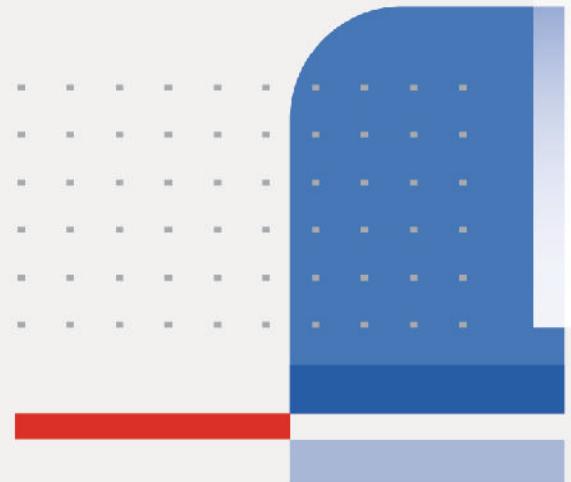


**DO NOT REPRINT**  
© FORTINET

# FortiAnalyzer Administrator Study Guide

FortiAnalyzer 7.6

**FORTINET®**  
Training Institute



# **DO NOT REPRINT**

## **© FORTINET**

**Fortinet Training Institute - Library**

<https://training.fortinet.com>

**Fortinet Product Documentation**

<https://docs.fortinet.com>

**Fortinet Knowledge Base**

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

**Fortinet Fuse User Community**

<https://community.fortinet.com/>

**Fortinet Forums**

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

**Fortinet Product Support**

<https://support.fortinet.com>

**FortiGuard Labs**

<https://www.fortiguard.com>

**Fortinet Training Program Information**

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

**Fortinet | Pearson VUE**

<https://home.pearsonvue.com/fortinet>

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

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



## TABLE OF CONTENTS

<b>01 Introduction and Initial Configuration.....</b>	<b>4</b>
<b>02 Administration and Management.....</b>	<b>39</b>
<b>03 ADOMs and HA.....</b>	<b>73</b>
<b>04 Managing Devices.....</b>	<b>112</b>
<b>05 Logs and Reports Management.....</b>	<b>156</b>
<b>Supplementary SQL and Datasets.....</b>	<b>198</b>

**DO NOT REPRINT**

© FORTINET



# FortiAnalyzer Administrator

## Introduction and Initial Configuration

 FortiAnalyzer 7.6

Last Modified: 16 July 2025

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

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

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview

Key Features and Concepts

Initial Configuration

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

**DO NOT REPRINT****© FORTINET**

## Key Features and Concepts

### Objectives

- Describe the purpose of FortiAnalyzer
- Describe FortiAnalyzer operating modes
- Describe logging in a Security Fabric environment
- Describe FortiAnalyzer Fabric
- Describe ADOMs



© Fortinet Inc. All Rights Reserved.

3

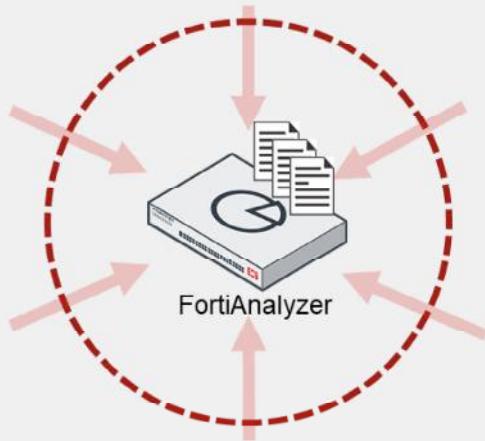
After completing this section, you should be able to achieve the objectives shown on this slide.

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

**DO NOT REPRINT**  
© FORTINET

## Centralized Log Repository

- FortiAnalyzer aggregates log data from one or more Fortinet devices
- Single view of security events taking place on a range of devices



### Supported devices:

- FortiGate/FortiCarrier
- FortiAnalyzer
- FortiCache
- FortiClient
- FortiDDoS
- FortiMail
- FortiManager
- FortiNAC
- FortiSandbox
- FortiSOAR
- FortiWeb
- Syslog
- Chassis

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](http://docs.fortinet.com).

