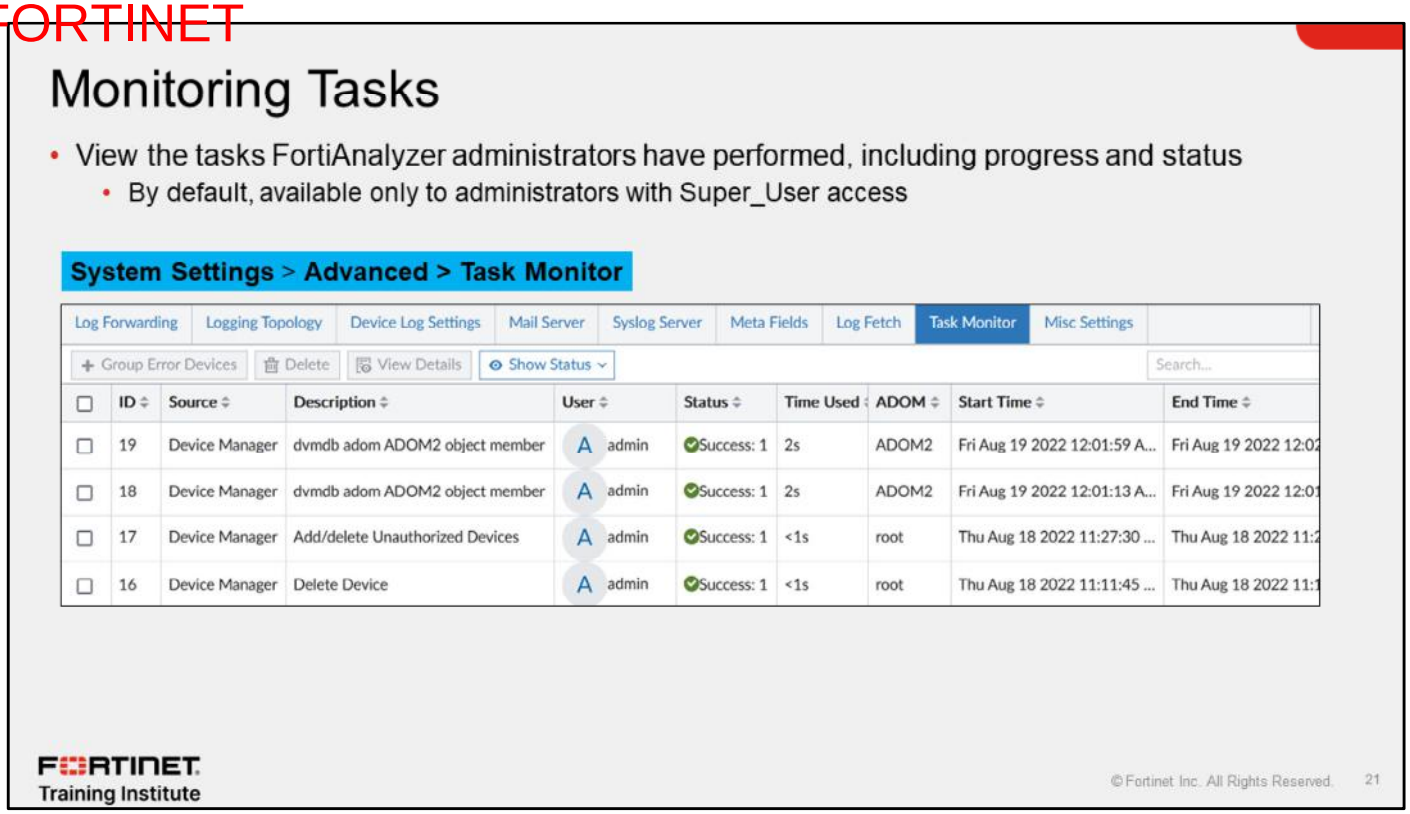
You can track administrator user sessions, including who is currently logged in and on what trusted host, through the **Administrators** page. By default, only administrators with Super_User access can see the complete list of administrators.

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



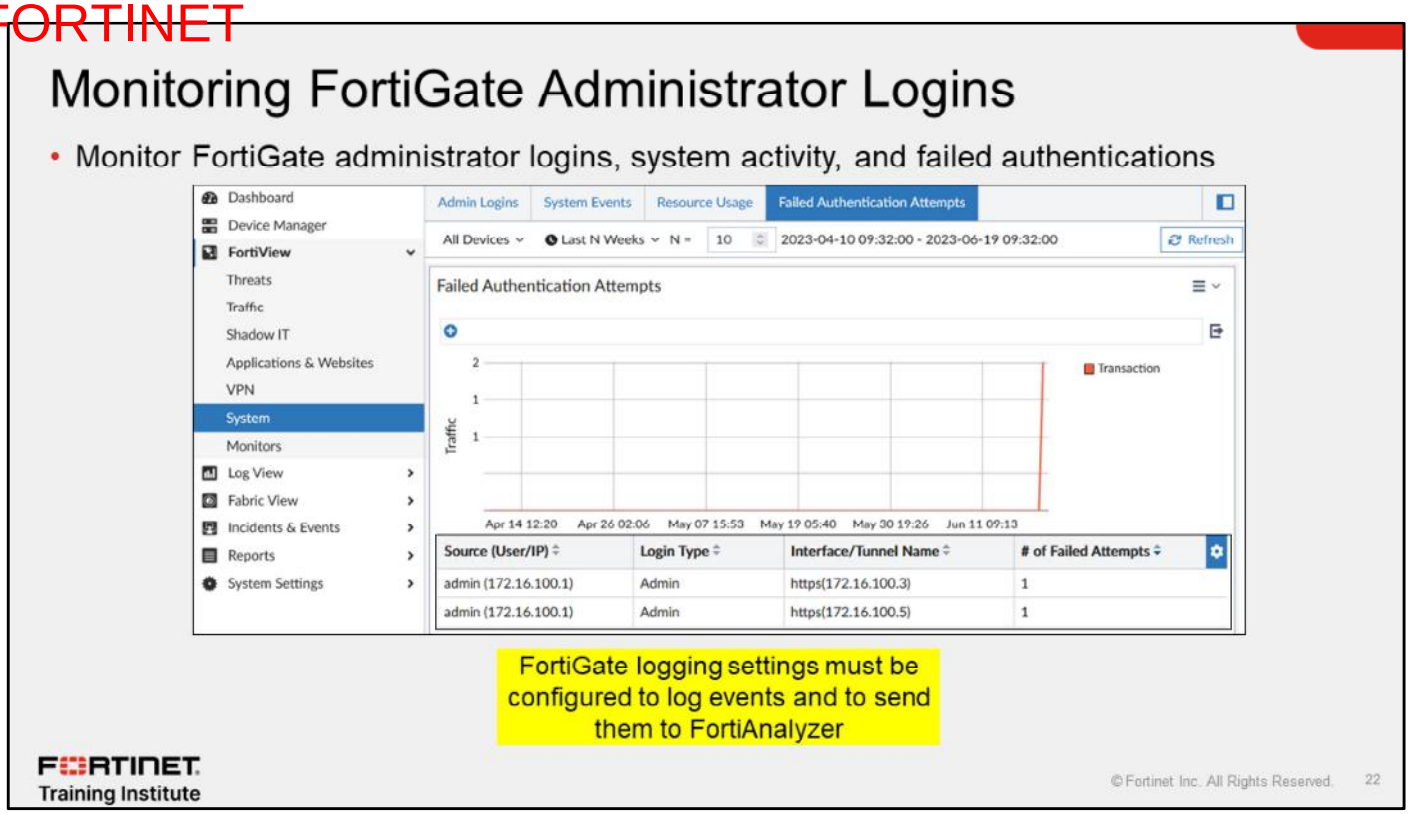
FortiAnalyzer audits administrator activity, so you can source changes to an individual.

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 user name.



The **Task Monitor** page allows you to view administrator tasks, as well as the progress and status of those tasks.

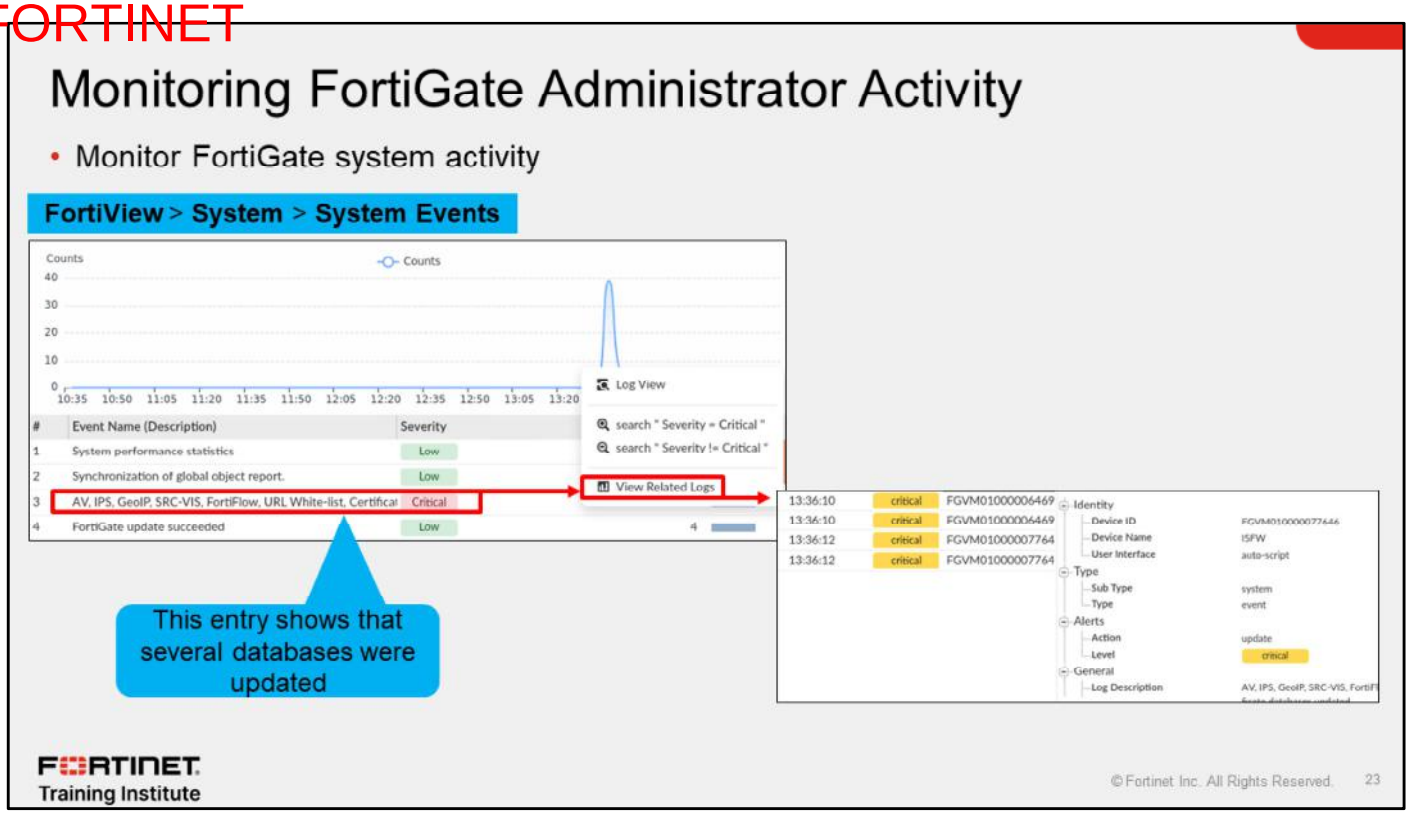
You can right-click on a task to view more details, including a progress report for each subtask inside the main task.



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 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.



FortiAnalyzer also allows you to monitor FortiGate administrative activity using FortiView.

The **System Events** page shows 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**.**

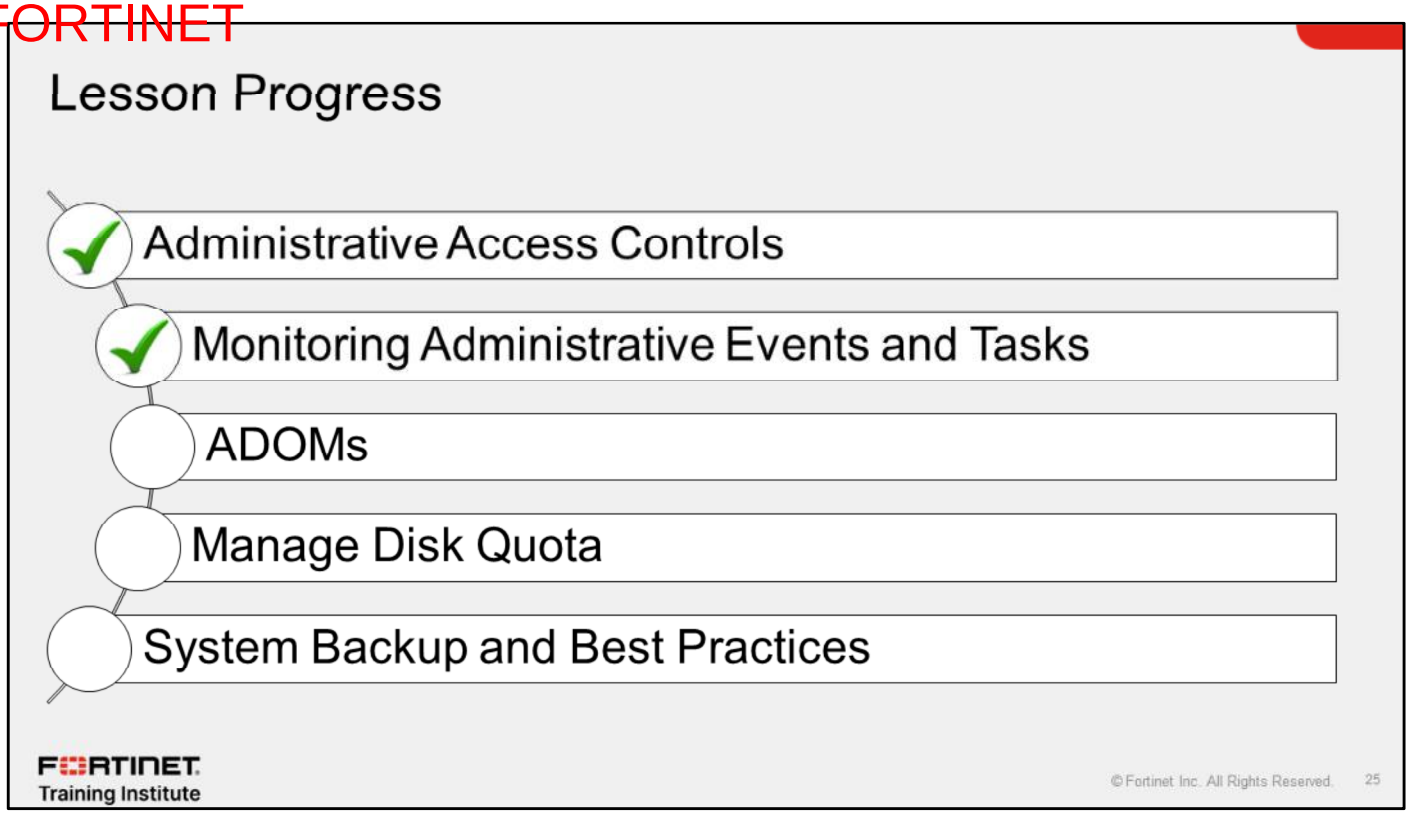
Knowledge Check

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

2. If an administrative user's job requires them to manage devices but not system settings, what is the most appropriate default administrator profile to assign them?
   - A. Super_User
   - ✓ B. Standard_User

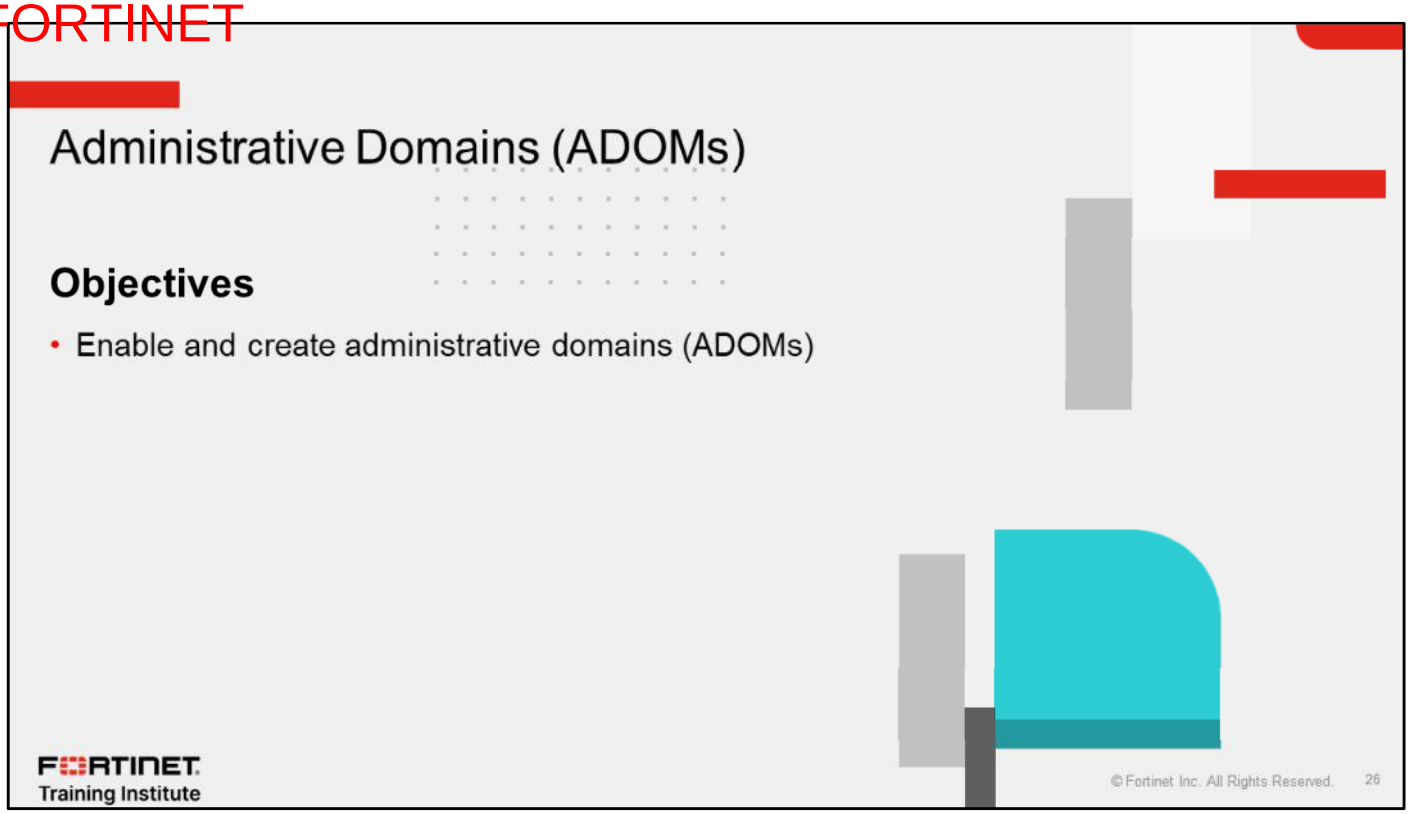
FORTINET Training Institute

 24



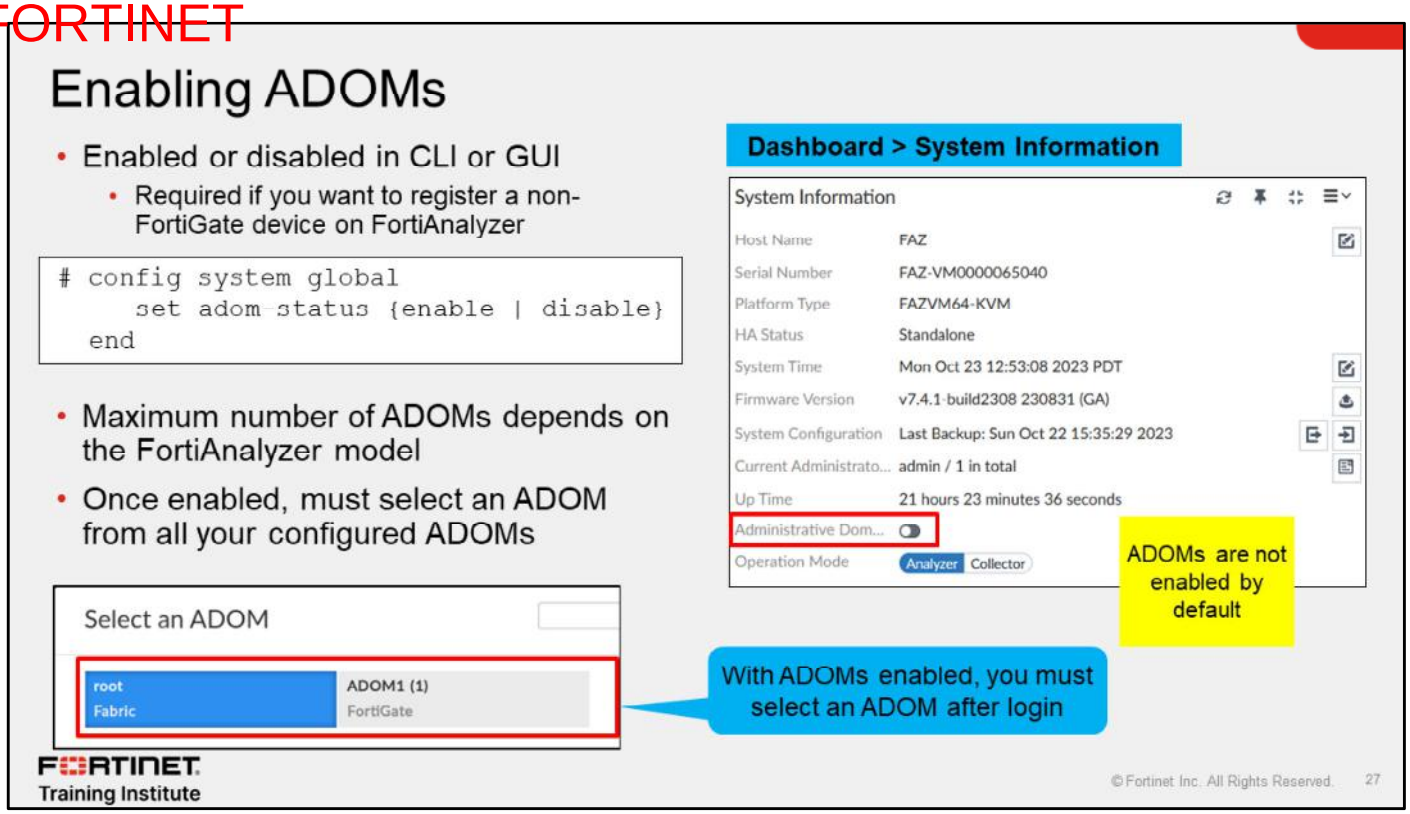
Good job! You now understand how to monitor administrative events and tasks.

Now, you will learn about administrative domains, known as ADOMs.



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.

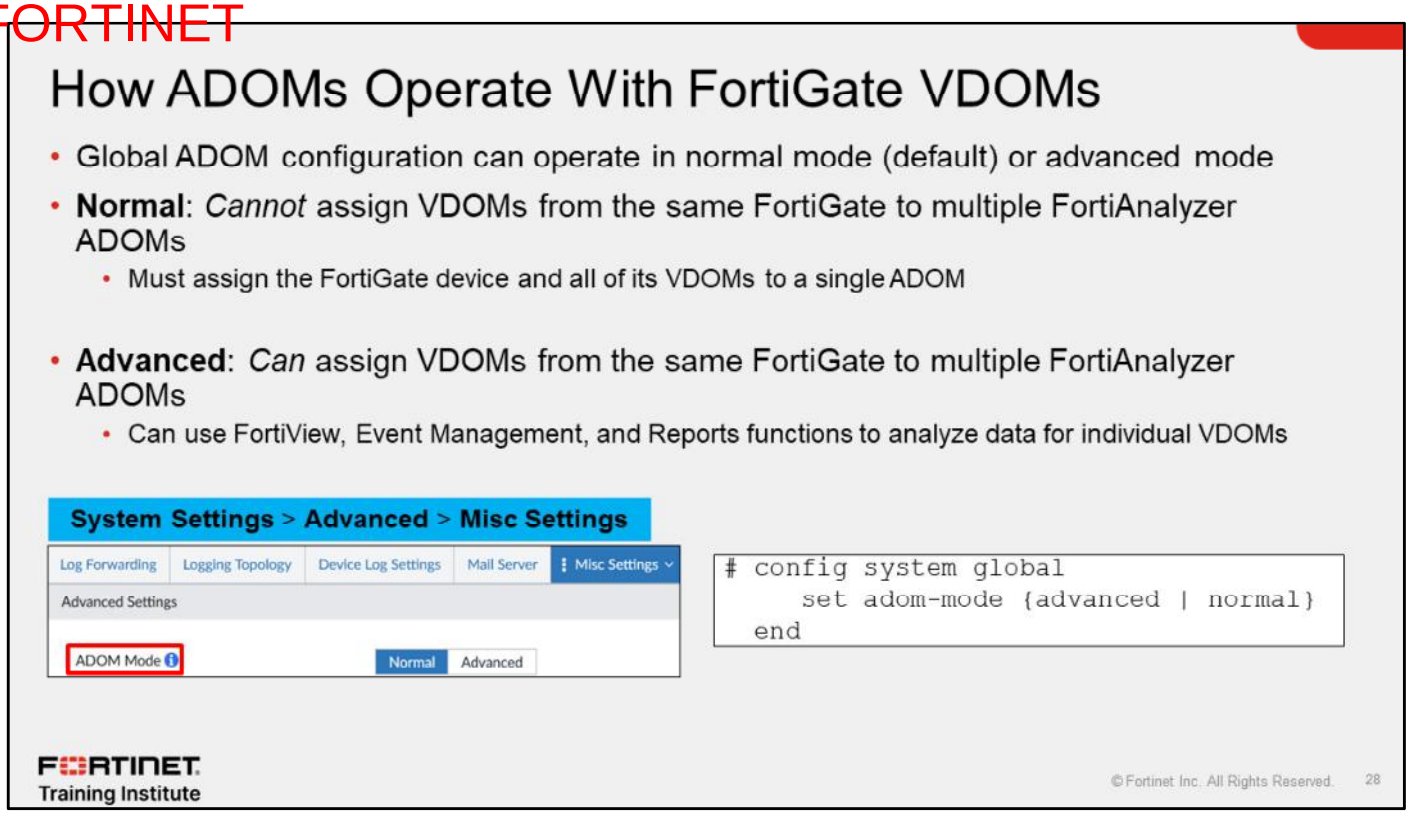


ADOMs are not enabled by default. In addition, by default only administrators with Super_User access can enable and configure ADOMs.

You can enable or disable ADOMs in the GUI through **System Settings** or the CLI with the command `config system global`.

After you enable ADOMs, the system logs you out so it can reinitialize with the new settings. The maximum number of ADOMs you can enable varies by FortiAnalyzer model.

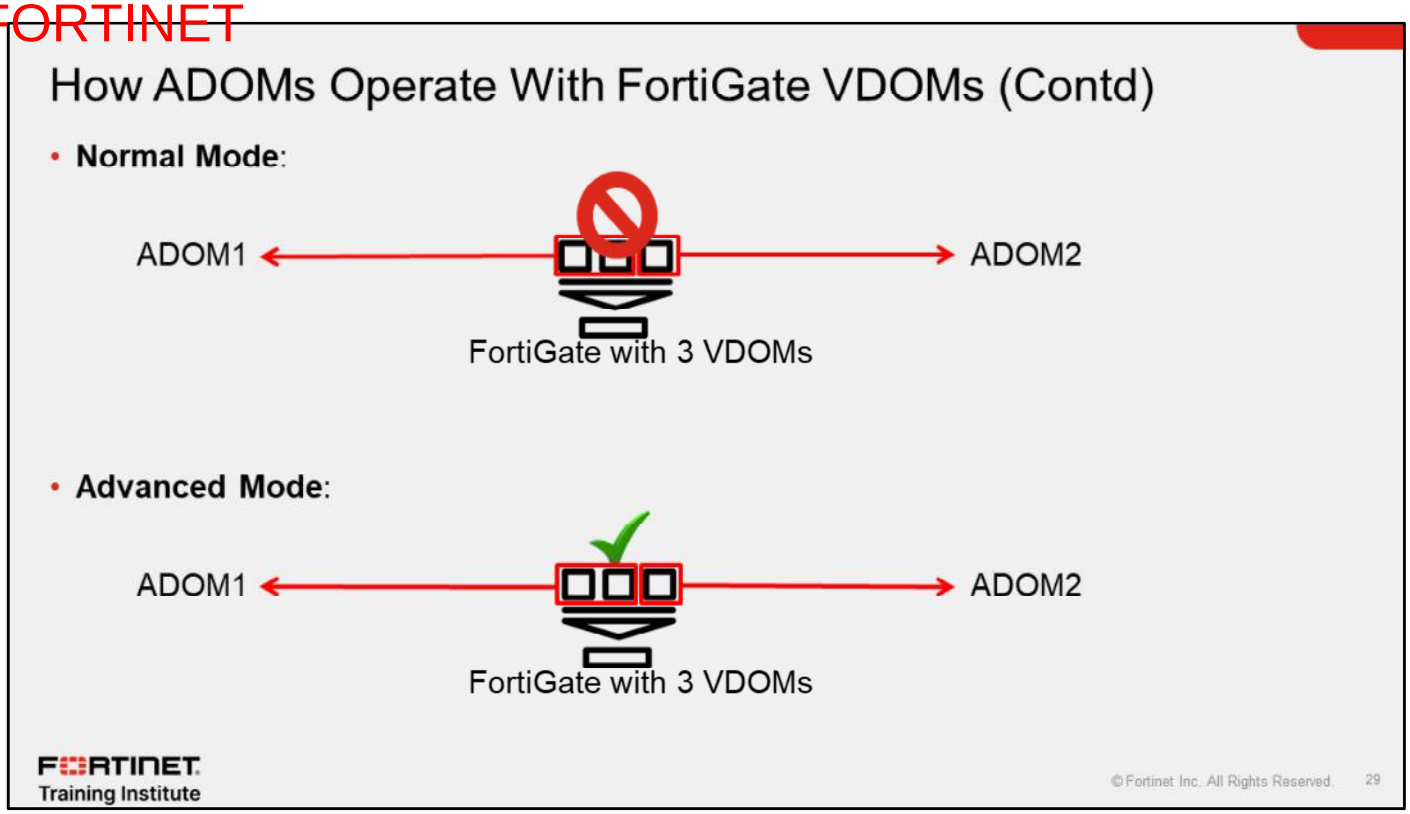
After you log in with ADOMs enabled, you must select the ADOM you want to view from the list of configured ADOMs.



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 device to multiple FortiAnalyzer ADOMs. You must assign the FortiGate device, and all of its VDOMs, to a single ADOM.

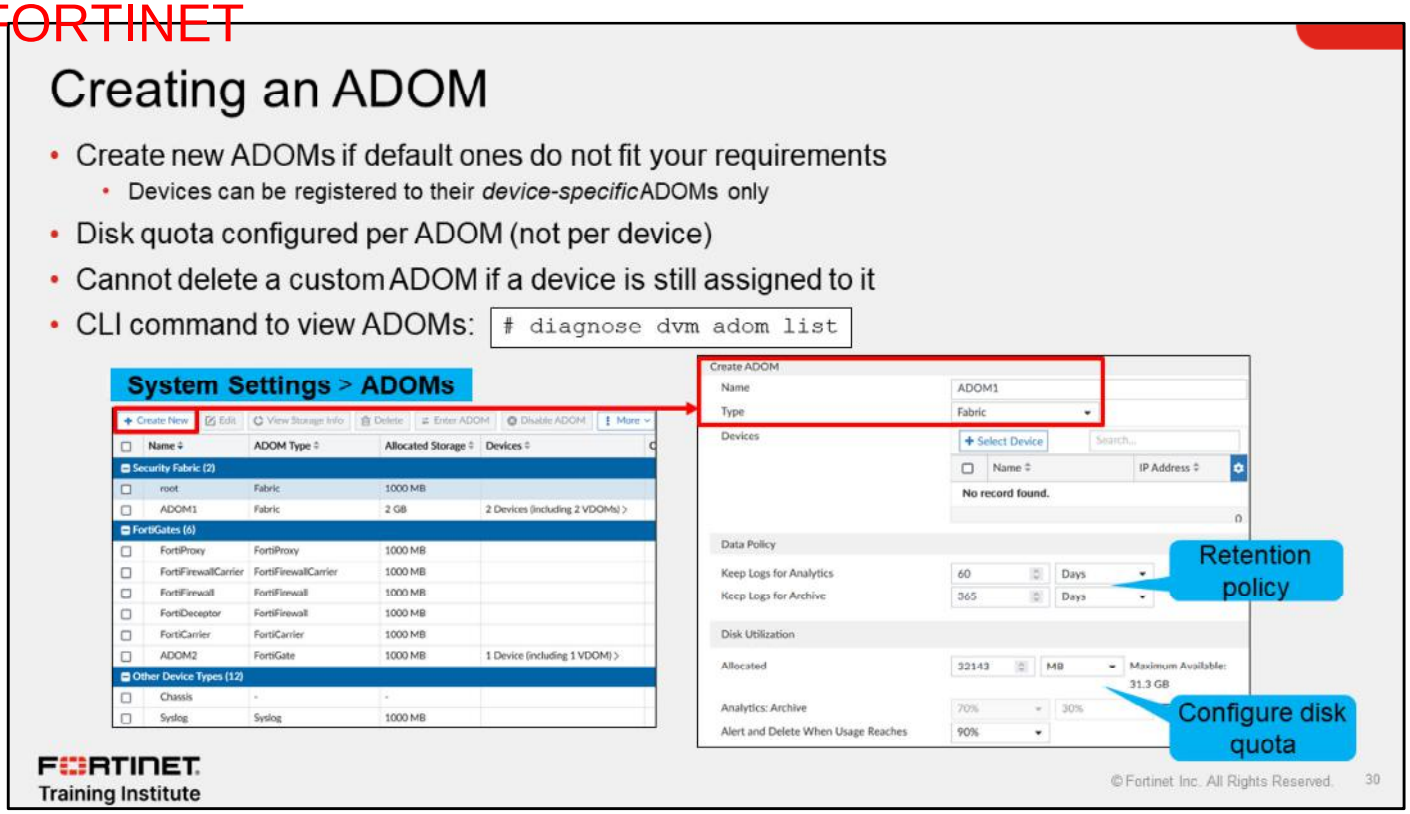
In advanced mode, you can assign VDOMs from the same FortiGate device to multiple FortiAnalyzer ADOMs. This mode allows you to use the FortiView, Event Management, and Reports functions to analyze data for individual VDOMs. Advanced mode results in more complicated management scenarios.



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

On the top, when using normal mode, it is not possible to assign different VDOMs to different ADOMs.

On the bottom, when using advanced mode, each VDOM can be assigned to a different ADOM.

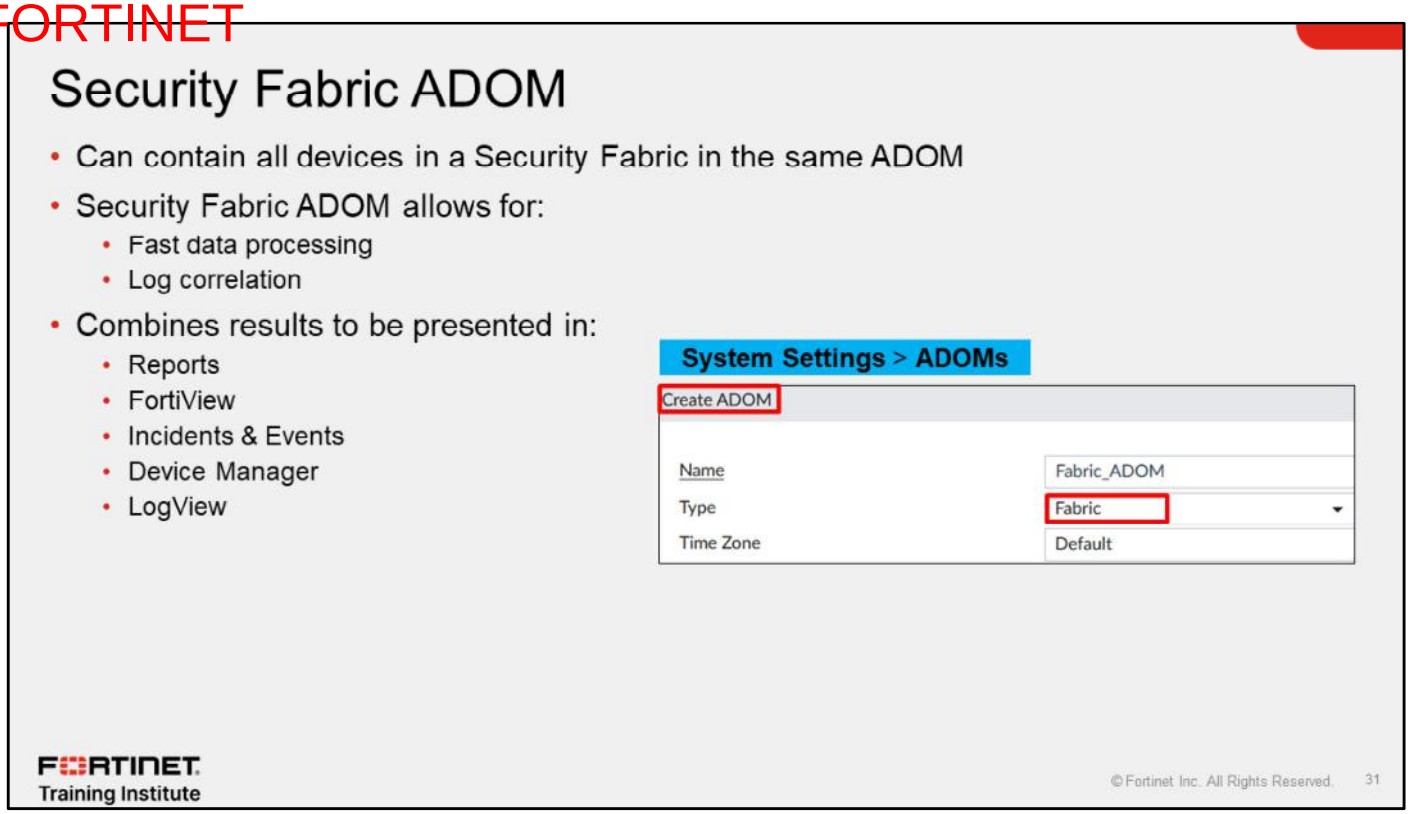


On the **ADOMs** page, you can see all configured ADOMs, as well as the default ADOMs for all non-FortiGate devices. If the default ADOMs do not fit your requirements, you can create your own.

The ADOM type you create must match the device type you are planning 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 new ADOM.

During the creation of a new ADOM, you can set the disk quota. This quota is assigned to the ADOM, and **not** to the individual devices added to it.

Note that you cannot delete default ADOMs. You also cannot delete custom ADOMs with assigned devices until you remove all devices from that ADOM.



In FortiAnalyzer, all Fortinet devices in a Security Fabric can be placed in the same ADOM.

This allows for fast data processing, log correlation and enables combined results to be presented in **Device Manager**, **Log View**, **FortiView**, **Incidents & Events**, and **Reports** panes.

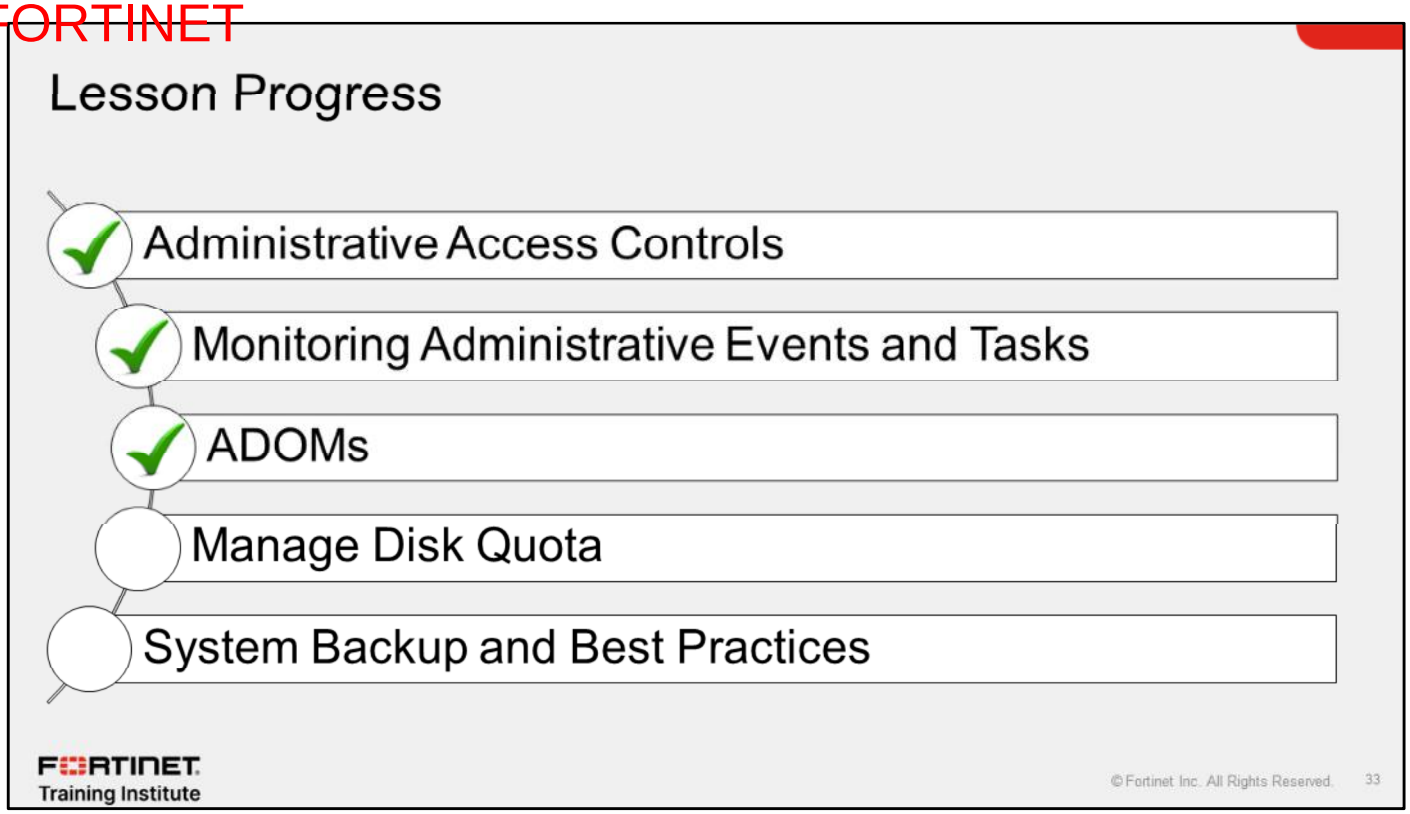
After a Fabric ADOM is created, it is listed under the **Security Fabric** section of **All ADOMs**.

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.

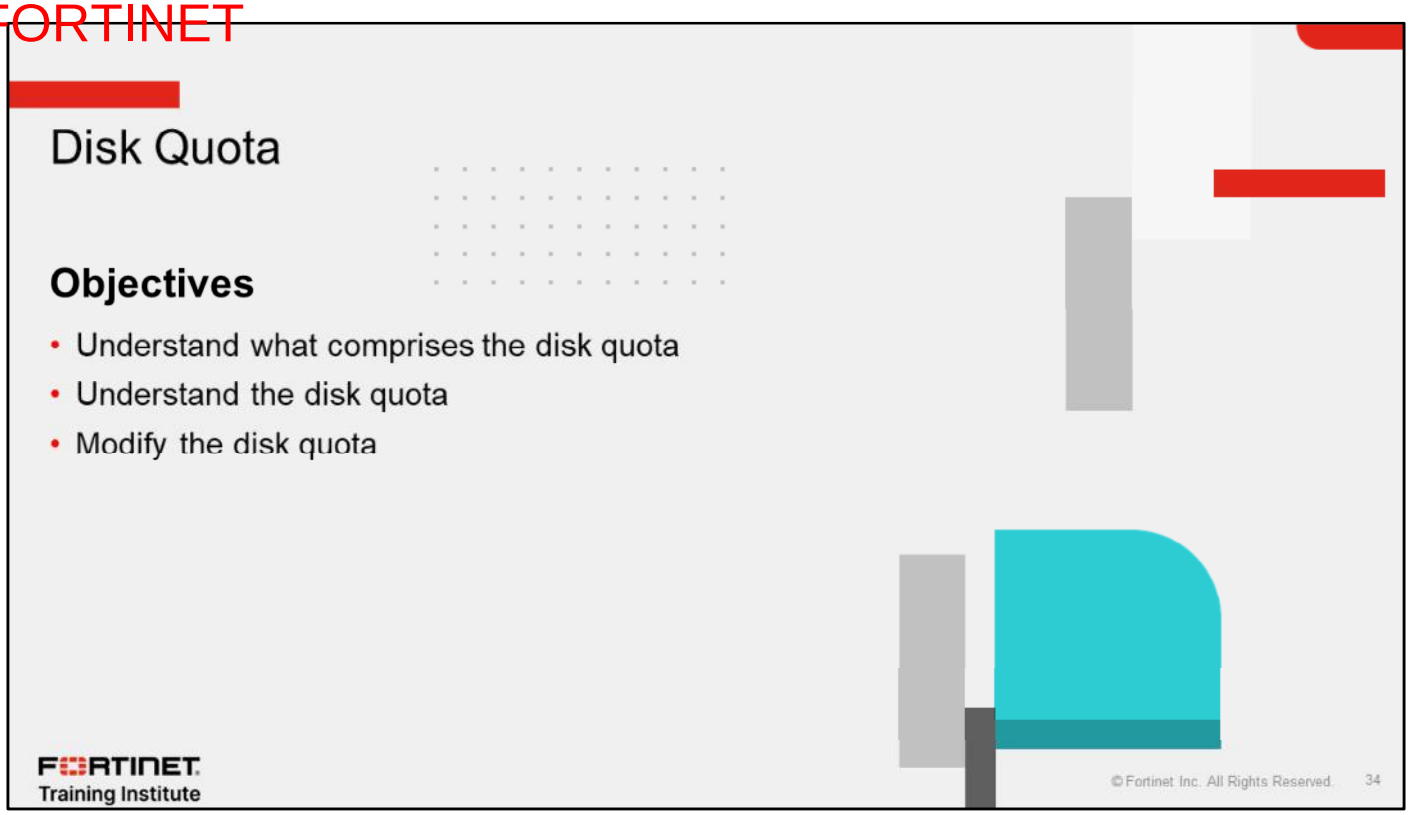
FORTINET Training Institute

 32



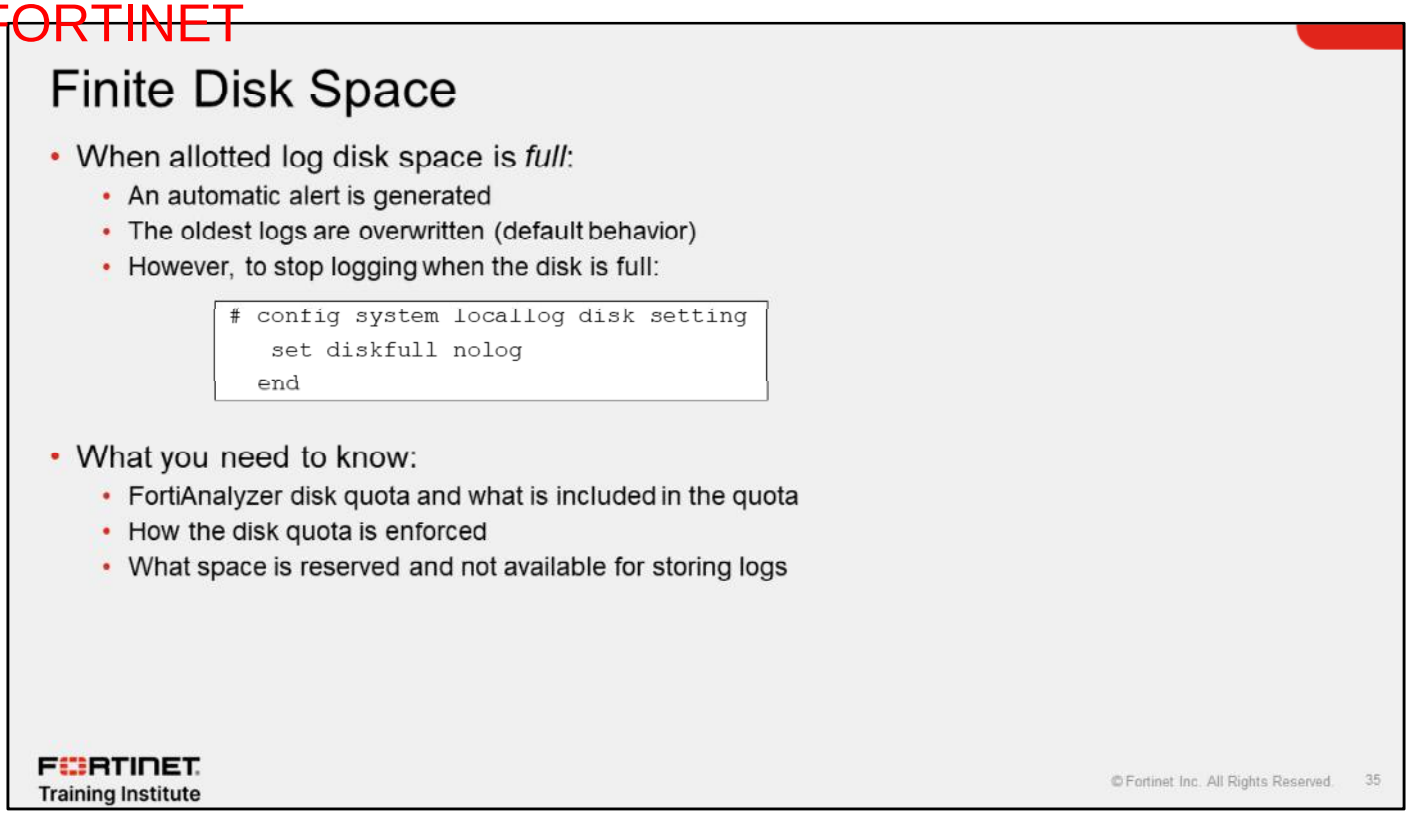
Good job! You now understand ADOMs.

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.

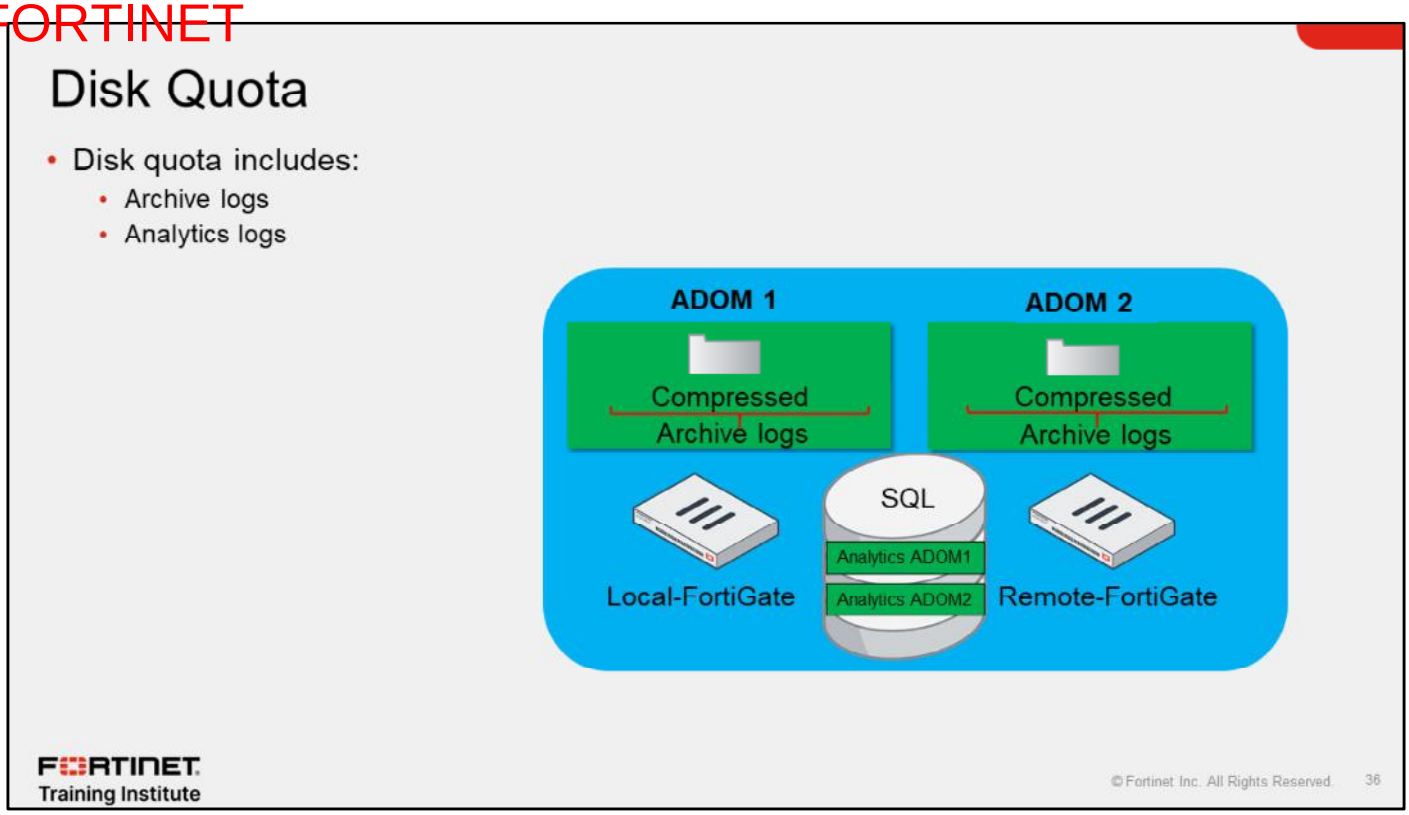
By demonstrating competence in understanding disk quota and how to modify it, you will be able to use disk quotas more effectively in your network.



FortiAnalyzer devices have finite disk space. When the allotted log disk space is full, the following occurs:

- An alert message automatically generates on the **Alert Message Console** as an event log with the level *warning*.
- The oldest logs are overwritten. This is the default setting, but you can adjust this behavior to stop logging when the disk is full instead.

No administrator wants to lose valuable log data and run the risk of noncompliance with regard to data retention. As such, it is vital you know your FortiAnalyzer disk quota, how it is enforced, and what space is reserved and thus not available for storing logs.



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.

Analytic logs indexed in the SQL database require more disk space than Archive logs. The only exception to this rule is when FortiAnalyzer is working in collector mode because the SQL database is not running.

An average indexed log is 600 bytes in size, and an average compressed log is only 80 bytes in size. Keep this difference in mind when specifying the storage ratio for Analytics and Archive logs. The default ratio is 70%-30%.

Reserved Disk Quota

- The system 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
```

See amount of reserved space on your FortiAnalyzer

- RAID levels determines the disk size and reserved disk quota level
  - For example, a FAZ 1000C with 4 x 1 TB hard drives configured in RAID 10 is considered a large disk (2 TB)

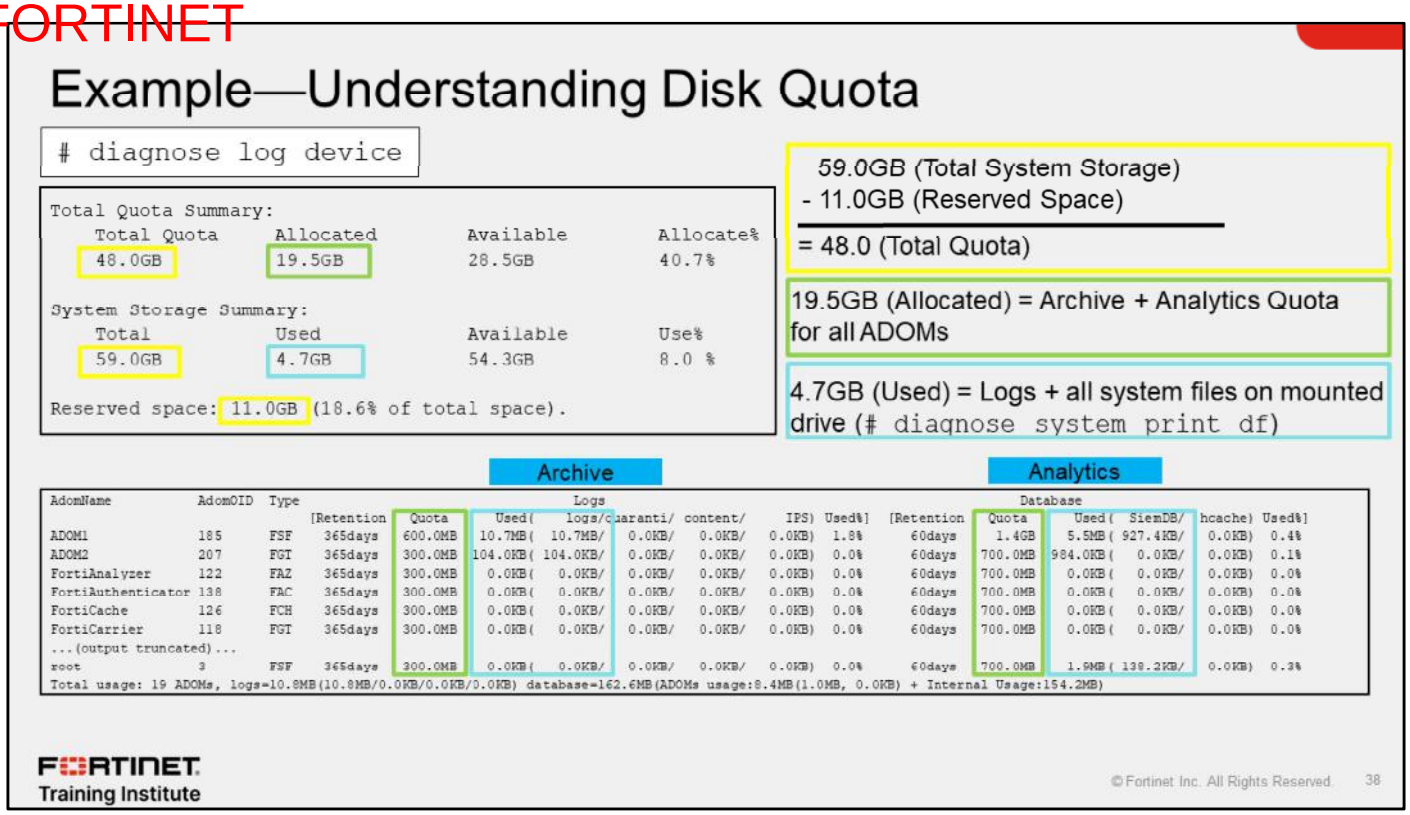
FORTINET Training Institute

 37

By default, each ADOM is allowed 1000 MB (or just under 1 GB) worth of drive space on FortiAnalyzer in order to store log data. However, this number is configurable. You can't set the minimum below 100 MB, and the maximum depends on the disk space allocation of the specific FortiAnalyzer device.

The FortiAnalyzer system reserves between 5% to 20% disk space for compression files, upload files, and temporary report files, leaving about 80% to 95% disk space for allocation to devices.

It is important to note that if using RAID, the RAID level determines the disk size and reserved quota level. See the table on the slide for more details.

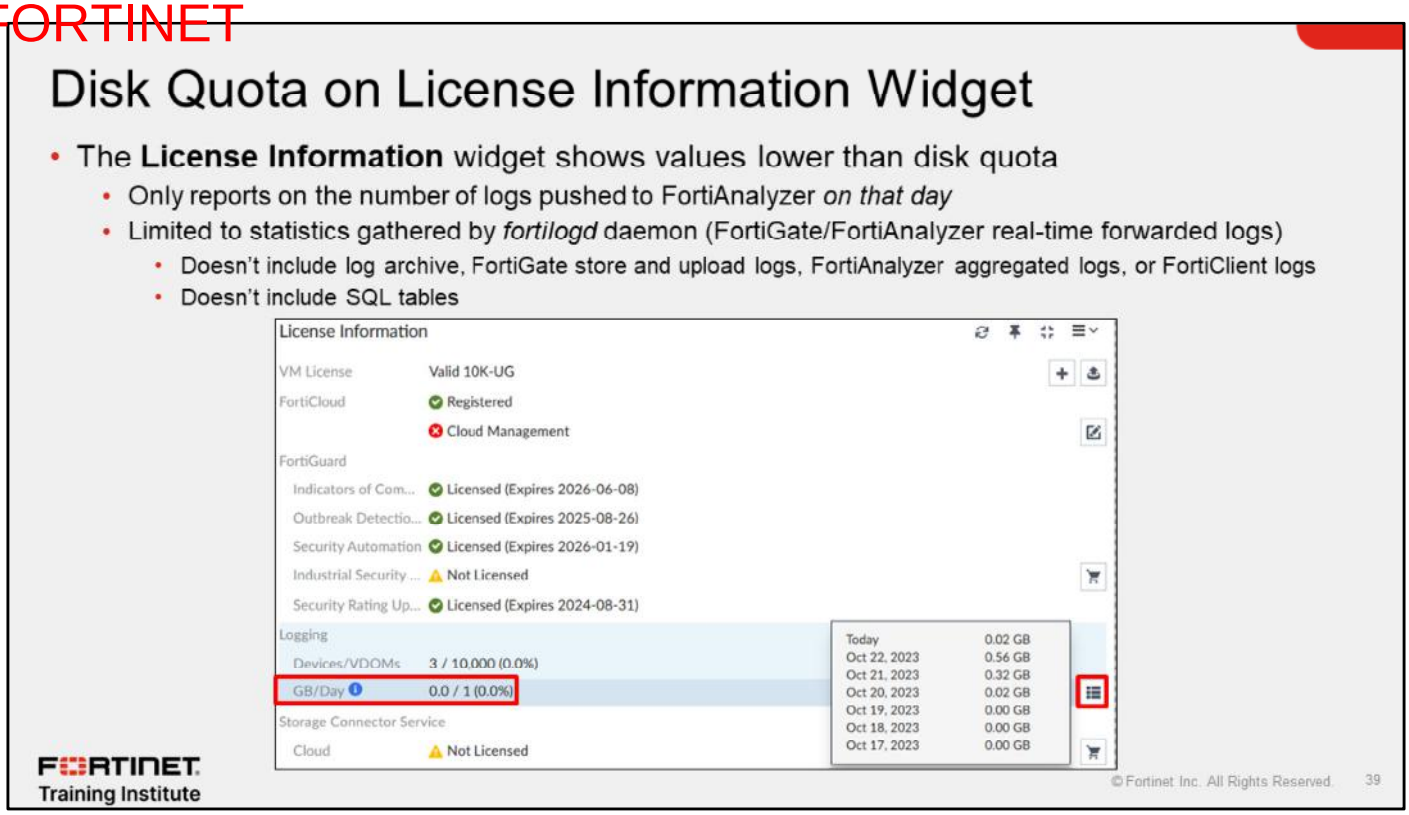


You can obtain your disk log usage, including usage for each ADOM, using the CLI command `diagnose log device`.

The total quota value is determined by subtracting the reserved space from the total system storage.

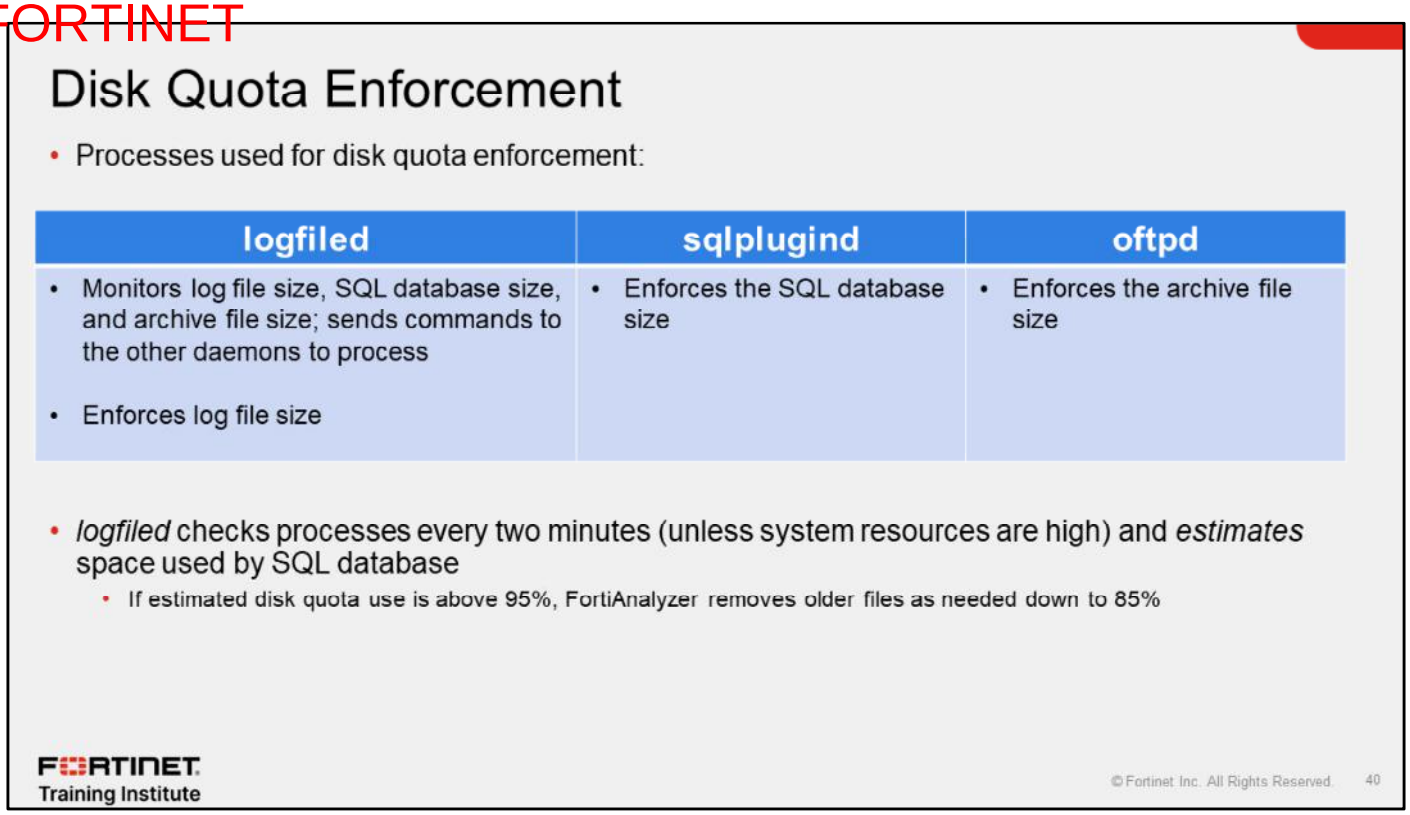
The allocated space is determined by adding the archive and analytics quota for all ADOMs.

The used space is determined by adding the archive and analytics logs and all the system files mounted on the drive. You can receive the system file value by using the CLI command `diagnose system print df`.



Note that the **License Information** widget shows a lower value than the disk quotas. This is because it reports only on the number of logs pushed to FortiAnalyzer *on that day*. You can click the show details icon to see the log volume for the previous 6 days. Furthermore, it reports only on the ingress traffic, which is limited to the raw log portion. It doesn't include the log archive, FortiGate store and upload logs, FortiAnalyzer aggregated logs, or FortiClient logs. The SQL database tables are not included either, because this indexing is done by FortiAnalyzer *after* the log has been received.

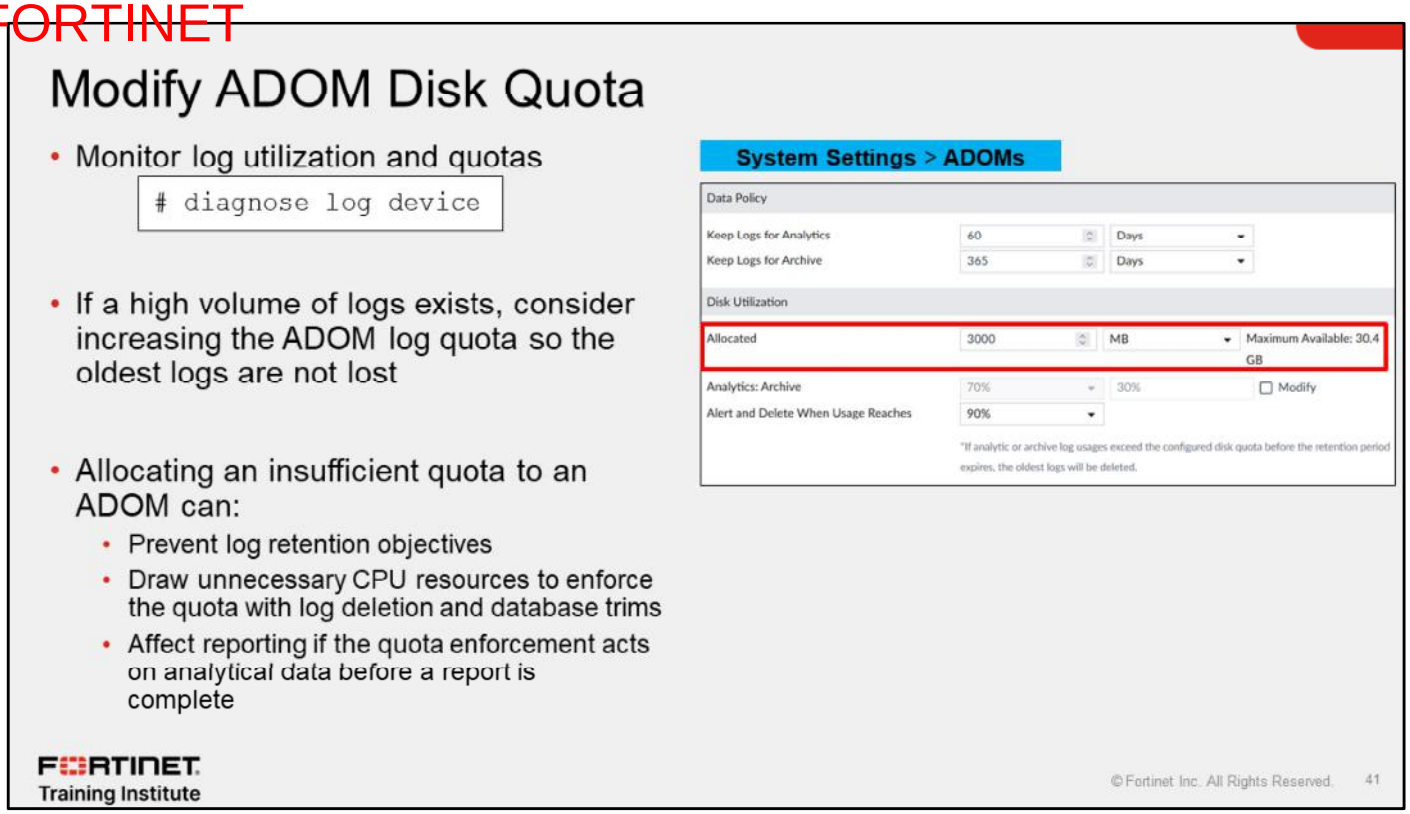
You must pay attention to both the daily log limit and the configured disk quotas. If you find that either is consistently approaching or going over the threshold, see if you can optimize your FortiAnalyzer configuration by reducing unnecessary logs, such as by filtering logs and removing unnecessary devices from being logged. If the network consistently generates traffic that exceeds the daily log limit, you can increase your licensing level. If you find that the disk quota is not sufficient to meet your logging requirments, you must allocate more resources.



Disk quota enforcement is performed by different processes:

- The *logfiled* process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes
- The *sqlplugind* process enforces the SQL database size
- The *oftpd* process enforces the archive file size

logfiled checks the processes every two minutes (unless system resources are high) and *estimates* the space used by the SQL database. If the disk quota is estimated to be above 95%, FortiAnalyzer removes files as needed until they are down to 85%.

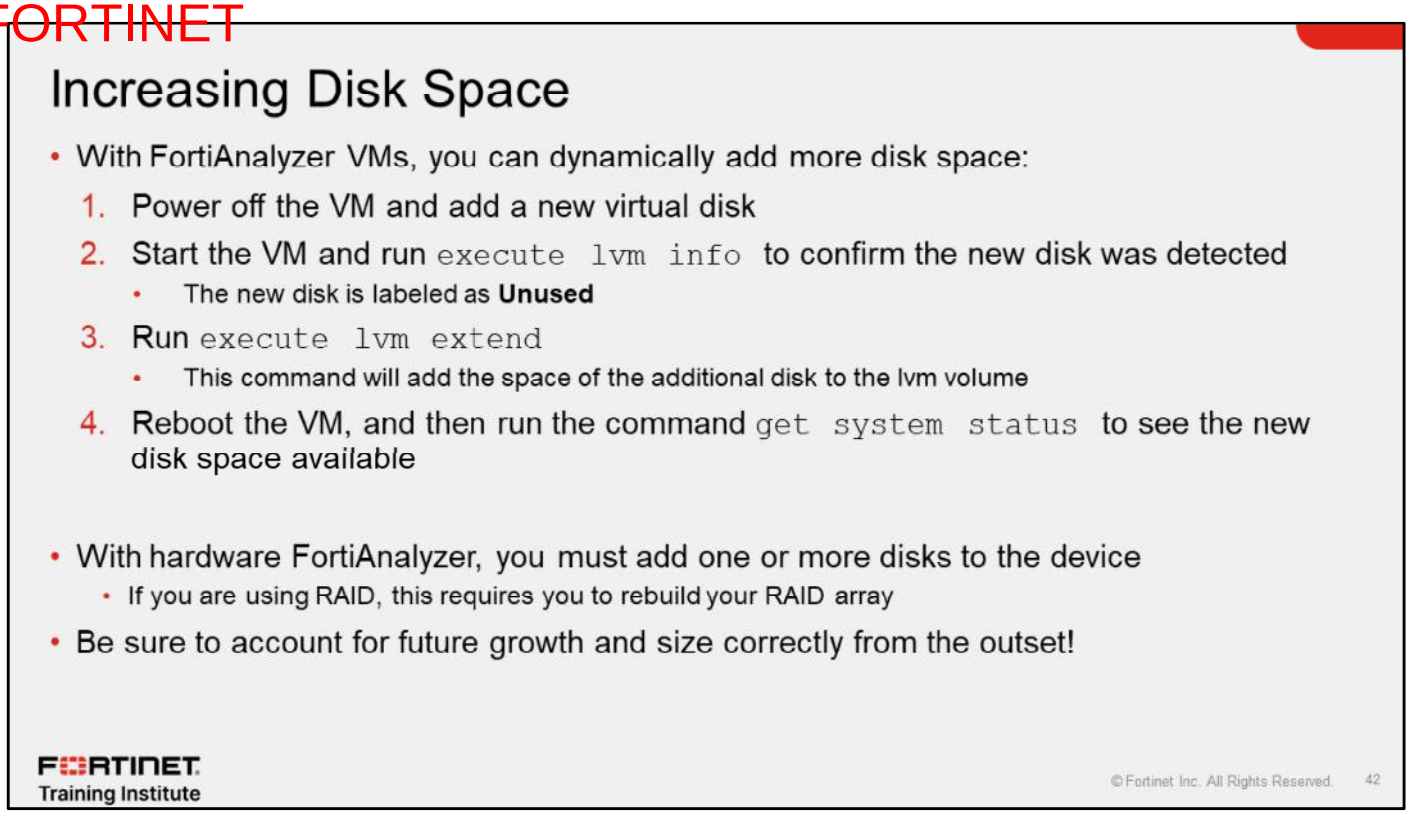


Based on your log rate and device usage statistics, you may need to adjust your ADOM disk quota so that you don't lose valuable log data.

Always monitor your log rate for each device in the ADOM. If you have a high volume of logs, increase the ADOM quota so the oldest logs are not lost prematurely.

Allocating an insufficient quota to an ADOM can cause many problems:

- It can prevent you from reaching your log retention objective.
- It can cause unnecessary CPU resources enforcing quota with log deletion and database trims.
- It can adversely affect reporting if the quota enforcement acts on analytical data before a report is complete.



If increasing the disk quota is insufficient based on your monitored log rate, you may need to increase your overall disk space.

With FortiAnalyzer VMs, you can dynamically add more disk space to your FortiAnalyzer by using the procedure shown on this slide.

With a hardware FortiAnalyzer, you must add one or more disks. If you are using RAID, you will also have to rebuild your RAID array if you add another disk. Therefore, it is important to account for future growth and size correctly from the outset.

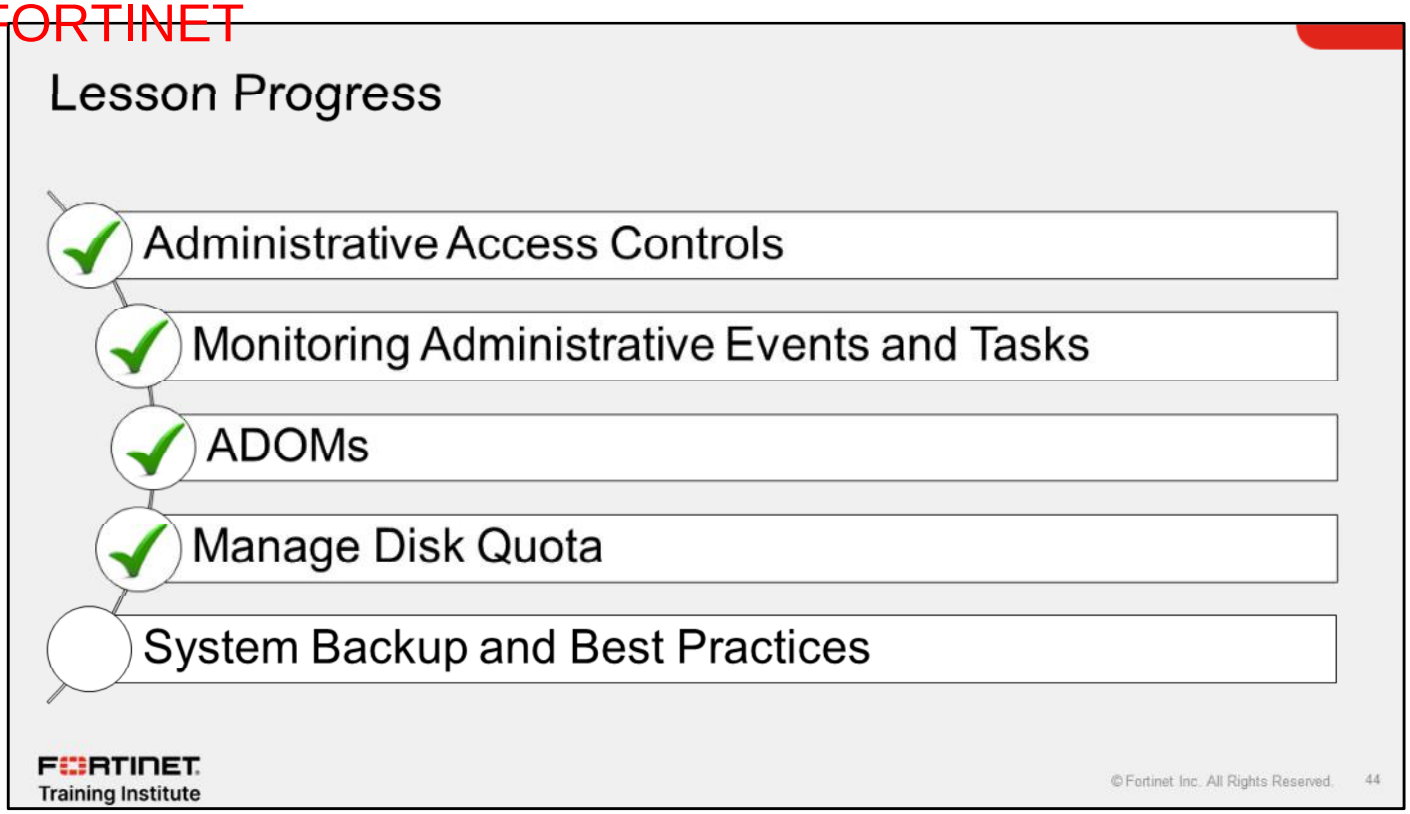
Knowledge Check

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

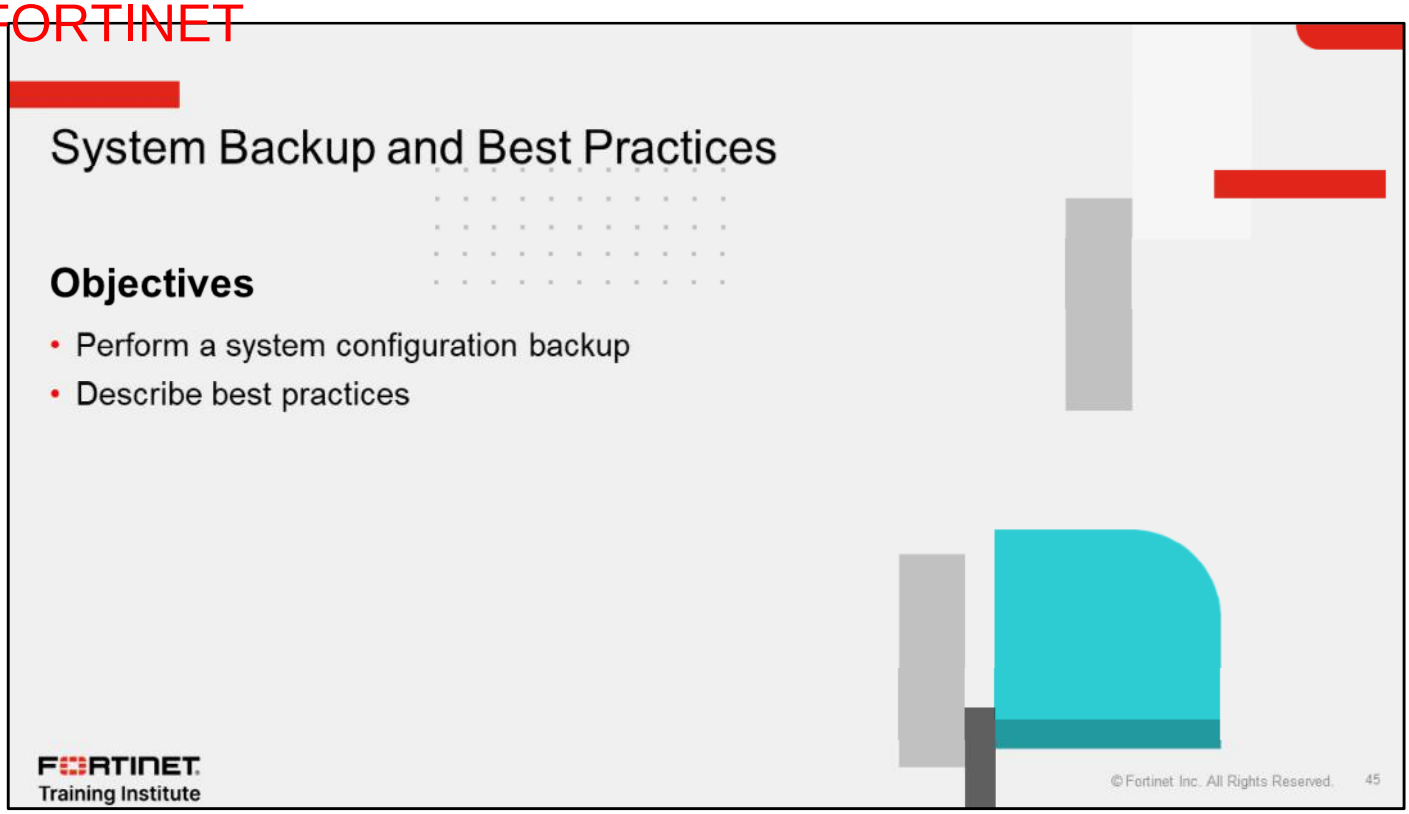
FORTINET Training Institute

 43



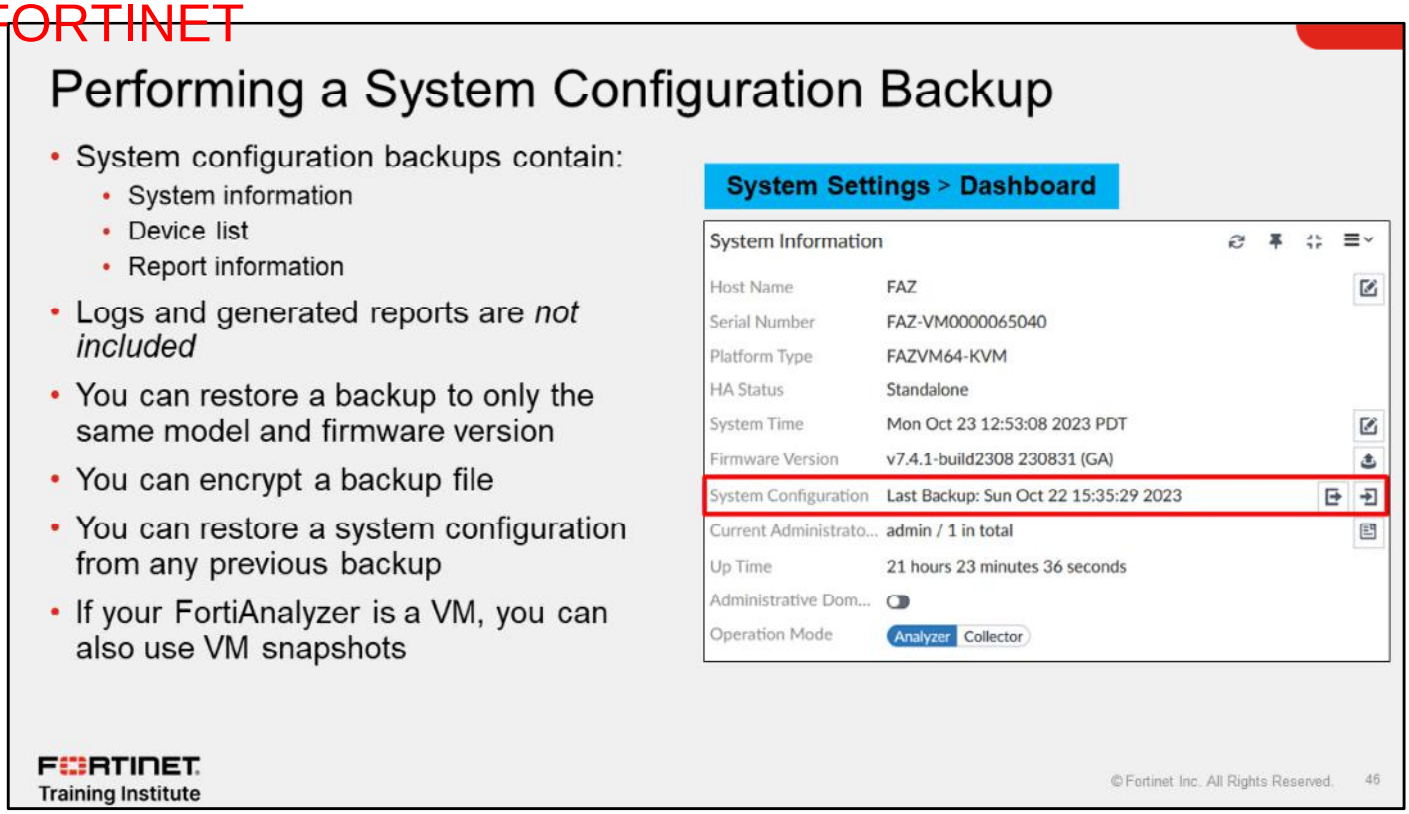
Good job! You now understand disk quotas.

Now, you will learn how to back up your FortiAnalyzer and some general 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 in the case of a system failure or accidental misconfiguration.



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

The **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:

- 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 any configured report settings, as well as all your custom report details. These details are not the actual reports.
- Automation and Incident & Events configurations, such as playbooks and event handlers

You can save the backup file as an encrypted file for additional security. Be aware that 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 changes are made to FortiAnalyzer that affect your network negatively, you can restore the configuration from any of your backups.

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

Performing a System Configuration Backup (Contd)

- Use the following commands to schedule your FortiAnalyzer backups and send them to a remote server:

```
config system backup all-settings
      set status {enable | disable}
      set server {<ipv4_address>|<fqdn_str>}
      set user <username>
      set directory <string>
      set week_days {monday tuesday wednesday thursday friday saturday sunday}
      set time <hh:mm:ss>
      set protocol {ftp | scp | sftp}
      set passwd <passwd>
      set cert <certificate_name>
      set crptpasswd <passwd>
    end
```

Supported servers include FTP, SCP and SFTP

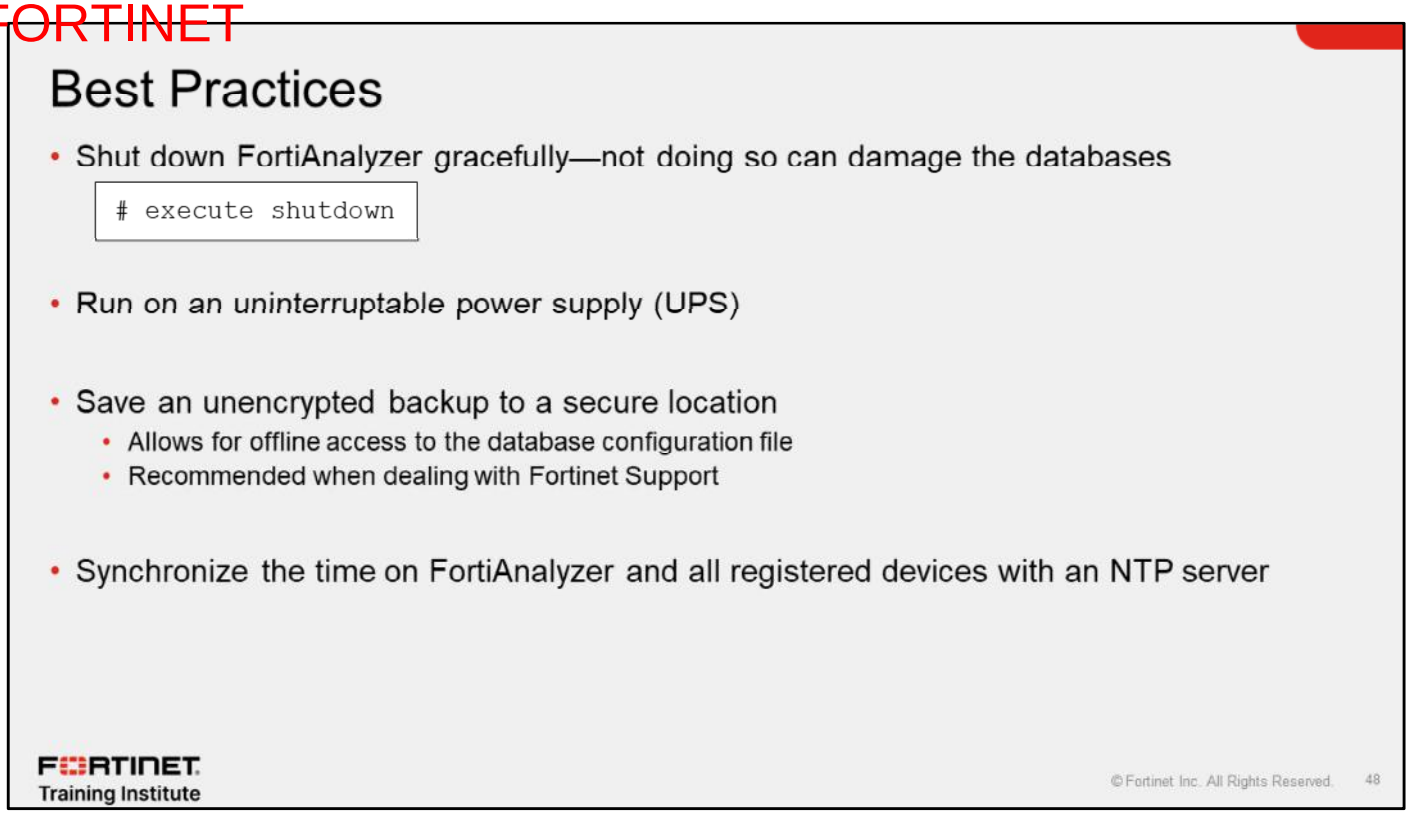
- You must configure the destination server before you send the backup files

FORTINET Training Institute

 47

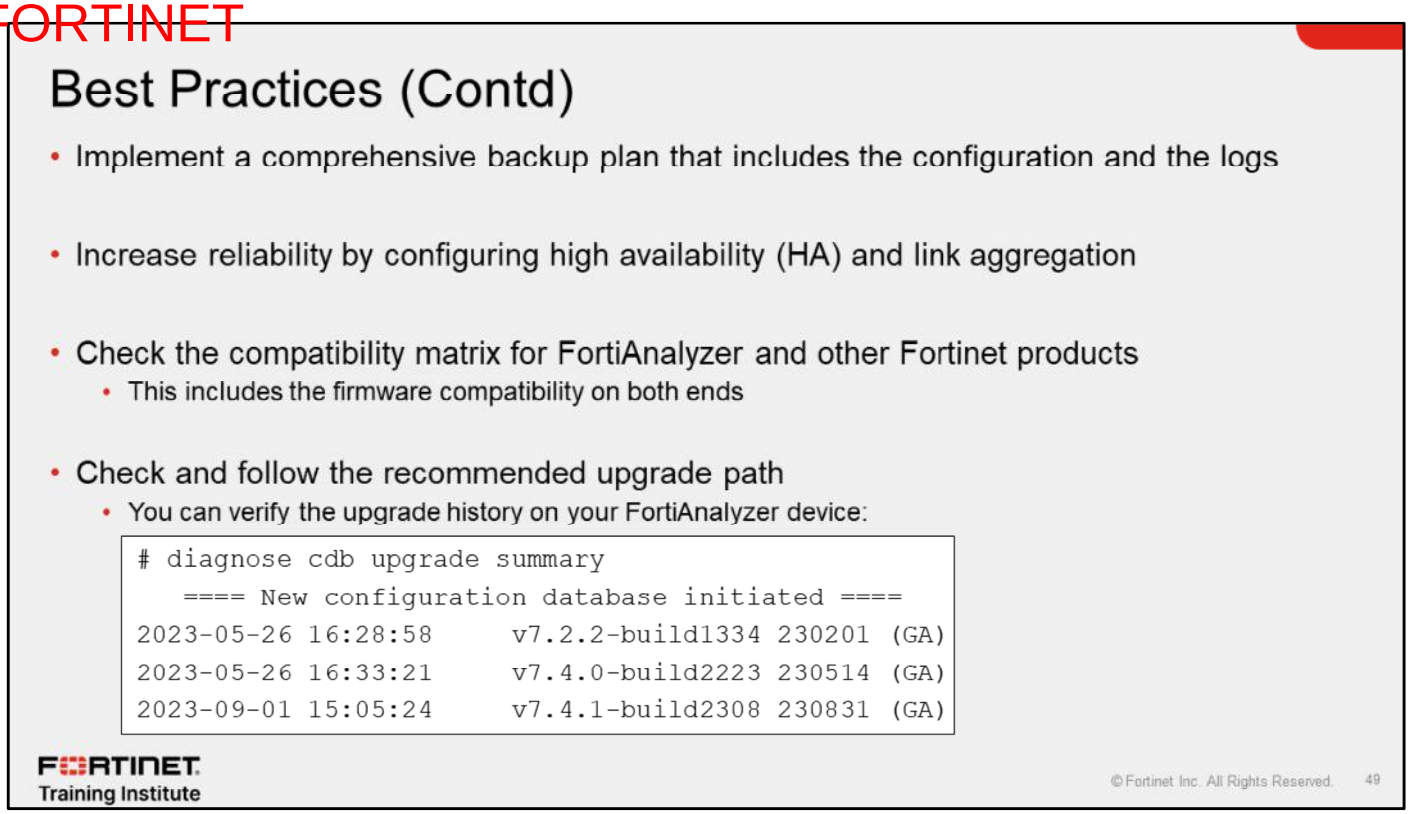
You can schedule your backups and store them on a remote server. FortiAnalyzer supports sending its backup files to FTP, SCP, and SFTP servers. You must configure the destination server to which you send the backup files. You must have valid credentials with read-write permissions in the destination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

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



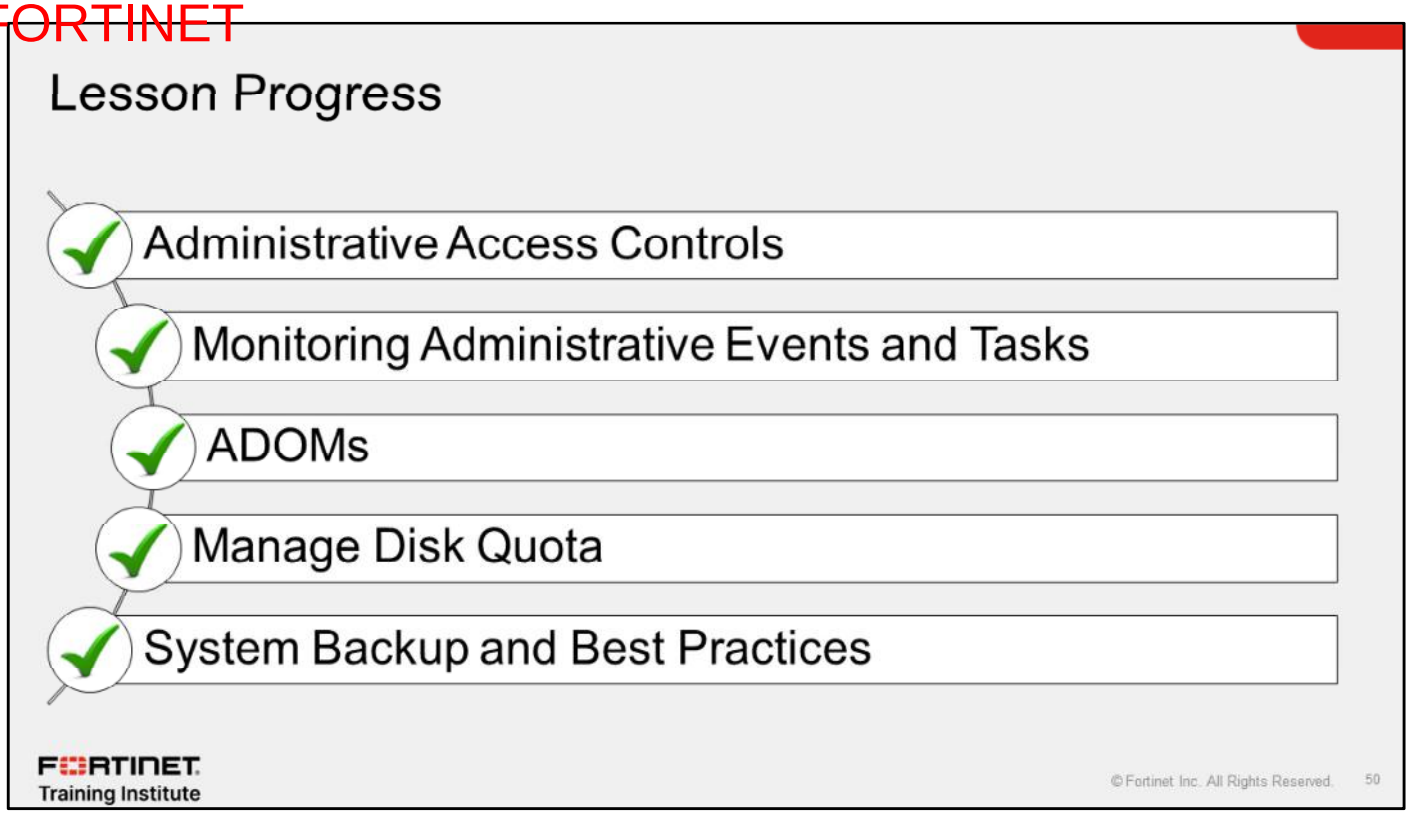
The following are some best practices for operating FortiAnalyzer:

- 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 ensure the expected behavior.
- For ease of use, save an unencrypted backup to a secure location. You should use an unencrypted backup when dealing with Fortinet Support because it allows for offline access to the database configuration file.
- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for correct log correlation.



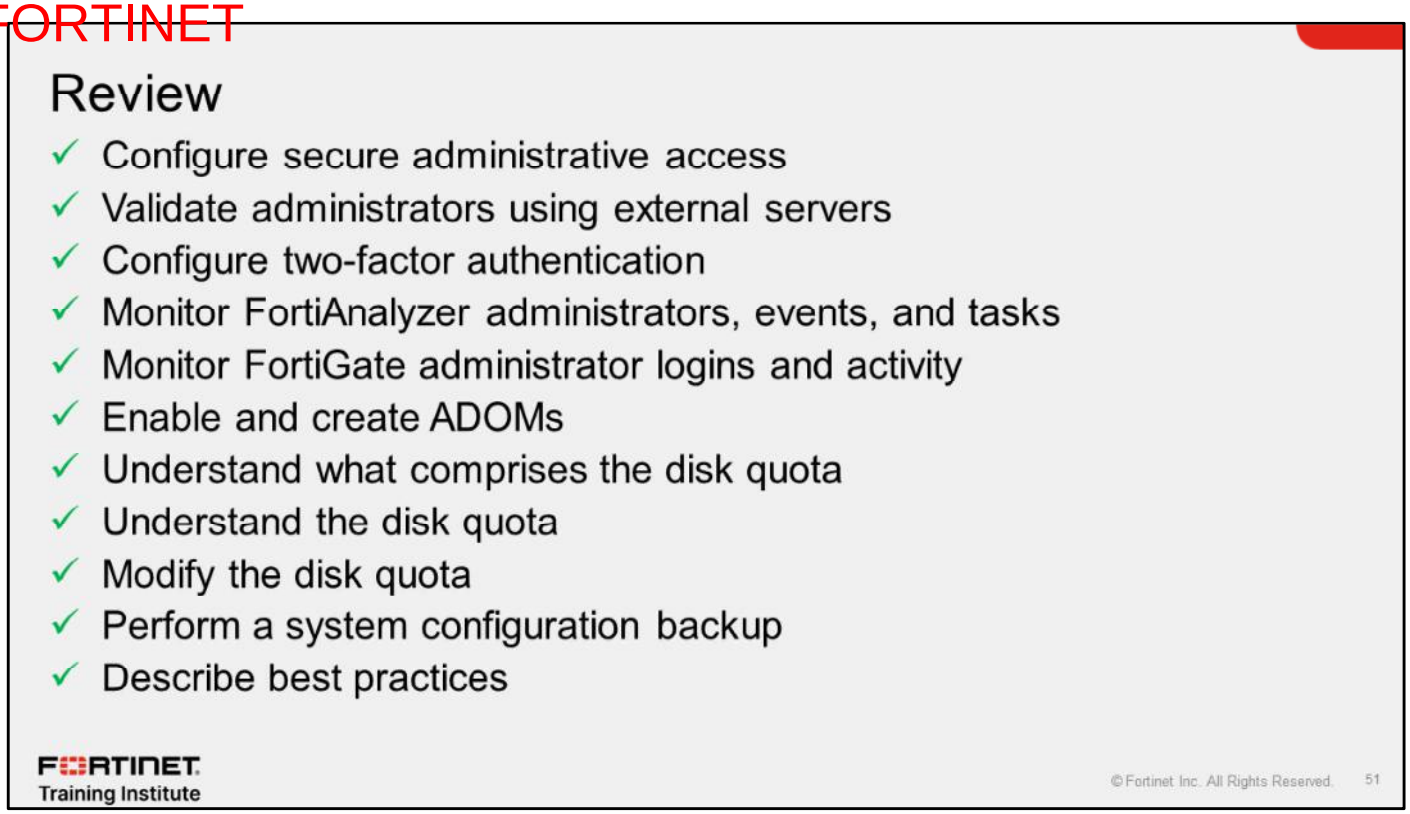
In addition, there are a few more best practices that should be followed:

- Implement a comprehensive backup plan that includes the configuration and the logs. Log backups will be discussed in Lesson 5 – *Logs and Reports Management*.
- Increase reliability by configuring high availability (HA) and link aggregation.
- Check the compatibility matrix for FortiAnalyzer and other Fortinet products. This include the firmware compatibility on both ends.
- Check and follow the recommended upgrade path. Consult docs.fortinet.com to find the appropriate upgrade path.



Congratulations! You have completed this lesson.

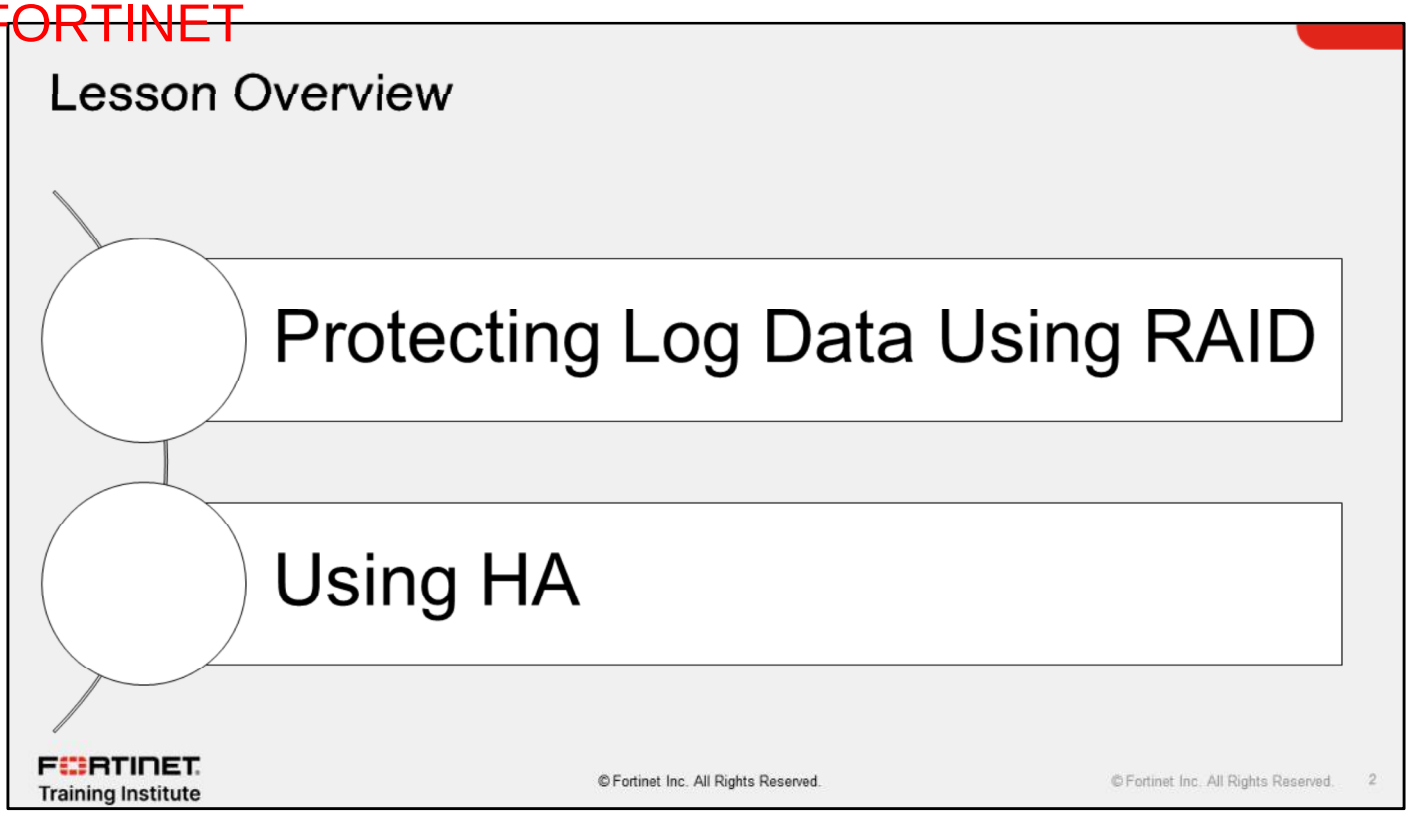
Now, you will review the objectives that you covered in this lesson.



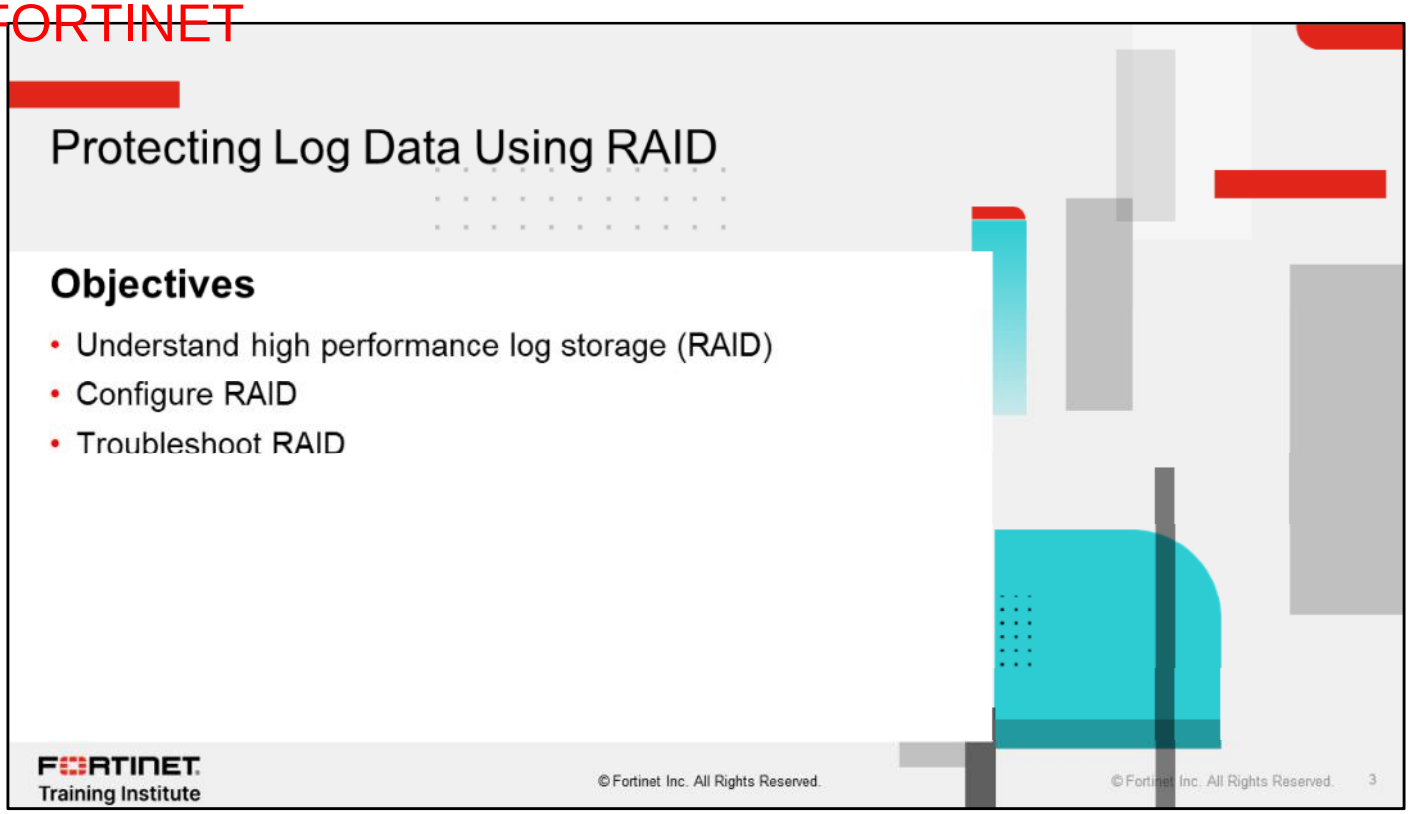
This slide shows the objectives that you covered in this lesson.

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 RAID and high availability (HA) to make your FortiAnalyzer device more resilient to hardware failures.

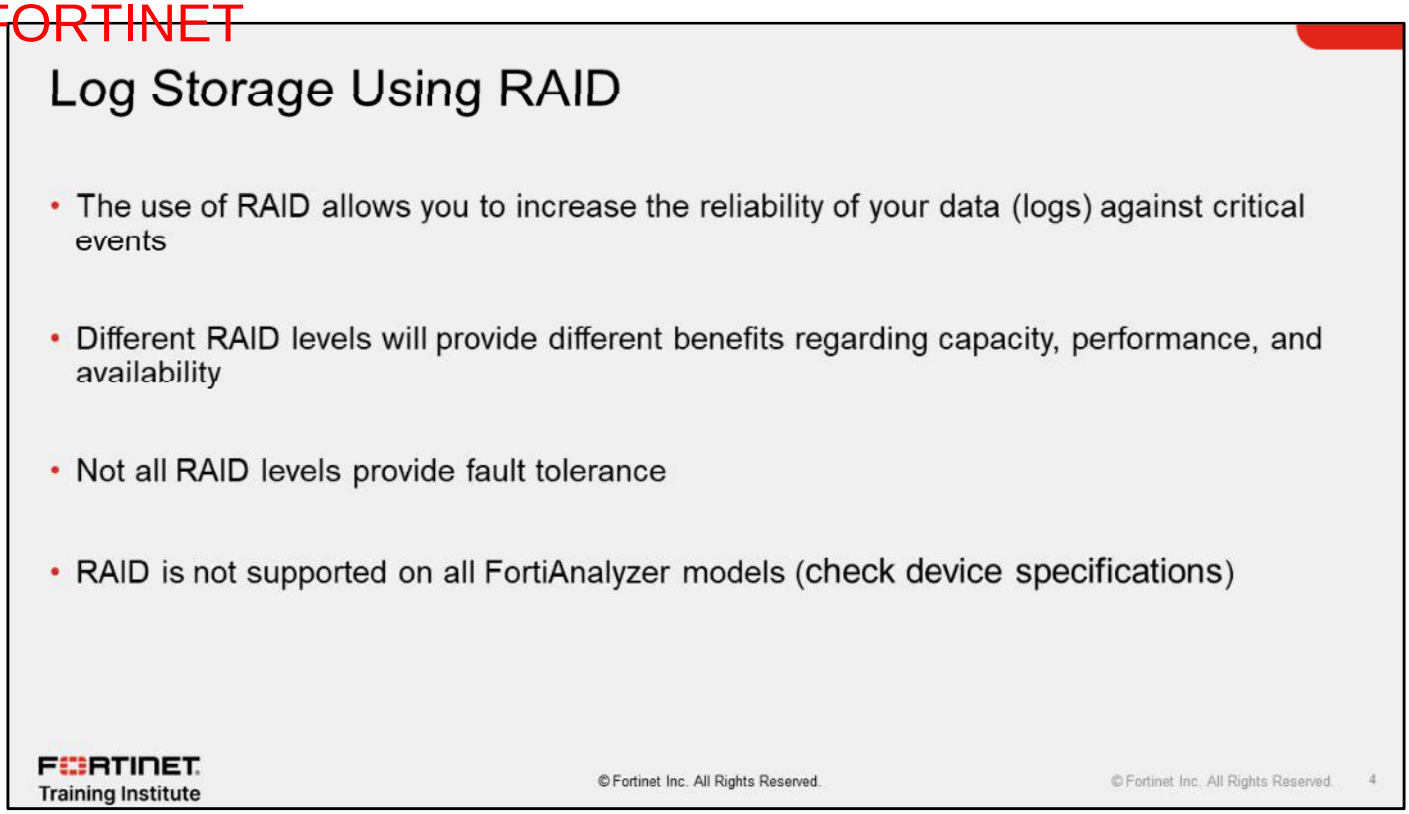


In this lesson, you will explore the topics shown on this slide.



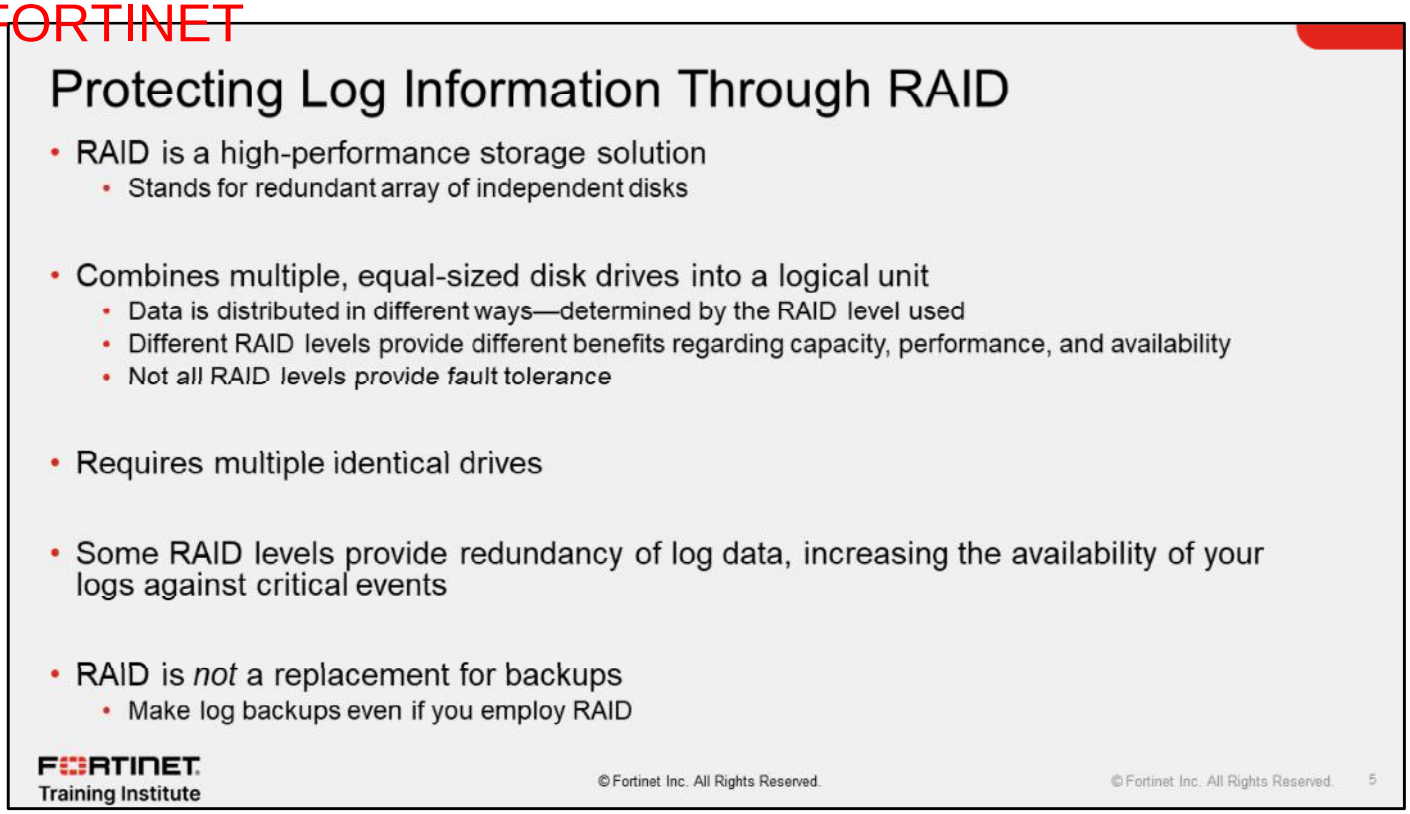
After completing this section, you should be able to achieve objectives shown on this slide.

By demonstrating competence in RAID, you will be able to better safeguard your logs while they are stored locally on FortiAnalyzer.



You can protect your logs by using a fault tolerant RAID solution. This improves your log availability should a critical event on your FortiAnalyzer occur.

RAID is not supported on all FortiAnalyzer models.



Administering and managing your system also includes protecting your log information. This can include introducing redundancy for your log data by making a copy of your logs to act as a backup, should your system stops running. The most commonly used method for high performance storage is RAID.

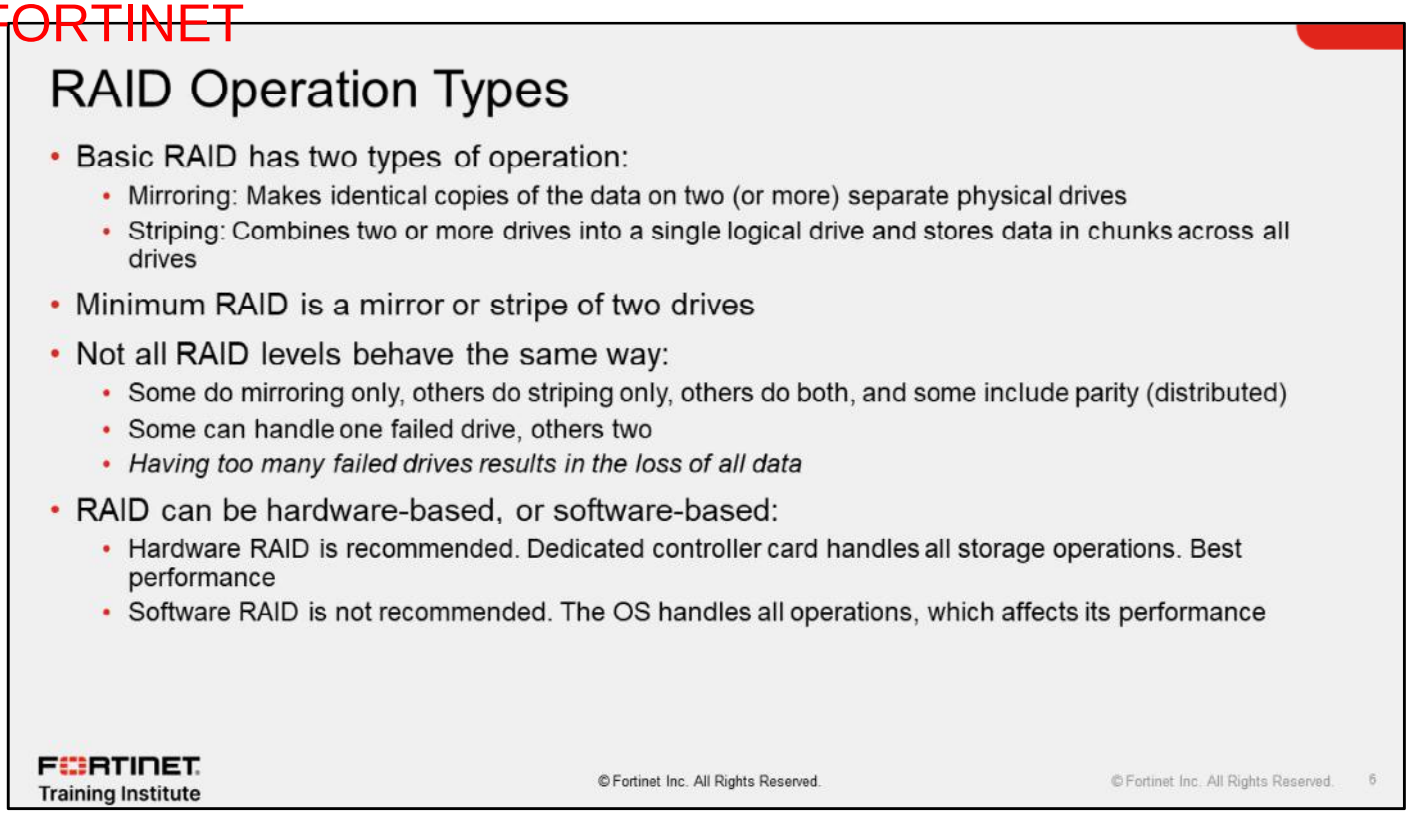
You can protect your logs by using a fault tolerant RAID solution. This improves your log availability, should a critical event on your FortiAnalyzer occur. However, keep in mind that not all FortiAnalyzer models support RAID. Check your device specifications to verify if RAID is supported.

RAID combines two or more physical drives into a single logical drive.

RAID enables you to distribute your data among multiple hard drives. RAID distributes data across drives in different ways, referred to as RAID *levels*. The level you select depends on your goal. Each level provides a different balance of reliability, availability, performance, and capacity.

You can configure most devices in many types of RAID arrays. To set up a RAID array, you must have multiple (at least two) drives that are the same size.

Note that RAID is not a replacement for backing up your logs. You should still back up your logs, even if you employ RAID.



Basic RAID has two types of operation: mirroring and striping.

With mirroring, instead of writing the files to a single hard drive, it writes them to another hard drive as well. This way you have a real-time copy of the data.

With striping, two or more drives are combined into a single logical drive. When data is stored on the logical drive, it gets split into pieces and distributed across all the physical drives in the array.

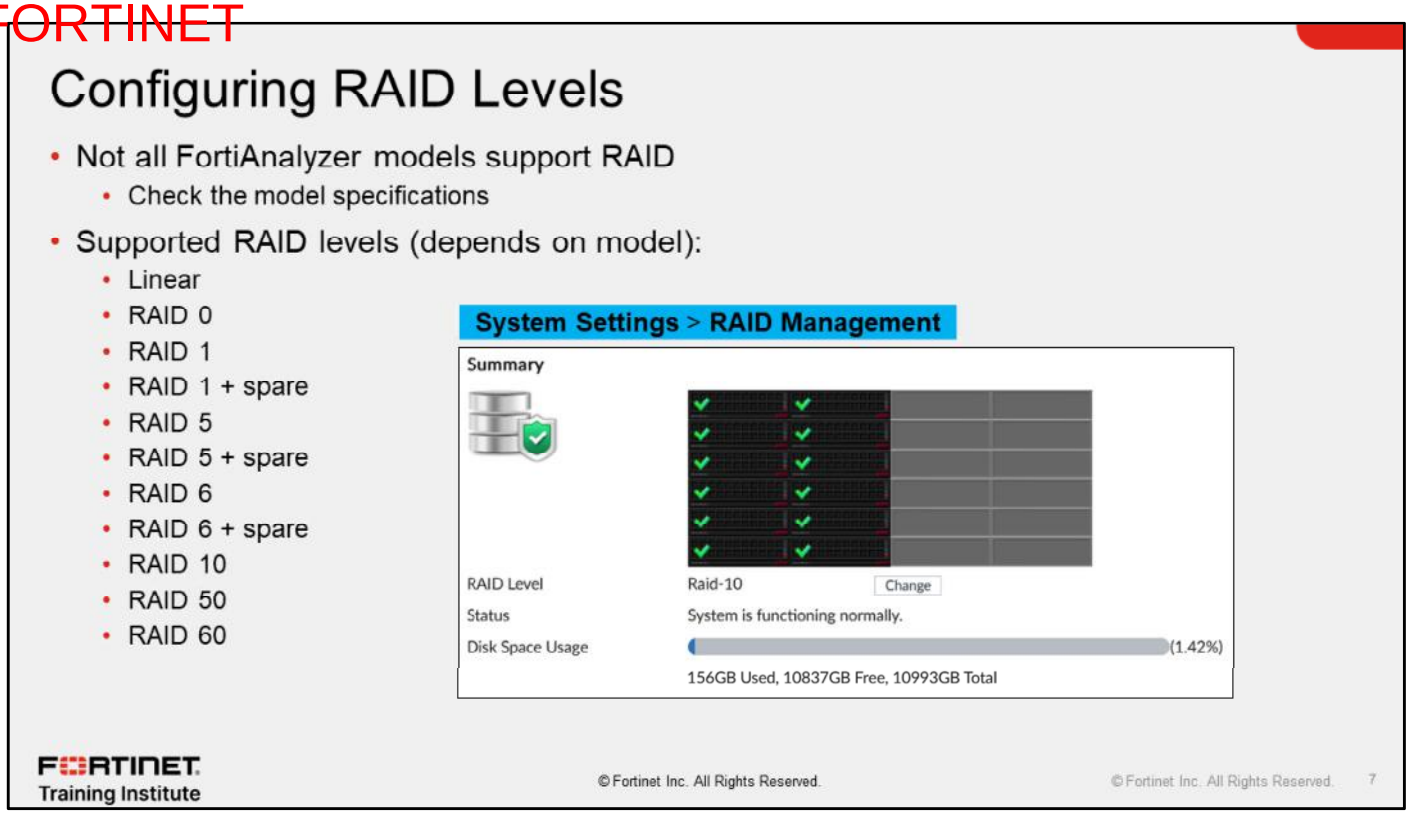
It is important to note that not all RAID levels operate the same way. Some do only mirroring, others do only striping, and some do both.

There are also versions that include distributed parity, which is a way to achieve data redundancy. With distributed parity, parity data is distributed among multiple drives and requires three or more disks (RAID 5 and above). Also, the number of drives that can fail depends on the RAID level. Regardless of the level, having too many failed drives results in the loss of data.

Depending on the device model, you can build hardware RAID and/or software RAID.

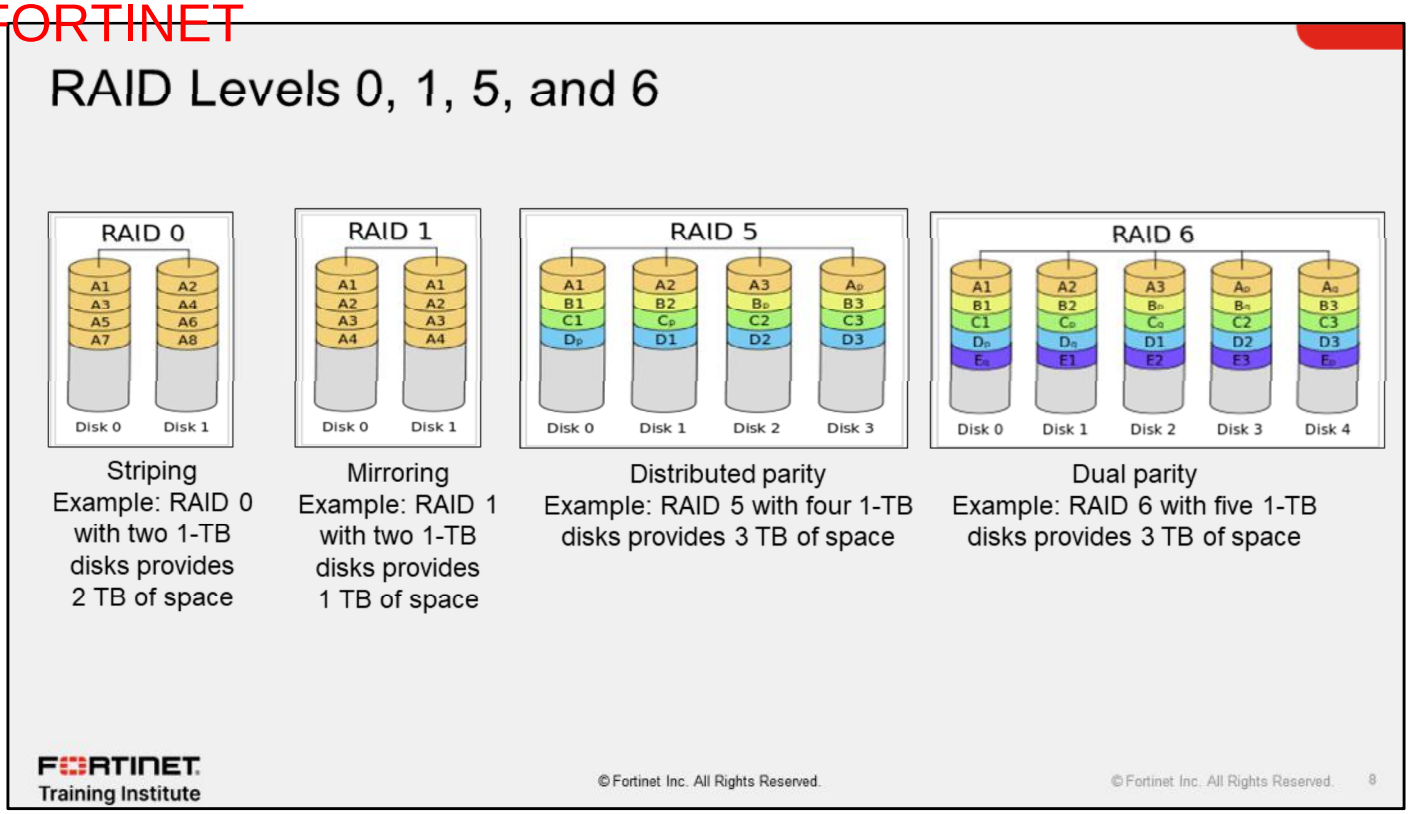
Hardware RAID is always recommended because a dedicated controller card handles all the RAID operations faster and more efficiently.

Software RAID means that the OS needs to handle all RAID operations on top of all its regular functions. This affects performance; therefore, it is not recommended unless it is the only option.



Not all FortiAnalyzer models support RAID, so the menu option to configure RAID may not appear on the GUI. Be sure to check the model specifications to see if RAID is supported, and to what level.

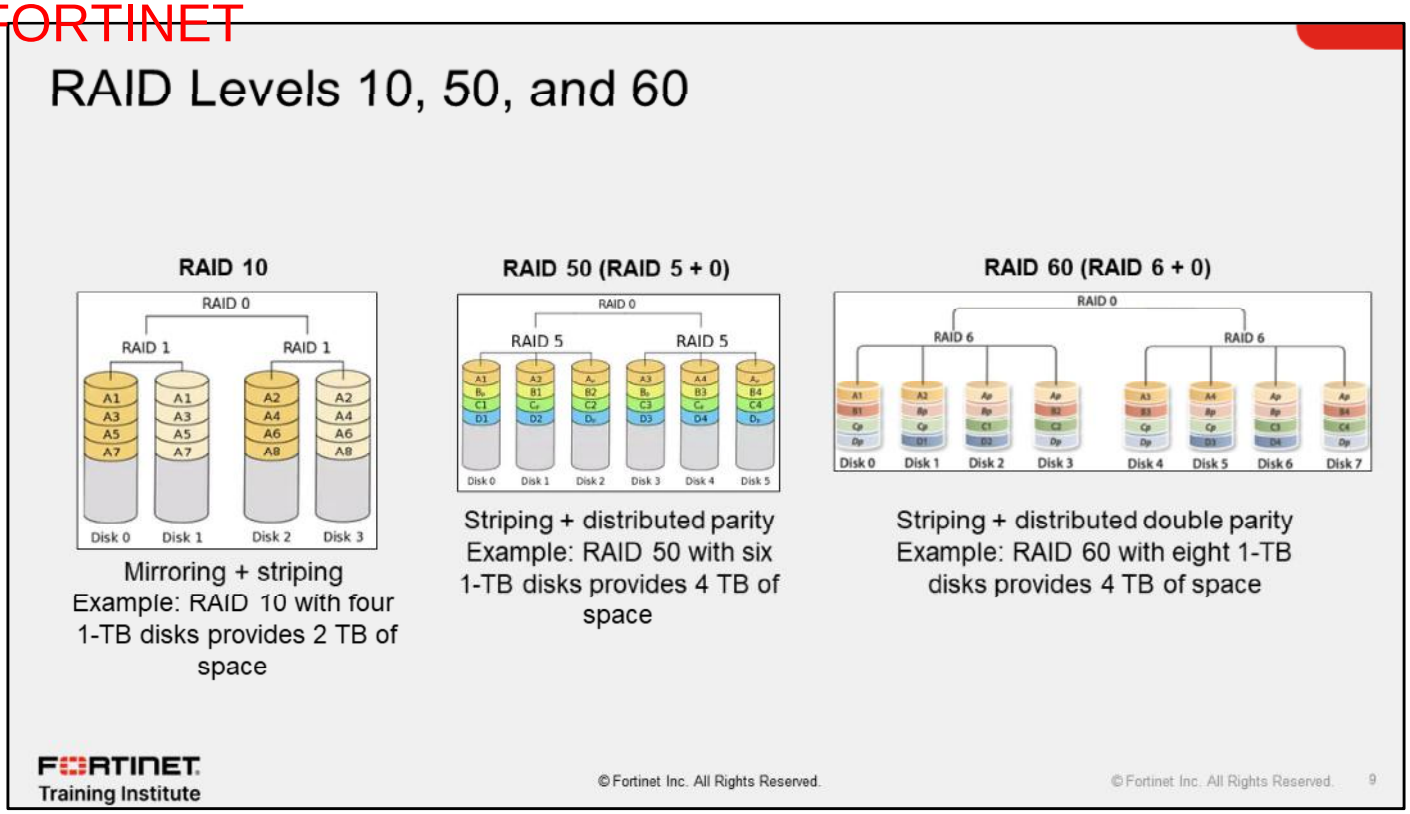
If RAID is supported, you can configure RAID on the **RAID Management** page. Supported levels include Linear, RAID 0, RAID 1, RAID 1 + spare, RAID 5, RAID 5 + spare, RAID 6, RAID 6 + spare, RAID 10, RAID 50, and RAID 60.



Some common RAID levels are: RAID 0 (striping), RAID 1 (mirroring) and its variants, RAID 5 (distributed parity), RAID 6 (double parity), RAID 50 (striping and distributed parity), and RAID 60 (striping and distributed double parity):

- RAID 0 consists of data split evenly across two or more disks. Speed and performance are the main goals, since the FortiAnalyzer device can distribute disk operations across multiple disks. However, there is no parity information or data redundancy. This means that there is no fault tolerance; if one disk fails, it affects the entire array and the data is lost.
- RAID 1 consists of an exact copy of a set of data on two (most common) or more disks. Read performance and reliability are the main goals. Write performance is not increased because data needs to be mirrored to all disks. RAID 1 includes fault tolerance, so if one disk fails the other one can keep working since it contains a complete copy of the data.
- RAID 5 consists of block-level striping with distributed parity. Data and parity are striped across three or more disks. This RAID level provides better performance than mirroring as well as fault tolerance. It can withstand the failure of a single drive, as subsequent reads can be calculated from the distributed parity, so that no data is lost.
- RAID 6 extends RAID 5 by adding another parity block. Accordingly, it consists of block-level striping with two parity blocks distributed across all member disks. It's more robust than RAID 5, as the system can remain operational even if two disks fail.

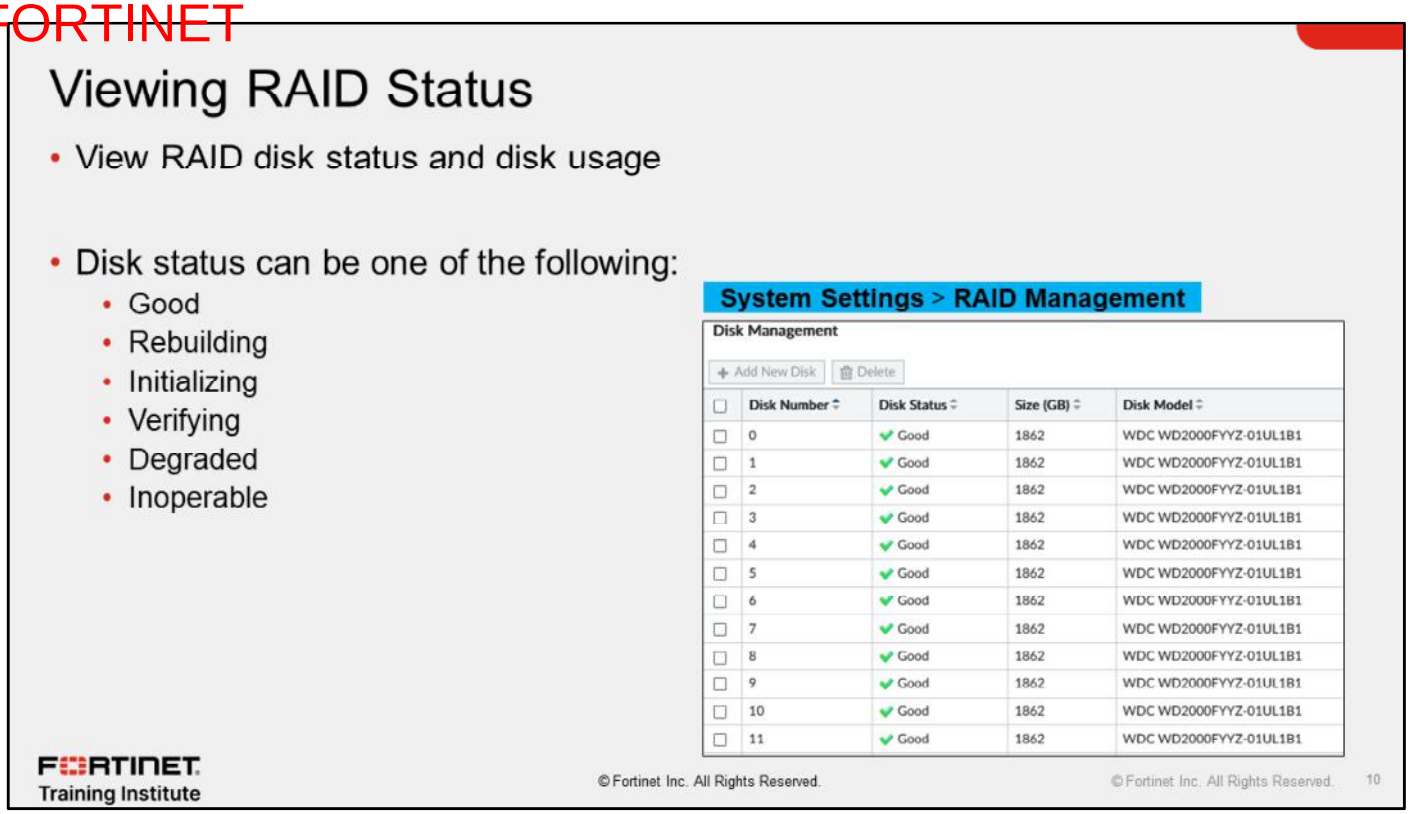
RAID Levels 10, 50, and 60



- RAID 10 combines the features of RAID 1 and RAID 0, making sure data is mirrored and spread across multiple disks. RAID 10 balances performance and data security. It's possible to recover data if two drives in a RAID 10 configuration fail, but it's dependent upon which two drives fail.
- RAID 50 combines block-level striping of RAID 0 with the distributed parity of RAID 5. Write performance is improved over RAID 5 and it provides better fault tolerance than a single RAID 5 level. With this level, one drive from each of the RAID 5 sets can fail.
- RAID 60 combines block-level striping of RAID 0 with the distributed double parity of RAID 6. Write performance is affected, but the enhanced redundancy provides peace of mind. Dual parity allows the failure of two disks in each RAID 6 array.

For more information about RAID levels, see the *FortiAnalyzer Administration Guide*.

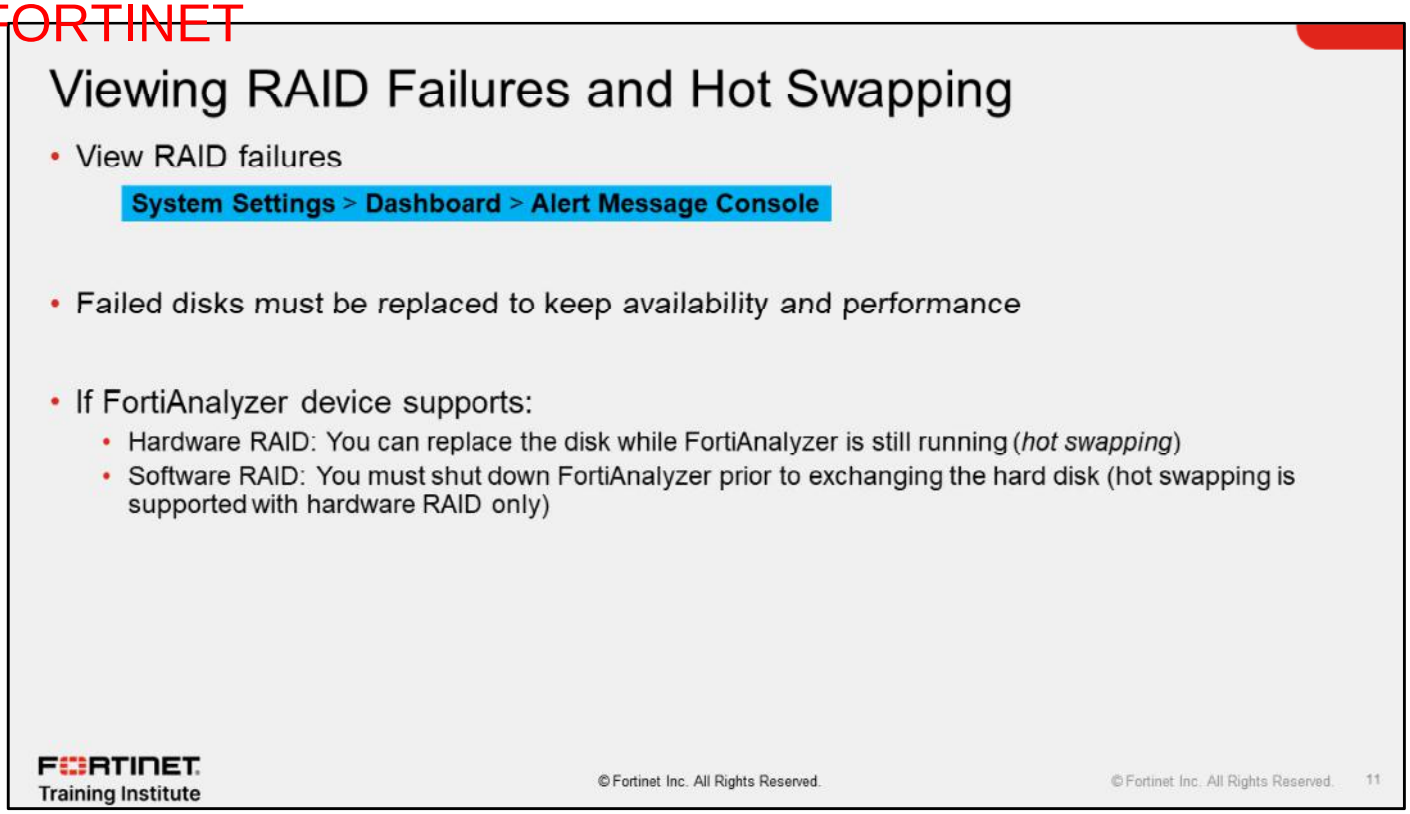
Source: Wikipedia, standard RAID levels, and nested RAID levels



On the **RAID Management** page, you can also view the status of each disk in the RAID array and disk space usage.

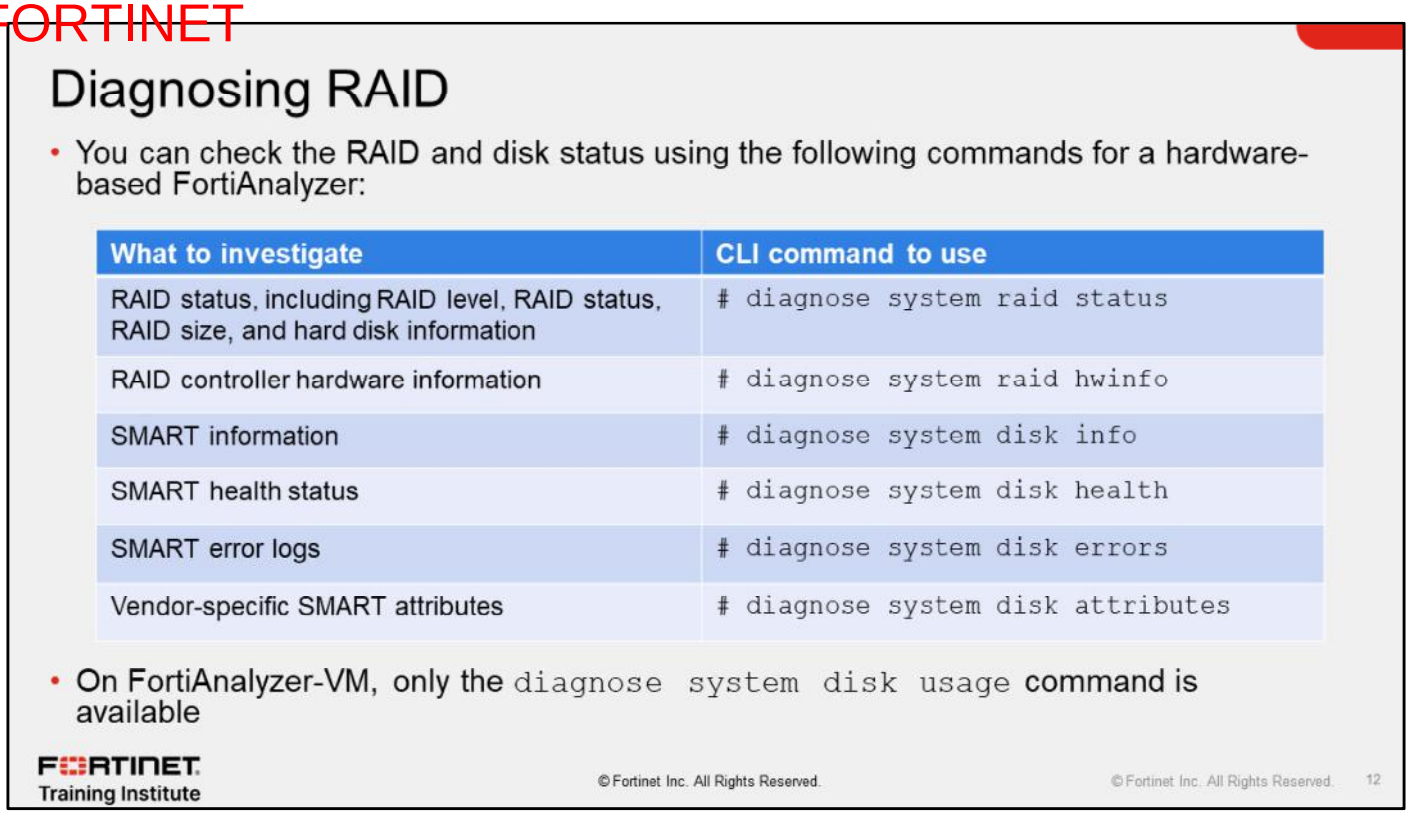
Disk status can be one of the following states:

- **Good**: The disk is functioning normally.
- **Rebuilding**: FortiAnalyzer is writing data to a newly added hard drive to restore logical drive to an optimal state. It is not fully fault tolerant until rebuilding is complete.
- **Initializing**: FortiAnalyzer is writing to all the hard drives in the device in order to make the array fault tolerant.
- **Verifying**: FortiAnalyzer is ensuring the parity data of a redundant drive is valid.
- **Degraded**: The hard drive is no longer being used by the RAID controller.
- **Inoperable**: One or more drives is missing—the drive is no longer available to the OS. Data in an inoperable state cannot be accessed.



You can view any RAID failures on the **Alert Message Console** widget on the dashboard. A log message appears in this widget if there are any failures.

If a hard disk on a FortiAnalyzer fails, you must replace it. On FortiAnalyzer models that support *hardware* RAID, you can replace the disk while FortiAnalyzer is still running. This is known as *hot swapping*. Fortinet supports hot swapping on hardware RAID only. On FortiAnalyzer devices with *software* RAID you must shut down FortiAnalyzer before exchanging the hard disk.



Use the CLI command `diagnose system raid status` to view the health of the RAID array, as well as the health of the individual disks.

Use the command `diagnose system raid hwinfo` to view detailed information about the hardware for the individual disks on FortiAnalyzer.

On FortiAnalyzer-VM, only the `diagnose system disk usage` command is available.

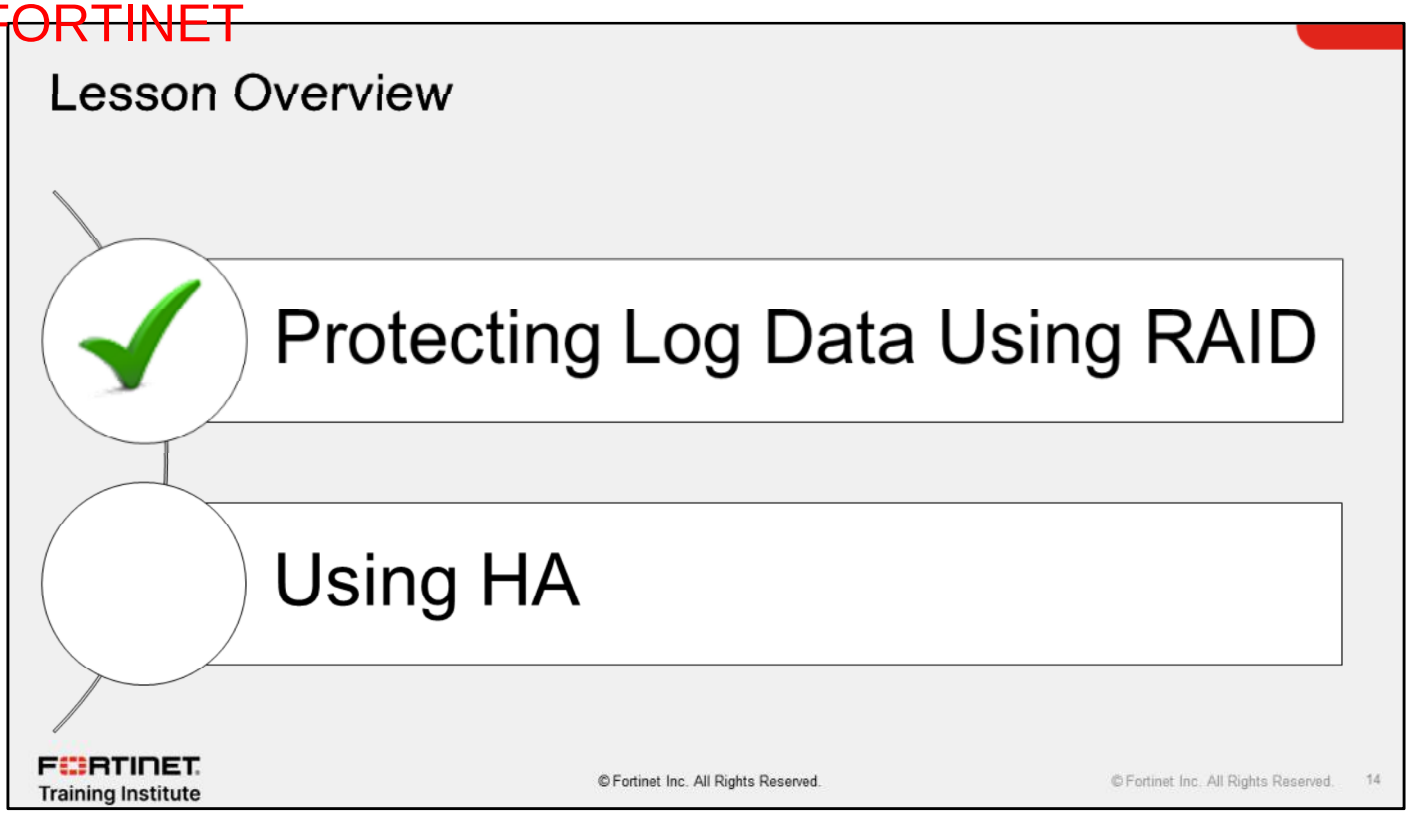
Knowledge Check

1. The RAID 10 level comprises what data format?
   A. Dual parity
   ✓B. Mirroring and striping

2. What must you do if a hard disk on a FortiAnalyzer that supports software RAID fails?
   A. Hot swap the disk.
   ✓B. Shut down FortiAnalyzer and replace the disk.

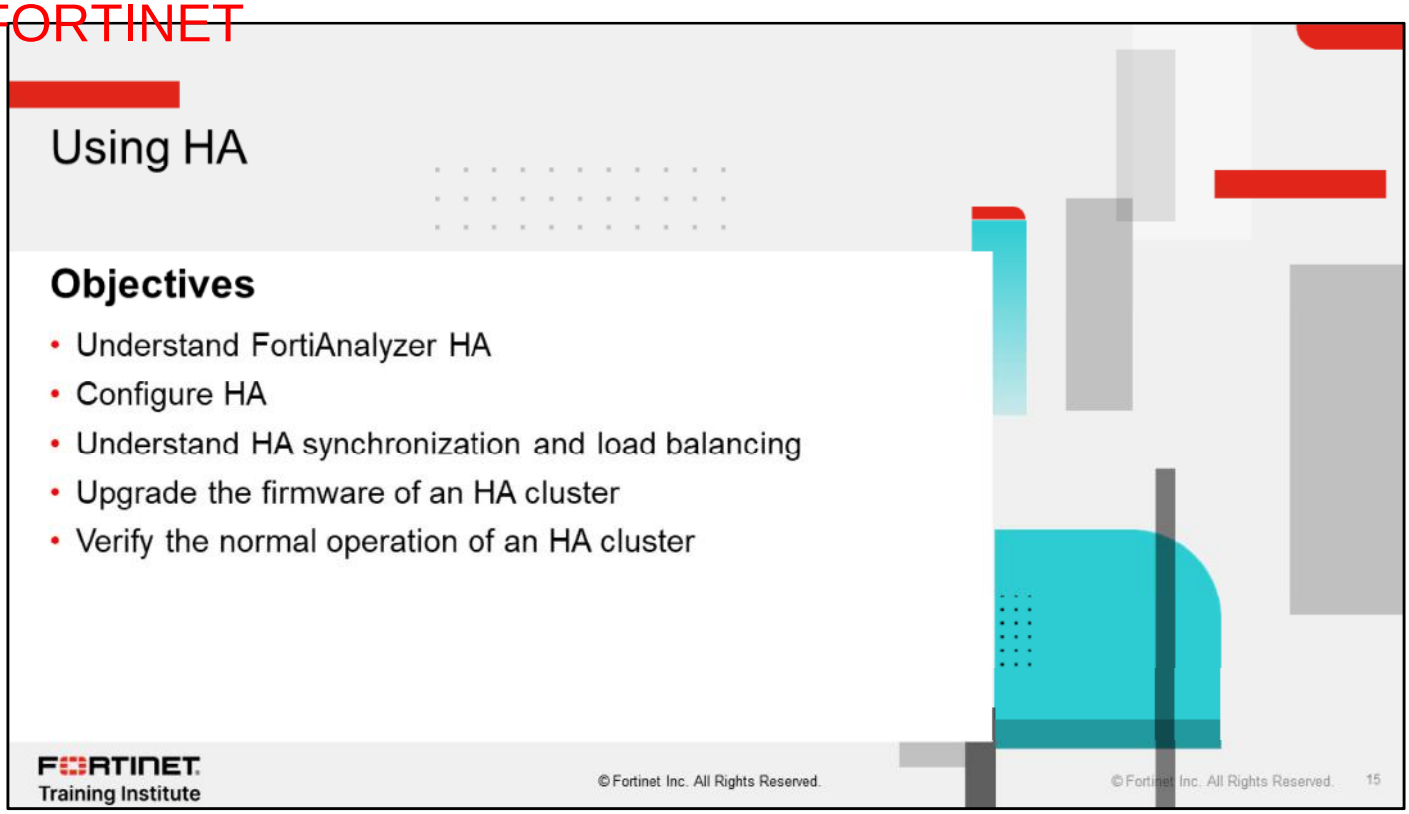
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13



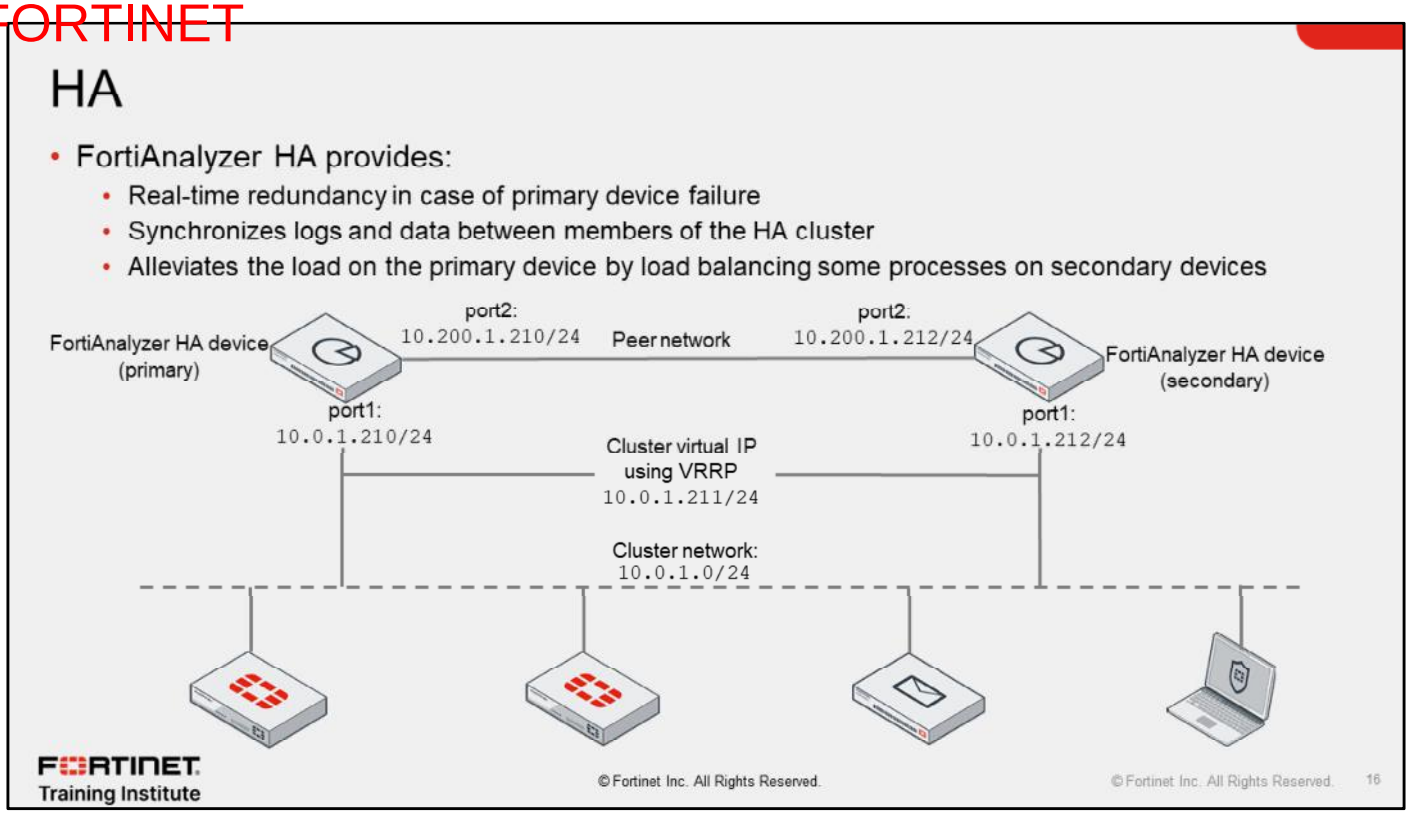