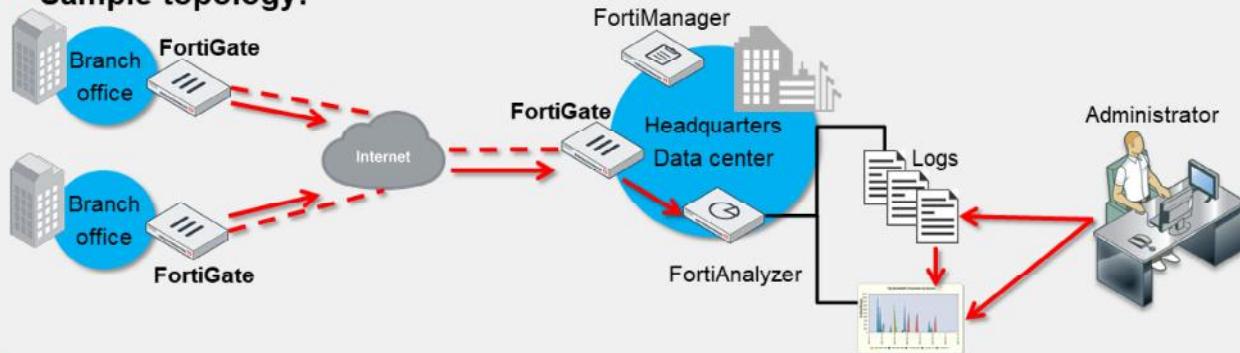
**DO NOT REPRINT**  
© FORTINET

## Centralized Log Repository (Contd)

### Workflow:

1. Registered devices send logs to FortiAnalyzer
2. FortiAnalyzer buffers, reorganizes, and stores the logs
3. Administrators:
  - View and search the logs
  - Configure, request, and view reports (based on log data)

### • Sample topology:



**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

5

The logging and reporting workflow operates as follows:

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

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

**DO NOT REPRINT****© FORTINET**

## Reports, Events, and Content Archiving

- **Reports**

- Network-wide reporting of events, activities, and trends of devices
- Archived, filtered, and mined for compliance or historical analysis purposes

- **Events**

- Identify and react to security threats quickly when configured conditions are met
- View events through **Event Monitor** (on the GUI), email, SNMP, or syslog
- Events that require further investigation can be used to generate new incidents

- **Content archiving**

- Simultaneously logs and archives full or summary copies of content transmitted over the network (email, FTP, NNTP, and web traffic)
- Typically used to prevent sensitive information from leaving your network



© Fortinet Inc. All Rights Reserved.

6

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Automation, IR, and Advanced Threat Detection

- **Automation**

- Automates routine tasks
- Includes automating responses to security incidents, generating reports, and adjusting security policies based on network behavior

- **Incidence response**

- Provides real-time detection and response capabilities for incidents
- Provides comprehensive visibility into network traffic and security events and correlates and analyzes events generated from all Fortinet devices
- Generates alerts when security events occur

- **Advanced threat detection**

- Integrates with FortiGuard Labs to provide real-time information on emerging threats and vulnerabilities
- Analyzes and correlates threat data from multiple sources, including third-party threat feeds



© Fortinet Inc. All Rights Reserved.

7

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

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

In incident response, FortiAnalyzer provides real-time detection and response capabilities. It provides comprehensive visibility into network traffic and security events and correlates and analyzes events generated from all Fortinet devices. This consolidates visibility to provide an accurate picture of security threats.

FortiAnalyzer generates alerts when security events occur, such as when a user attempts to access a restricted website.

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

**DO NOT REPRINT****© FORTINET**

## Deployment Options

### Hardware



- High-volume data processing
- 500 GB/day to 20,000 GB/day

### Virtual Machine



- Public or private cloud deployments
- Stackable daily log limits (GB/day)

### FortiAnalyzer Cloud



- SaaS-based model
- Stackable daily log limits (GB/day)
- Easy deployment and auto-scalable

FortiAnalyzer offers various deployment options to suit various organizational needs.