Good job! You now know how to use RAID to protect the log data.

Now, you will learn about using HA.



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

By demonstrating competence in the configuration and troubleshooting of HA, you will be able to increase the availability of your FortiAnalyzer implementation.



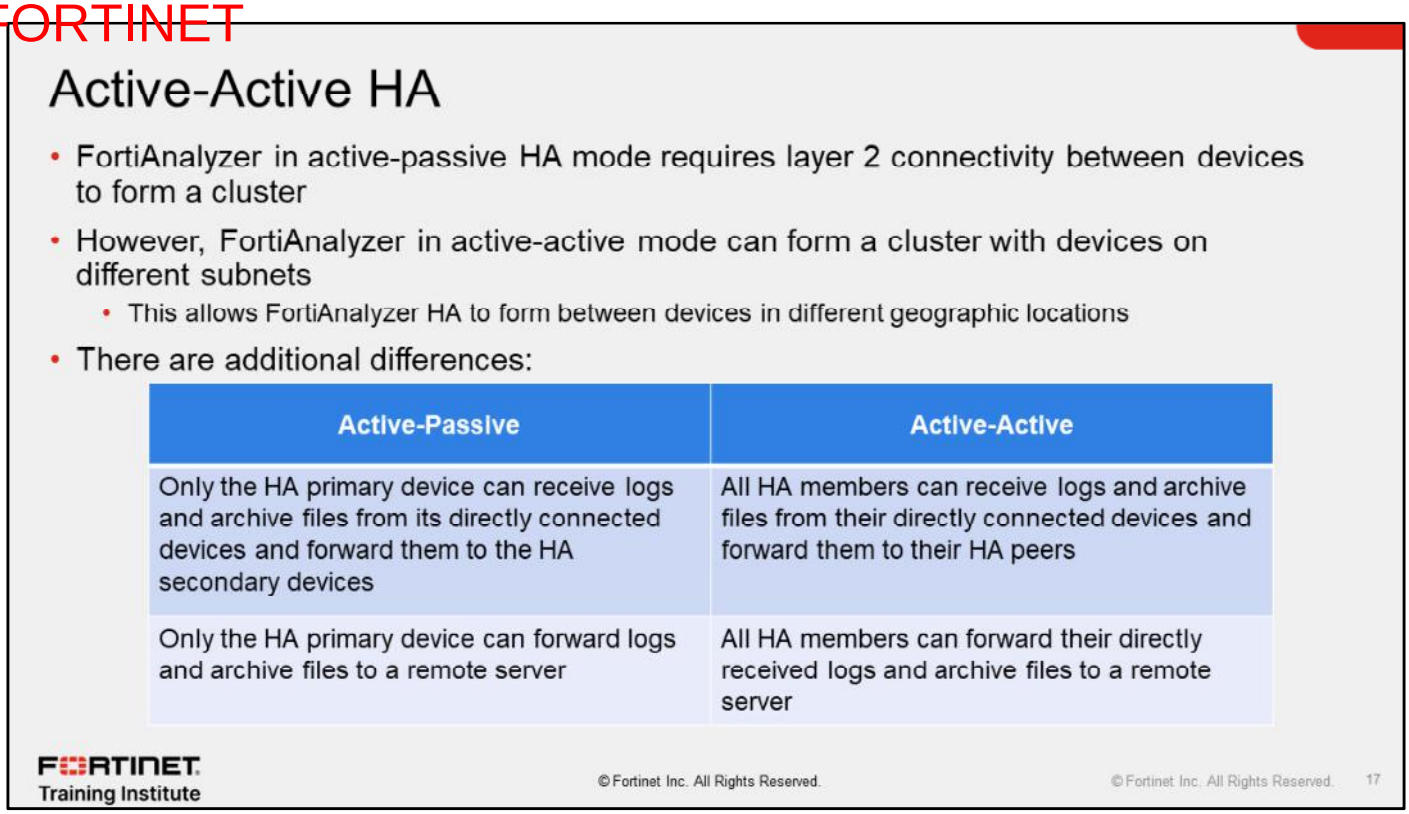
A FortiAnalyzer HA cluster provides the following:

- Applies real-time redundancy when the FortiAnalyzer primary device fails. If the primary device fails, another device in the cluster is selected as the primary device.
- Synchronizes logs and data securely among multiple FortiAnalyzer devices. System and configuration settings applicable to HA are also synchronized.
- Alleviates the load on the primary device by using secondary devices for processes, such as running reports and sharing load for FortiView widgets.

A FortiAnalyzer HA cluster can have a maximum of four devices: one primary device with up to three secondary devices. All devices in the cluster must be from the same FortiAnalyzer series, use the same firmware, and be visible to each other on the network. All devices must run in the same operation mode: analyzer or collector.

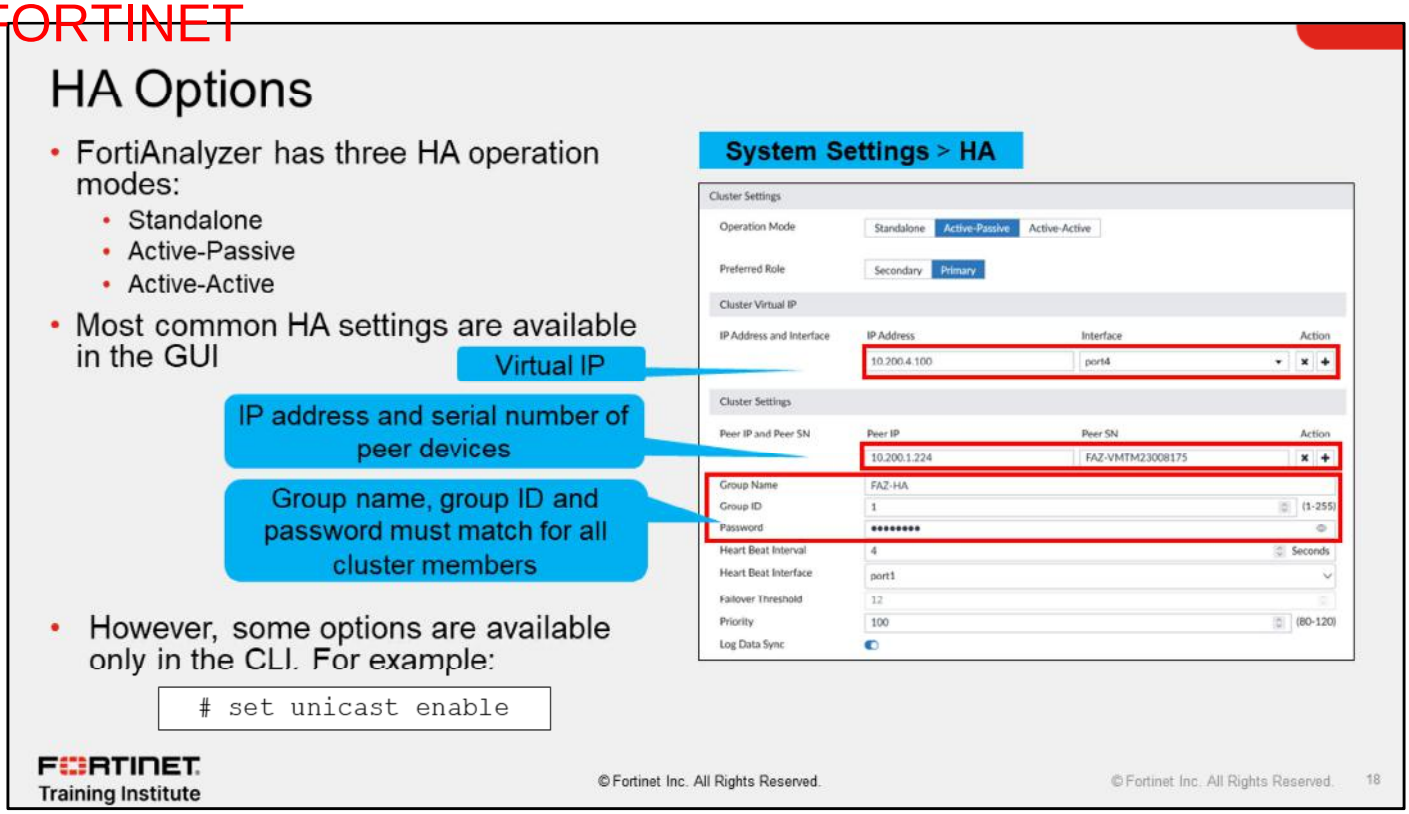
Although the available disk space doesn't need to match, it is important to ensure all cluster members have enough storage for the expected logs. It's recommended that all members have the same available storage.

When using FortiAnalyzer VMs as cluster members, all VMs must be running on the same platform. For example, a VM running on VMware can't form a cluster with a VM running on KVM. When FortiAnalyzer devices with different licenses are used to create an HA cluster, the license that allows for the smallest number of managed devices is used.



FortiAnalyzer HA in active-passive mode requires a layer 2 connection between HA members in order to set up the HA cluster virtual IP. 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.



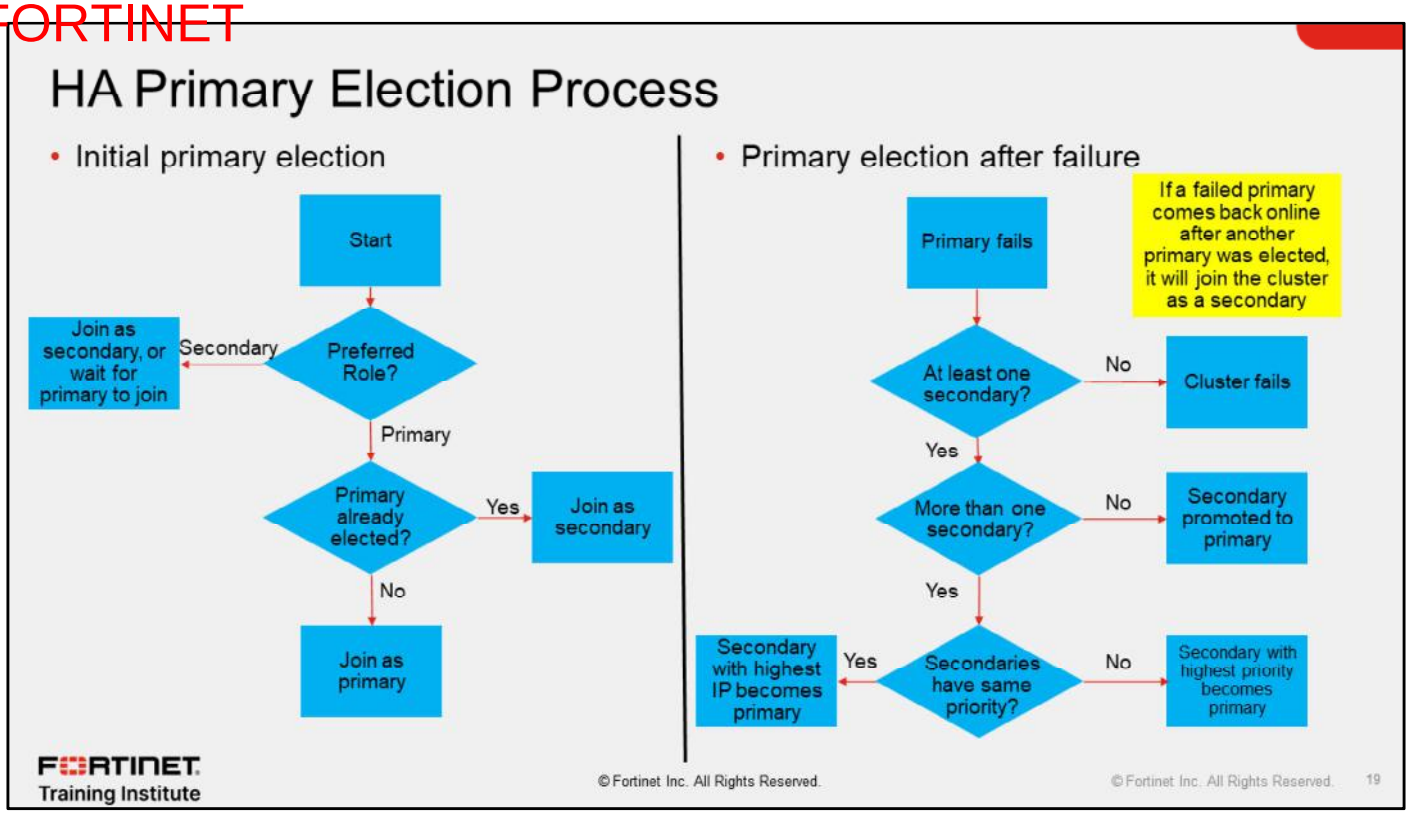
In **System Settings** > **HA**, use the **Cluster Settings** section to create or change the HA configuration. To configure a cluster, set the **Operation Mode** of the primary device to **High Availability**, and then select the preferred role for the device when it joins the HA cluster.

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

Once the cluster is up, the devices sending their logs must point to this IP. By default, the 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, you add the IP addresses and serial numbers of each secondary device to the primary device peer list. The IP address and serial number of the primary device and all secondary devices must be added to each secondary device. Cluster members need to be reachable at these IP addresses for the log synchronization traffic. As shown on this slide and the previous one, these IP addresses don't have to be on the same subnet as the cluster virtual IP. On the contrary, it is recommended they are 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.

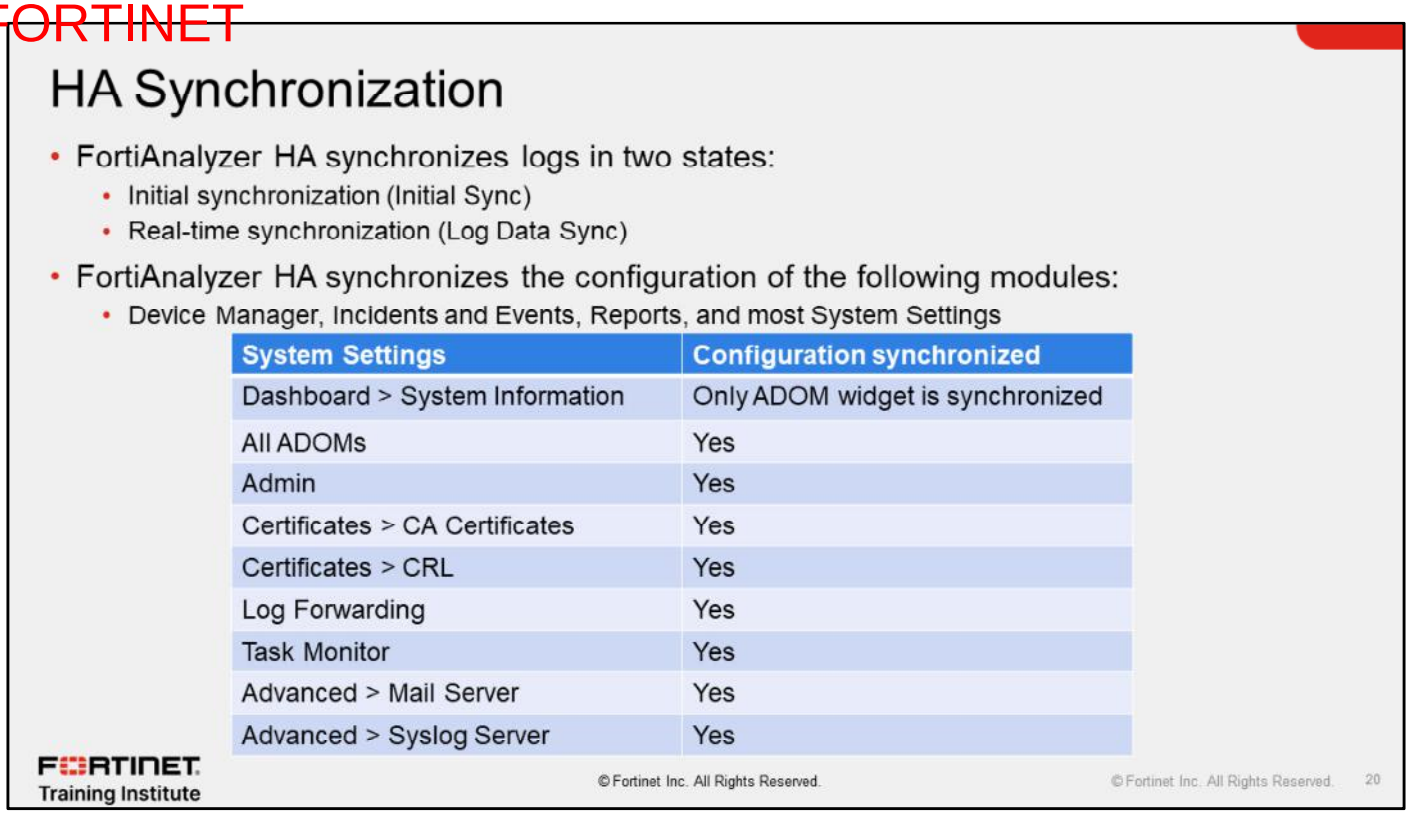


The initial selection of the primary device is based on the preferred rode configured. If the preferred role is **Primary**, then this device becomes the primary device if it is configured first in a new HA cluster. If there is an existing primary device, then this device becomes a secondary device. The default role is **Secondary**, so that the device can synchronize with the primary device. A secondary device cannot become a primary device until it is synchronized with the current primary device.

In the case of a primary device failure, FortiAnalyzer HA uses the following rules to select a new primary:

- All cluster devices are assigned a priority from 80 to 120. The default priority is 100. If the primary device becomes unavailable, the device with the highest priority is selected as the new primary device. For example, a device with a priority of 110 is selected over a device with a priority of 100.
- If multiple devices have the same priority, the device whose primary IP address has the greatest value is selected as the new primary device. For example, `123.45.67.124` is selected over `123.45.67.123`.
- If a new device with a higher priority or a greater value IP address joins the cluster, the new device does not replace (or pre-empt) the current primary device automatically.

By default, the only parameter checked to trigger an automatic failover is the network reachability among the cluster members. You can optionally configure HA to check the status of the Postgres database process to initiate a failover if that process stops working. This is done from the CLI with the command `set healthcheck DB`, under the `system ha` configuration mode.



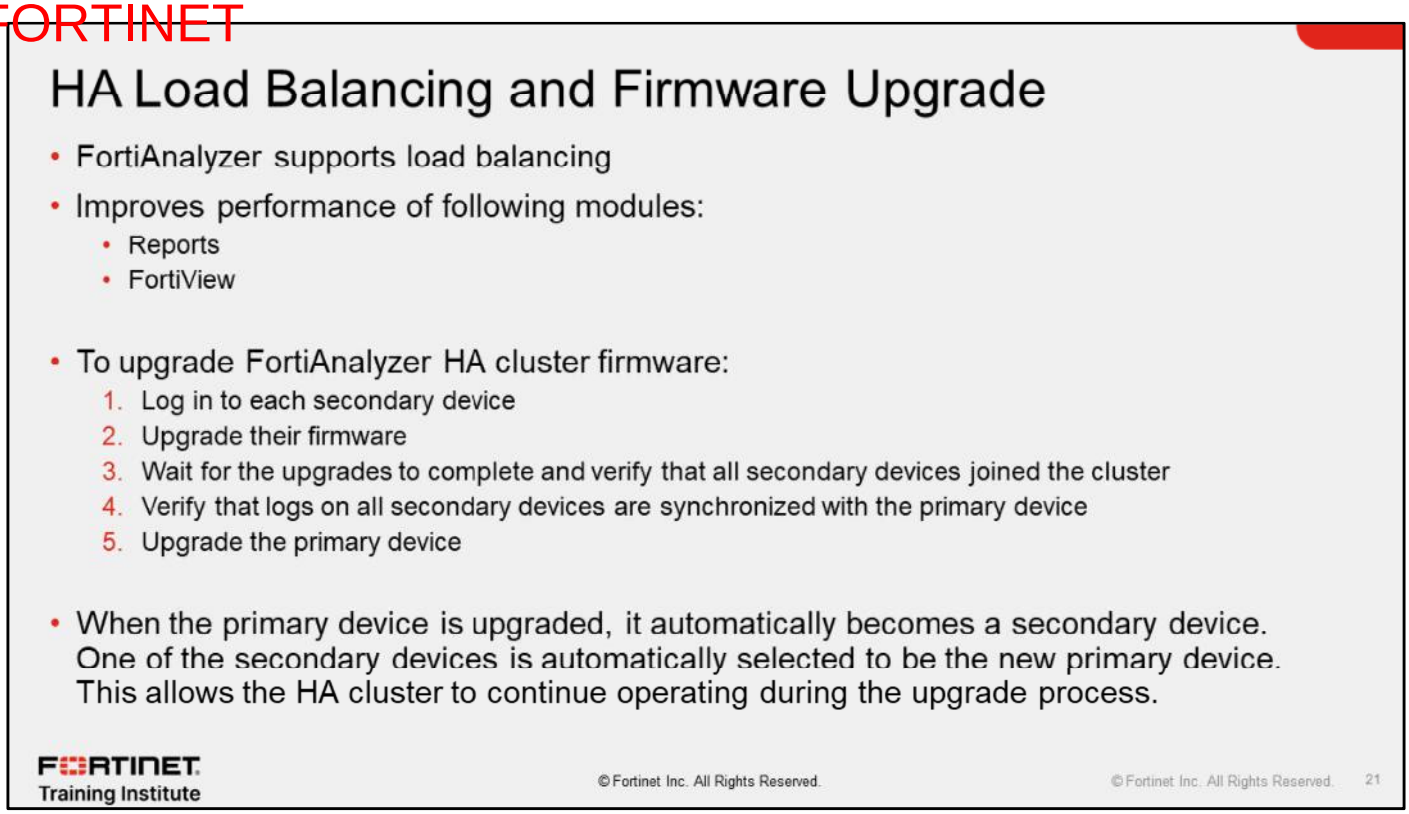
To ensure logs are synchronized among all HA devices, FortiAnalyzer HA synchronizes logs in two states: initial synchronization and real-time synchronization.

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

Real-time synchronization: After the initial log synchronization, the HA cluster goes into the real-time log synchronization state. **Log Data Sync** is enabled by default for all devices in the HA cluster. When **Log Data Sync** is enabled in the primary device, the primary device forwards logs in real time to all secondary devices. This ensures that the logs in the primary and secondary devices are synchronized. If the primary device fails, the secondary device selected to be the new primary device continues to synchronize logs with secondary devices. If you want to use a FortiAnalyzer device as a standby device (not as a secondary), then you don't need real-time log synchronization, so you 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 cluster devices:
- 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.



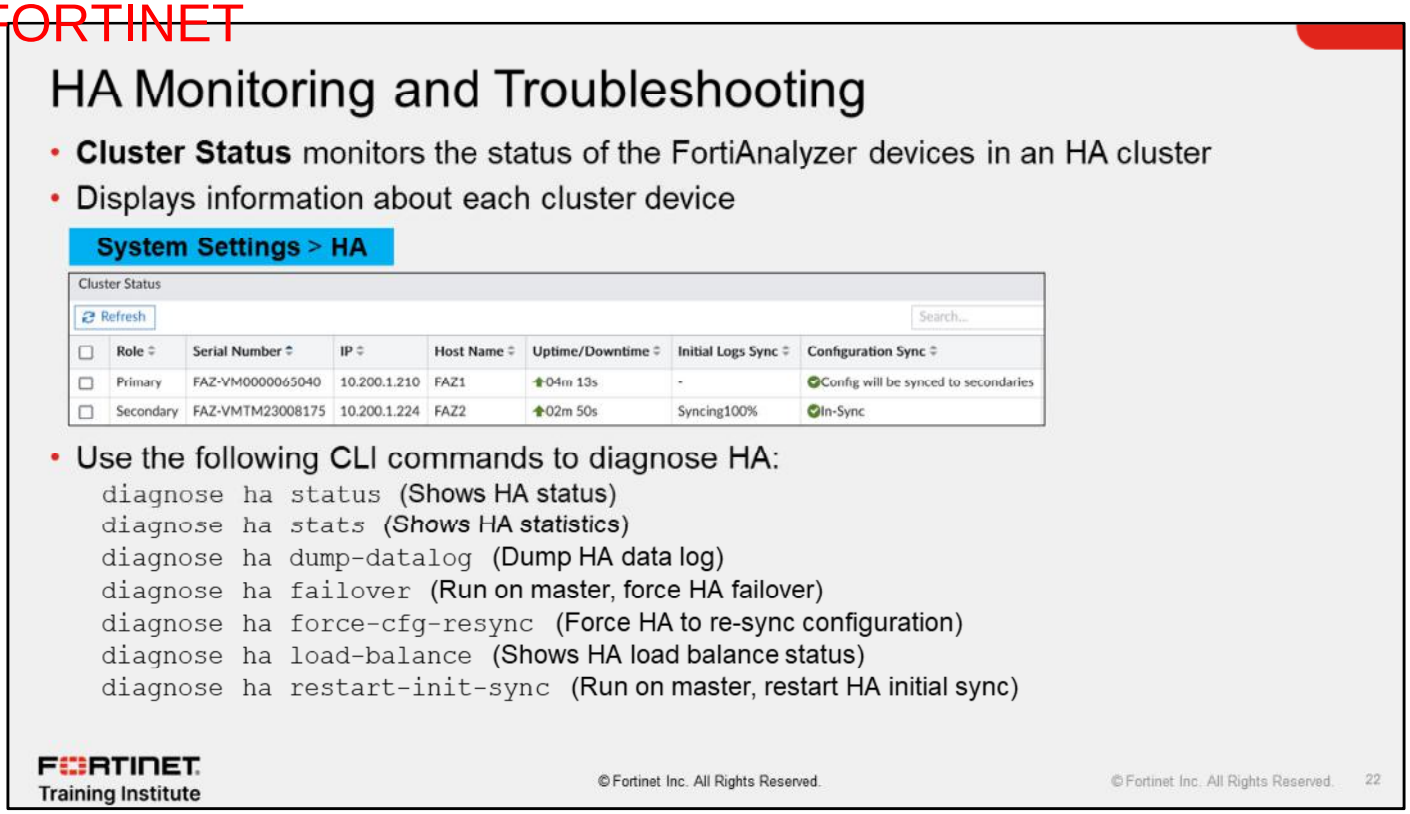
The FortiAnalyzer HA cluster can also balance the load and improve overall performance. Load balancing enhances the following modules:

- 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.

Like upgrading the firmware of a standalone FortiAnalyzer device, normal FortiAnalyzer operations may cause temporary interruptions while the cluster firmware upgrades. Because of these interruptions, you should upgrade the cluster firmware during a maintenance period. The steps to upgrade HA cluster firmware are shown on this slide.

Note that you might not be able to connect to the FortiAnalyzer GUI until the upgrade synchronization process is complete. During the upgrade, using SSH or Telnet to connect to the CLI might be slow. If necessary, use the console to connect to the CLI.



The **Cluster Status** pane monitors the status of FortiAnalyzer devices in an HA cluster. This pane 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.

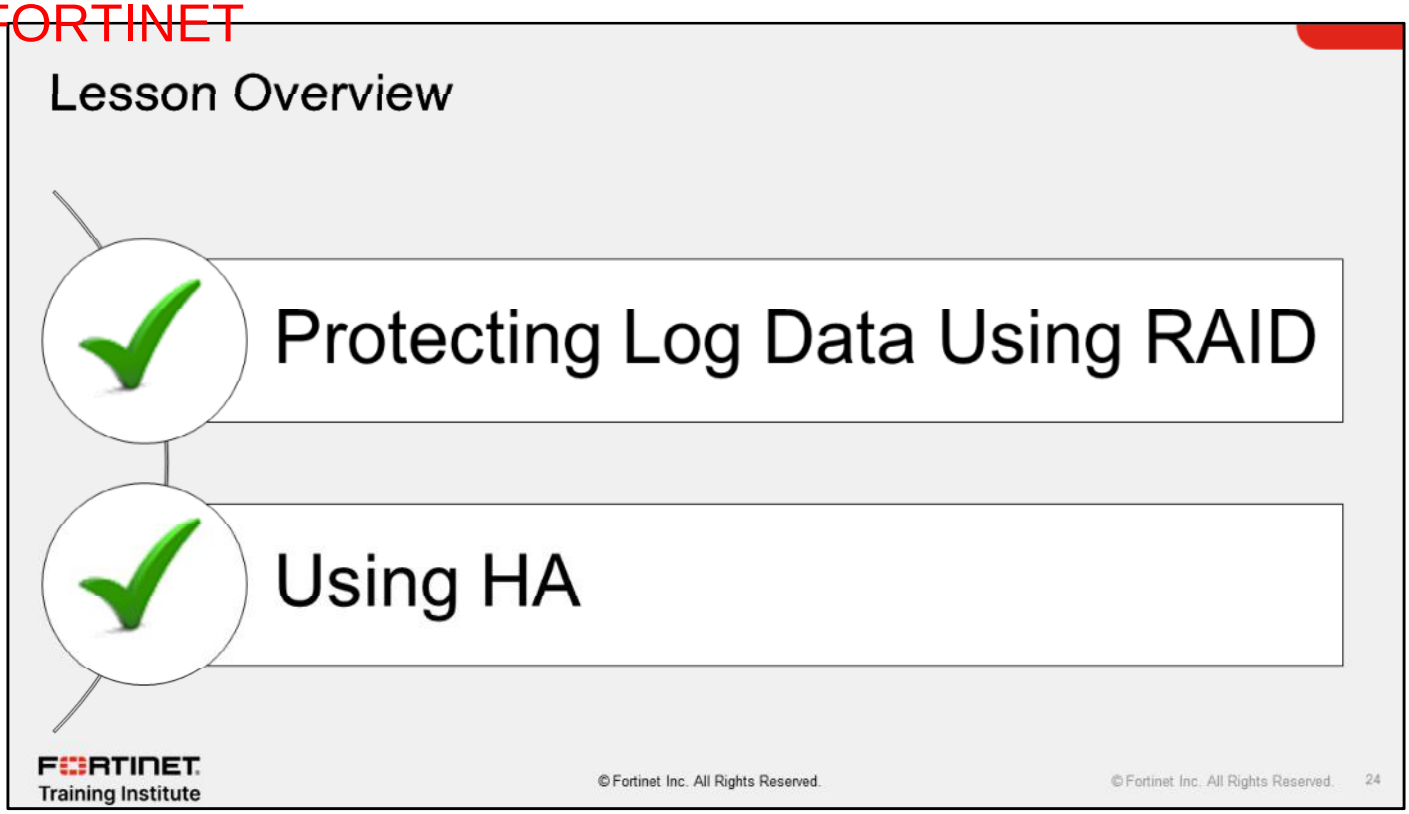
Knowledge Check

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

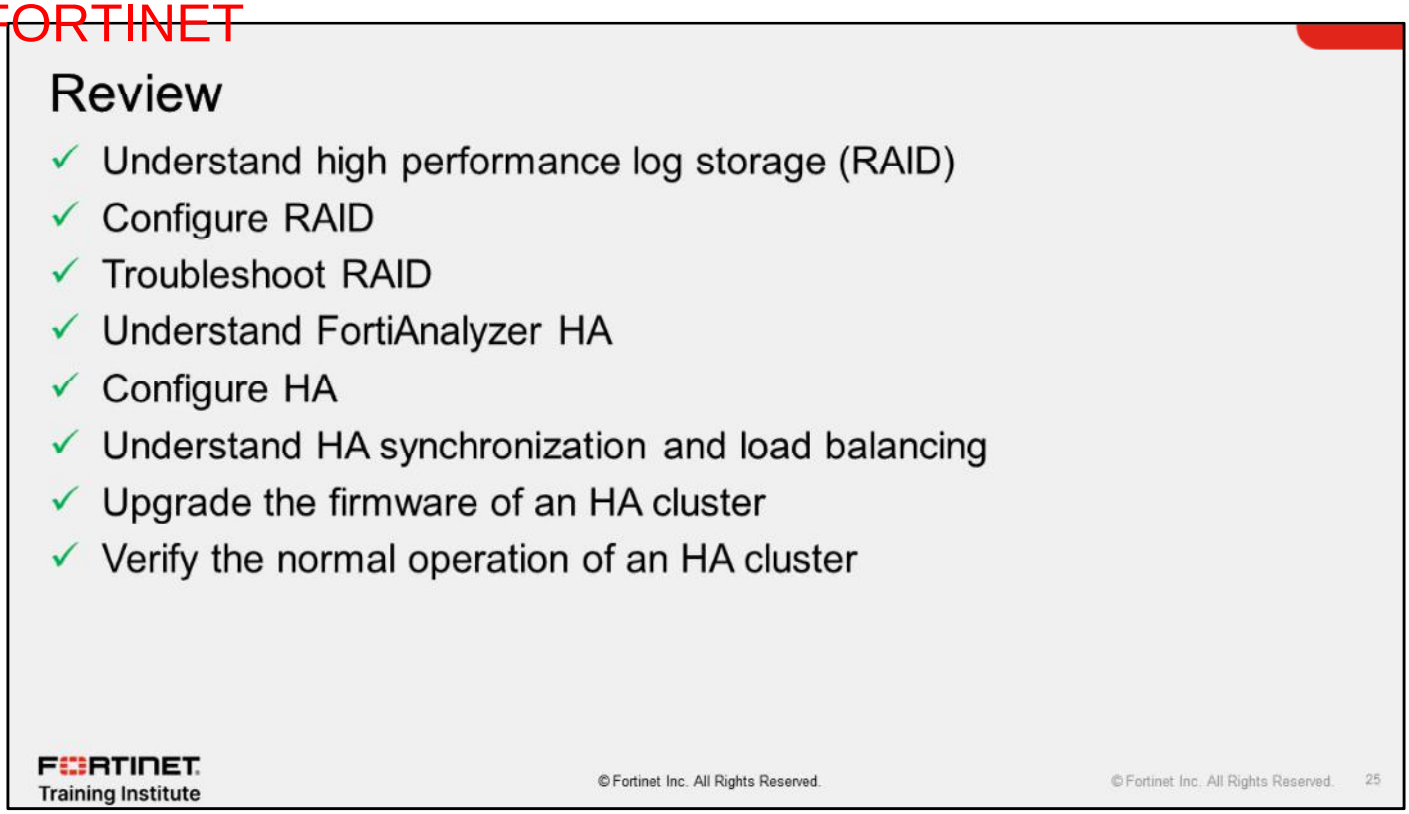
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23



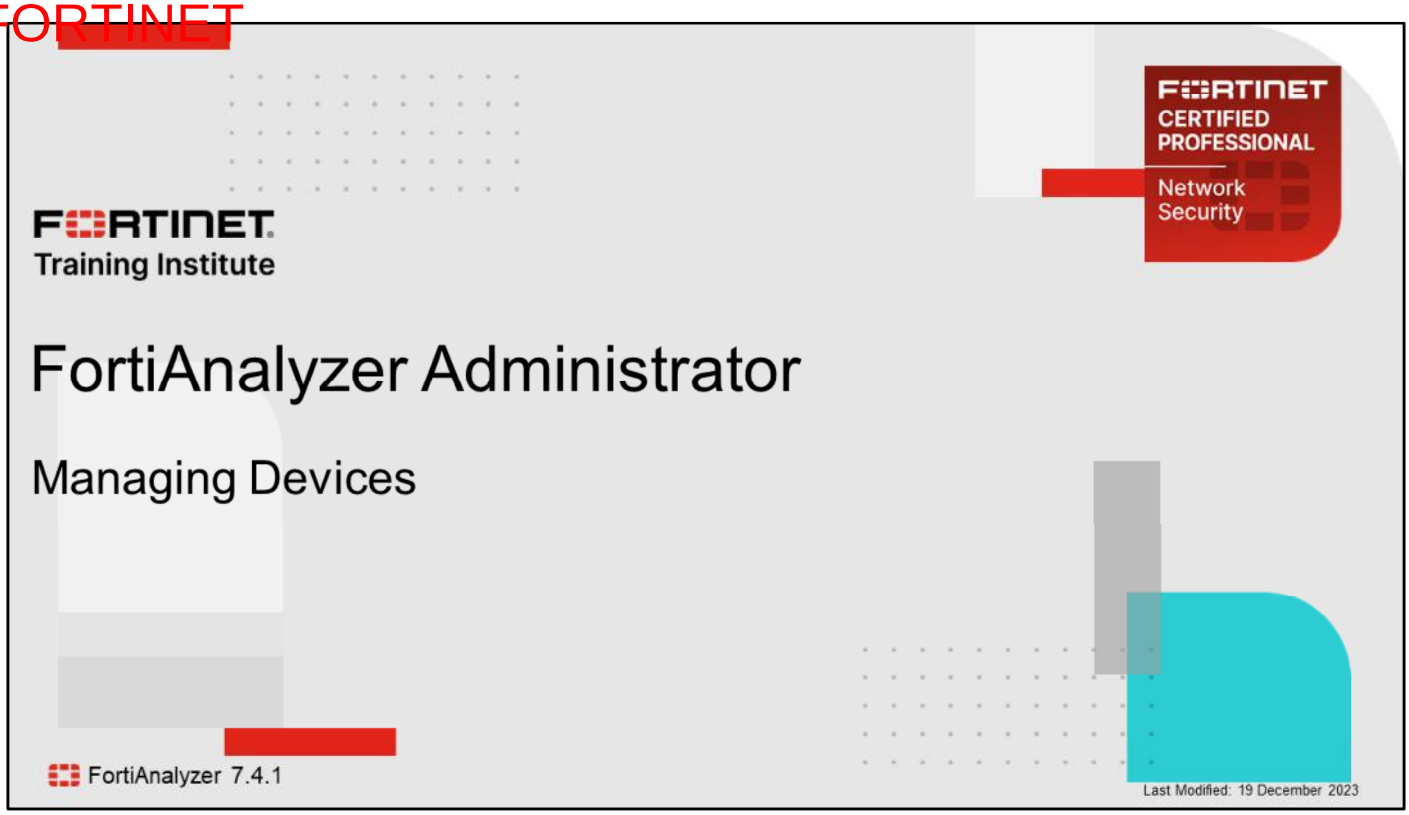
Congratulations! You have completed this lesson.

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

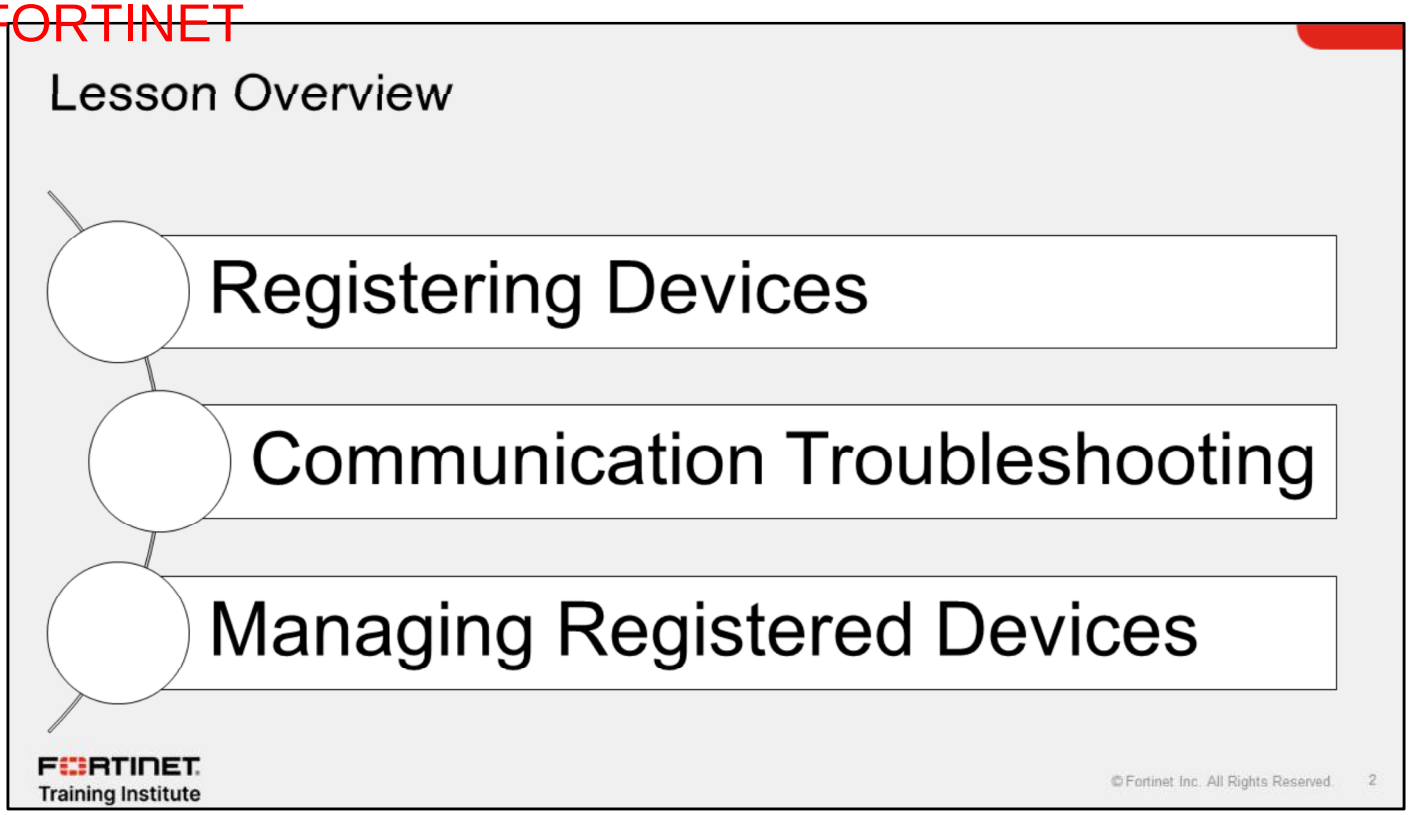


This slide show the objectives that you covered in this lesson.

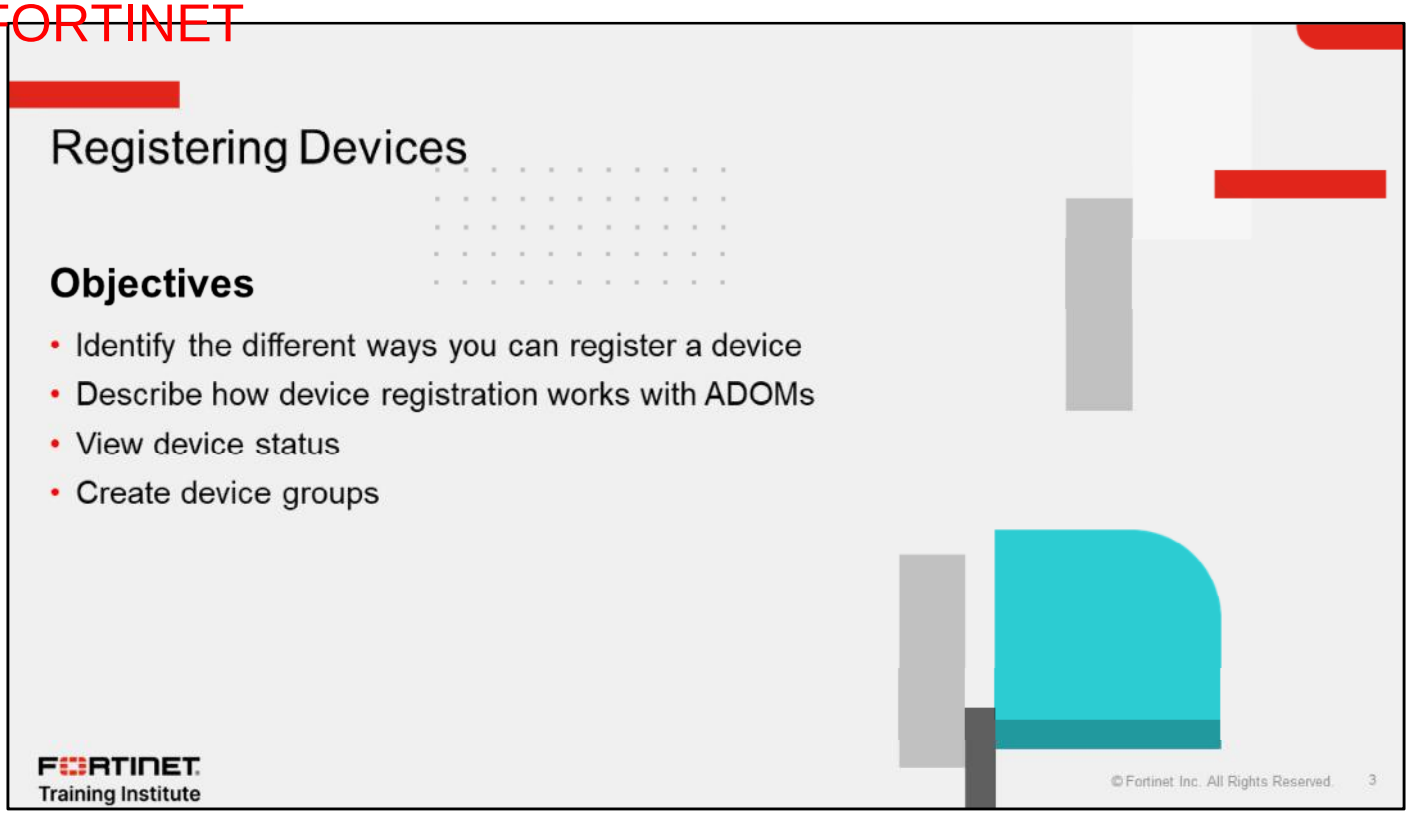
You learned how to use RAID and HA to make your FortiAnalyzer device more resilient against hardware failures.



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.

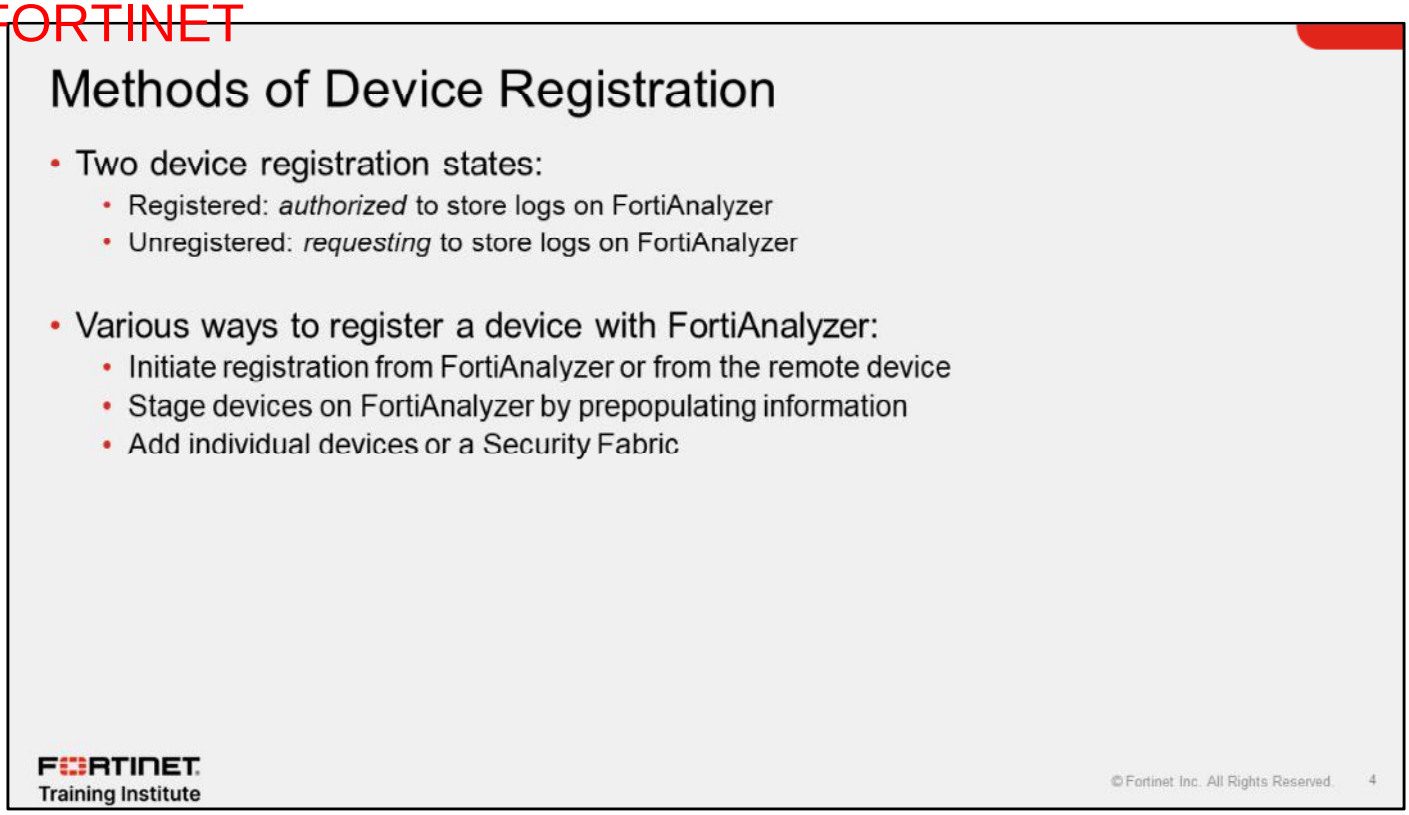


In this lesson, you will explore the topics shown on this slide.



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.

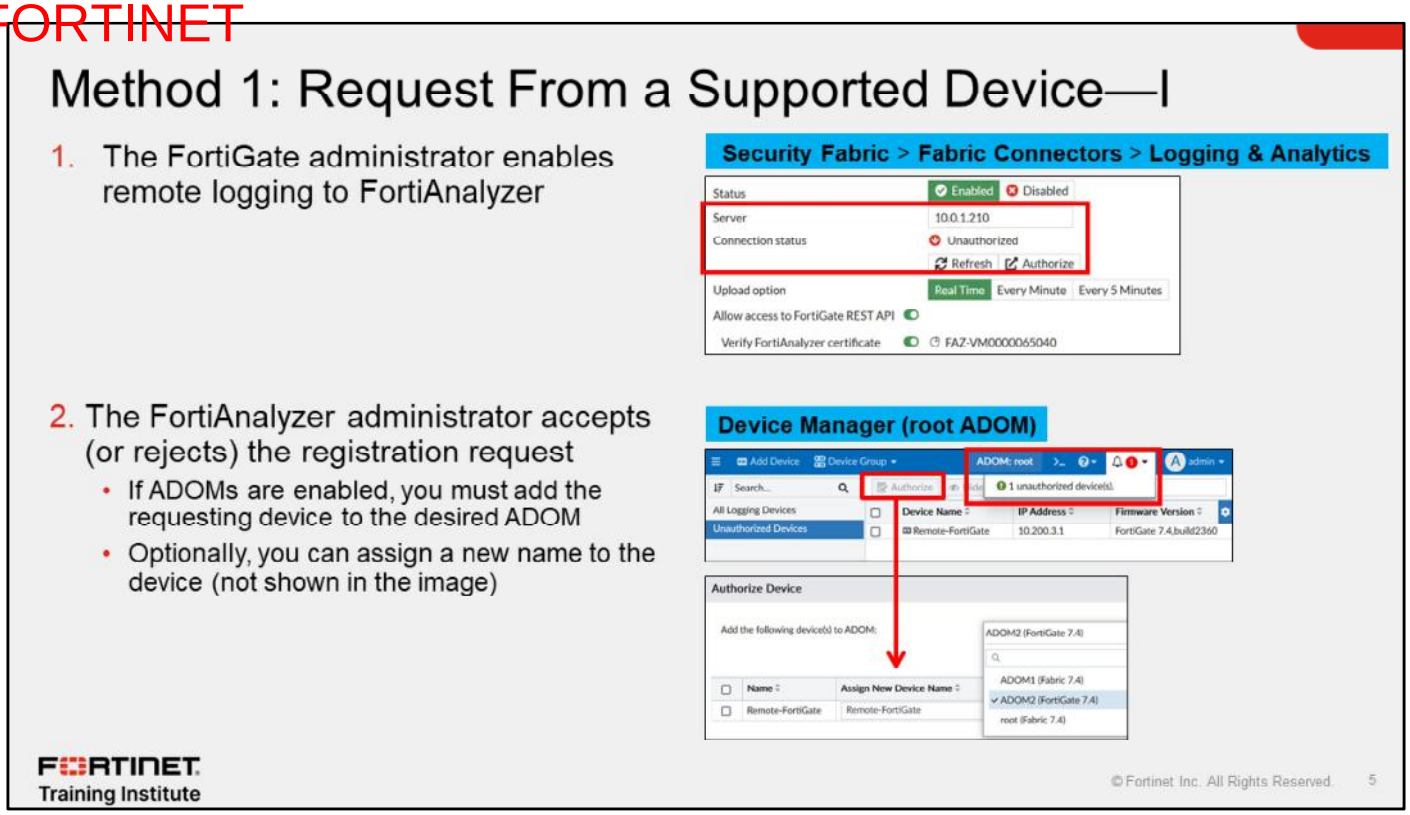
A registered device is one that has been *authorized* to store logs on FortiAnalyzer, whereas an unregistered device is one that is *requesting* to store logs on FortiAnalyzer.

There are various ways you can register a device with FortiAnalyzer.

A supported device can send a registration request. When the FortiAnalyzer administrator receives that request, the request can be accepted or denied.

You can also add devices on FortiAnalyzer using the **Add Device** wizard. The device can be added based on its serial number or a pre-shared key. If the device is supported, and all the details of the device are correct, the device is registered.

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.

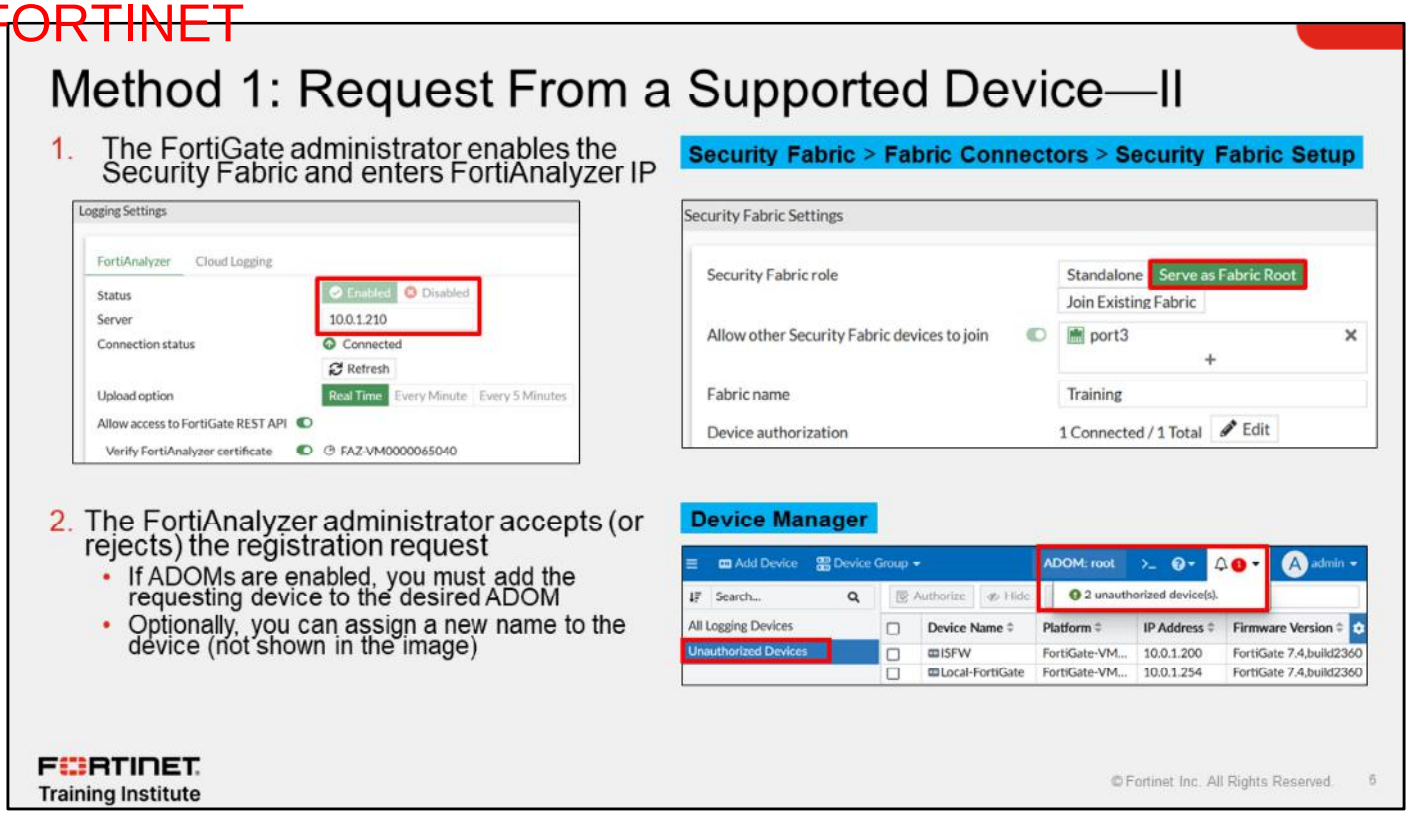
In the first method, FortiGate requests registration on FortiAnalyzer by enabling FortiAnalyzer logging and entering its IP.

After you click **Apply**, and if the request reaches the FortiAnalyzer successfully, you receive a message asking you to confirm the serial number of the FortiAnalyzer device if **Verify FortiAnalyzer certificate** is enabled.

Note that if you click **Test Connectivity**, you will see the connection status as **Unauthorized**. 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 request is made by the supported device, 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.

During acceptance of the registration request, if ADOMs are enabled, you have the option of keeping FortiGate in the root ADOM, or adding it to any custom FortiGate ADOMs you may have configured, as illustrated on this slide.



Another method involves creating a Security Fabric. By enabling the Security Fabric on FortiGate, FortiAnalyzer logging is enabled by default. After configuring the FortiAnalyzer IP on the root FortiGate, all the fabric member devices receive the configuration for FortiAnalyzer, and they will all request to register. If **Verify FortiAnalyzer certificate** is enabled, you will need to confirm the FortiAnalyzer serial number on the root FortiGate.

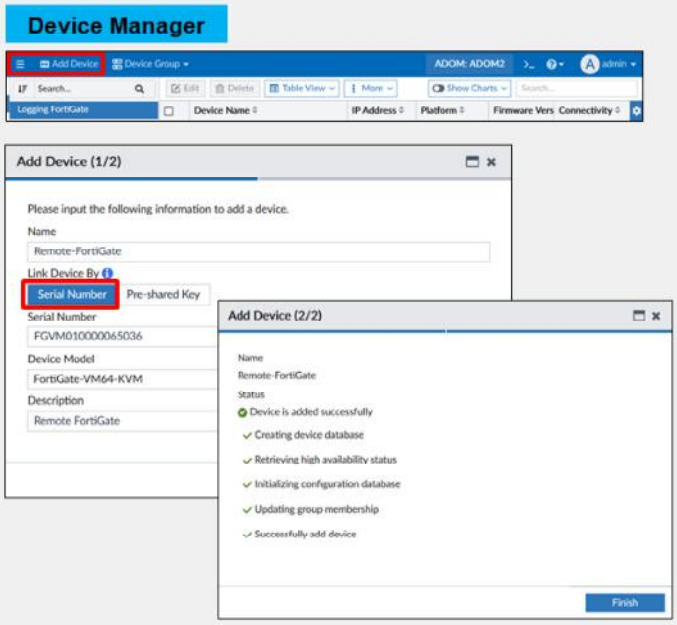
While the registration requests of the fabric members are sent together, the FortiAnalyzer administrator must still review and authorize them individually. It is recommended to add all the FortiGate devices connected through the Security Fabric under one ADOM. However, it is possible to separate the FortiGate devices and assign them to different ADOMs.

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

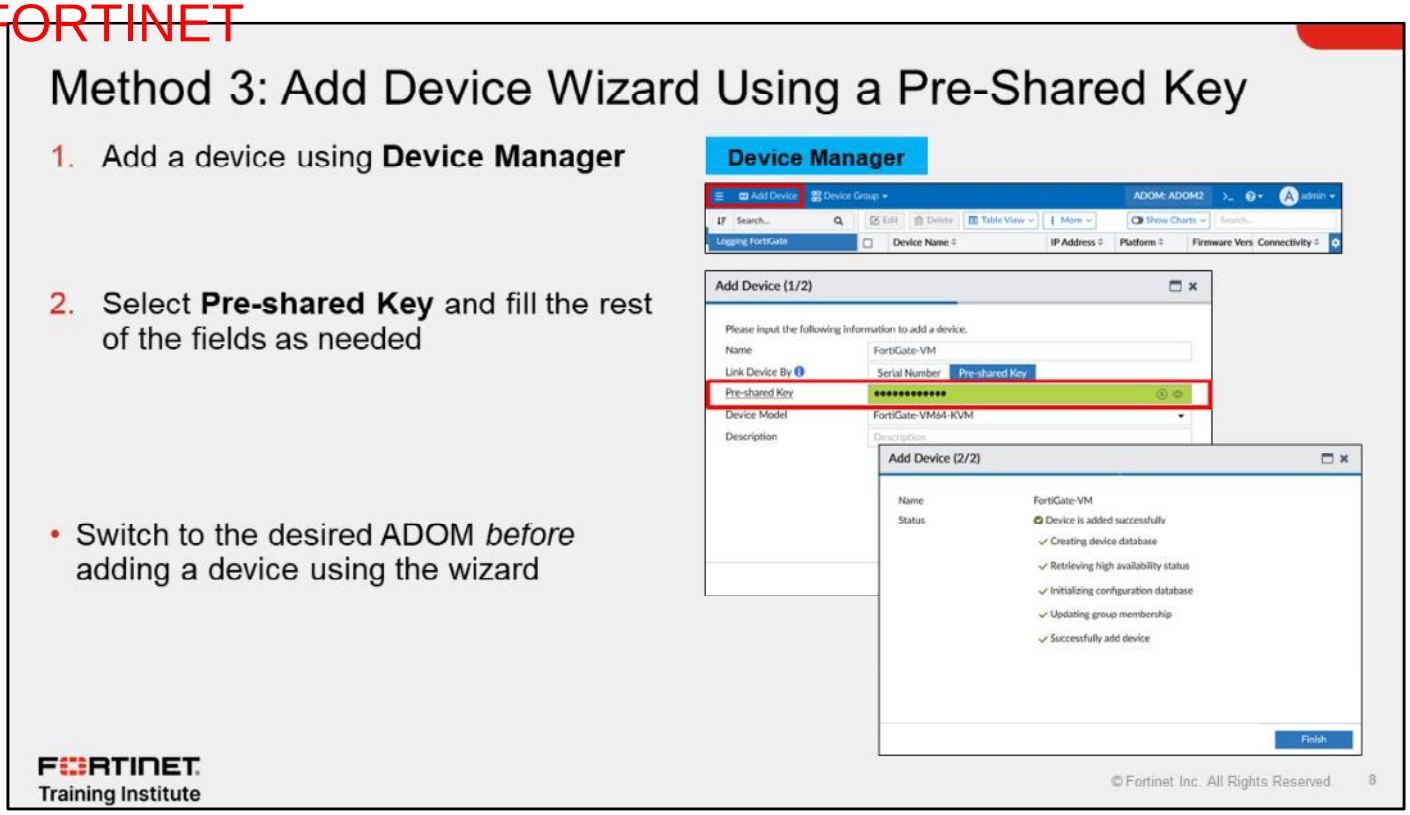


FORTINET Training Institute

 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 that is to be registered. If the device information is verified, the status reads "Device is added successfully", and 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 fill in the other details about the device that is to be registered, such as the device model. If the device information is verified, the status reads “Device is added successfully”, and the device appears under **Device Manager**.

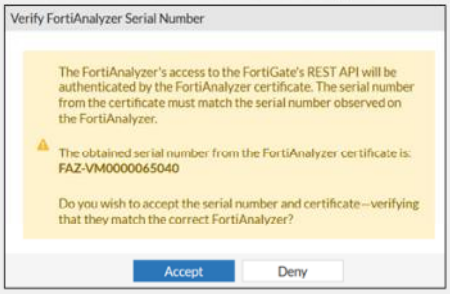
If ADOMs are enabled, the device is automatically registered to its device-specific ADOM. However, if you have already created a custom ADOM and want to add the device directly to that ADOM instead, switch to the ADOM *before* adding a device using the wizard.

Method 3: Add Device Wizard Using a Pre-Shared Key II

3. 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
```

4. Authorize FortiAnalyzer on FortiGate

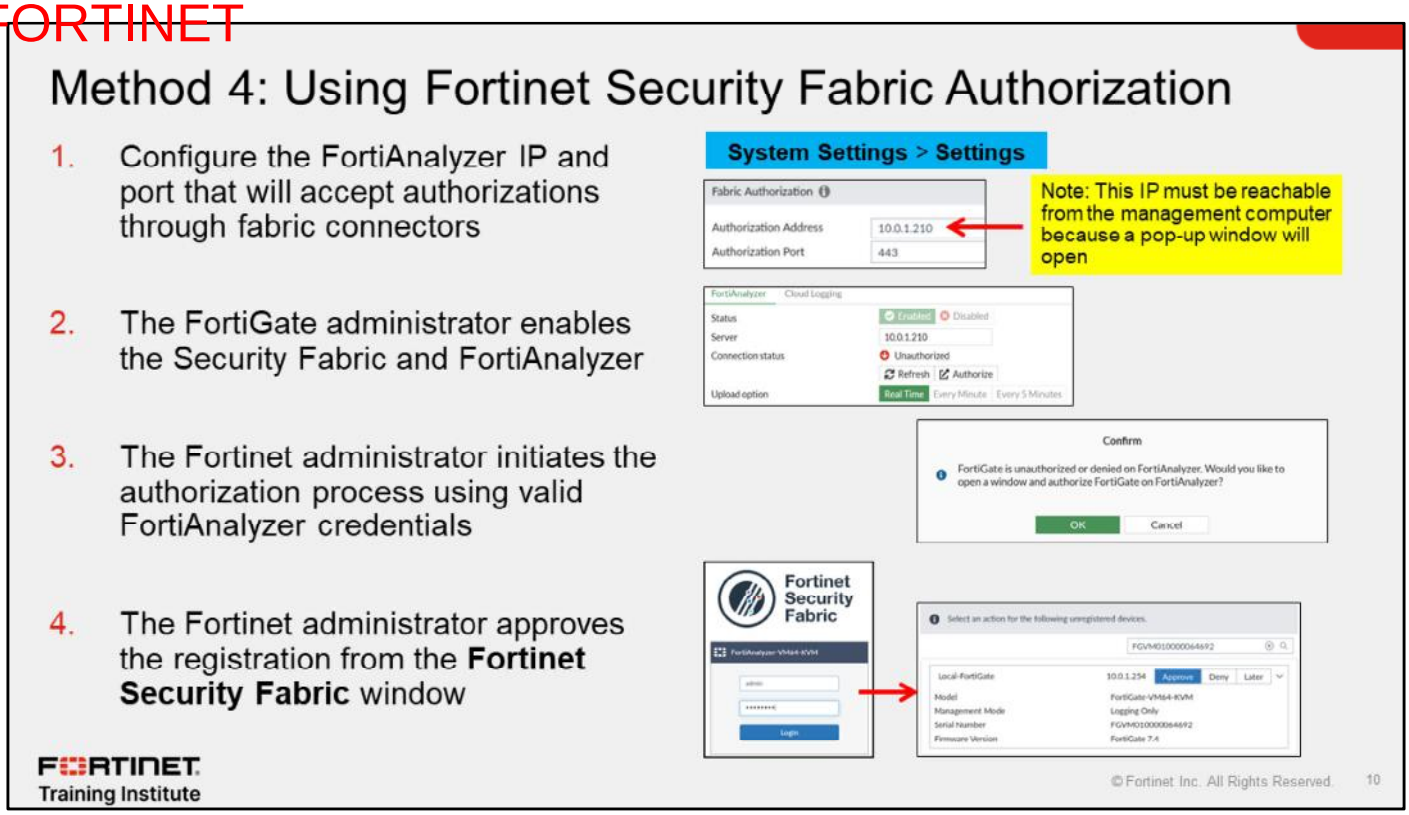


FORTINET Training Institute

 9

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

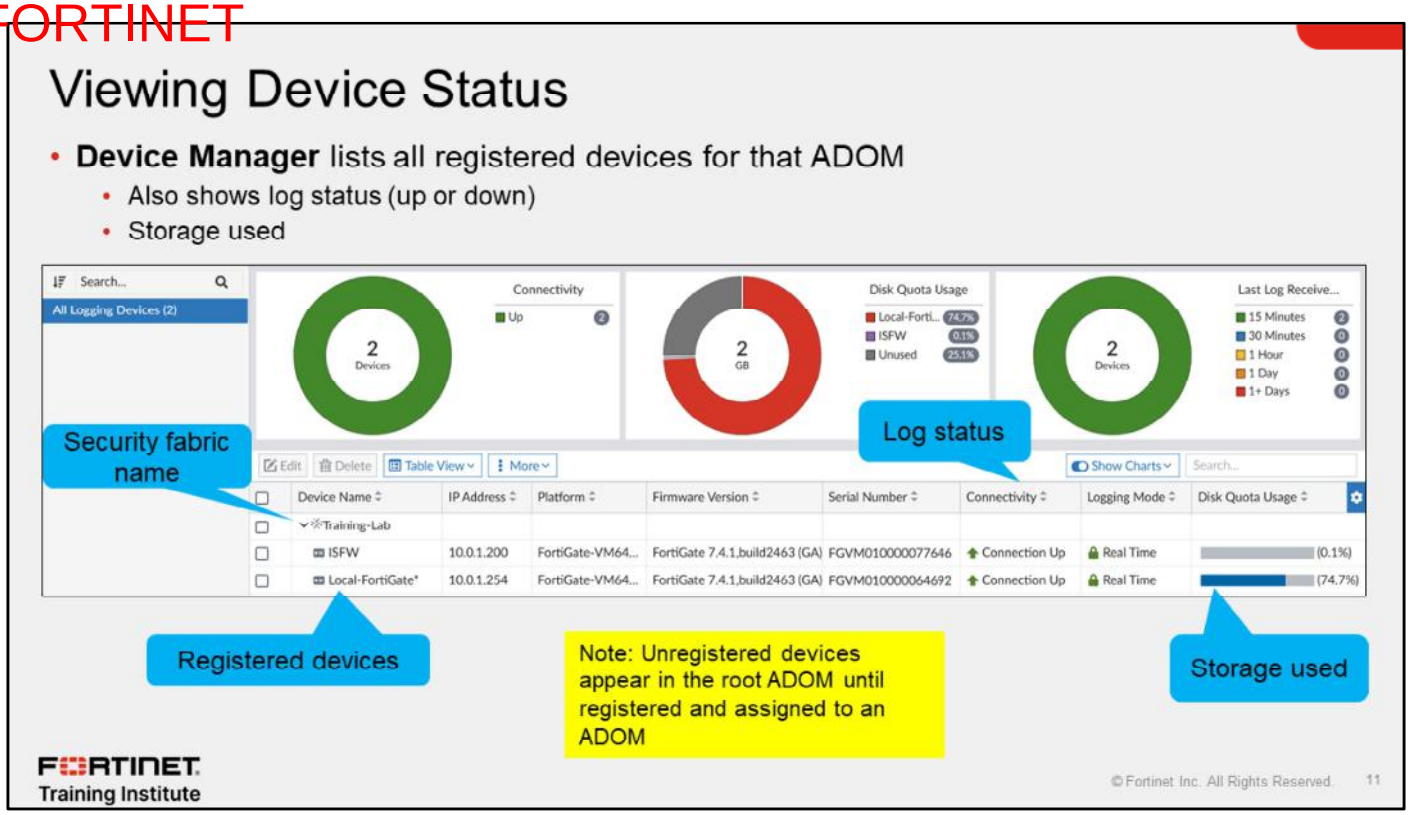
Note that you can add only FortiGate devices using this method.



To use this method, you 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.

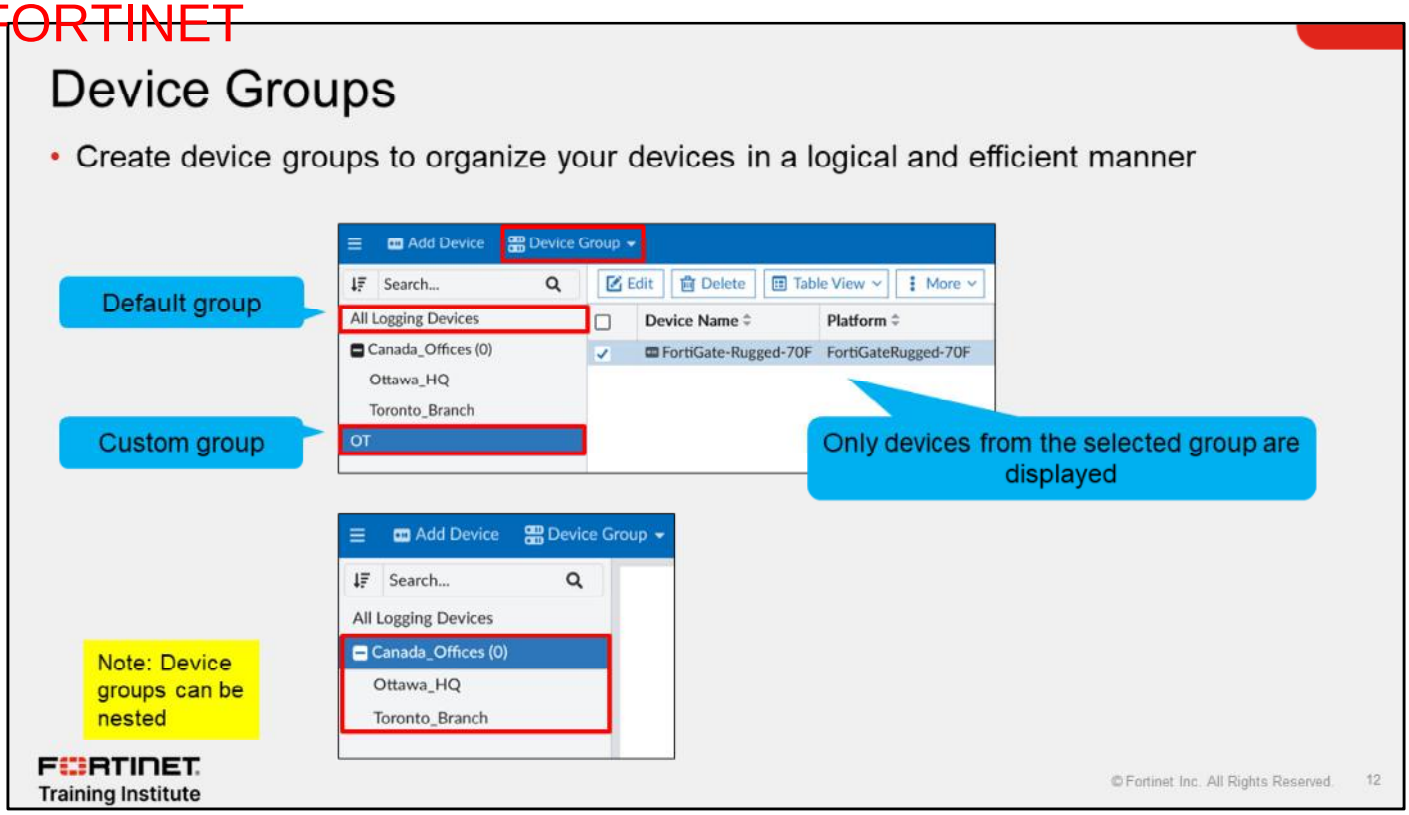
Next, the FortiGate administrator enables the Security Fabric to use FortiAnalyzer for logging, and then initiates the authorization process by clicking **OK** in the pop-up window shown in step 3. Alternatively, you can click on **Authorize** as shown in step 2.

The FortiGate administrator must have valid credentials on FortiAnalyzer to complete the registration process. This is done by clicking **Approve** in the **Fortinet Security Fabric** window.



After you register various Fortinet devices, they appear on the **Device Manager** tab for that ADOM. You can also view details about the log status and used storage for that ADOM.

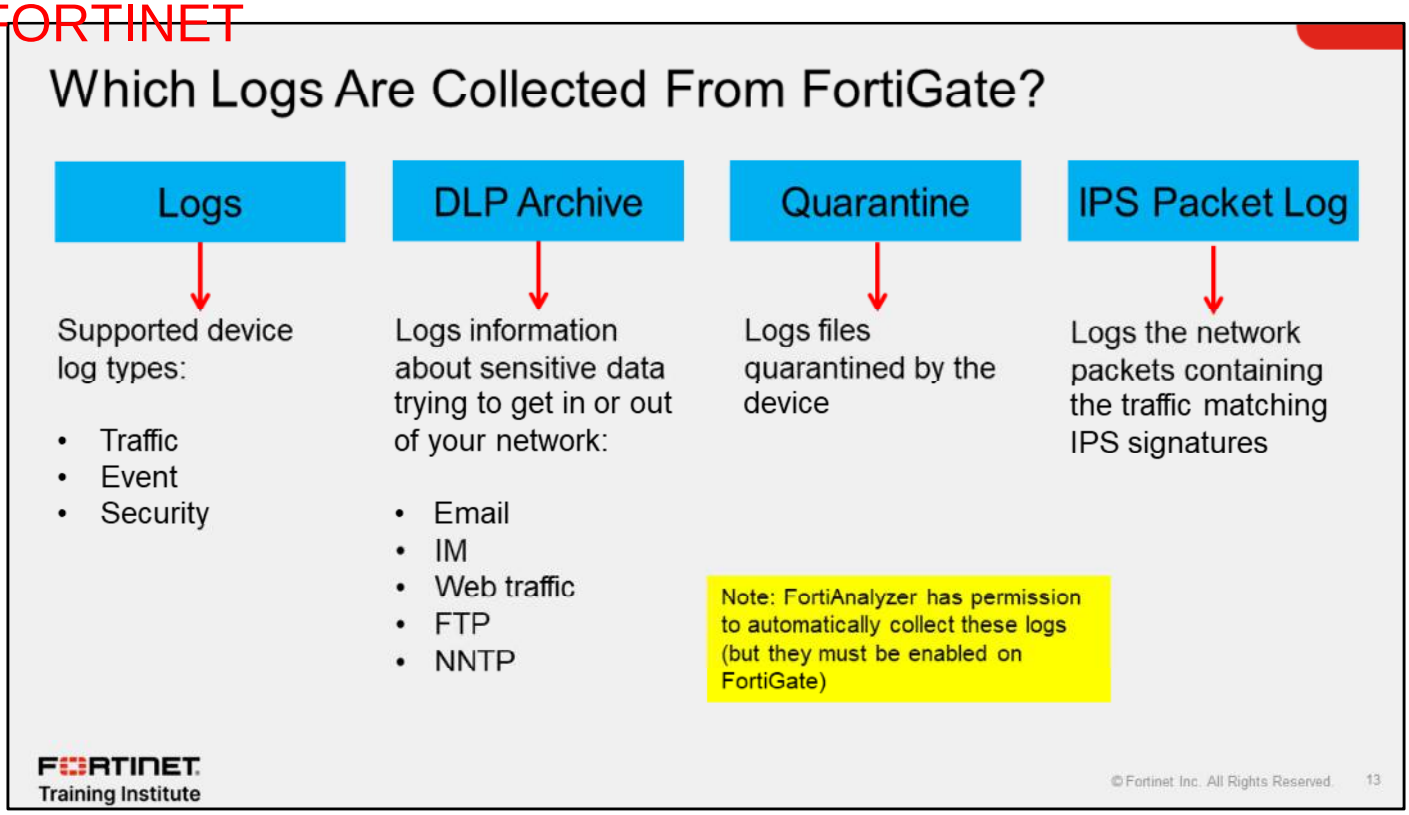
Unregistered devices appear under the **root** ADOM only until they are registered and assigned to an ADOM.



By default, all registered devices are included in a default device group. You can create custom device groups for better organization and more efficient management of those devices. For example, you can create custom groups based on physical location and functionality.

Additionally, if your environment justifies it, device groups can be nested. In the example shown on this slide, a device group named **Canada_Offices** contains a nested group with two branches.

Spaces are not allowed in the names of custom device groups.



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

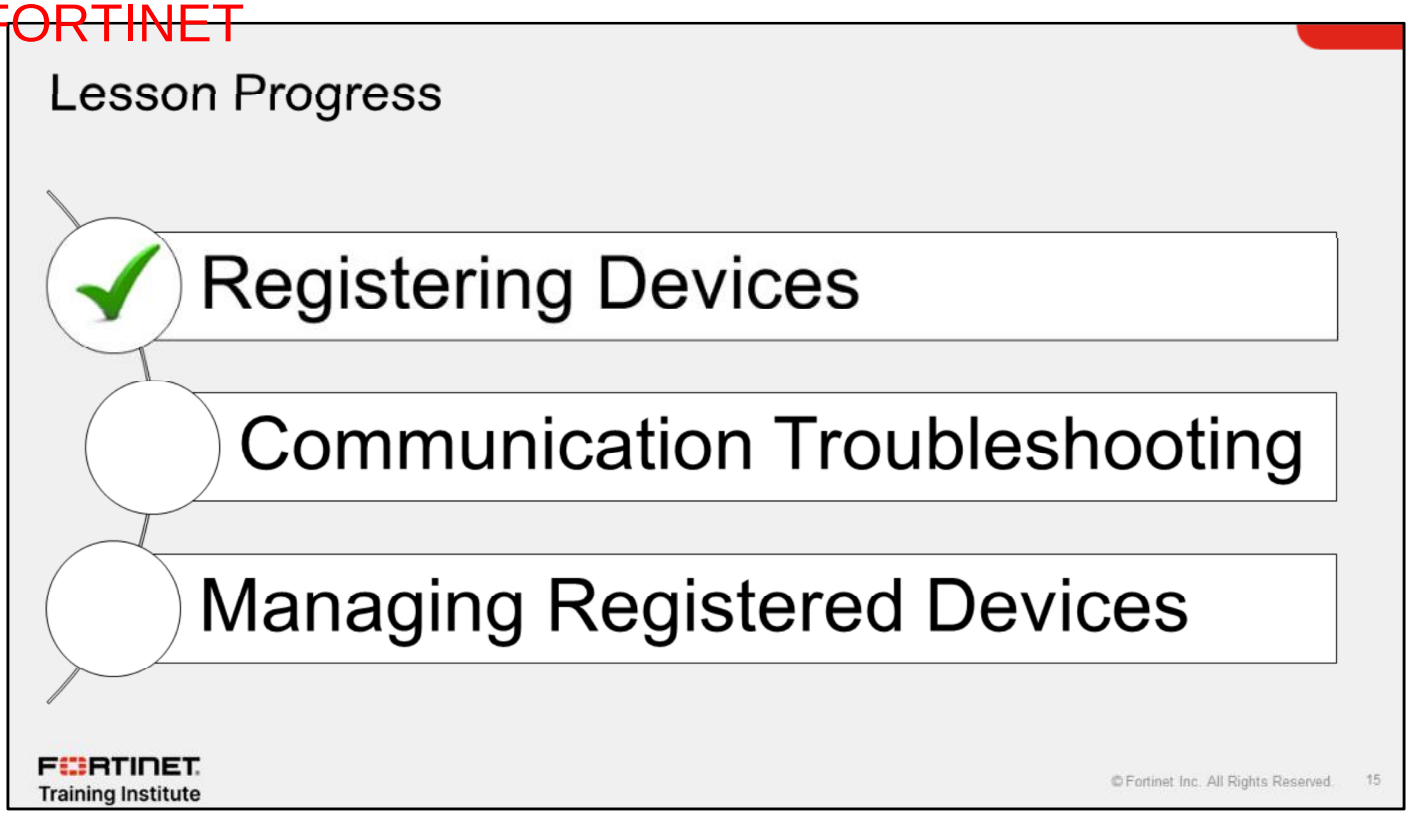
- Logs: This log type details information about traffic, events, and security.
- DLP Archive: This log type details information about any sensitive data trying to get in or out of your network.
- Quarantine: This log type details files that have been placed into quarantine by the device sending the logs.
- 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. The logging device and FortiAnalyzer can both initiate the registration request.

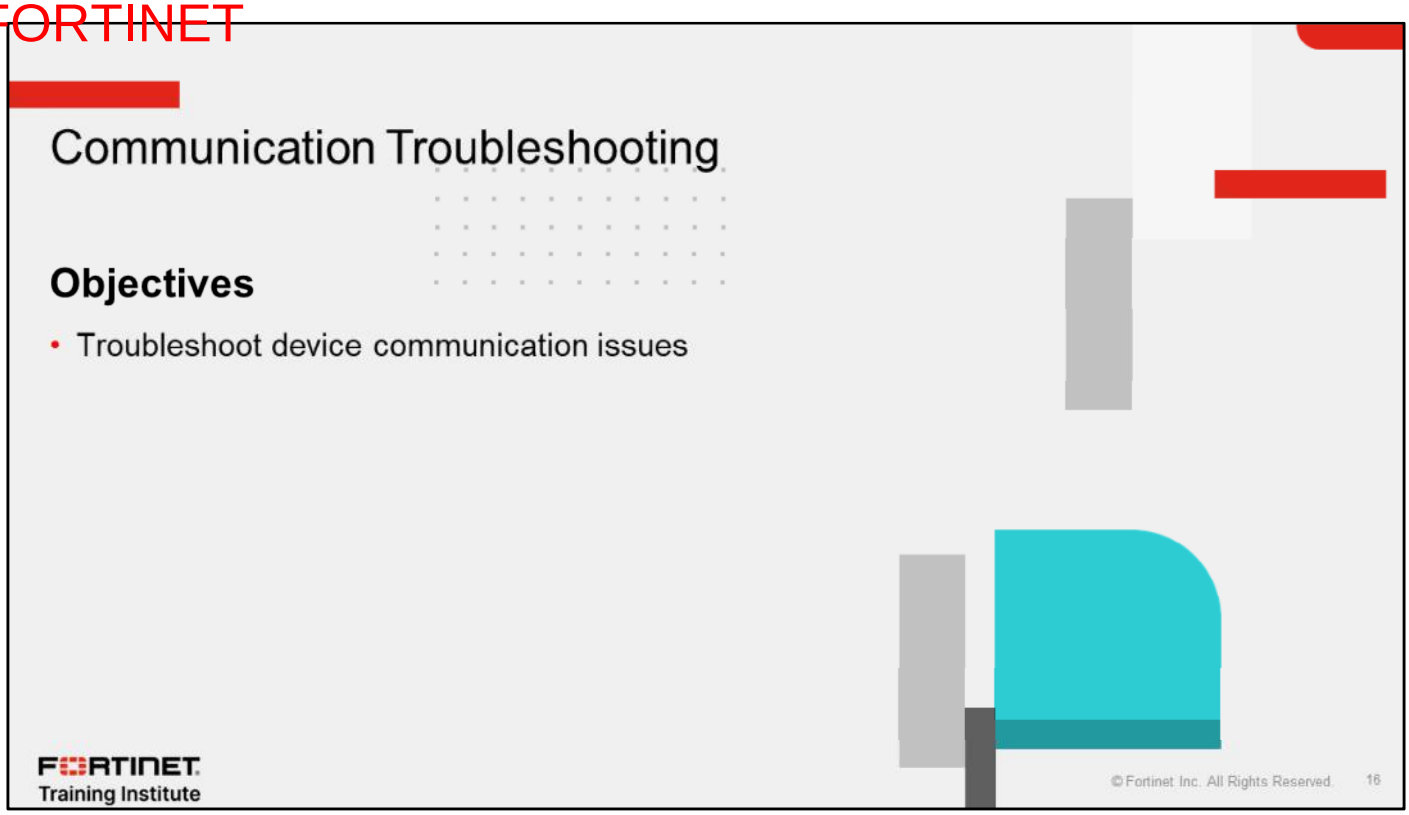
FORTINET Training Institute

 14



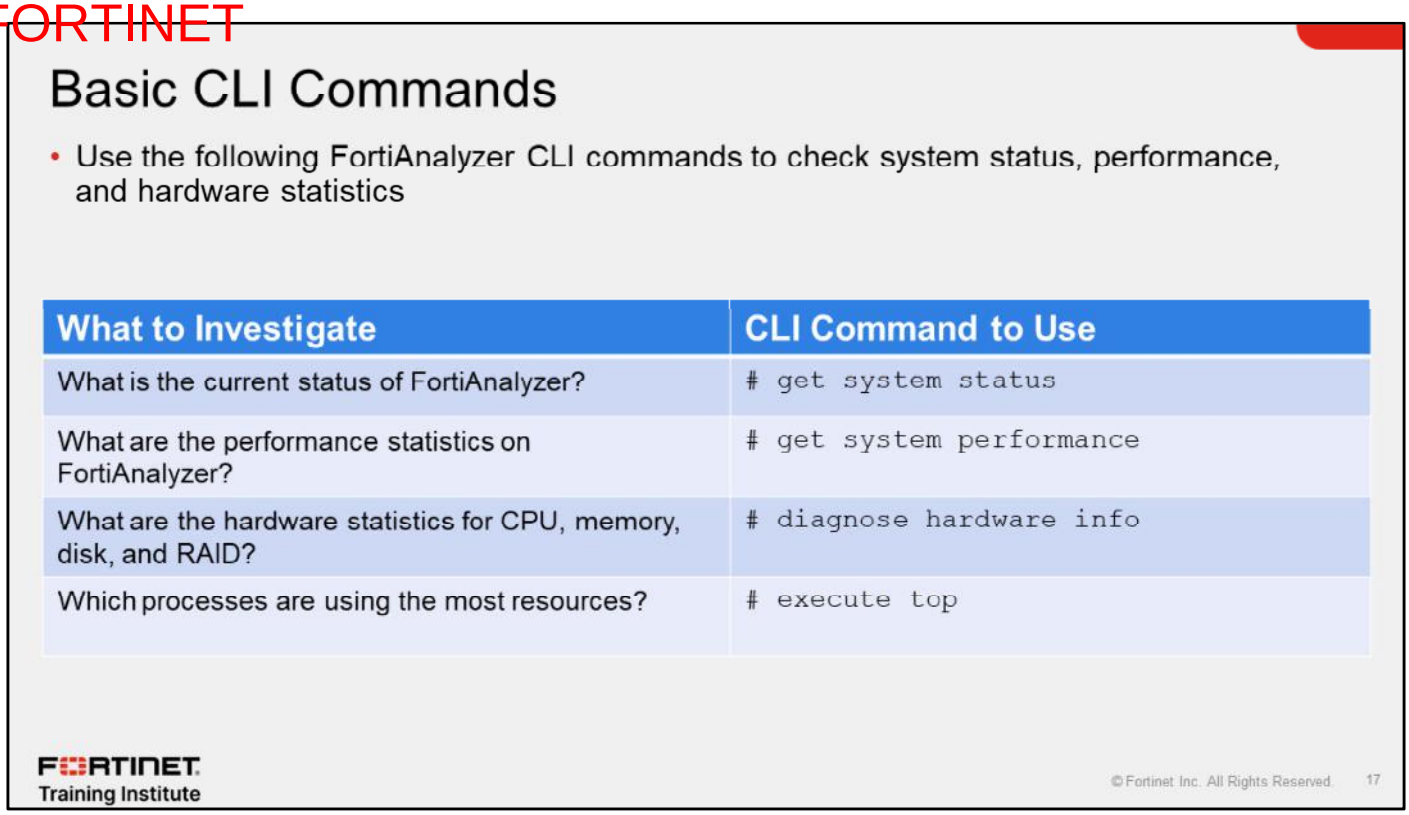
Good job! You now understand how to register a device.

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

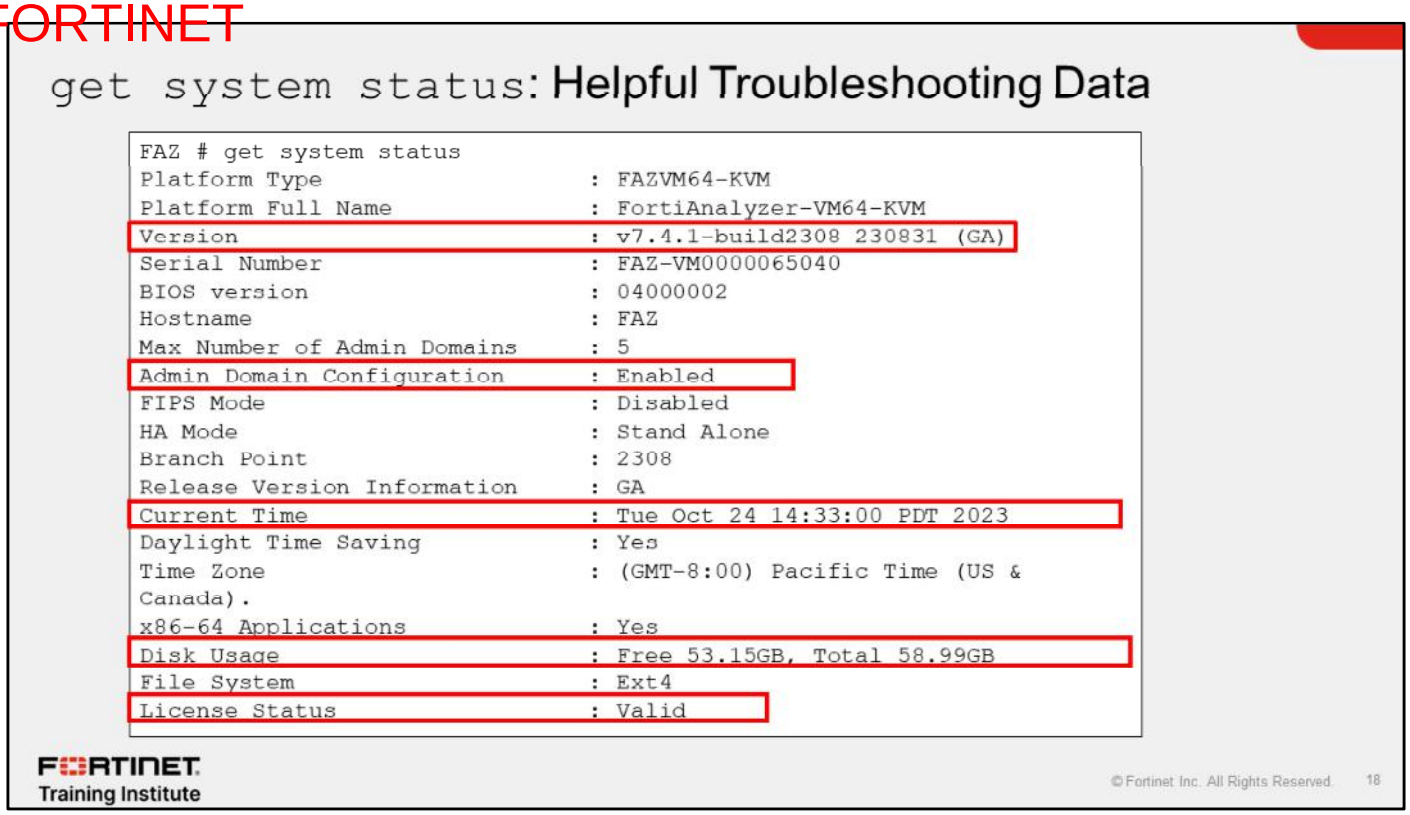


After completing this section, you should be able to achieve the objective shown on this slide.

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

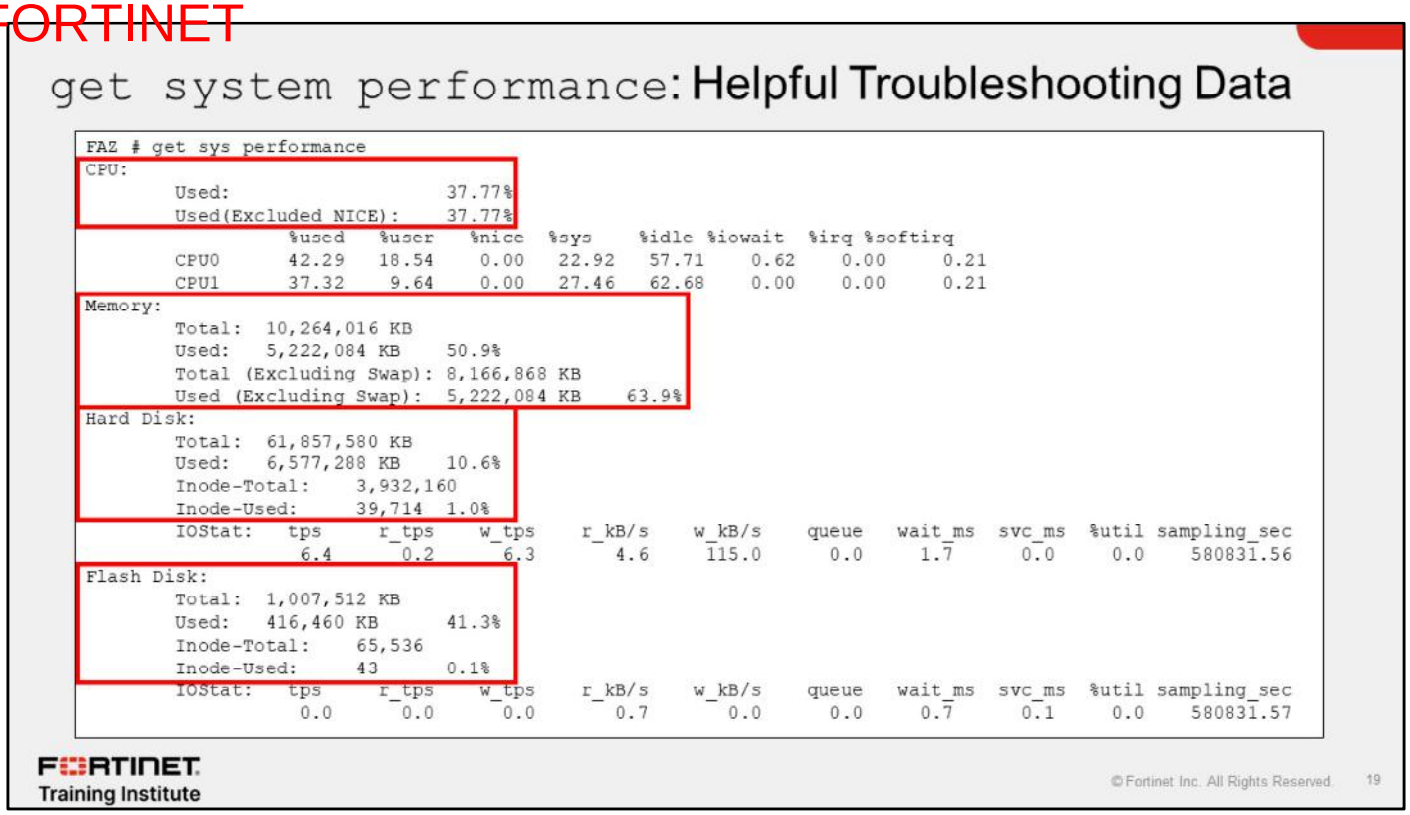


This slide shows some basic CLI commands that you can use to check system status, performance, hardware statistics, and processes.