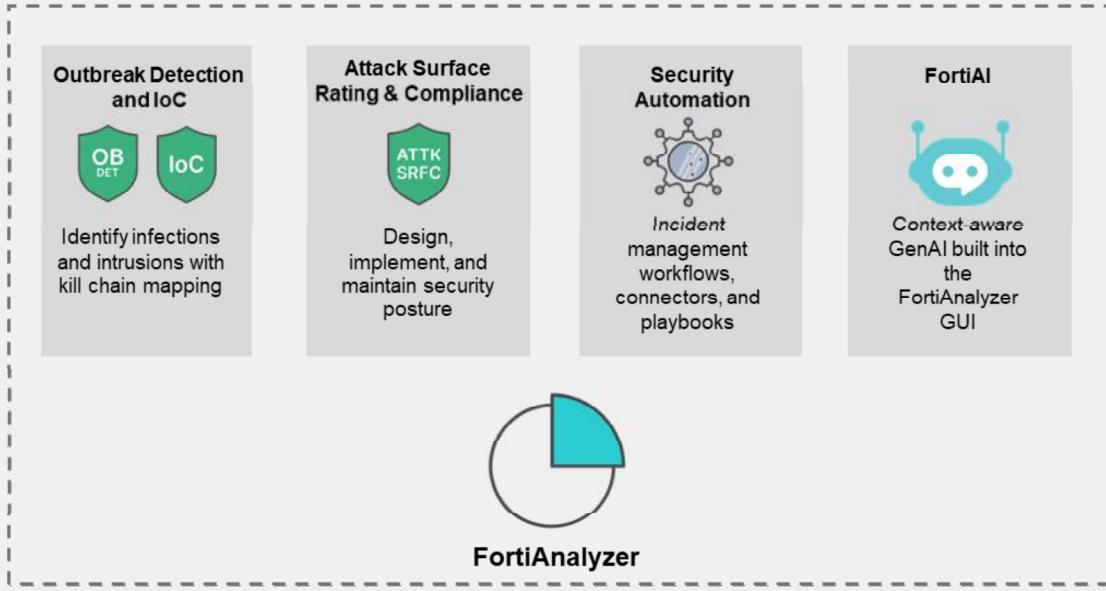
The hardware-based appliances offer different capacities with various performance levels. They are suitable for organizations that prefer on-premises deployments and have specific storage and processing requirements. The higher-end model, especially FortiAnalyzer Big Data, can handle high log volumes.

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

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

**DO NOT REPRINT****© FORTINET**

## FortiGuard Services



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

9

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

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

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Database Language Support

- FortiAnalyzer supports SQL for logging and reporting
- FortiAnalyzer inserts log data into the SQL database for log view and report generation
- Starting in version 7.6.0, FortiAnalyzer stores logs in a ClickHouse database rather than in a Postgres SQL database
- *Advanced reporting capabilities require some knowledge of SQL, datasets, and databases*



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

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

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

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

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

**DO NOT REPRINT**  
© FORTINET

## FortiAnalyzer Operating Modes—Analyzer

Dashboard > System Information

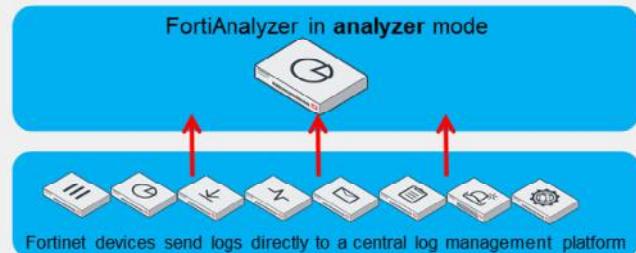
Operation Mode

Analyzer

Collector

Analyzer is the default mode

- Central log aggregator for one or more logging devices, or FortiAnalyzer in collector mode
  - Can still forward logs to another FortiAnalyzer (or syslog/CEF server)



**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

11

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

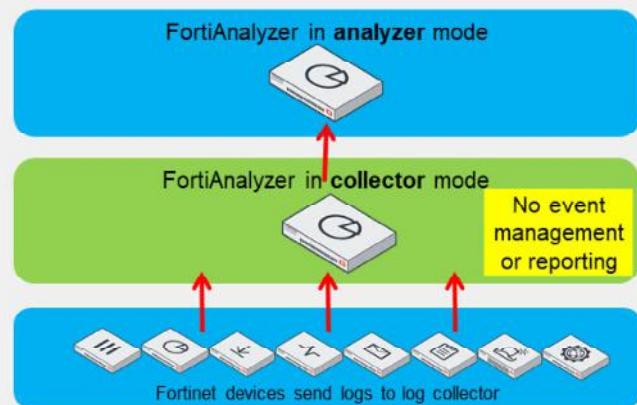
You can change the operating mode in the **System Information** widget on the dashboard.

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

**DO NOT REPRINT****© FORTINET**

## 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

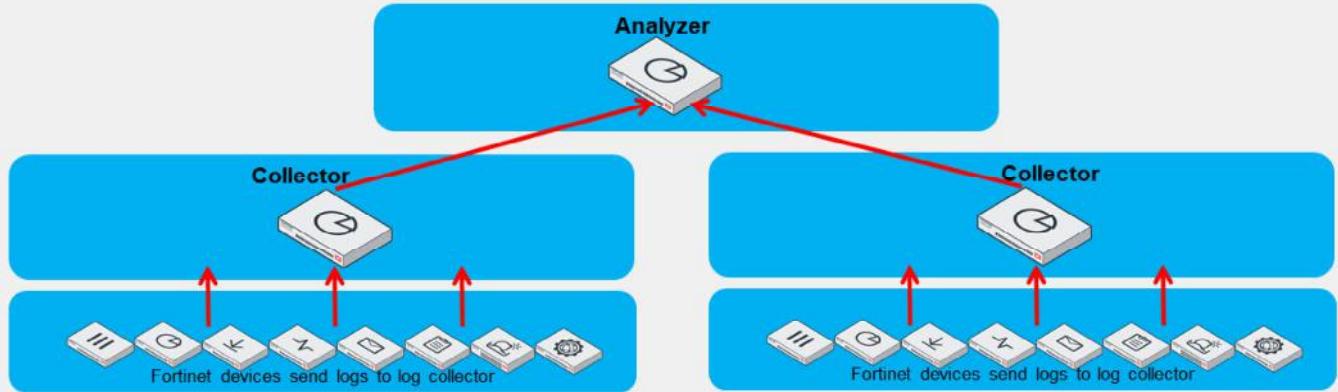


When operating in collector mode, the device collects logs from multiple devices. Then, it forwards those logs, in their original binary format, to another device, such as FortiAnalyzer operating in analyzer mode.

Depending on the forwarding mode, it can also send them to a syslog server or a Common Event Format (CEF) server. A collector does not have the same feature-rich options as an analyzer because its only purpose is to collect and forward logs. It does not allow event management or reporting.

**DO NOT REPRINT**  
**© FORTINET**

## Analyzer—Collector Collaboration



- Increase FortiAnalyzer performance by using both modes
- Offload the log receiving task to the collector
- Use the analyzer node to focus on data analysis and reporting
- Enable the collector to assist with slow or unreliable links by storing logs and forwarding them later
- Allocate most of the disk space on the collector for archive logs

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

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Security Fabric Logging

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

The screenshot shows the FortiAnalyzer web interface. On the left is a navigation sidebar with 'Dashboards', 'Device Manager', 'FortiView', 'Log View' (selected), 'Logs', 'Log Settings', 'Fabric View' (highlighted with a red box), 'Incidents & Events', and 'FortiAI'. The main area has tabs for 'All', 'Fortinet Logs', 'Threat Hunting', and 'Log Browse'. Below the tabs are icons for 'FortiGate', 'Traffic', 'Security', 'Event', and 'FortiSwitch'. A search bar and date range filters ('All Devices', 'Last 1 Day', '06-15 08:24:19 - 06-16 08:24:19') are present. The 'Fabric View' section shows a tree structure: 'All Devices' → 'All FortiGate' → 'Training-Lab' (highlighted with a red box). Other nodes like 'HQ-NGFW-11' and 'HQ-ISFW' are also visible. A blue callout bubble points to the 'Training-Lab' node with the text: 'Training-Lab is the name of the Security Fabric containing two or more FortiGate devices'. The bottom right corner of the interface includes the Fortinet logo and 'Training Institute'.

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

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

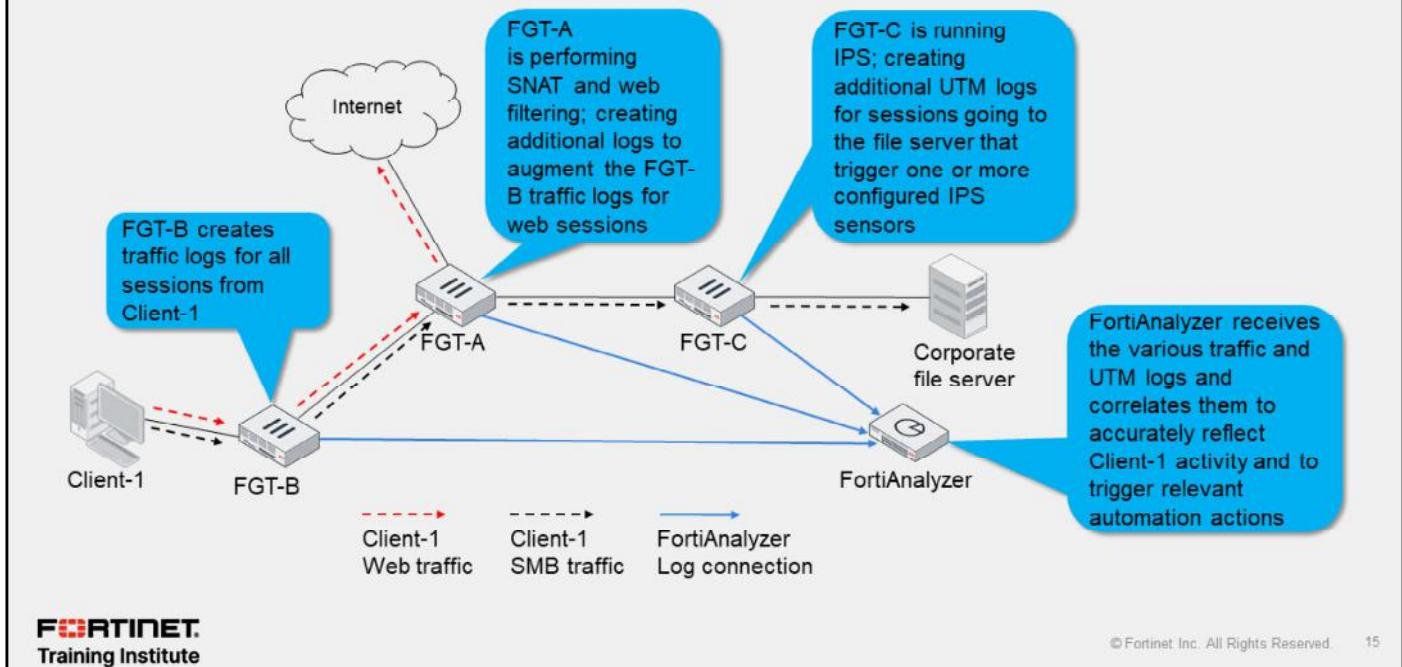
One exception to this behavior occurs when the upstream FortiGate device performs NAT. In this situation, FortiGate generates an additional log to capture NAT details, such as the translated ports and addresses.