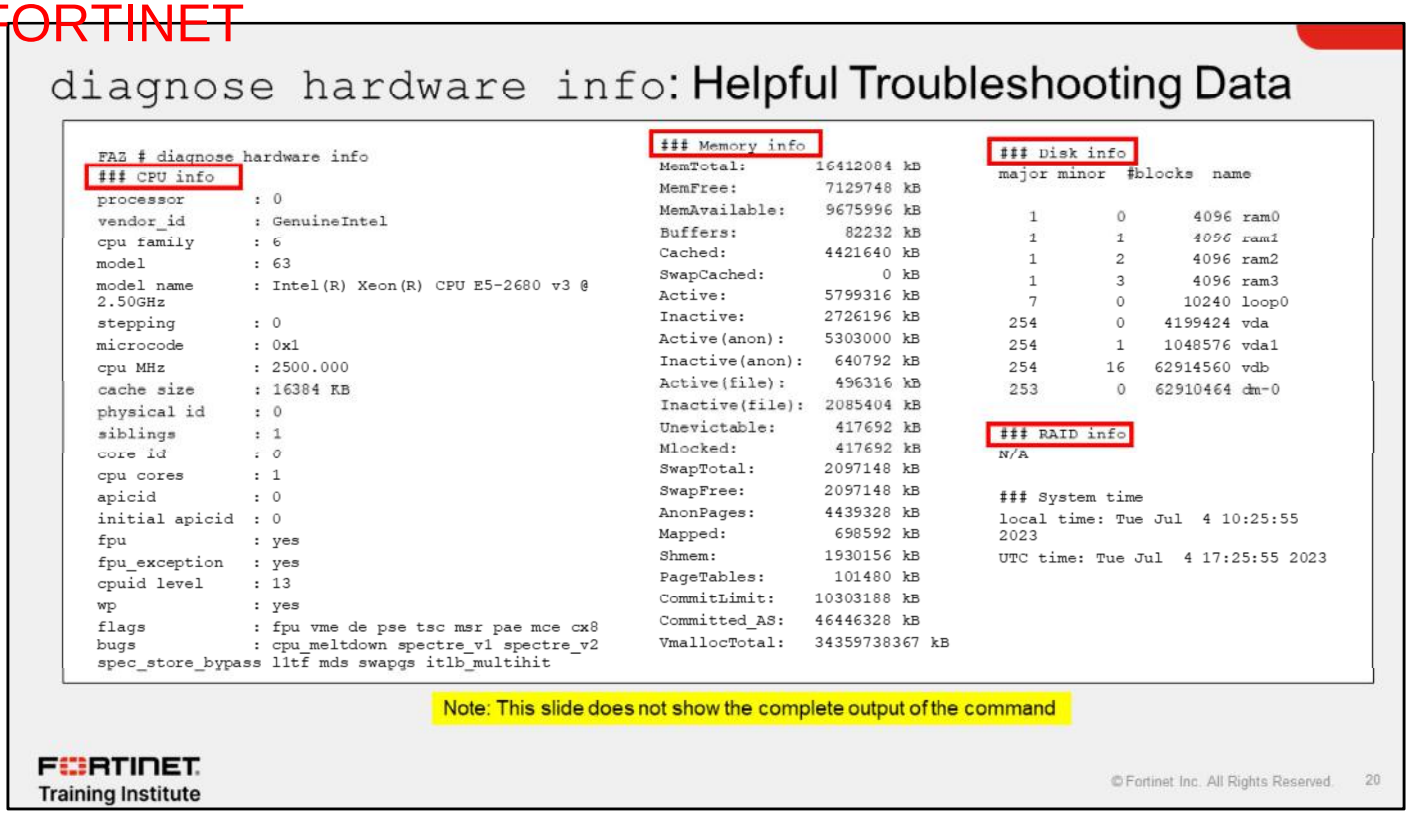
When using the `get system status` command to troubleshoot system issues, the following information can be helpful:

- `Version`: Ensure the FortiAnalyzer firmware version is compatible with the device you are registering. See the *FortiAnalyzer Release Notes* for supported firmware versions.
- `Admin Domain Configuration`: Ensure ADOMs are enabled if you are attempting to register a non-FortiGate device.
- `Current Time`: Ensure your date and time is set according to your needs. For many features to work, including scheduling, logging, and SSL-dependent features, the FortiAnalyzer system time must be accurate. 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 licence. 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 experience problems. For example, the space assigned to a hard disk quota is not fully available for logs, because some of it is reserved for system usage and unexpected quota overflow.

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



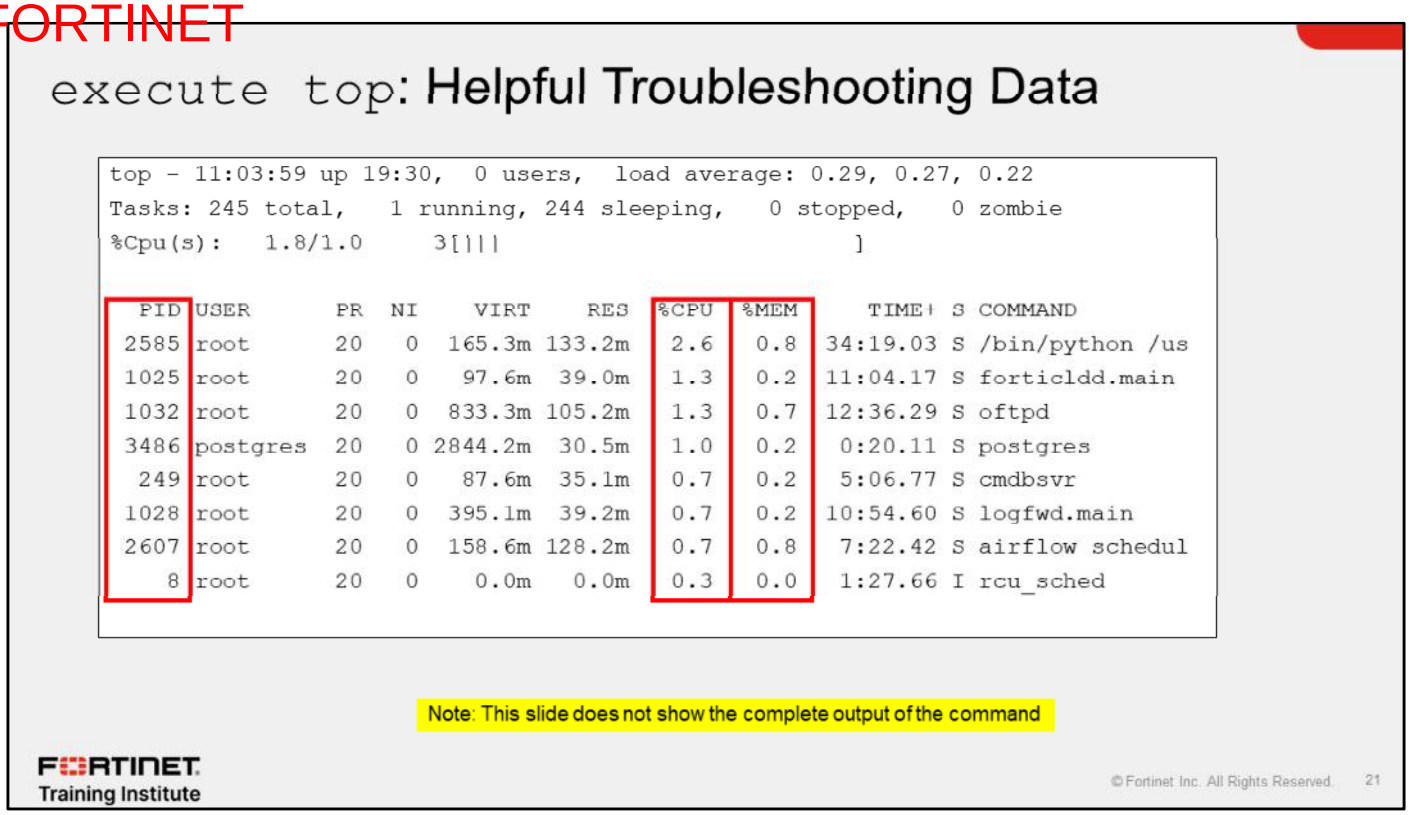
The `diagnose hardware info` command provides useful details about CPU, memory (RAM), and disks.

The memory and RAID sections can be very useful while troubleshooting system issues.

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

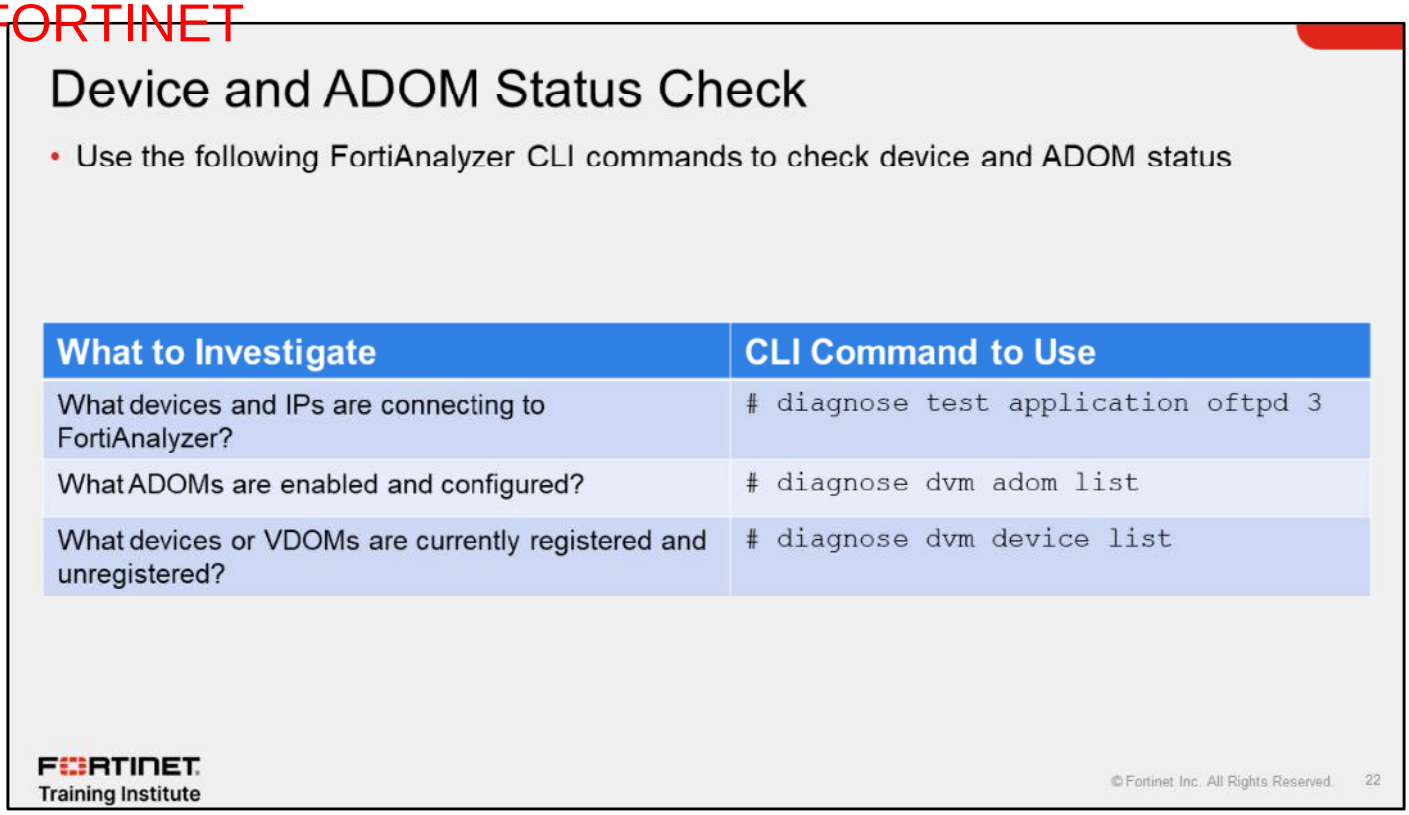
Swap memory refers to the disk space available to use when the physical memory is full, and the system requires more memory. For a temporary period, inactive pages in memory are moved to the swap space.

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

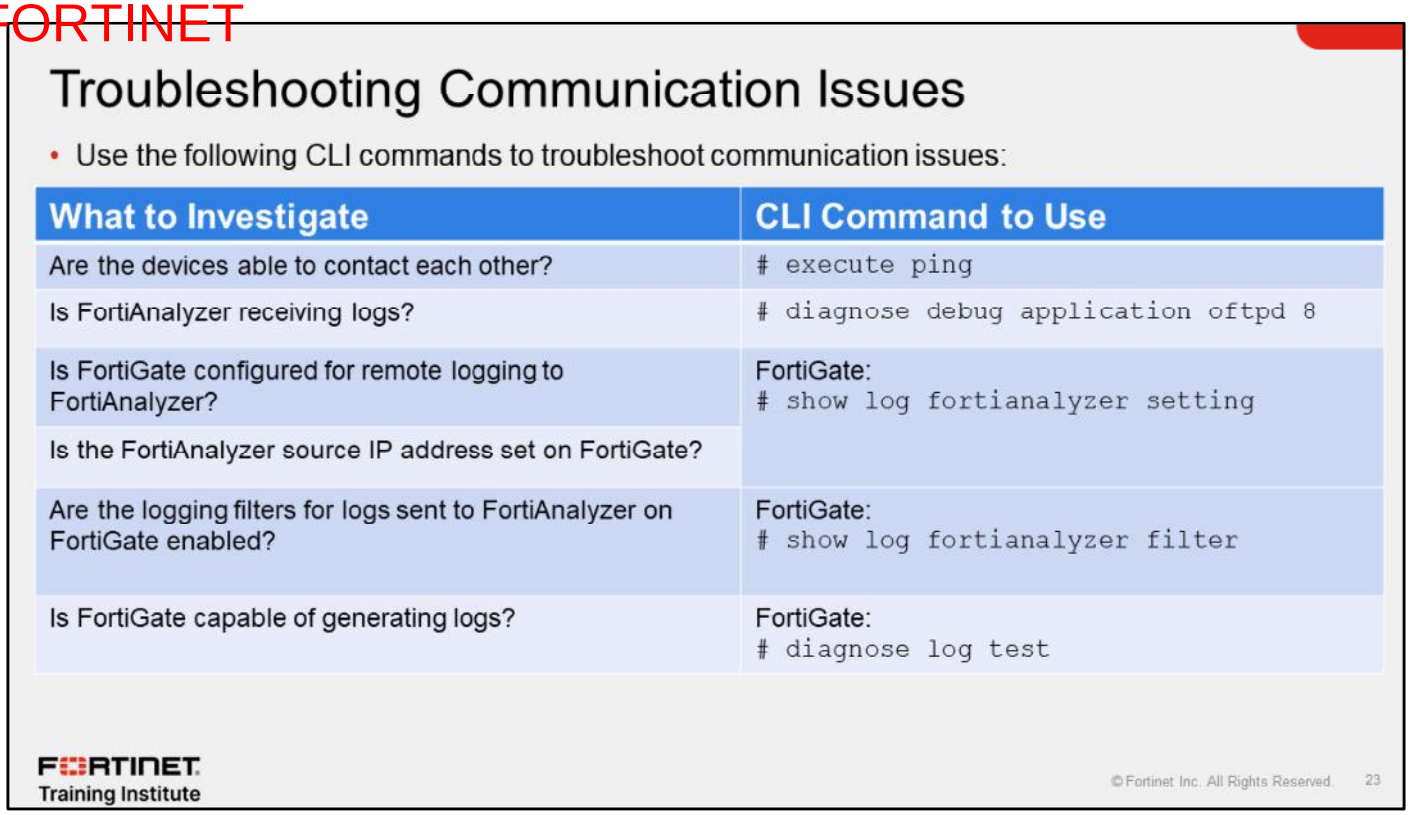


The `execute top` command provides real-time information about processes on FortiAnalyzer. You can see the process ID, CPU usage, memory usage, and other fields for each process. If you see high resource usage from the `get system performance` command, you can use `execute top` to look deeper into how the 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.



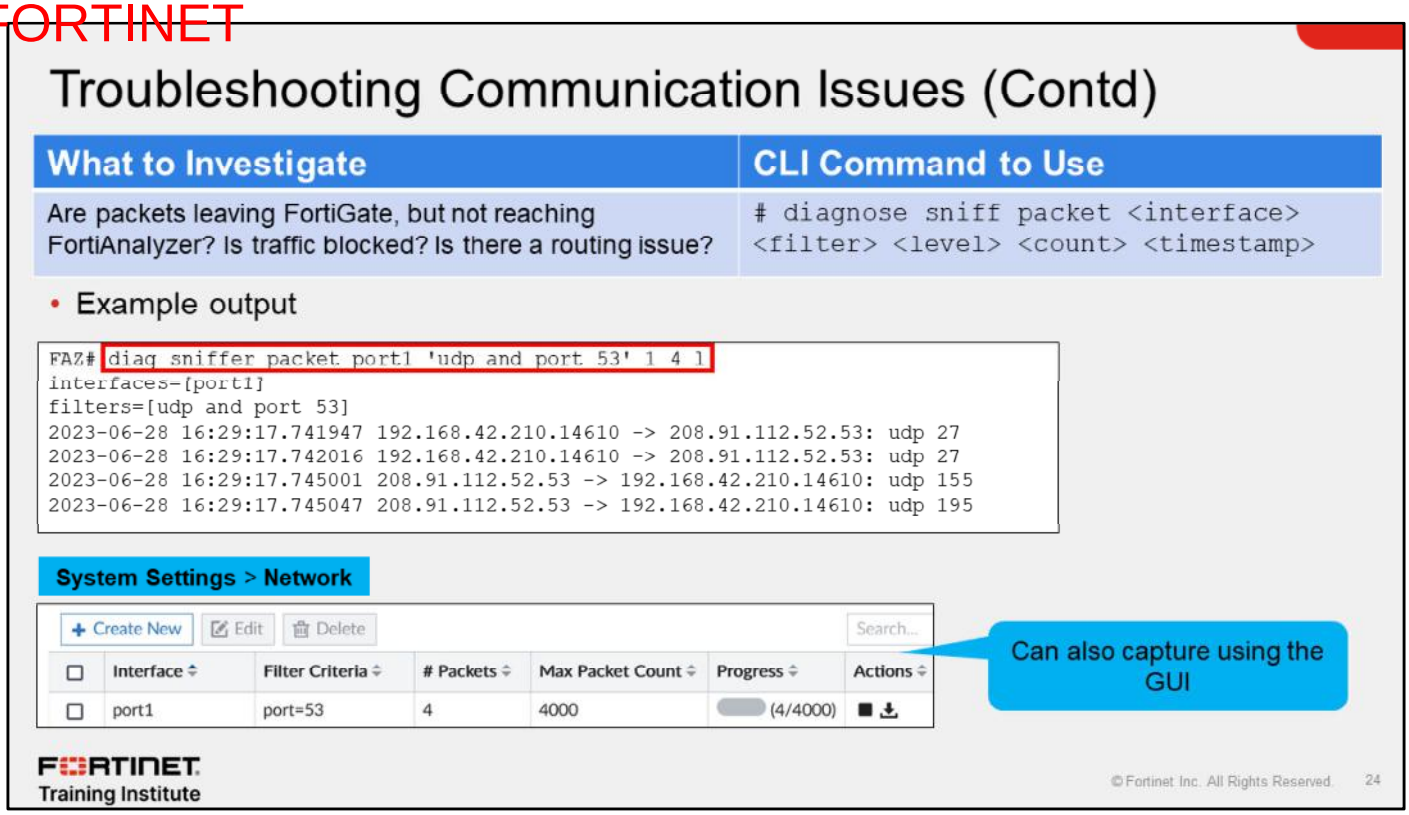
This slide shows the FortiAnalyzer CLI commands you can run to discover which devices and IP addresses are connecting to FortiAnalyzer, which ADOMs are enabled and configured, and which devices are currently registered and unregistered.



If you are experiencing communication issues between other devices and FortiAnalyzer, first 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 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 proceeding with troubleshooting the FortiAnalyzer side.

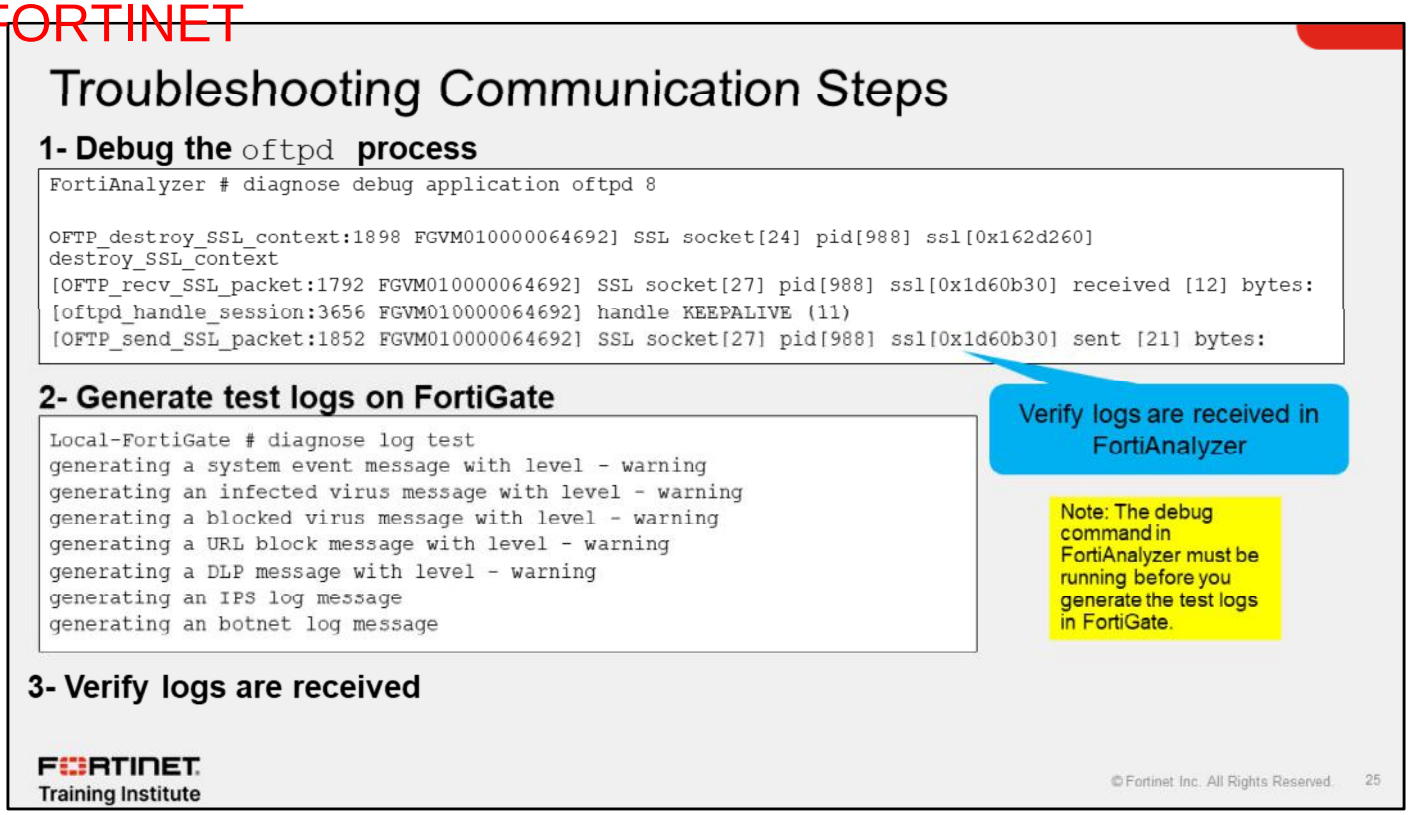


You can also run sniffers on both devices to see if packets that leave FortiGate are reaching FortiAnalyzer. If packets are leaving FortiGate, but not reaching FortiAnalyzer, look at other devices in the network, because an intermediate router or firewall may be blocking the traffic or routing it inappropriately.

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

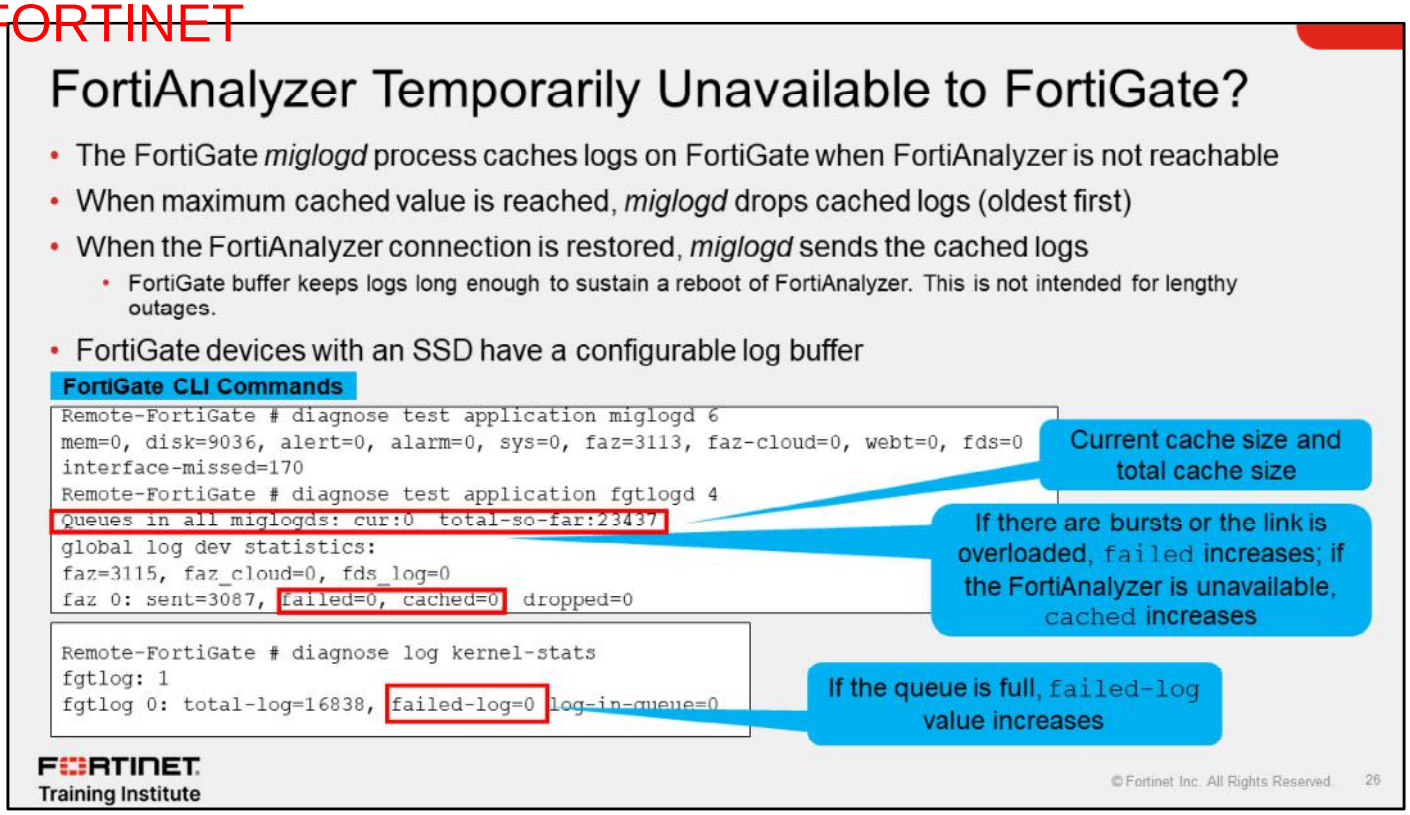
In the CLI example shown on this slide, the capture has the following characteristics:
- Traffic on port1
- UDP port 53 (DNS traffic)
- Level 1 verbosity
- Capture limit of four packets
- Local time

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 the FortiAnalyzer side.



If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache 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 begins to send the cached logs to FortiAnalyzer. The FortiGate buffer keeps logs long enough to sustain a restart of FortiAnalyzer (if you are upgrading 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 cache size and maximum cache size.

The CLI command `diagnose log kernel-stats` shows an increase in `failed-log` if the cache is full and needs to drop logs.

FortiGate devices with an SSD disk have a configurable log buffer. When the connection to FortiAnalyzer is unreachable, FortiGate can buffer logs on disk if the memory log buffer is full. The logs queued on the disk buffer can be sent successfully after the connection to FortiAnalyzer is restored.

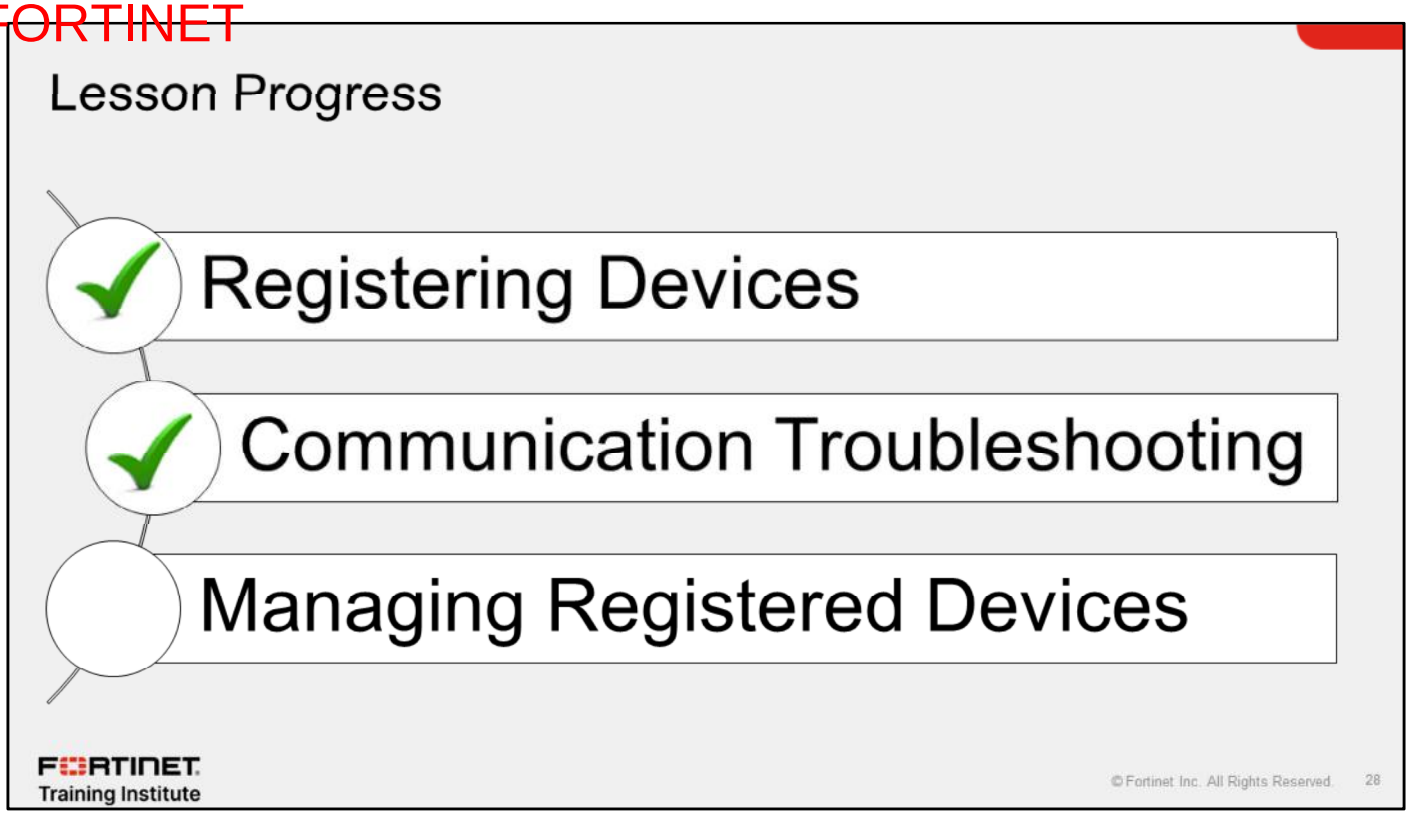
Knowledge Check

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

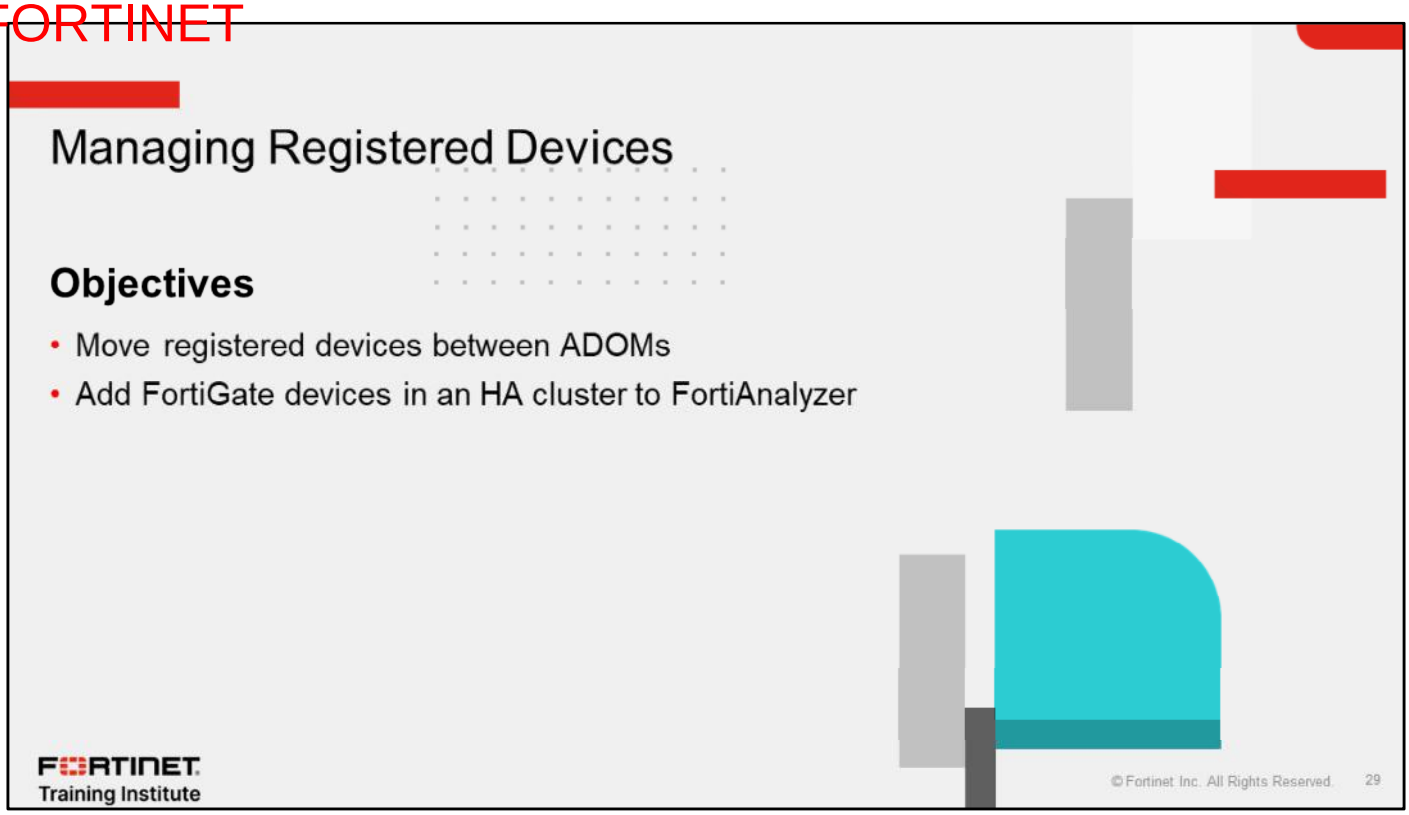
FORTINET Training Institute

 27



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

Now, you will learn how to manage registered devices.

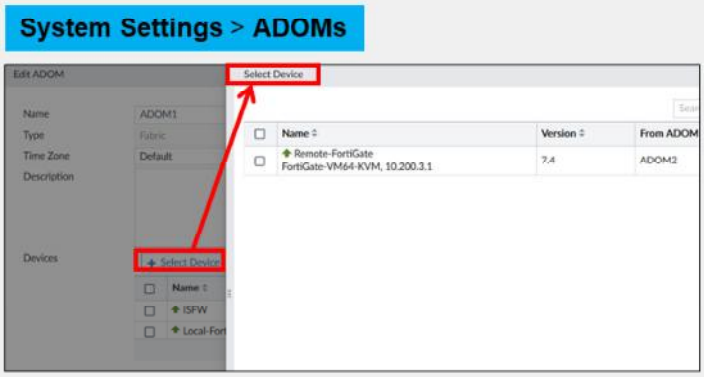


After completing this section, you should be able to achieve the objectives shown on this slide.

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.

Moving Registered Devices Between ADOMs

- Do not move devices between ADOMs unless you have to
- 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

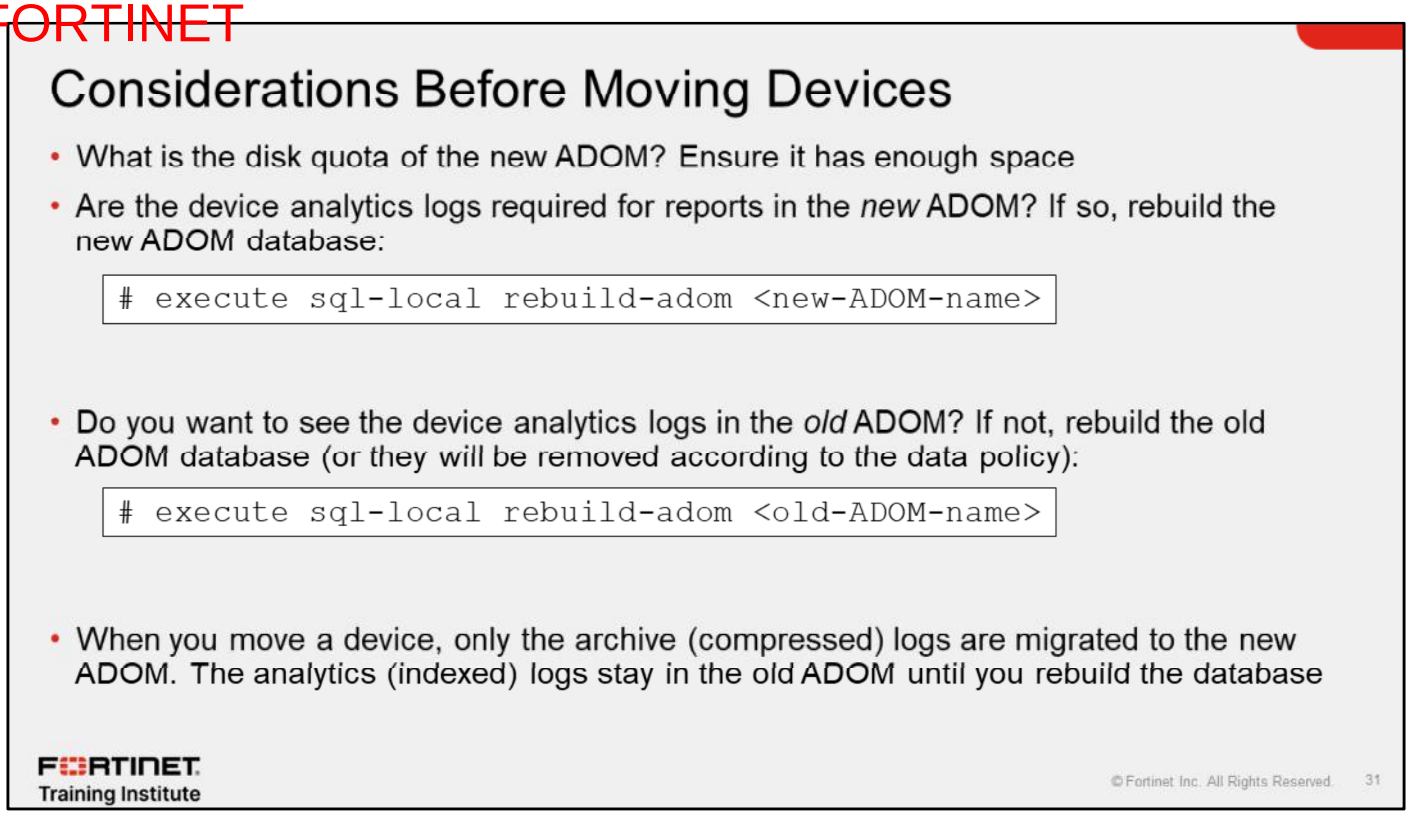
 30

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

While you shouldn't move devices between ADOMs unless you have to, one such use case is if you have a mix of low-volume and high-volume log rates in one ADOM. In this situation, it is recommended that you place low-volume log rate devices in one ADOM and high-volume log rate devices in another ADOM. This prevents quota enforcement from adversely affecting low-volume log devices.

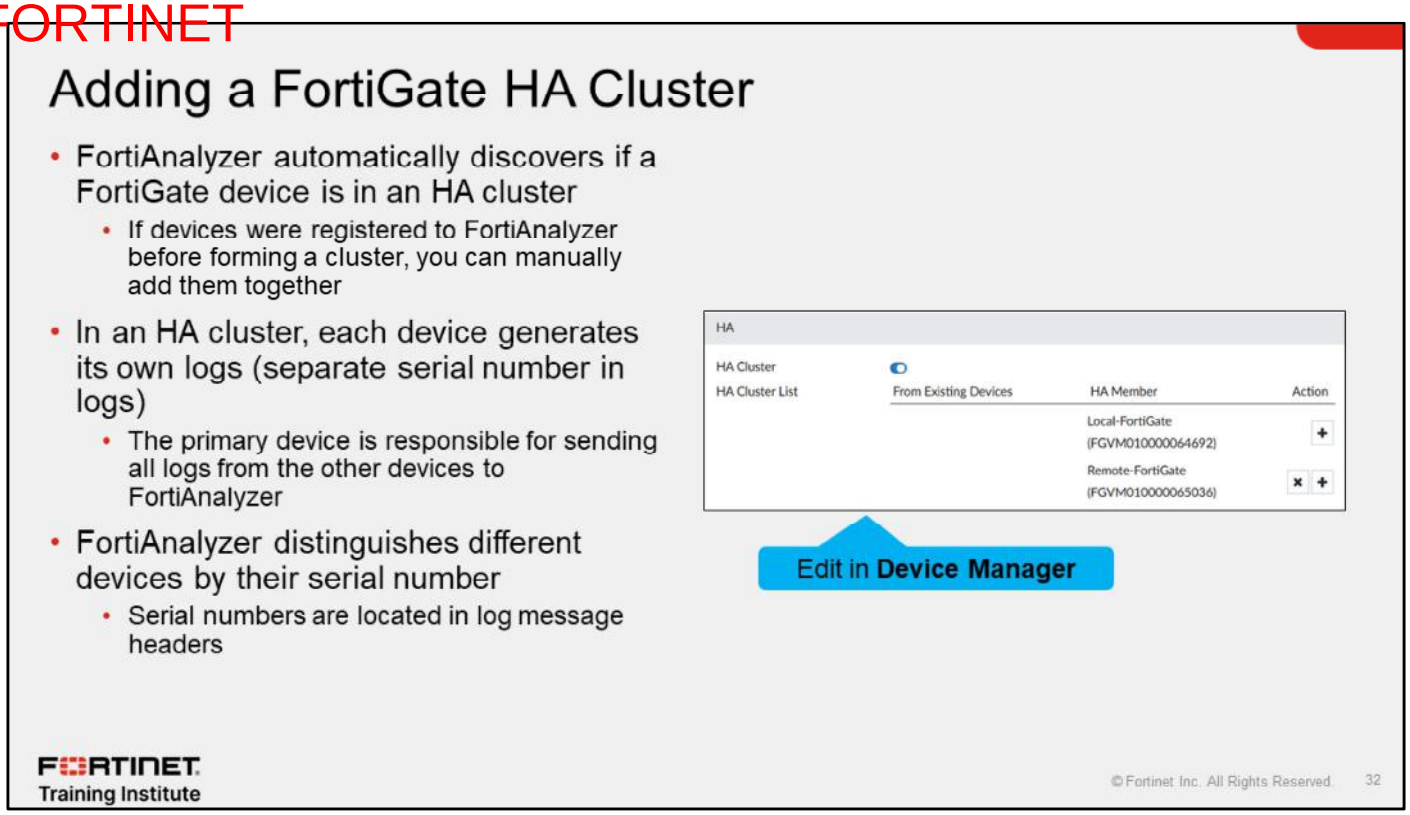
You can move devices between ADOMs by editing the custom ADOM you want to add the device to, and then selecting the device to add to it.

Note that you do not need to move devices into a new ADOM if 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. When you move a device, only the archive logs (compressed logs) are migrated to the new ADOM. 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 discovers if a FortiGate device is in an HA cluster. However, 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, the only device that communicates with FortiAnalyzer is the primary device in the cluster. The other devices send their logs to the primary, which then 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 associated with each device.

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

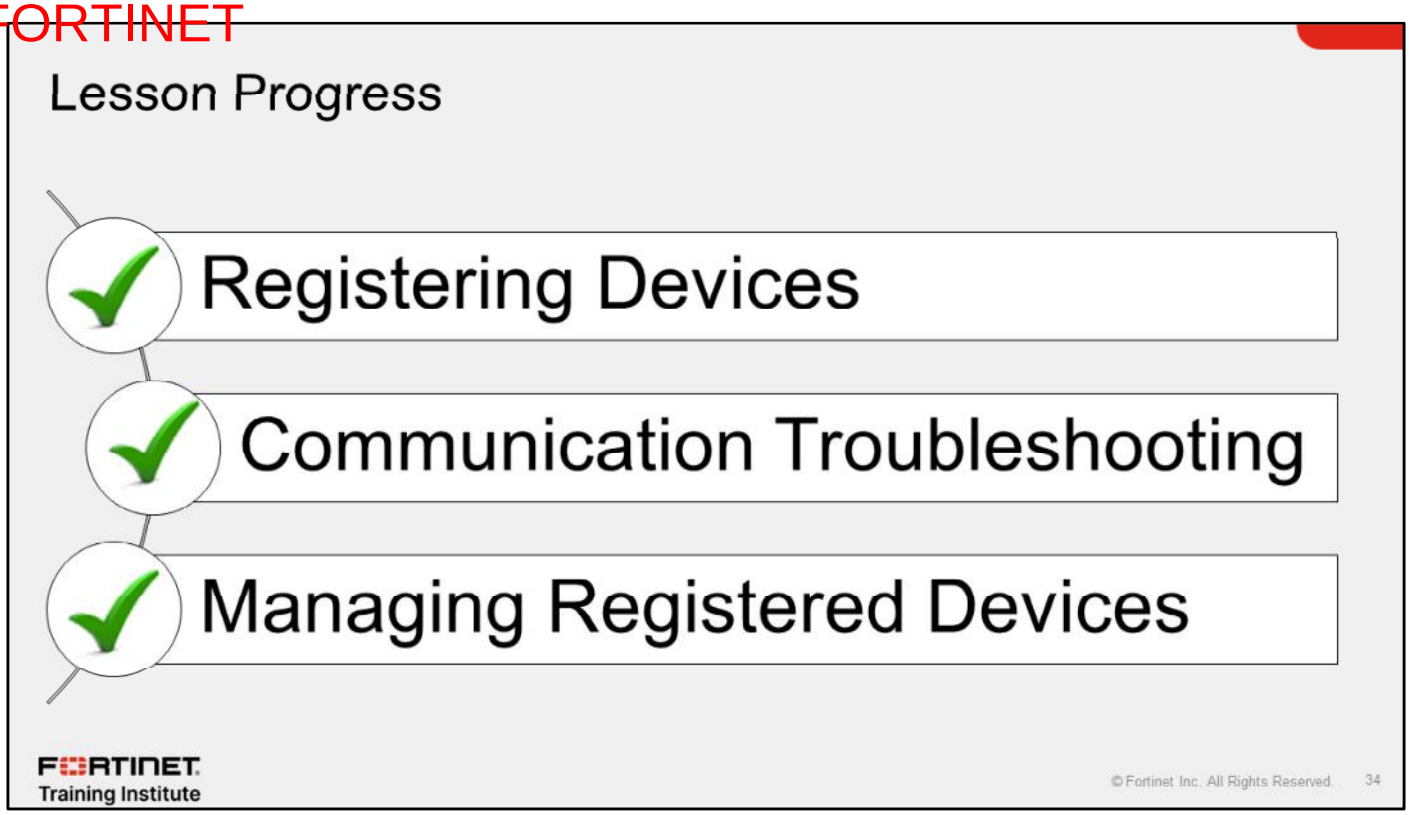
Knowledge Check

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

✓ A. Archive logs
B. Analytic logs

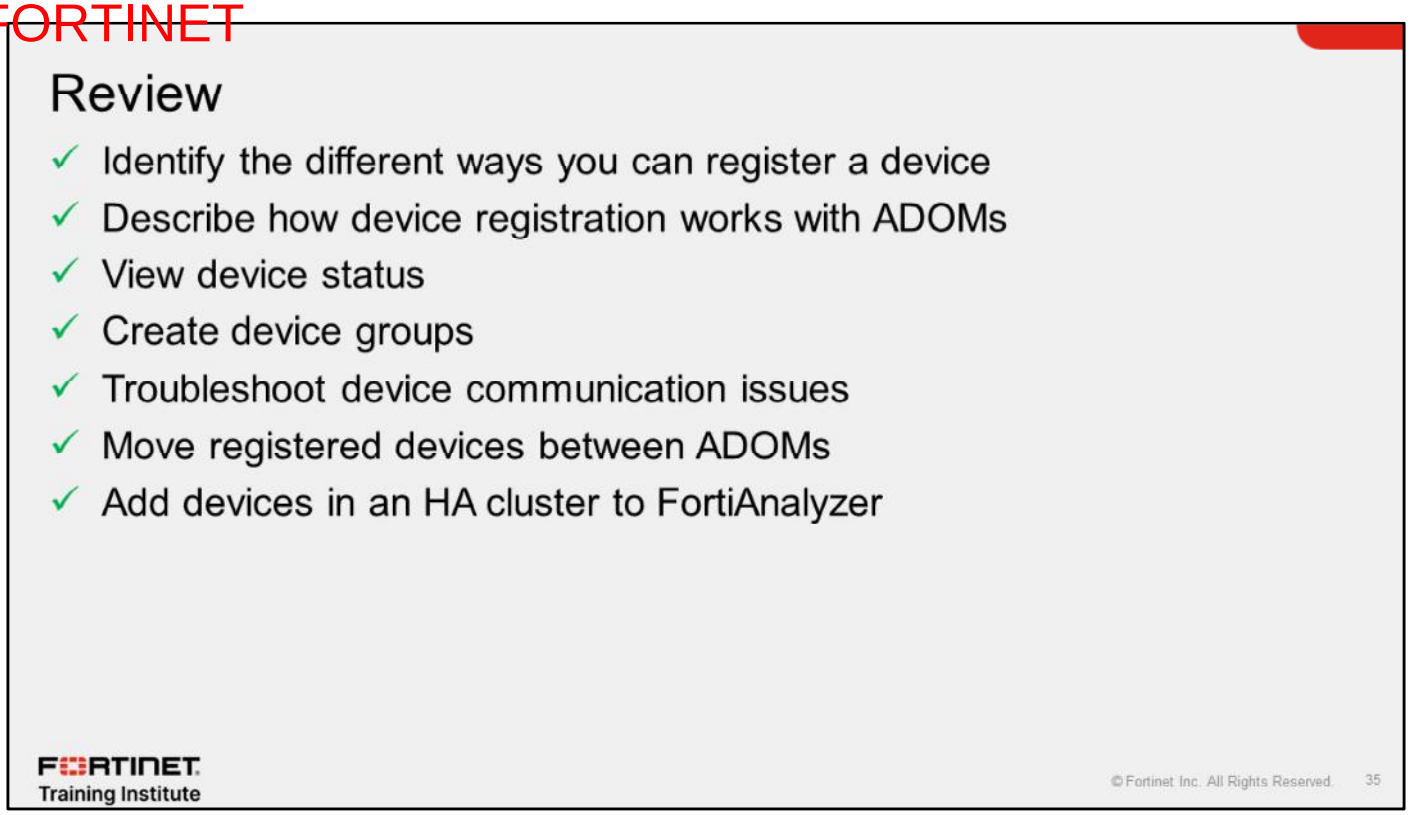
FORTINET Training Institute

 33



Congratulations! You have completed this lesson.

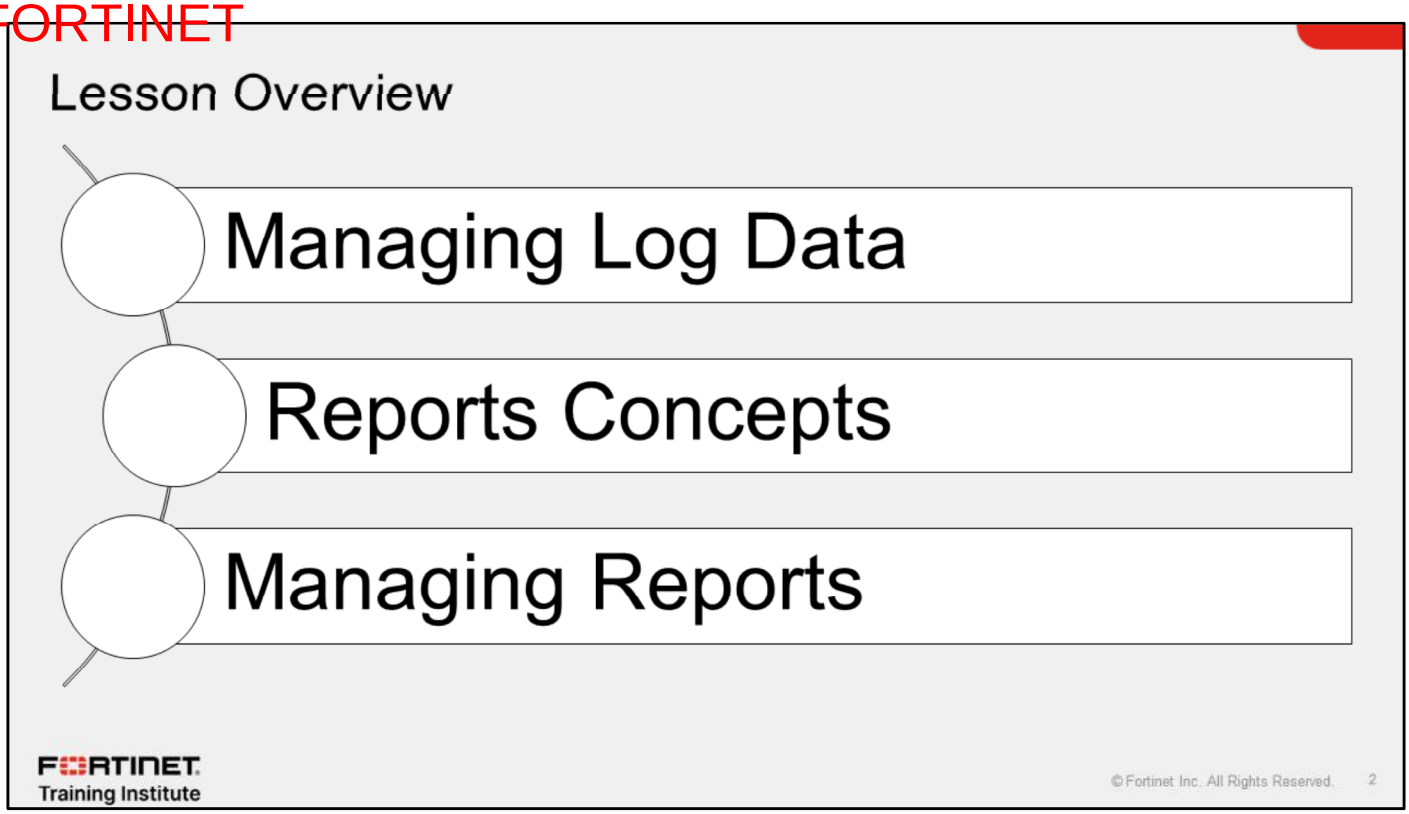
Now, you will review the objectives that you covered in this lesson.



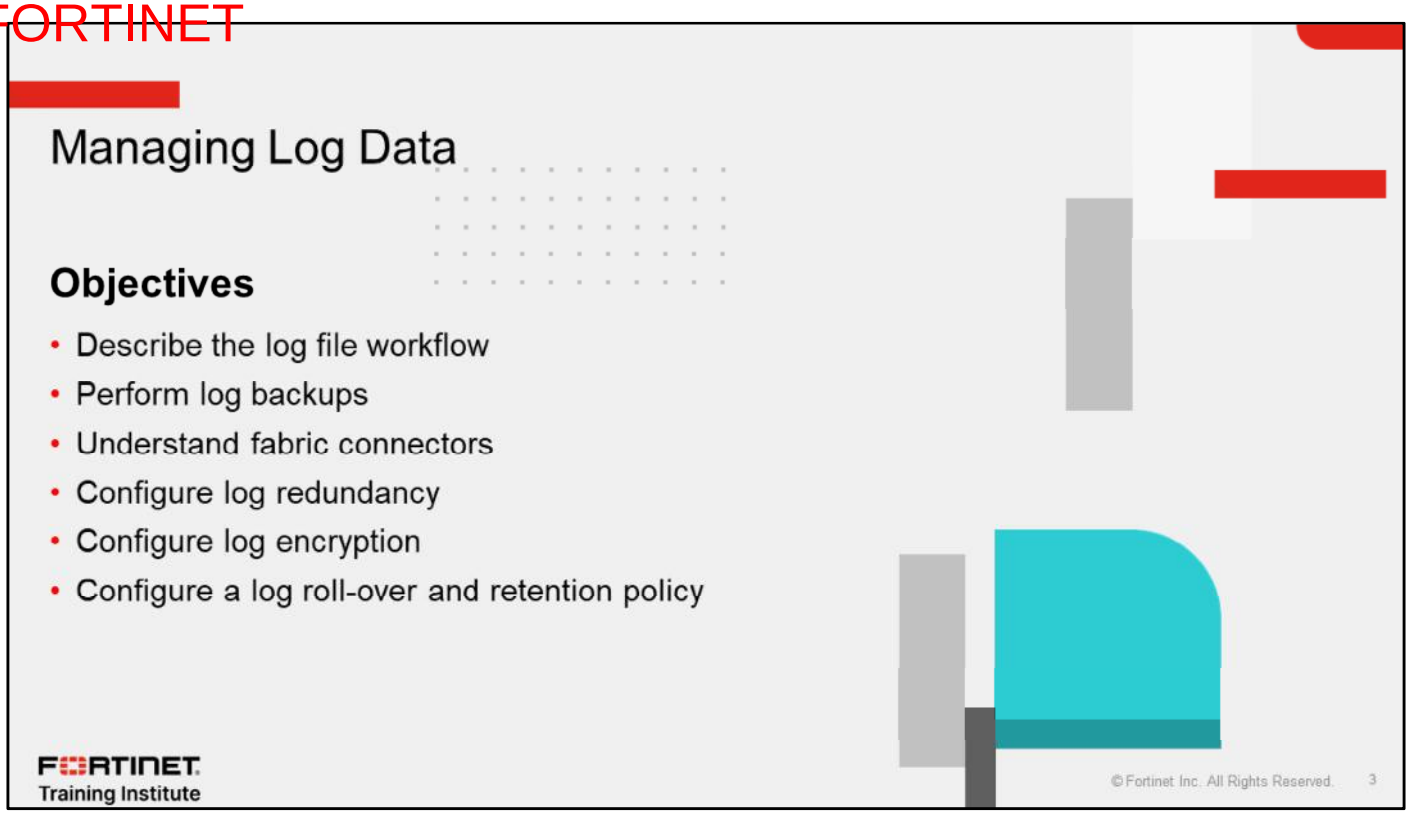
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned 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.

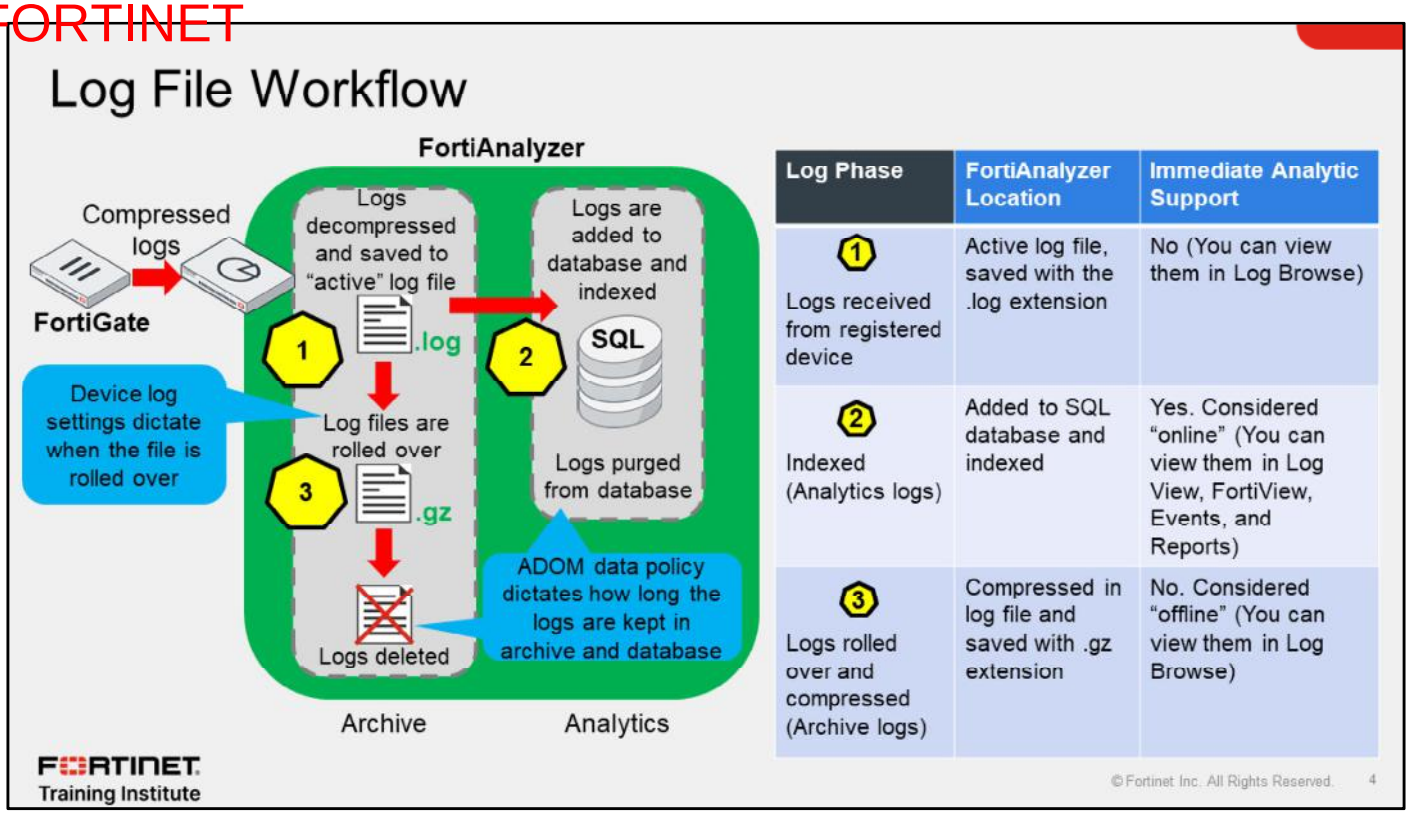


In this lesson, you will explore the topics shown on this slide.



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

By demonstrating competence in 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.



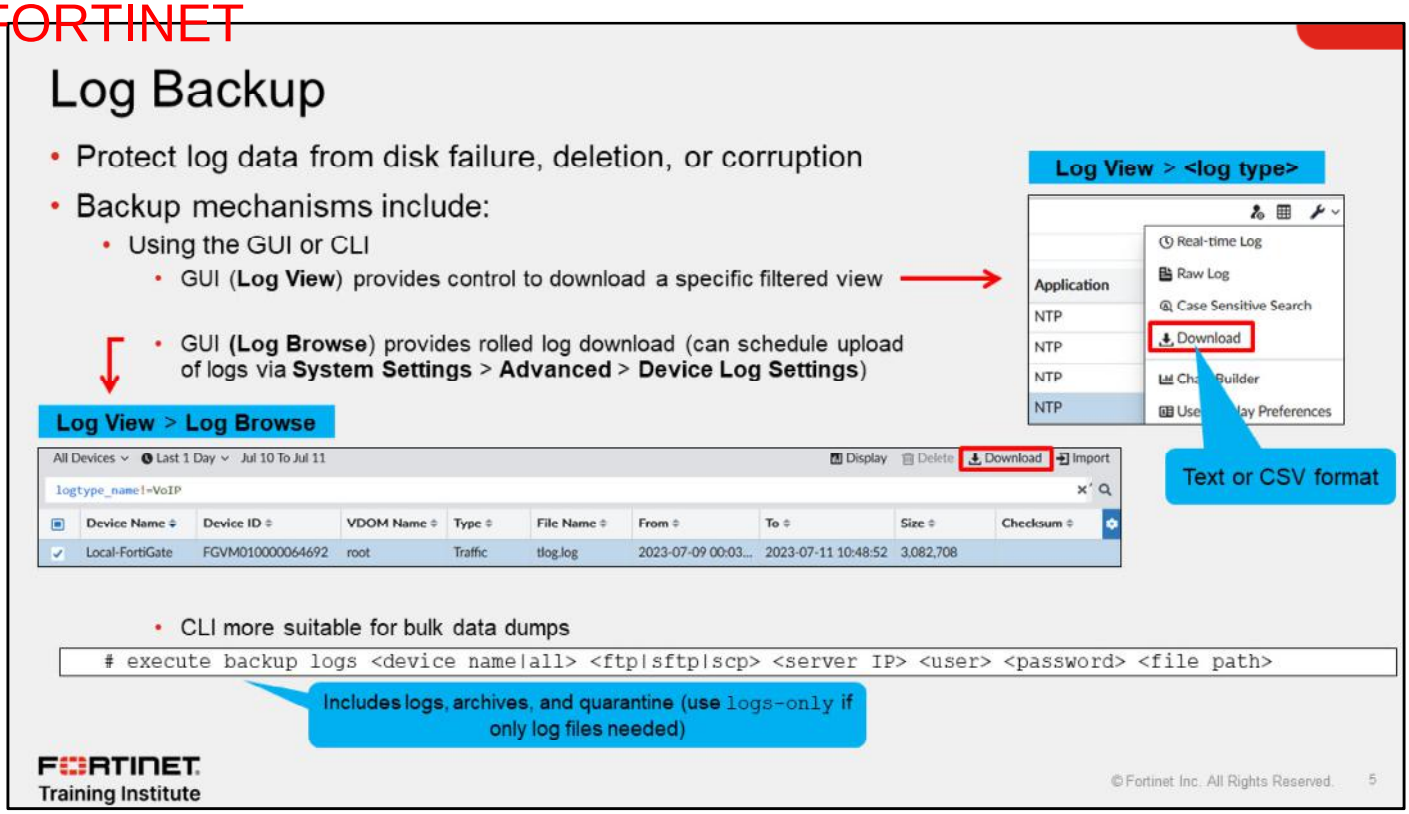
Log Phase	FortiAnalyzer Location	Immediate Analytic Support
1 Logs received from registered device	Active log file, saved with the .log extension	No (You can view them in Log Browse)
2 Indexed (Analytics logs)	Added to SQL database and indexed	Yes. Considered "online" (You can view them in Log View, FortiView, Events, and Reports)
3 Logs rolled over and compressed (Archive logs)	Compressed in log file and saved with .gz extension	No. Considered "offline" (You can view them in Log Browse)

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

1. Logs received are decompressed and saved 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 SQL database to support analysis. Logs in the indexed phase are known as *analytics* logs. These logs are considered online and offer immediate analytic support. You can view these logs using **Log View**, **FortiView**, **Incident & Events**, and **Reports**. FortiAnalyzer purges analytics logs from the SQL database as specified in the ADOM data policy.

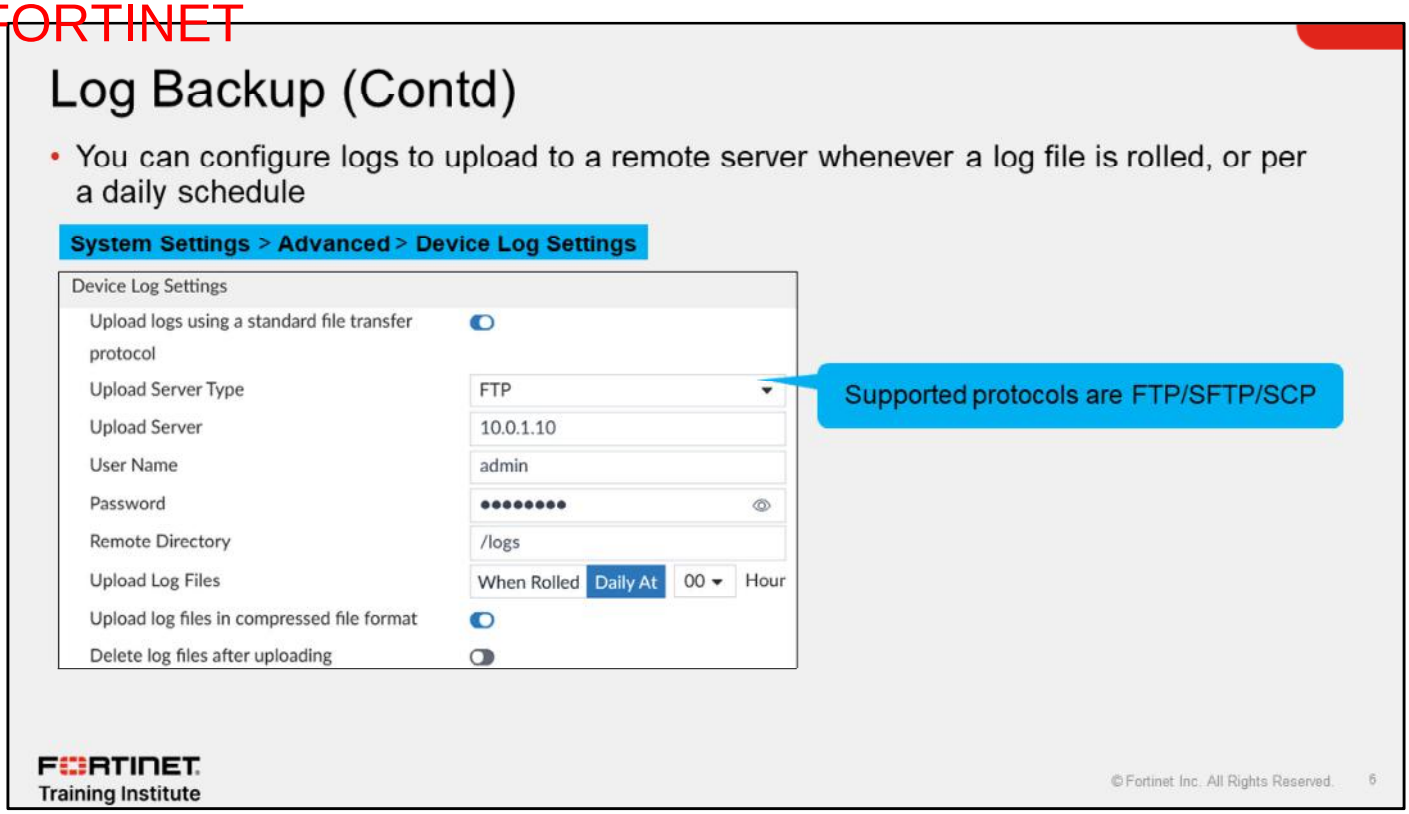
3. Eventually, when the log file reaches a configured size, or at a set schedule, it is rolled over. The process of rolling over consists of renaming the file, adding a timestamp, and then compressing it, which adds the *.gz* extension. These files are known as *archive* logs and are considered offline, 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 can view these logs using **Log Browse**.



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

- **Log View** allows you to download a specific filtered view.
- **Log Browse** allows you to download rolled logs. FortiAnalyzer also provides the option to upload logs to an FTP, SFTP, or SCP server on a scheduled basis.
- The CLI command `execute backup logs` sends everything to whatever device or devices you specify. FortiAnalyzer compresses the data before sending, so the transfer doesn't begin instantaneously. The device needs to process the logs and store them in an archive, which can take some time. This bulk data dump may include a lot of data, so make sure your server has enough disk space.

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

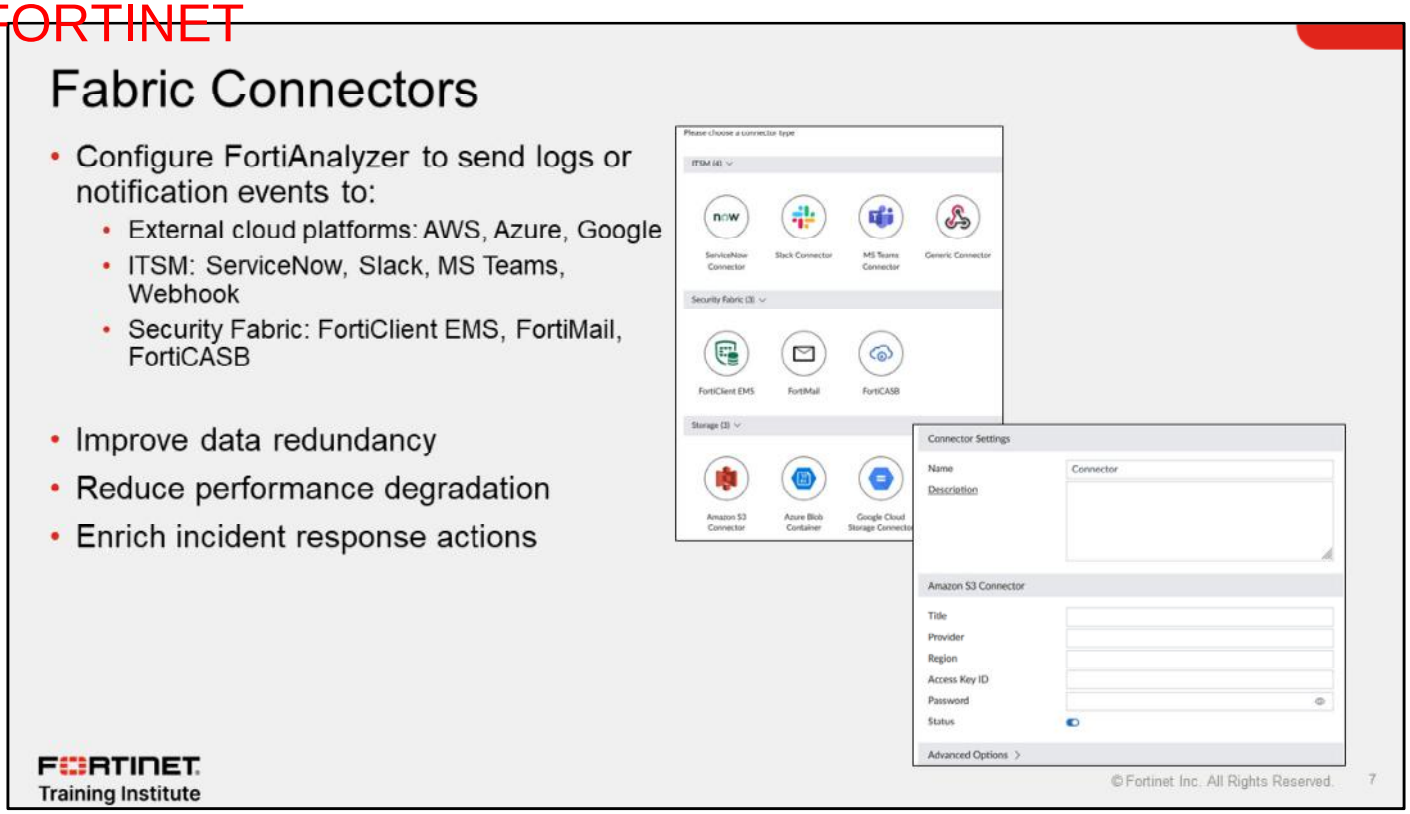


You can configure FortiAnalyzer to upload logs to a remote server whenever a log file is rolled, or based on a daily schedule.

The supported protocols for the remote server are FTP, SFTP, and SCP.

If you enable **Upload log files in compressed file format**, the device log files are compressed before uploading, which results in smaller logs and faster upload times.

If you enable **Delete log files are uploading**, the device log files are removed from FortiAnalyzer after they have been uploaded to the server.



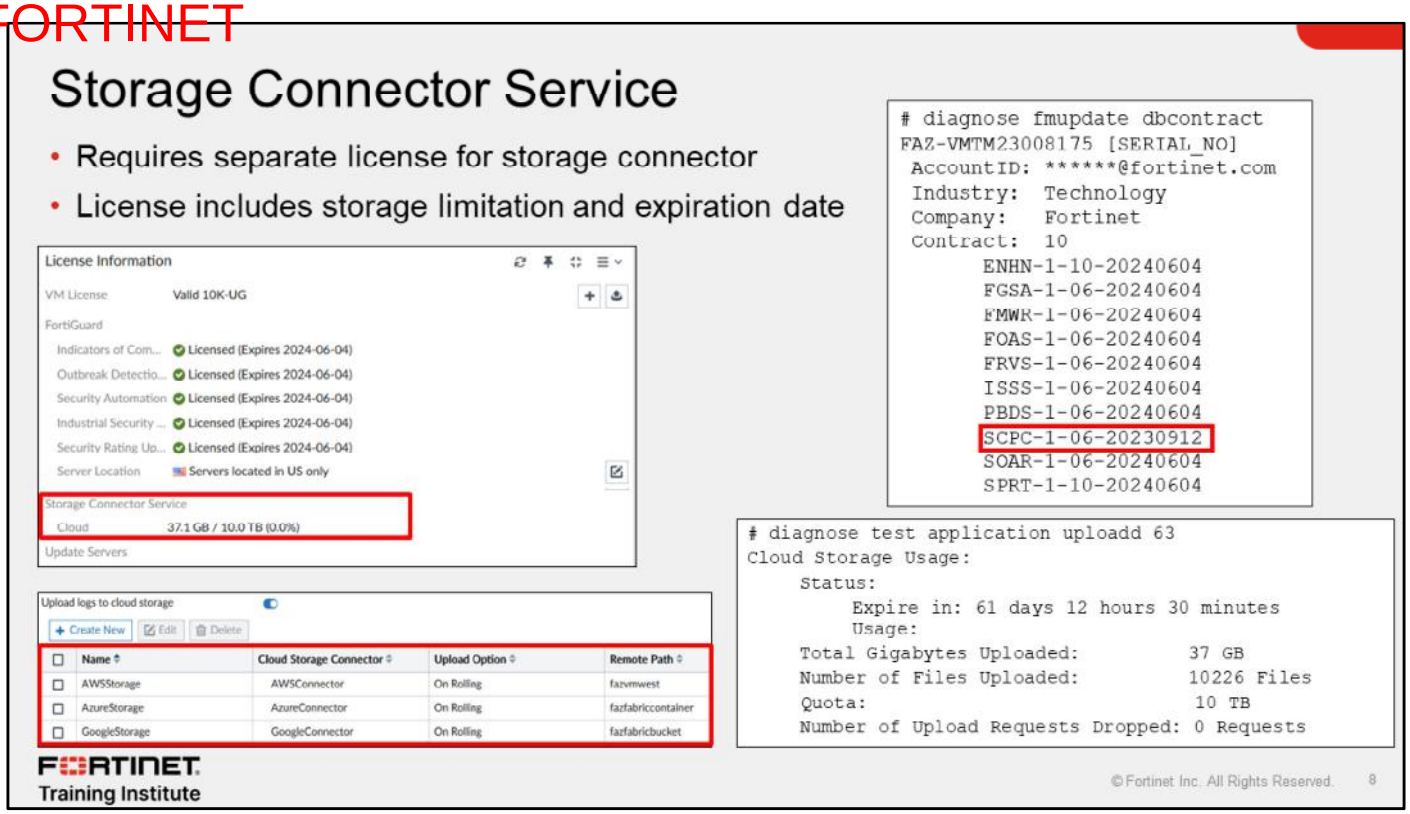
FortiAnalyzer supports integration with other products through fabric connectors.

Storage connectors allow you to back up data to public cloud accounts in Amazon S3, Microsoft Azure, and Google Cloud.

Support for this feature requires you to configure the following components on FortiAnalyzer:
- Create a fabric connector for Amazon S3, Microsoft Azure, or Google Cloud.
- Configure cloud storage.

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.

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



In order to send logs to cloud platforms, you must purchase a separate license for the **Storage Connector Service**. This license includes:

- Storage limitation: amount of data that can be uploaded to the cloud platform
- Expiry date: the date up to which you can send the storage data. This is usually valid for one year.

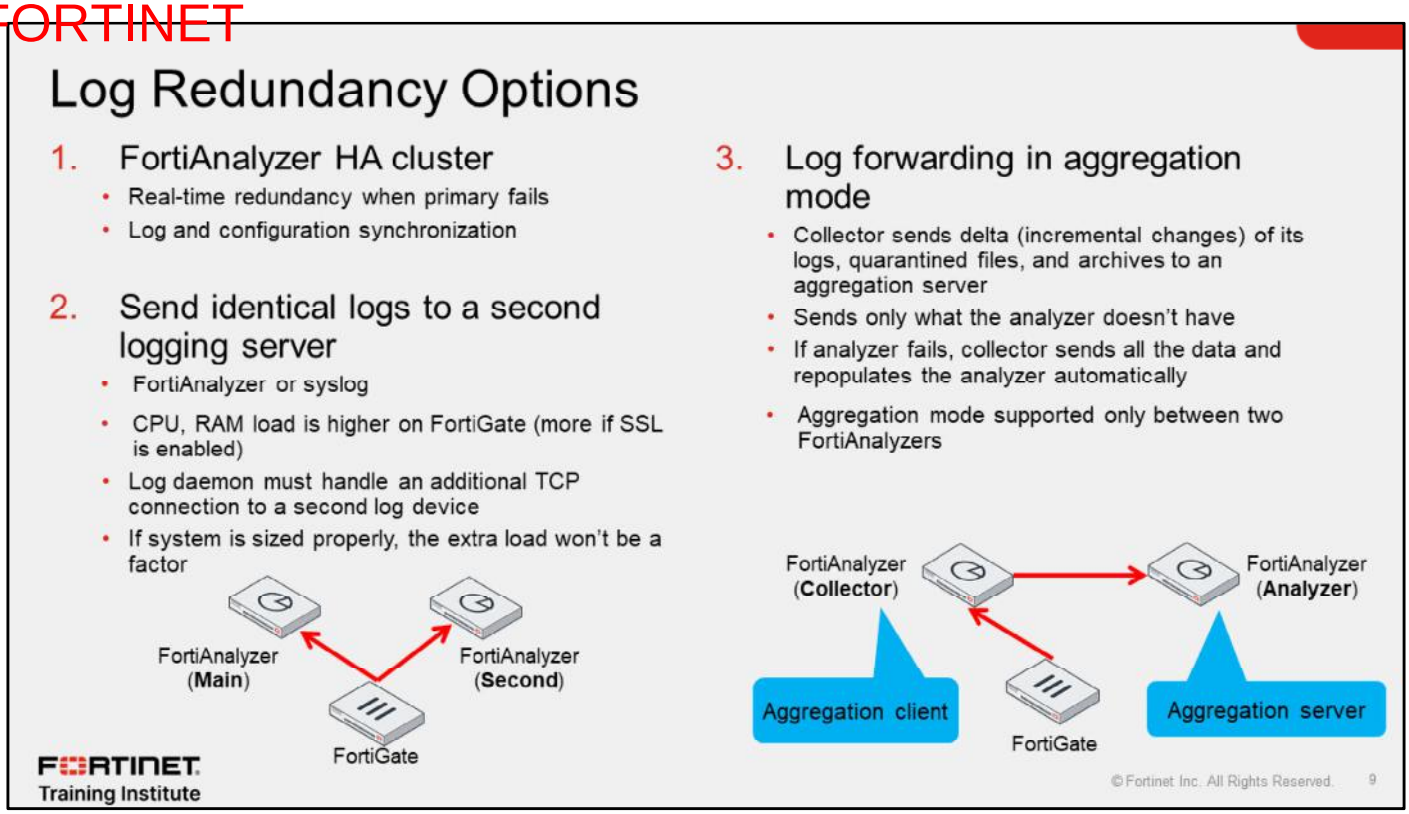
This license *does not* include the storage used on the cloud provider. It includes only the amount of data that you can transfer. To configure this feature, you must have an account with permissions to access the cloud storage. Refer to the *FortiAnalyzer Administration Guide* for more details.

Note that if uploaded logs reach data storage limitations before the license expires, you must renew the license in order to continue to use this service.

After the license is uploaded, you can enable the **Upload logs to cloud storage** feature under **System Settings** > **Advanced** > **Device Log Settings**, and then select the cloud storage platforms that the data will be sent to.

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

The `diagnose test application uploadd 63` command gives 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.

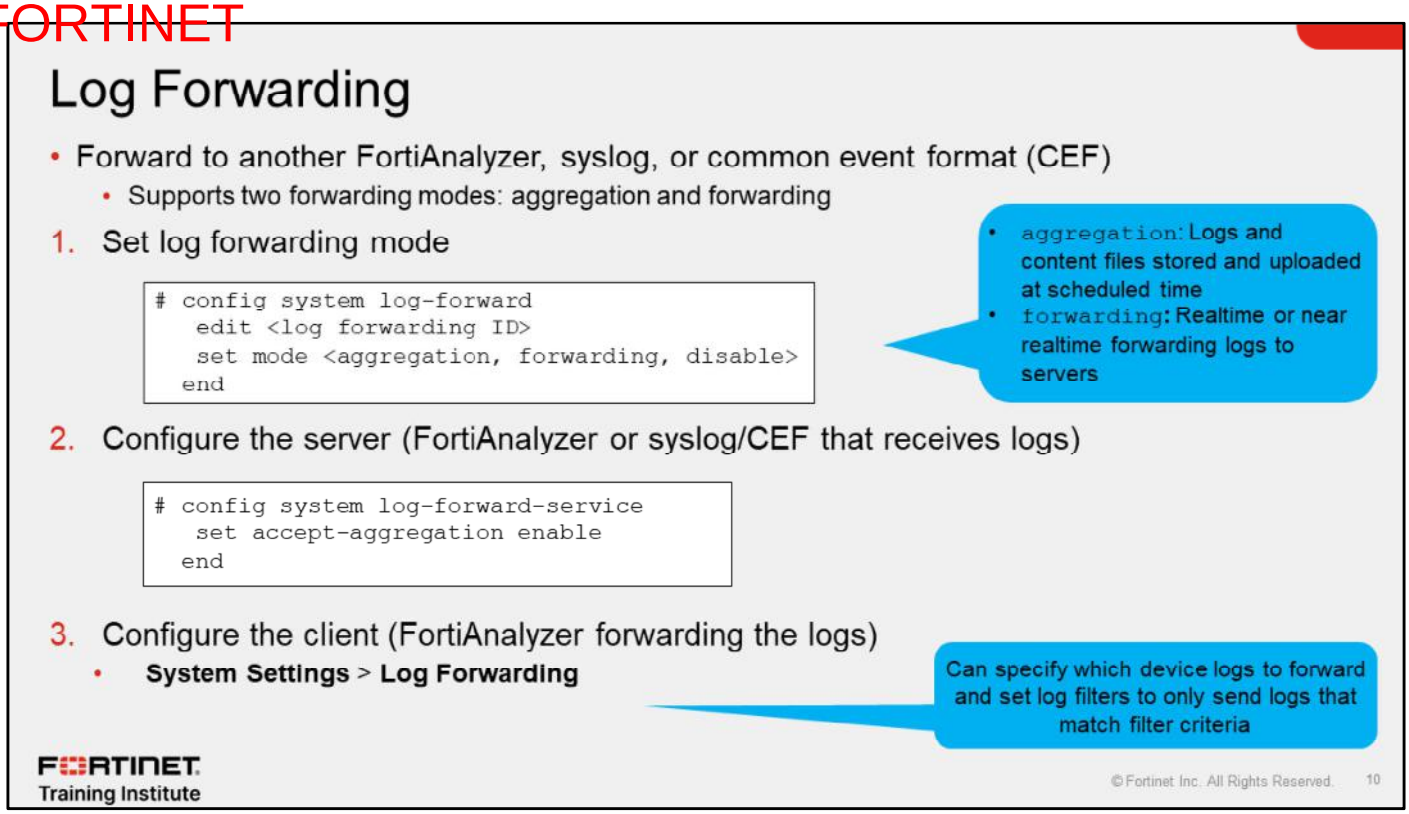


To protect your logs during log delivery, you can add redundancy to your environment. In a FortiGate-FortiAnalyzer environment, there are a few options.

One option is to configure a FortiAnalyzer HA cluster. FortiAnalyzer HA provides real-time redundancy when a FortiAnalyzer primary device fails. If the primary device fails, another device in the HA cluster is selected as the primary device. It 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.

The second 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 increases the load on the FortiGate device because the log daemon must handle an additional TCP connection to the second log device. However, with proper system sizing, this additional load is not a factor. This option is not available for smaller FortiGate devices that do not support a second device.

Another option is to set up log forwarding in aggregation mode. Generally, your central (aggregating) device is a larger FortiAnalyzer, but this is not a requirement. The collector sends a delta (incremental changes) of the logs 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 that is sent, and provides a level of redundancy. If there is a failure of the analyzer device, the collector sends all the data it has and repopulates the restored analyzer automatically. Aggregation mode is only supported between two FortiAnalyzer devices.

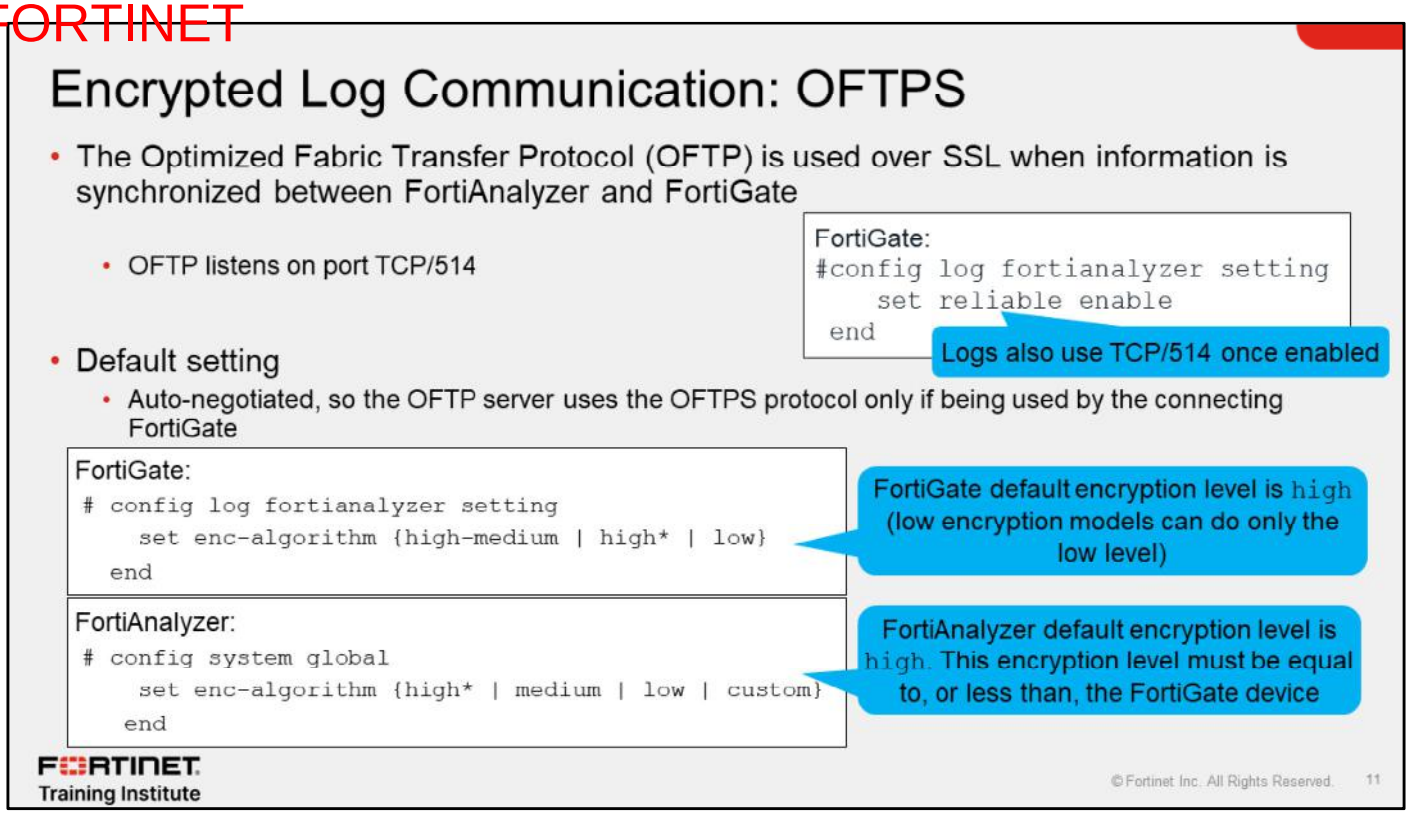


Log forwarding can run in modes other than aggregation mode, which is only applicable between two FortiAnalyzer devices. In forwarding mode, FortiAnalyzer can also forward logs in real-time mode to a syslog server (such as FortiSIEM), a Common Event Format (CEF) server, or another FortiAnalyzer. You can also forward logs to a public cloud service through an output plugin. The FortiAnalyzer that forwards logs to another plays the role of the client, while the recipient plays the role of the server.

To configure log forwarding, you must complete the following:

1. Set 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 only requires configuration on the client side. In aggregation mode, the FortiAnalyzer acting as the server must be configured to accept the logs from the client.
3. Configure the client (the FortiAnalyzer forwarding the logs). Here you can also specify which device logs to forward and set log filters to send only logs that match filter criteria.

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

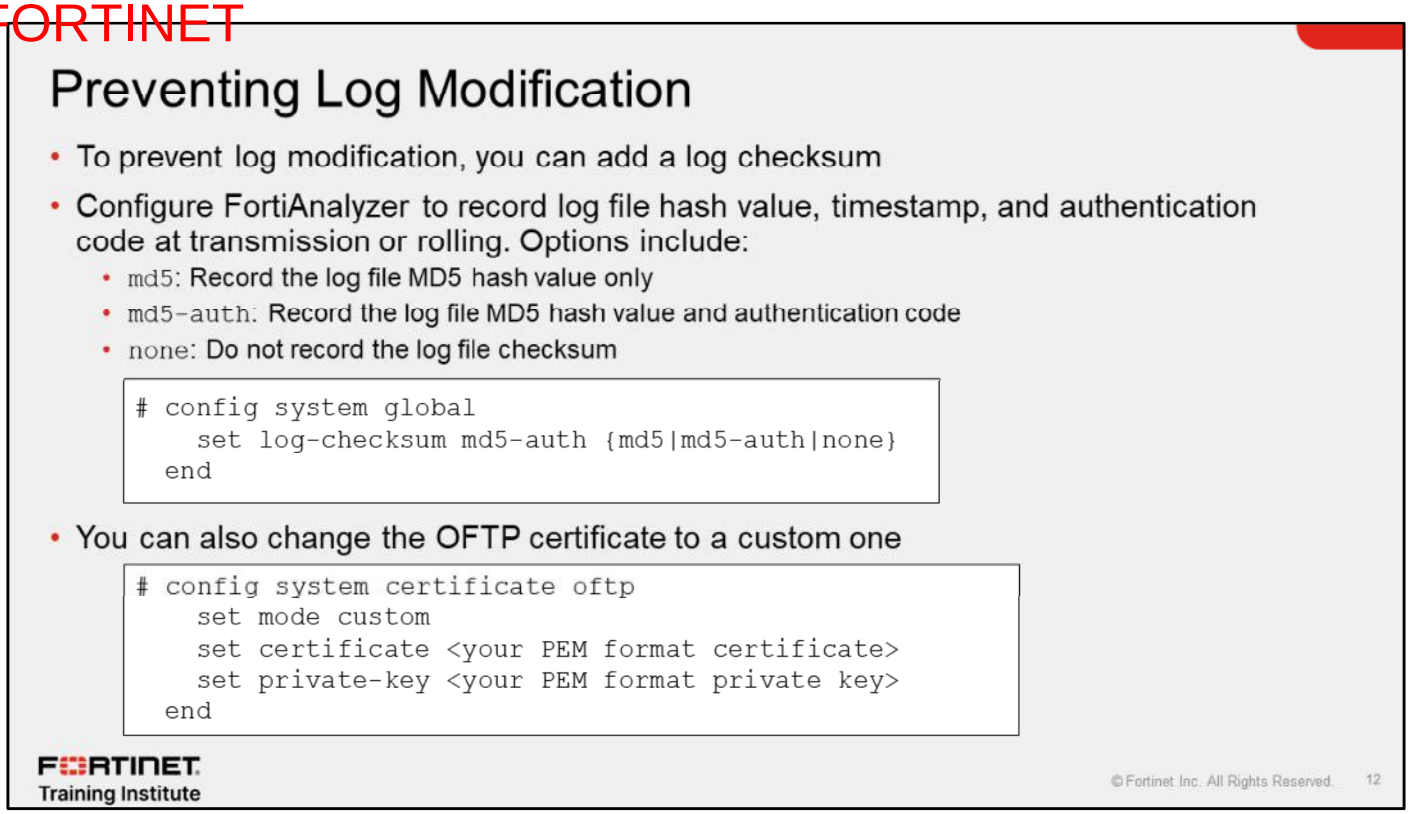


In the default configuration, there are two communication streams between FortiGate and FortiAnalyzer. One is the OFTP communication, which is encrypted, and the other is the log communication, which is not.

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.

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

SSL communications are auto-negotiated between FortiAnalyzer and FortiGate, so the OFTP server uses SSL-encrypted FTP only if it is being used by the connecting FortiGate. By default, FortiGate uses the *high* encryption level and FortiAnalyzer uses 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.

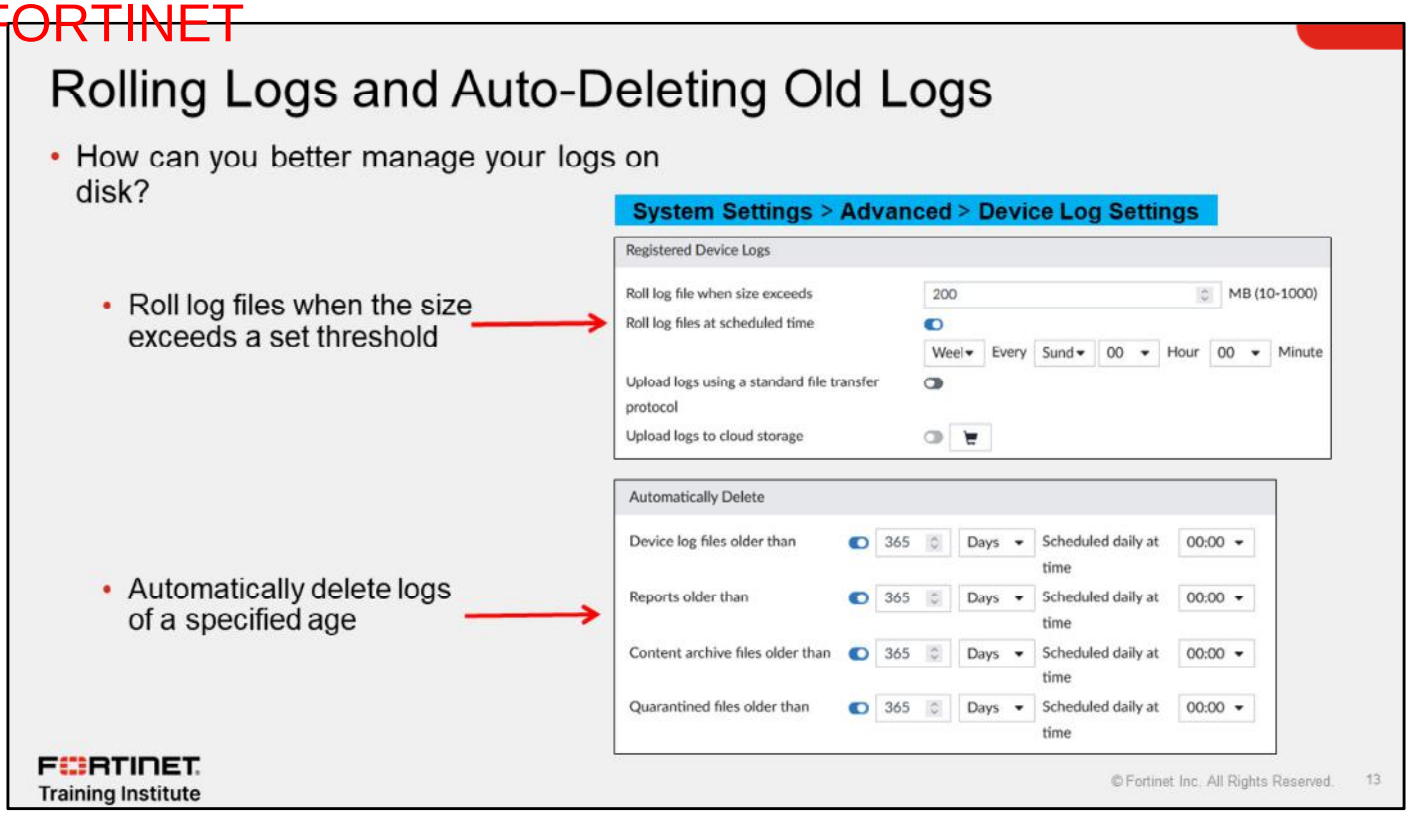


To prevent logs from being tampered with while in storage, you can add a log checksum using the `config system global` command. You can configure FortiAnalyzer to record a log file hash value, timestamp, and authentication code when the log is rolled and archived and when the log is uploaded (if that feature is enabled). This can also help against man-in-the-middle only 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 active on the FortiAnalyzer unit at all times. Therefore, you should carefully configure each policy. For example, if the disk utilization policy reaches its threshold before the global automatic file deletion policy for the FortiAnalyzer device, 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 logs regardless of the log storage settings associated with the device.