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Security Fabric Logging (Contd)



**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

15

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

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

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

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

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

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

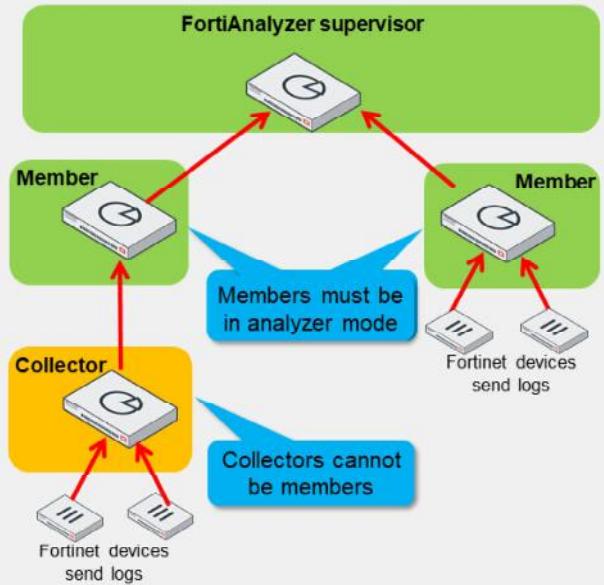
# DO NOT REPRINT

## © FORTINET

### FortiAnalyzer Fabric

- Centralized viewing of devices, incidents, and events across multiple FortiAnalyzer devices
- Ideal for environments with many FortiAnalyzer devices and high log volume
- Two operation modes:
  - Supervisor—one per Fabric; acts as the root
  - Member—sends information to supervisor
- Supervisor and members can be in different time zones
- Supervisor includes only the following modules:
  - Device Manager
  - Log View
  - Incidents & Events
  - System Settings

The supervisor can view the information on the members using an API. Members *do not* forward their logs to the supervisor



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

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

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

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

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

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

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

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

# DO NOT REPRINT

## © FORTINET

### ADOMs

- ADOMs group devices for administrators to monitor and manage
  - One or more devices are assigned to ADOMs, and administrators are assigned to administer one or more ADOMs
- Purpose:
  - To divide the administration of devices and restrict access
    - VDOM, a feature of FortiGate, further restricts access
  - To more efficiently manage data policies and disk space allocation
    - Set for each ADOM (not for each device)

ADOMs are disabled by default

The screenshot shows the 'System Information' section of the FortiAnalyzer dashboard. The 'Administrative Domain' field is highlighted with a red box. Below the dashboard, a command-line interface (CLI) window displays the configuration command:

```
# config system global
  set admom-status {enable | disable}
end
```

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

The purpose of ADOMs is to:

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

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

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

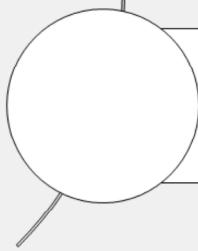
**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



**Key Features and Concepts**



**Initial Configuration**

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

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

**DO NOT REPRINT****© FORTINET**

## Initial Configuration

### Objectives

- Identify the tools you can use to configure FortiAnalyzer
- Access FortiAnalyzer for the first time
- Configure network settings



© Fortinet Inc. All Rights Reserved.

20

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.

**DO NOT REPRINT****© FORTINET**

## Factory Default Settings

- Use factory default settings to log in to FortiAnalyzer and begin the initial configuration
  - You can find default settings in your FortiAnalyzer *QuickStart* guide ([docs.fortinet.com](http://docs.fortinet.com))
  - Always use port1 to connect the management computer to FortiAnalyzer
- If you are deploying the FortiAnalyzer VM, the management IP address depends on the virtualization platform or the cloud provider

User name	Password
admin	<none>

Port	IP address	Netmask	Management access
port1	192.168.1.99	255.255.255.0	https, ssh

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

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

If you deploy the FortiAnalyzer VM, the management IP address and its assignment depend on the virtualization platform. Visit [docs.fortinet.com](http://docs.fortinet.com) for more details.

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

**DO NOT REPRINT**  
**© FORTINET**

## Tools to Configure FortiAnalyzer



**FortiAnalyzer GUI**

**FortiAnalyzer CLI**

Can use the **CLI Console** widget on dashboard of GUI and terminal emulation program (for example, PuTTY)

**PuTTY Configuration**

PUTTY Configuration window showing connection settings for Host Name (IP address) 10.0.1.210, Port 22, and Connection type SSH.

Requires a separate Telnet, SSH, or local console connection

= Not available in Collector mode

- Can use both tools locally and remotely
- Features depend on the profile of the administrator logged in and the operation mode of FortiAnalyzer (analyzer or collector)
- Changes take effect immediately

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 22

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

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

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

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

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

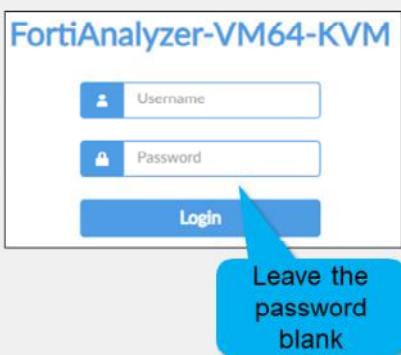
# DO NOT REPRINT

## © FORTINET

### Logging in for the First Time

#### FortiAnalyzer GUI

- In a supported browser, use the factory default information to log in:
  - <https://192.168.1.99>

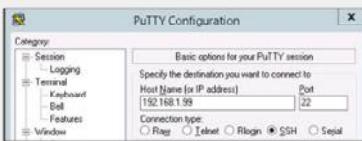


#### FortiAnalyzer CLI

- Log in to the GUI and click the >\_ icon
- Click inside the **CLI Console** widget (you are automatically logged in)



- Or use a terminal emulator



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

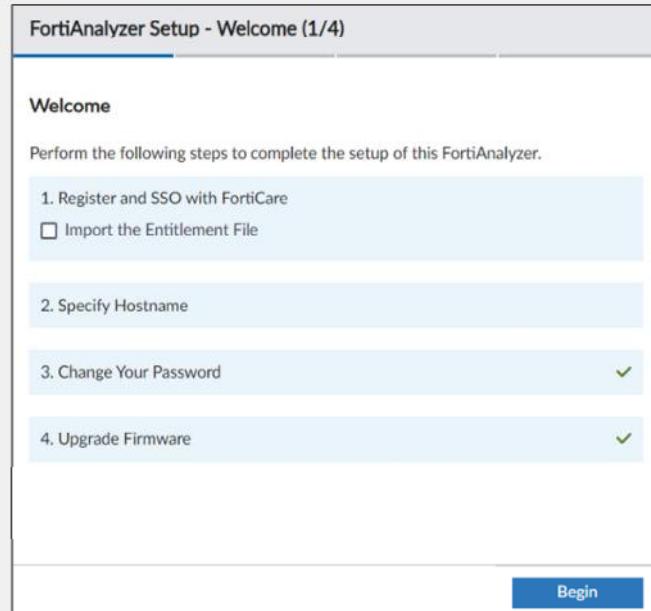
To log in to the CLI for the first time, you can use one of two methods:

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

**DO NOT REPRINT**  
© FORTINET

## FortiAnalyzer Setup Wizard

- The wizard appears after you log in for the first time
- You can choose to complete it immediately, or finish it later
- Option to enable login with FortiCloud SSO users



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

24

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

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

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Configuring FortiAnalyzer for Your Network

The screenshot shows the FortiAnalyzer configuration interface under the 'Network' tab. It includes three main sections: 'Interface', 'DNS', and 'Routing Table'.

- Interface:** A table listing physical interfaces. The first three rows (port1, port2, port3) are highlighted with a red border. A blue callout points to this row with the text "Set IP addresses and admin access".
- DNS:** A section for setting DNS servers. The 'Primary DNS Server' and 'Secondary DNS Server' fields are highlighted with a red border. A blue callout points to this section with the text "Set DNS".
- Routing Table:** A table for defining default routes. One route entry (ID 1) is highlighted with a red border. A blue callout points to this entry with the text "Set gateway".