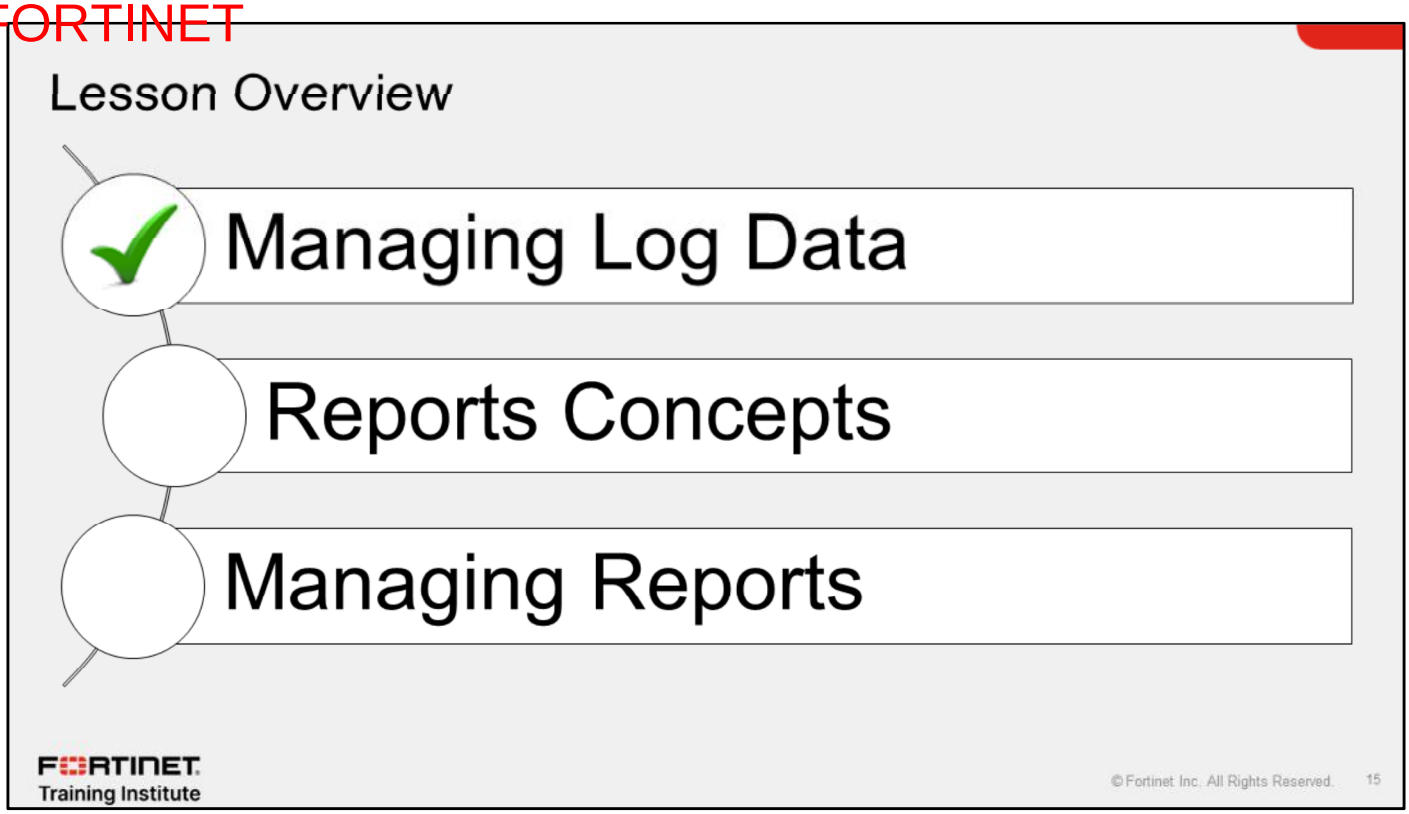
Knowledge Check

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

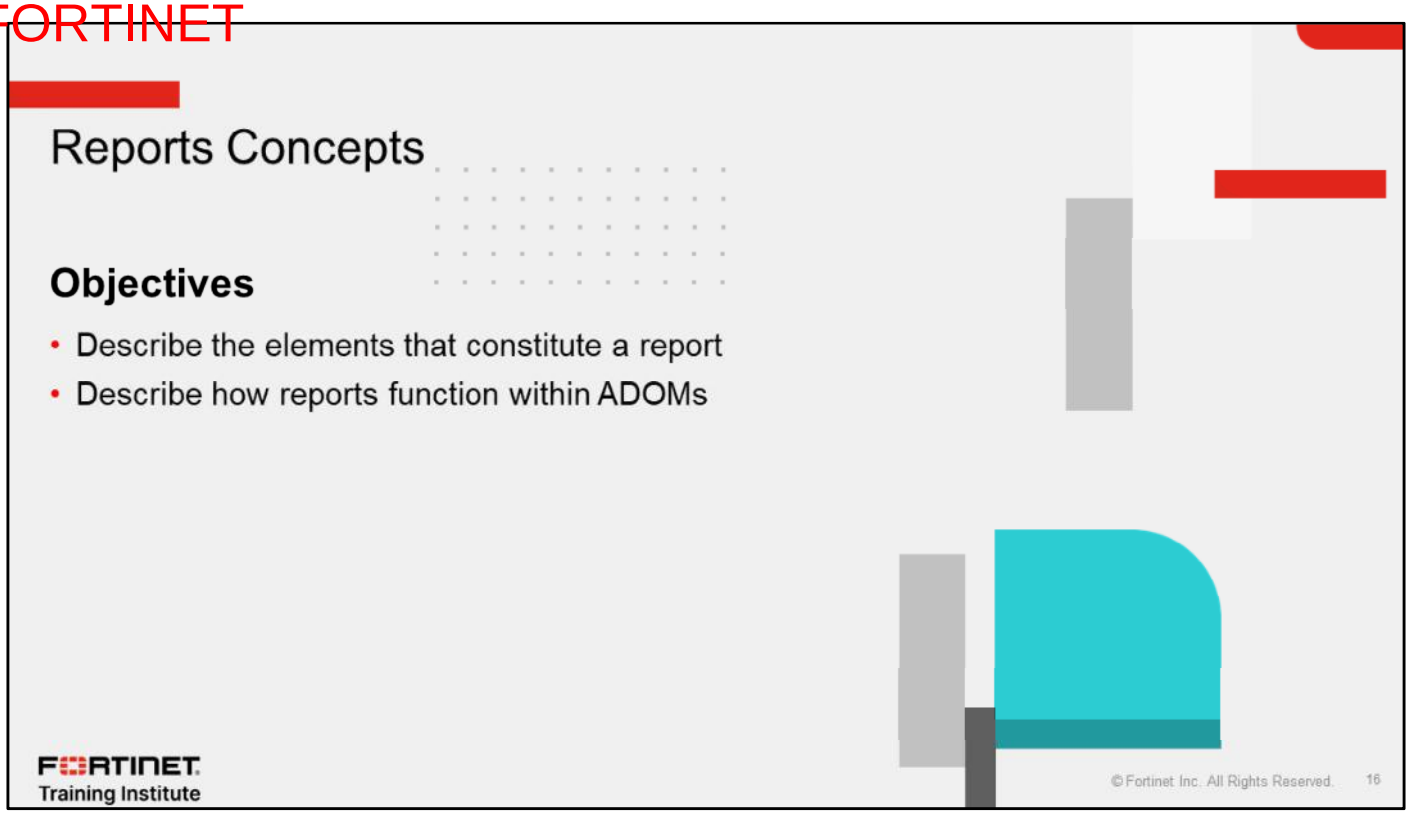
FORTINET Training Institute

 14



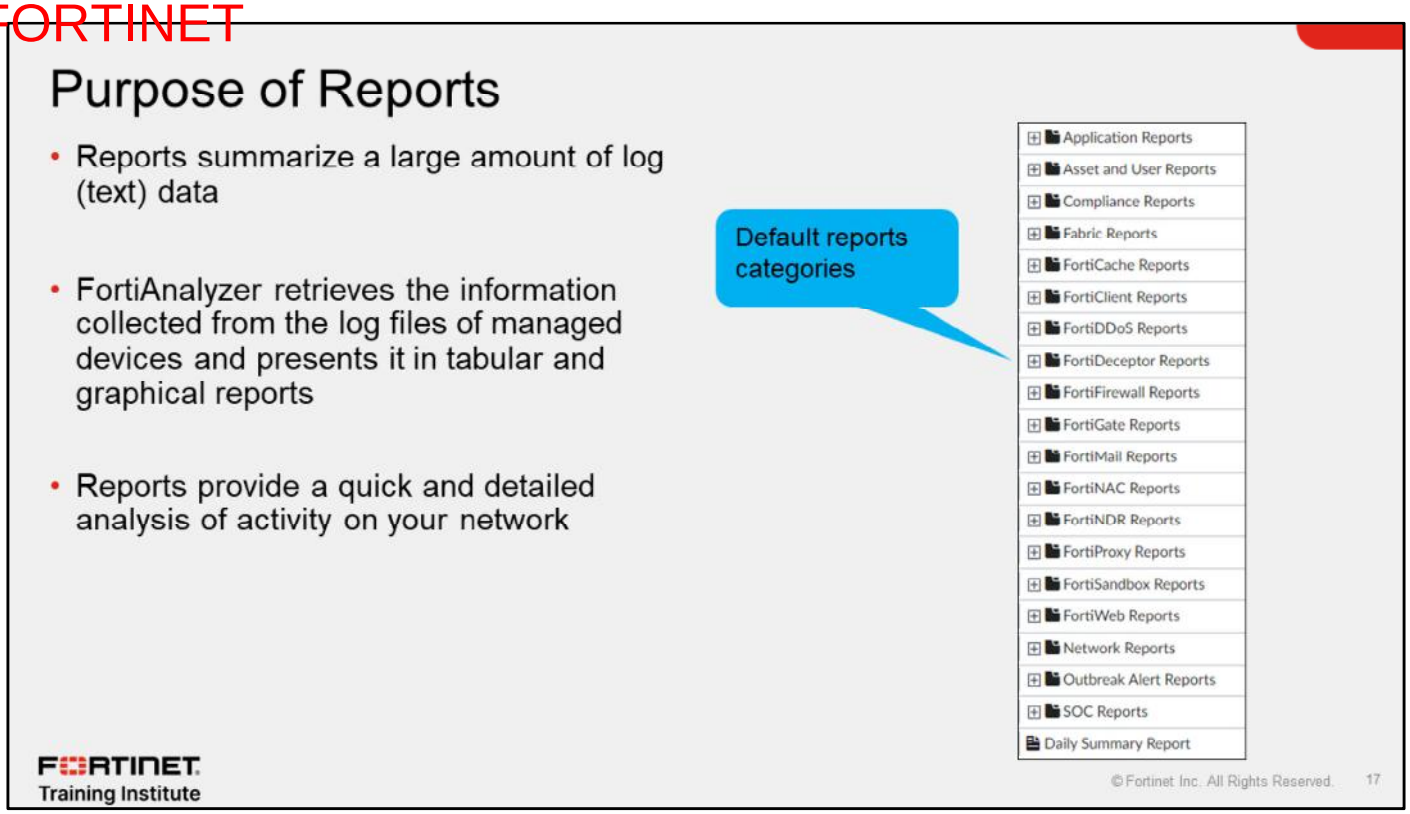
Good job! You now understand how to manage your log data.

Now you will learn about basic report concepts.



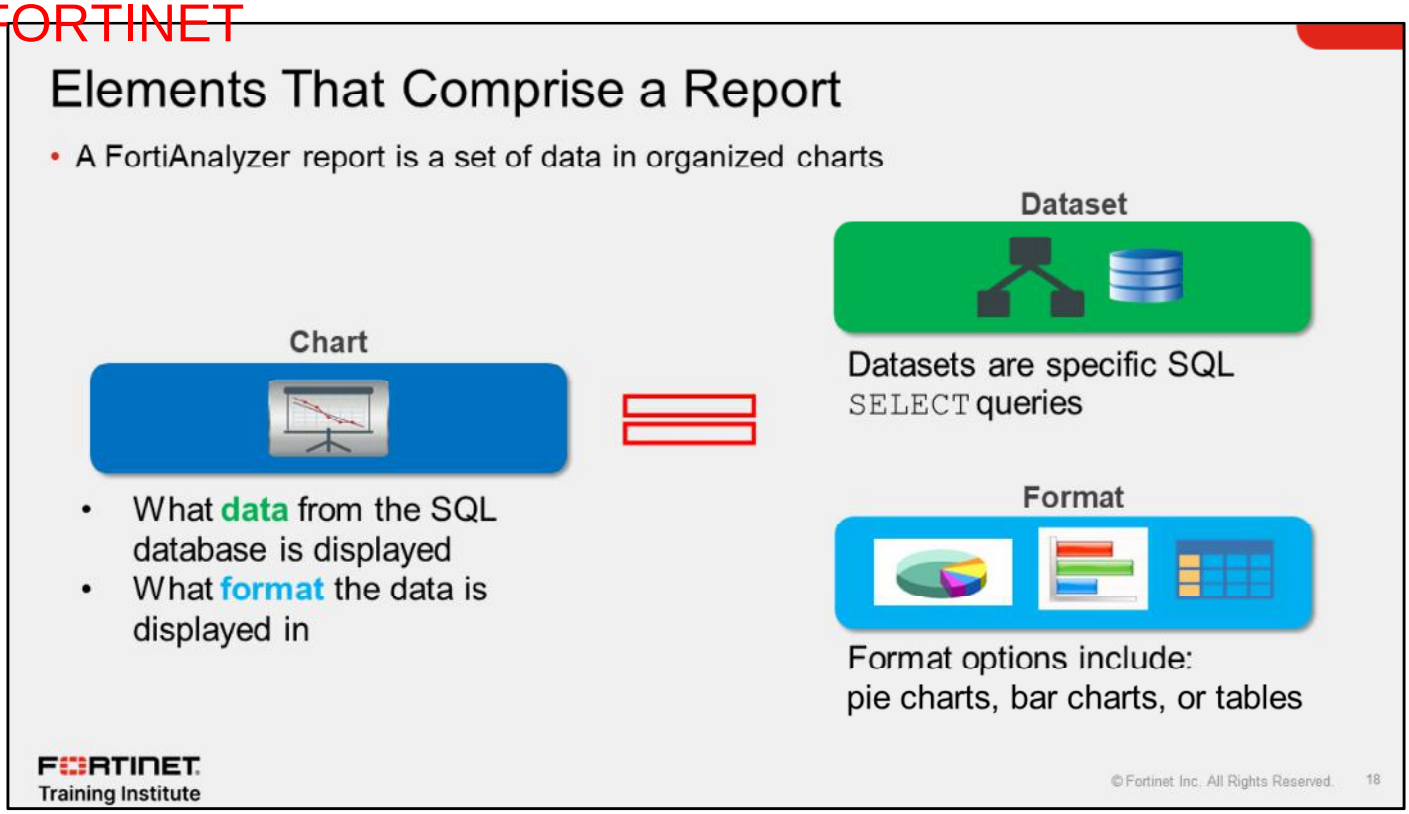
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding report concepts, you will be able to use reports more effectively to extract collected log data from your database.



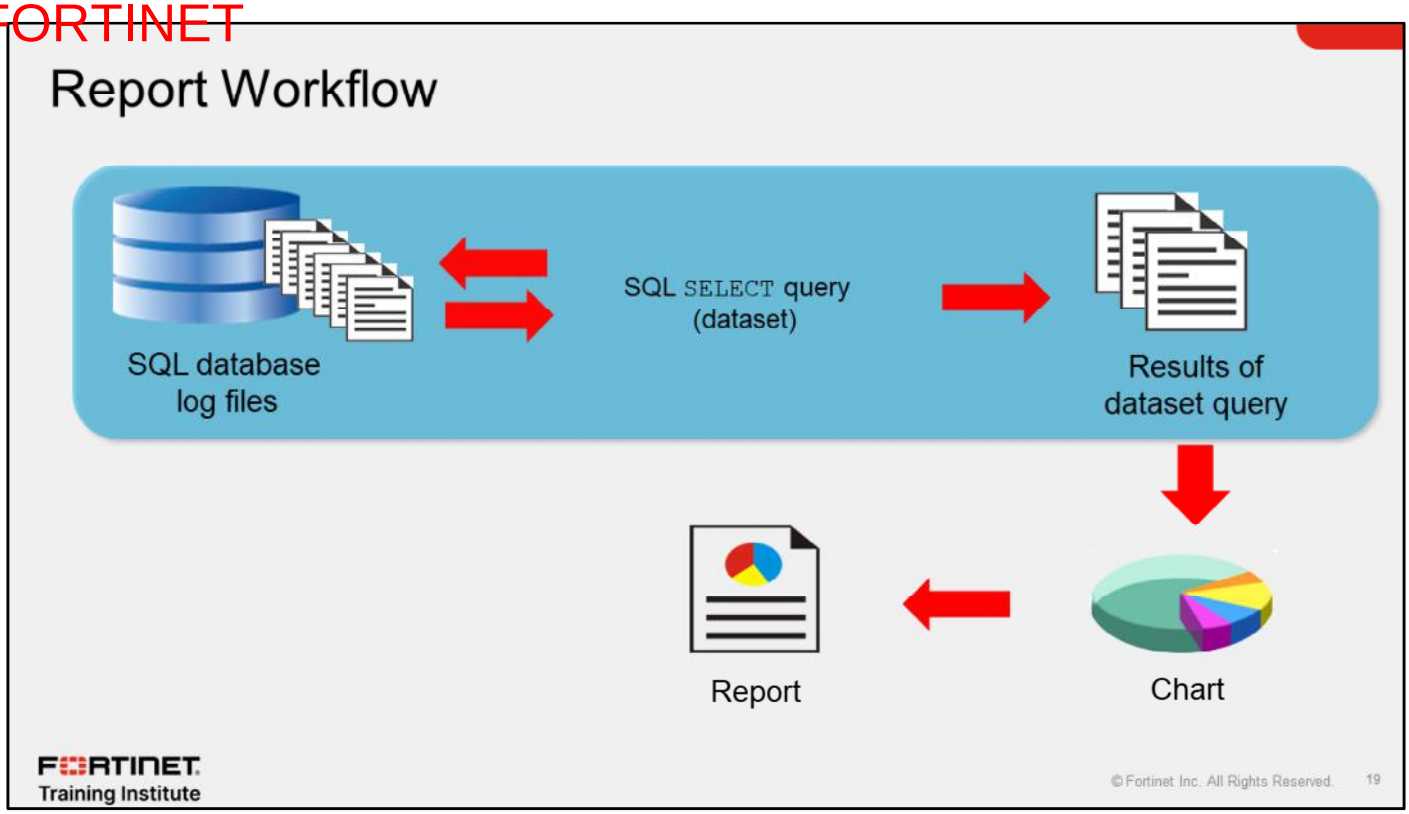
The purpose of a report is to summarize large amounts of logged data. Based on configured report parameters, FortiAnalyzer extracts data and presents it in a graphical manner that makes it easier—and quicker—to digest. The patterns and trends that reports reveal already exist as several points of data within your database, but it would be difficult and time consuming to manually locate, cross-reference, and analyze multiple log files, 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 then use that information to better understand your network or improve your network security.

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



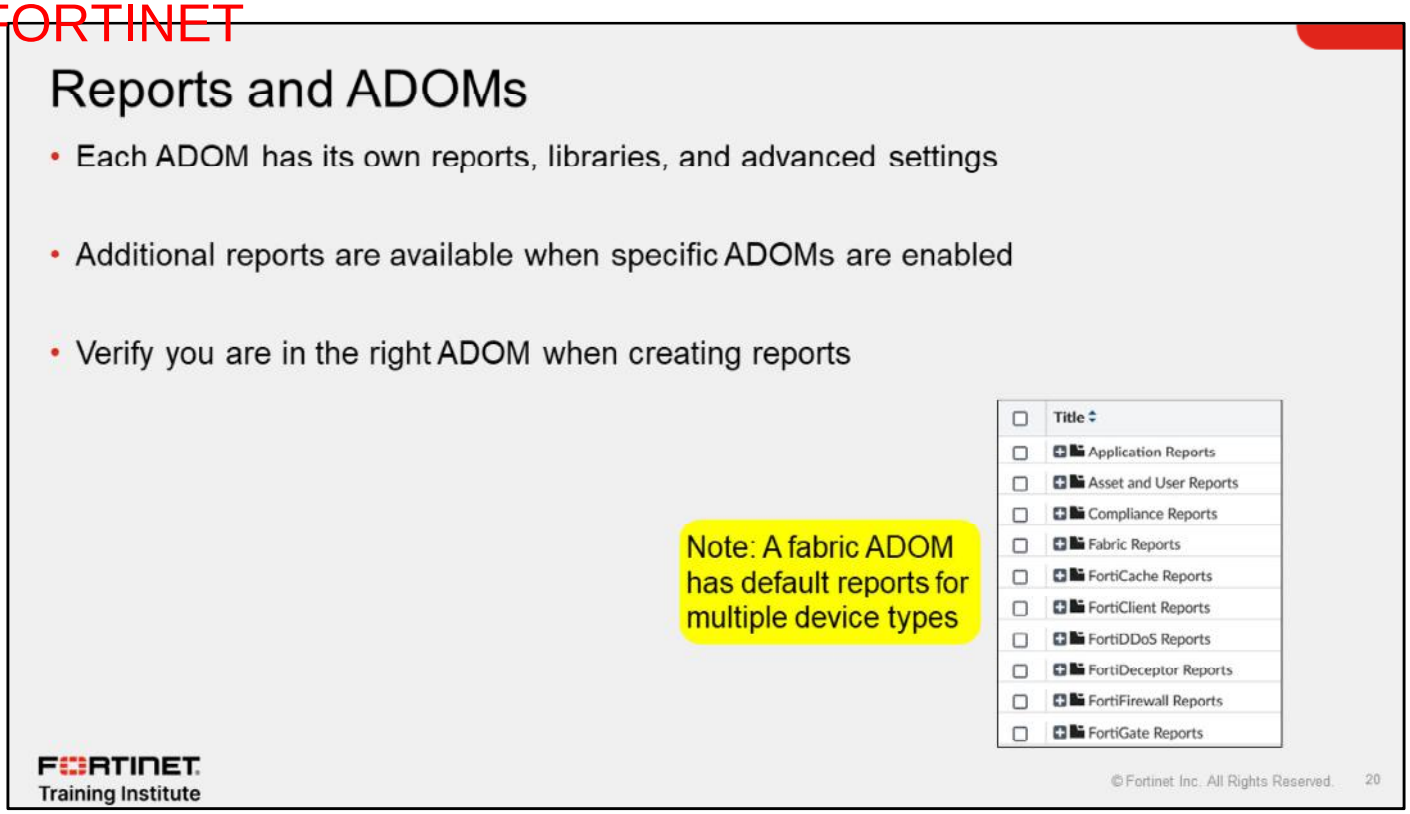
A FortiAnalyzer report is a set of data organized in charts. Charts consist of two elements:

- **Datasets**: SQL `SELECT` queries that extract specific data from the database
- **Format**: how the data is displayed (for example, pie charts, bar charts, or tables)



As the graphic on this slide shows, the SQL database contains all the logs. A SQL `SELECT` query polls the database for specific information. Based on the query, a subset of information stored in the logs is extracted.

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, make sure that you are in the correct ADOM before selecting a report.

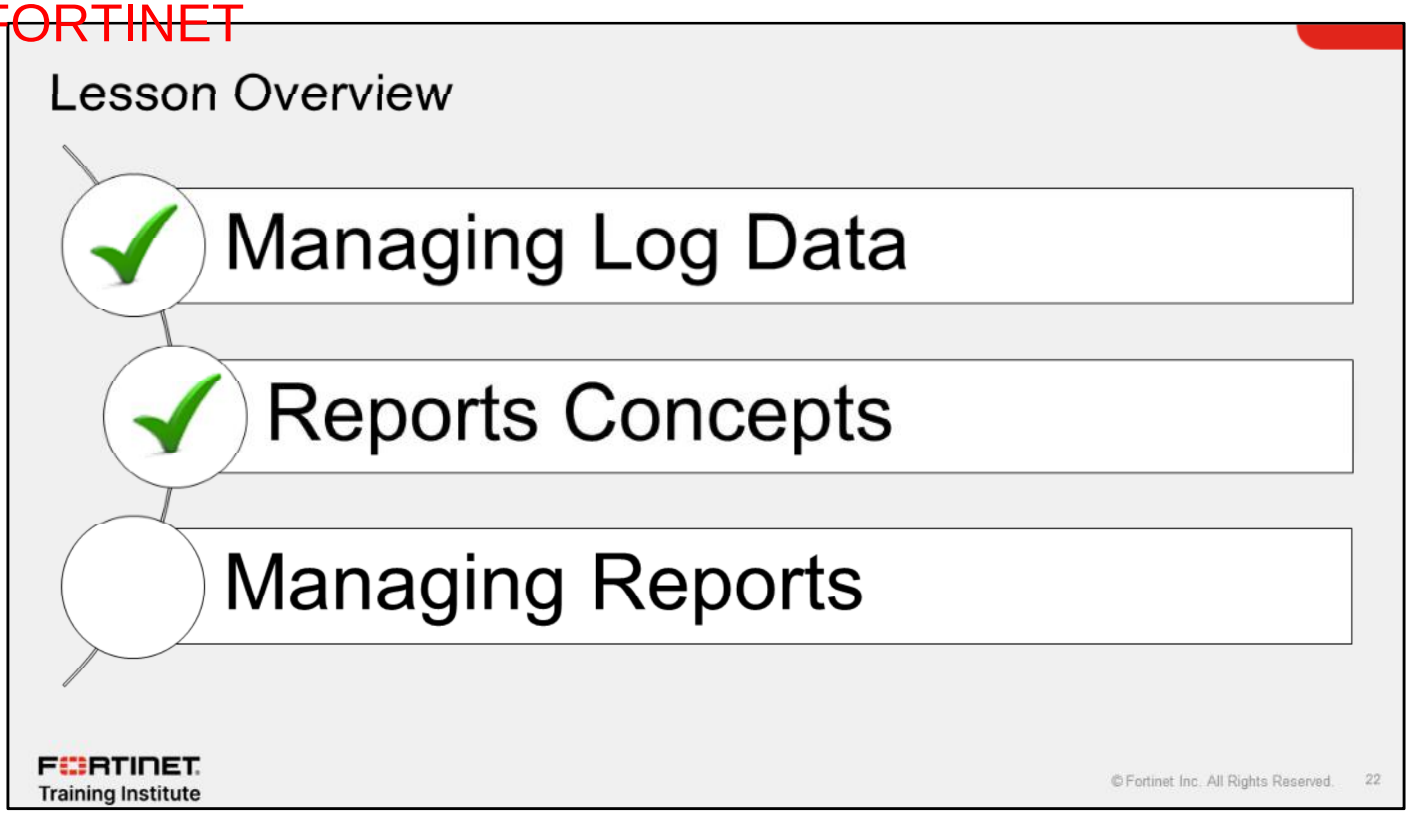
Additional reports for specific Fortinet devices are available only when you enable ADOMs. This slide does not show all the available default report types. You can configure and generate reports for these devices within their respective ADOMs. These devices also have device-specific charts and datasets.

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

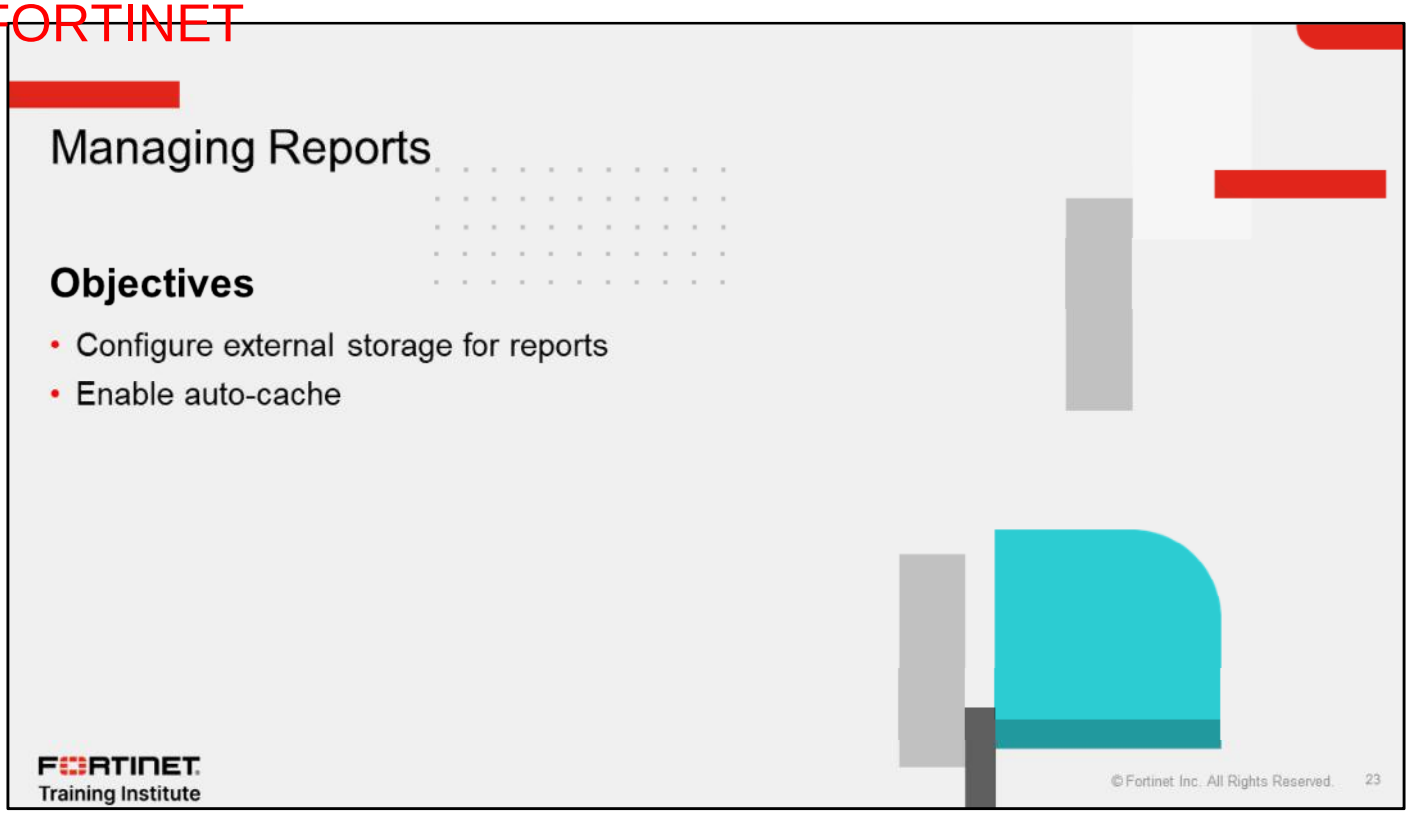
FORTINET Training Institute

 21



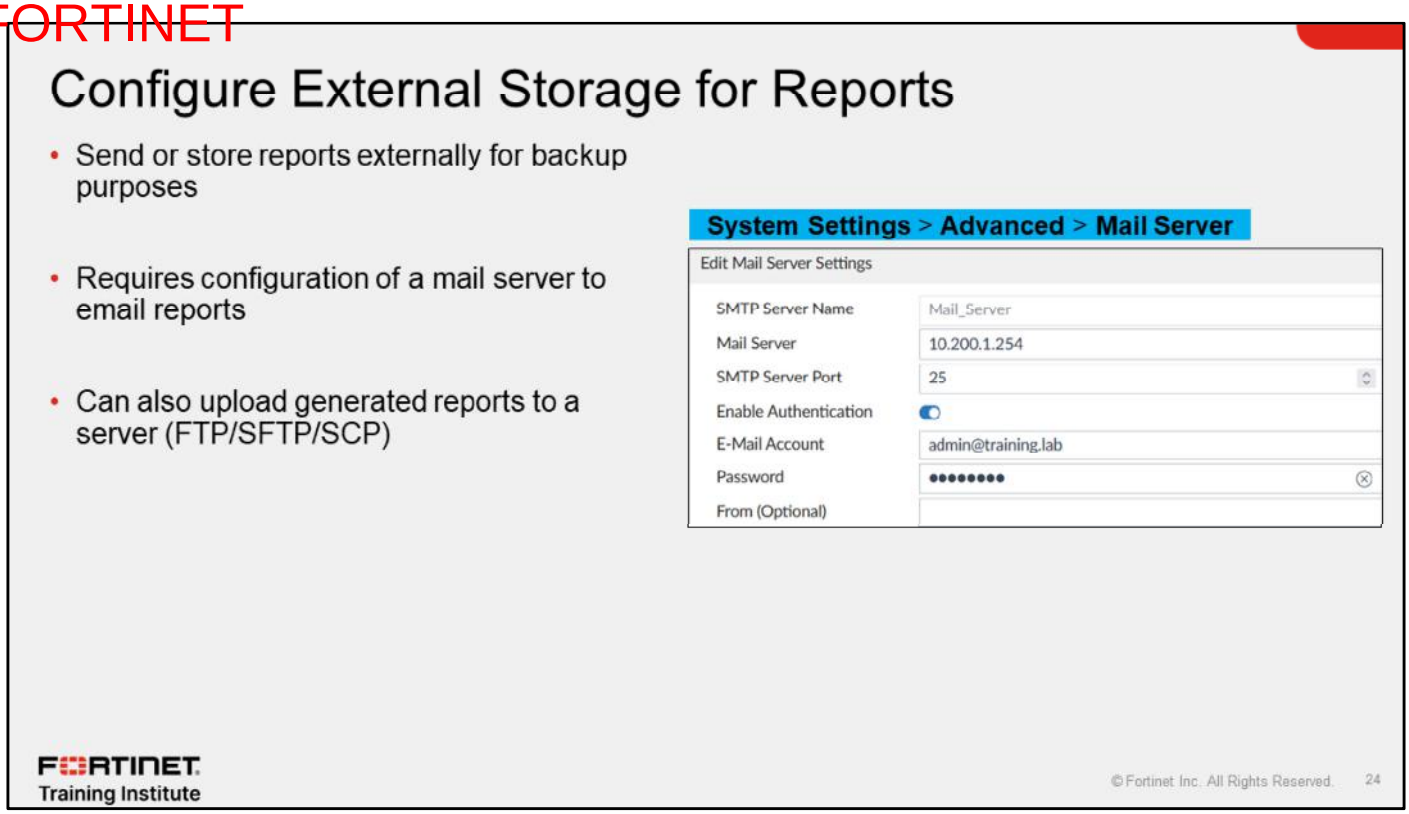
Good job! You now understand the basic concepts of reports on FortiAnalyzer.

Now, you will learn how to manage reports.



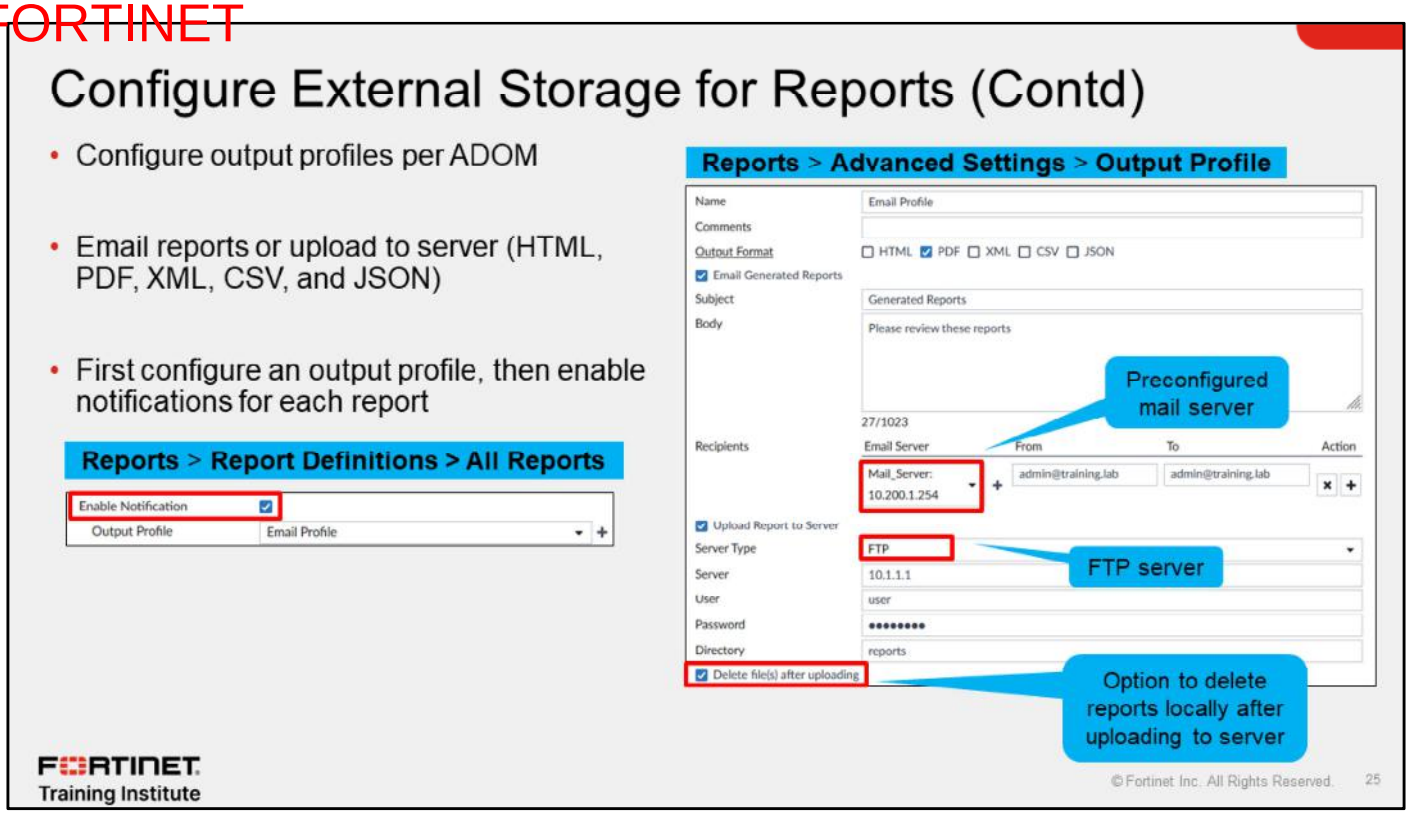
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in report management, you will be able to handle, store, and more efficiently control reports and report generation.



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

In order 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 shown on this slide. To upload logs to a server, you must first configure the mail server to accept connections from FortiAnalyzer.

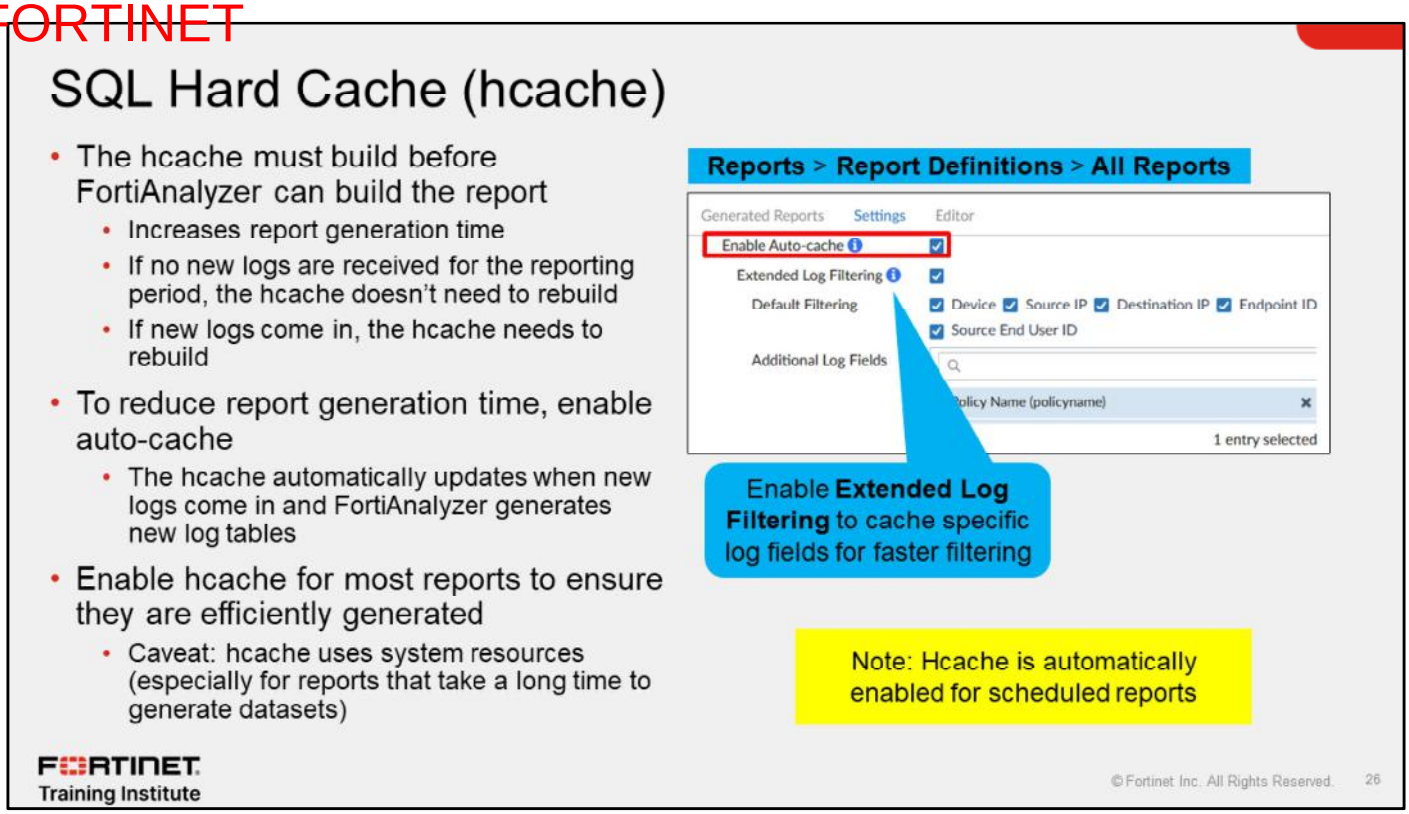


To send reports to an external location, each report must have notifications enabled and an appropriate output profile selected.

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, 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.

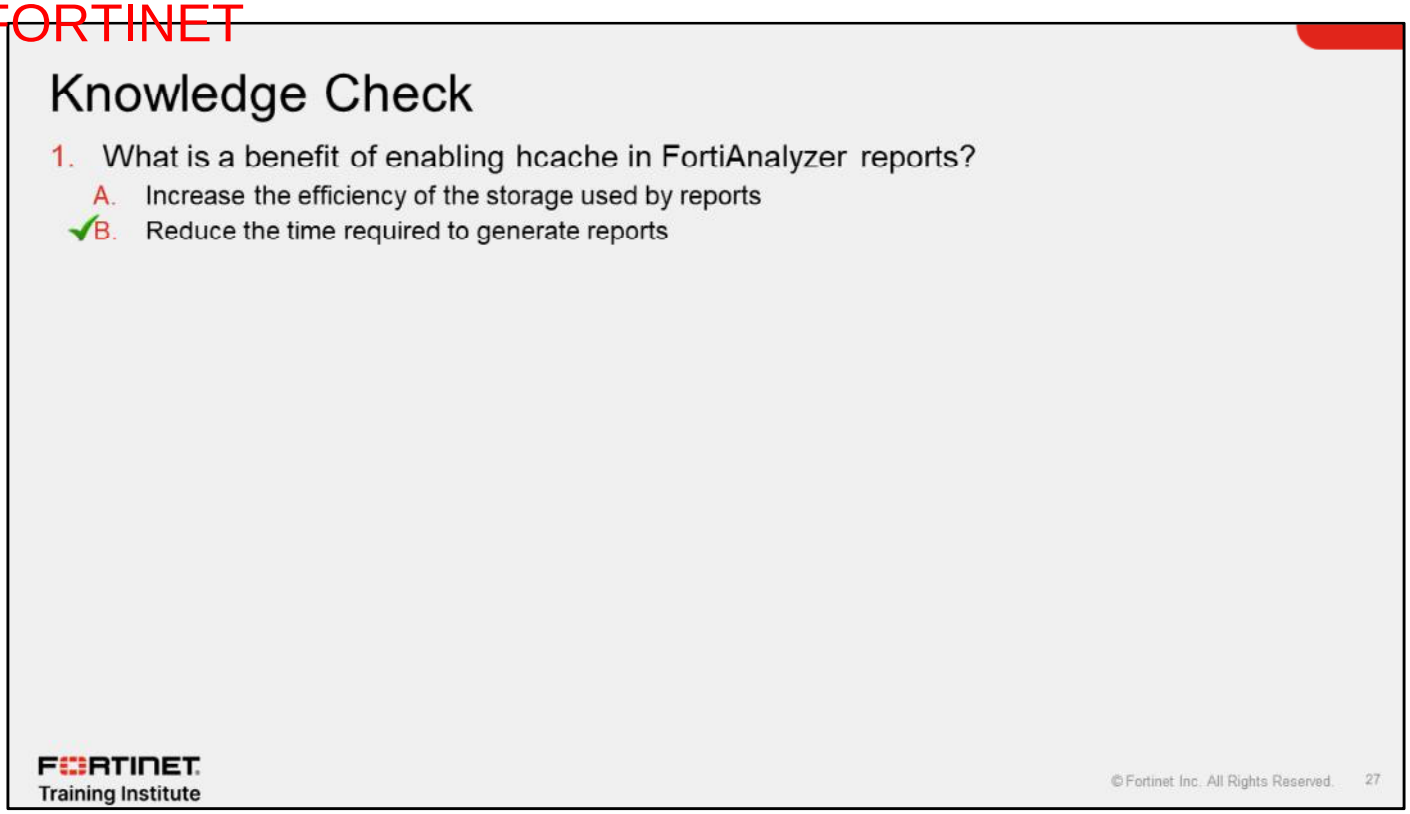


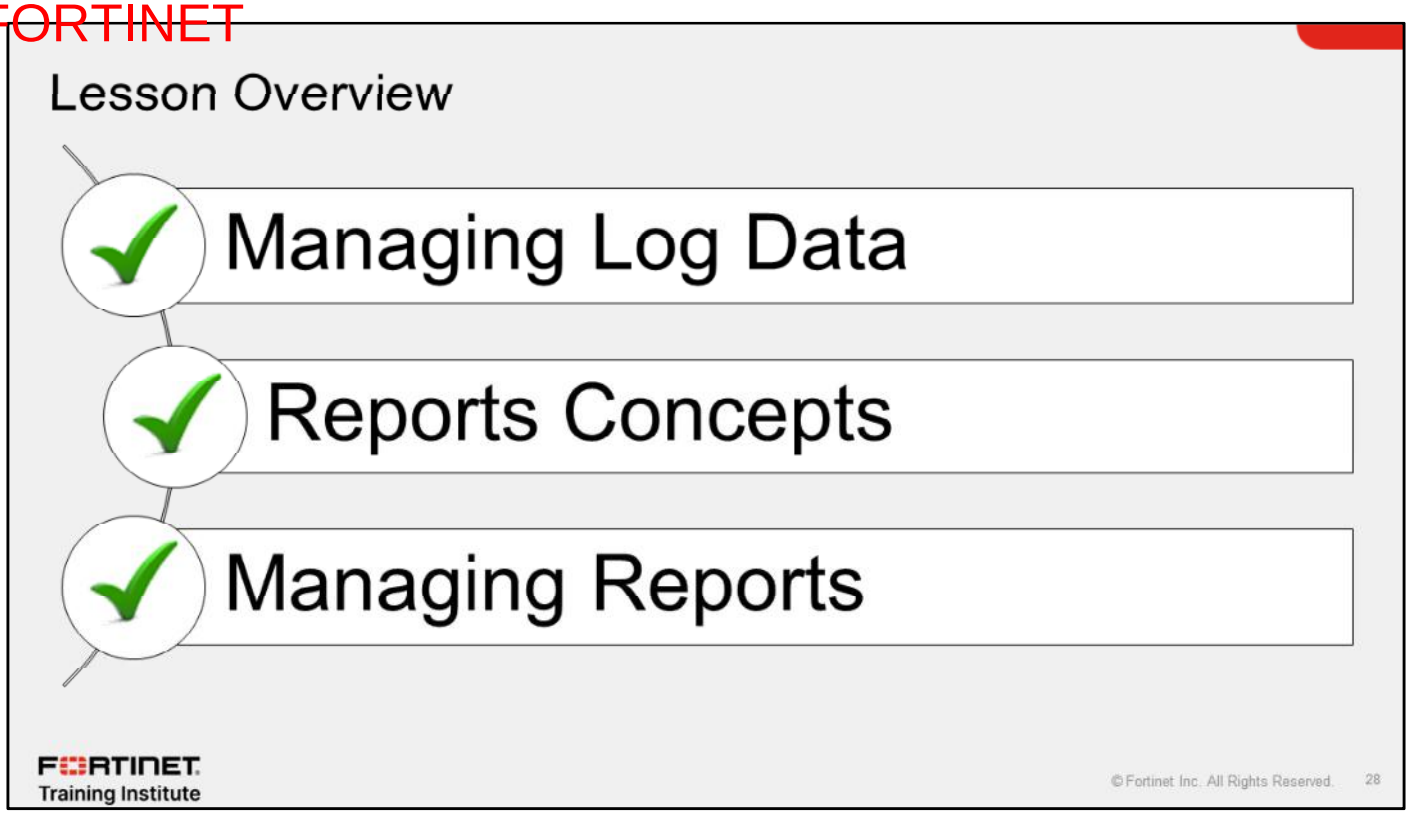
When a report generates, the system builds the charts from precompiled SQL hard-cache data, known as the hcache. If the hcache is not built when you run the report, the system must create the hcache first and then build the report. This adds time to the report generation. However, if FortiAnalyzer does 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 the report performance and reduce report generation time, you can enable auto-cache in the settings of the report. In this case, the hcache is automatically updated when new logs come in and new log tables are generated.

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 reports are efficiently generated. 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.

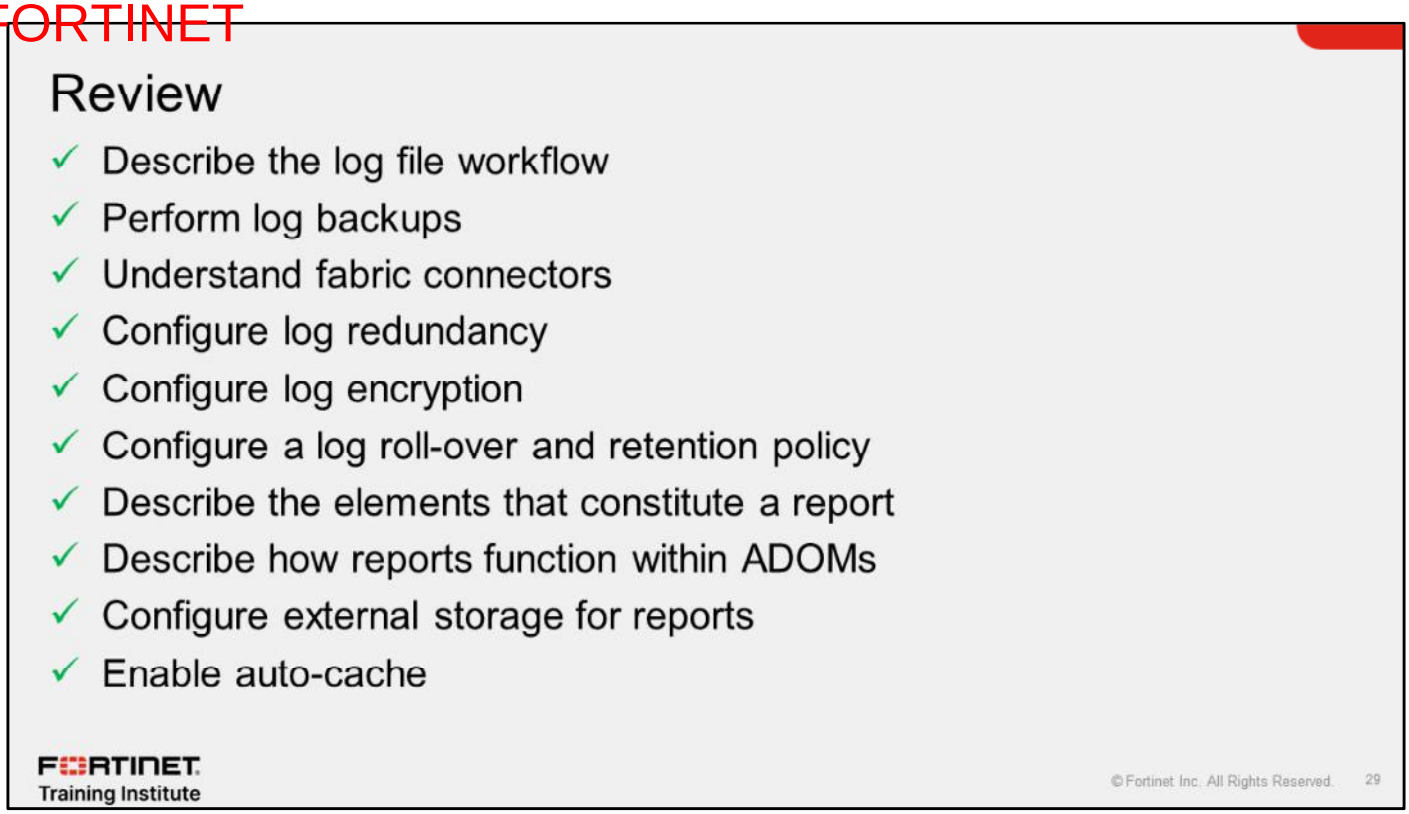
Additionally, you can opt for enabling **Extended Log Filtering** to cache specific log fields for faster filtering.





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.