At the bottom left is the Fortinet Training Institute logo, and at the bottom right are copyright and page number information: © Fortinet Inc. All Rights Reserved. 25

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Configuring FortiAnalyzer for Your Network (Contd)

System Settings > Network

Edit Network Interface

Name	port1
Alias	
IP Address/Netmask	10.0.1.210/255.255.255.0
IPv6 Address	::/0
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> Web <input type="checkbox"/> FortiManager Service
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> Web <input type="checkbox"/> FortiManager Service
Status	<input checked="" type="radio"/>

Configure management IP address

Enable protocols to support (default = HTTPS and SSH)

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 26

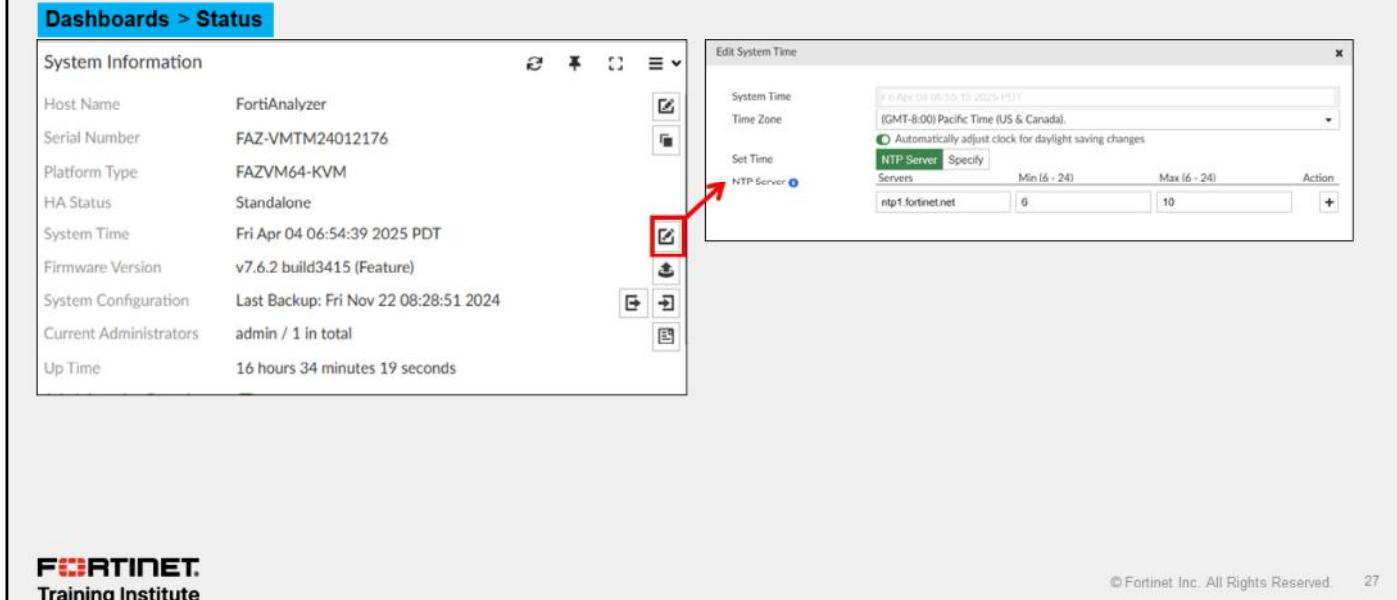
Setting your own IP address and netmask provides more security than using the default address. If more than one FortiAnalyzer device is in the same network, different network settings are mandatory. The management interface must have a dedicated (unique) address. You should be careful if you need to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

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Common Time Synchronization



The screenshot shows the FortiAnalyzer dashboard under 'Dashboards > Status'. On the left, there's a 'System Information' card with the following details:

Host Name	FortiAnalyzer
Serial Number	FAZ-VMTM24012176
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Fri Apr 04 06:54:39 2025 PDT
Firmware Version	v7.6.2 build3415 (Feature)
System Configuration	Last Backup: Fri Nov 22 08:28:51 2024
Current Administrators	admin / 1 in total
Up Time	16 hours 34 minutes 19 seconds

To the right of the card is a modal window titled 'Edit System Time' with the following fields:

- System Time: Fri Apr 04 06:54:39 2025 PDT
- Time Zone: (GMT-8:00) Pacific Time (US & Canada)
- Set Time:
- NTP Server:  Specify
- Servers: ntp1.fortinet.net
- Min (6 - 24): 6
- Max (6 - 24): 10
- Action: +

A red arrow points from the 'Specify' link in the NTP Server section to the 'Specify' checkbox in the 'Edit System Time' modal.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 27

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

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Other Network Settings

- Include a DNS server to resolve hostnames in the logs
  - Recommended to have both primary and secondary servers

DNS	
Primary DNS Server	208.91.112.52
Secondary DNS Server	208.91.112.53

FortiGuard DNS servers (default)

- Assign IPv4/IPv6 static routes to a different gateway so that packets are delivered by a different route

Routing Table

		+ Create New	Edit	Delete
	ID	Type		
<input type="checkbox"/>	ID	Type		

Create New Network Route

IP Type	IPv4
Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	
Interface	None
<input type="text"/> port1	

**FORTINET.**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

28

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Other Network Settings (Contd)

- Configure a reliable NTP server to ensure the system time is accurate
- Configure link aggregation to increase the available bandwidth and to add network redundancy
  - Can set the minimum number of ports to consider the link status as up
- Configure VLAN interfaces to isolate sensitive traffic from the rest
  - Two protocol options: 802.1Q and 802.1AD

Set Time	<input checked="" type="checkbox"/> Synchronize with NTP Server
Servers	Min 1 Max 1 ntp1.fortinet.net
+ [button]	

Name	LinkAggregate-1
Alias	LinkAggregate-1
Type	VLAN <b>Aggregate</b>
Members	<input type="text"/> Q port7 port8 2 Entries Selected

Name	VLAN100
Alias	FortiGate-VLAN
Type	VLAN <b>Aggregate</b>
VLAN ID	100
Interface	port5

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

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

**DO NOT REPRINT**  
© FORTINET

## Resetting the Configuration

- To reset to factory default settings from flash:

```
# execute reset all-settings
```

**Note:** The FortiAnalyzer configuration is stored in flash, but logs are stored on disks

- To reset all settings from flash except current IP addresses and routes:

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

- To erase all device settings and images, databases, and log data from disk, but preserve IP and routing info:

```
# execute format disk
```

- You should always format the disk after resetting the configuration
- A low-level disk format option, deep-erase, is available

- You should connect to the console port before running these commands



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

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Basic CLI Commands for System and Network Settings

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

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

- Example:
 

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

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

In general, the first word of a command indicates what you are trying to achieve in the CLI:

- The `get` commands allow you to view information in a more readable format.
- The `show` commands allow you to view the exact CLI configuration for that section, including the correct indentation.
- The `execute` commands allow you to perform a function in FortiAnalyzer.

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

**DO NOT REPRINT**  
**© FORTINET**

## Viewing Server Information

- Use these commands to view system information:

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

- Example:

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

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](http://docs.fortinet.com).

**DO NOT REPRINT****© FORTINET**

## 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.

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



**Key Features and Concepts**



**Initial Configuration**

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Describe the purpose of FortiAnalyzer
- ✓ Describe the FortiAnalyzer operating modes
- ✓ Describe logging in a Security Fabric environment
- ✓ Describe FortiAnalyzer Fabric
- ✓ Describe ADOMs
- ✓ Access and navigate the GUI
- ✓ Identify the tools you can use to configure FortiAnalyzer
- ✓ Configure network settings

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.

DO NOT REPRINT

© FORTINET



# FortiAnalyzer Administrator

## Administration and Management

 FortiAnalyzer 7.6

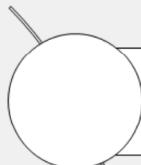
Last Modified: 16 July 2025

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

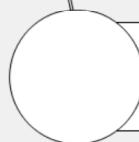
**DO NOT REPRINT**

**© FORTINET**

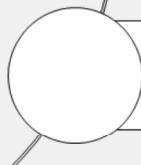
## Lesson Progress



Administrative Access Controls



Administrative and Event Task Monitoring



System Backup and Best Practices

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

**DO NOT REPRINT****© FORTINET**

## Administrative Access Controls

### Objectives

- Configure secure administrative access
- Authenticate administrators using external servers
- Configure two-factor authentication



© Fortinet Inc. All Rights Reserved.

3

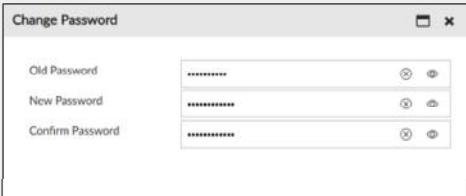
After completing this section, you should be able to achieve the objectives shown on this slide.

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.

**DO NOT REPRINT**  
**© FORTINET**

## Changing the Default Administrator Password

- It is necessary to change the default administrator password
- Must change for security reasons
  - Select a secure password
- No password recovery

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

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

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

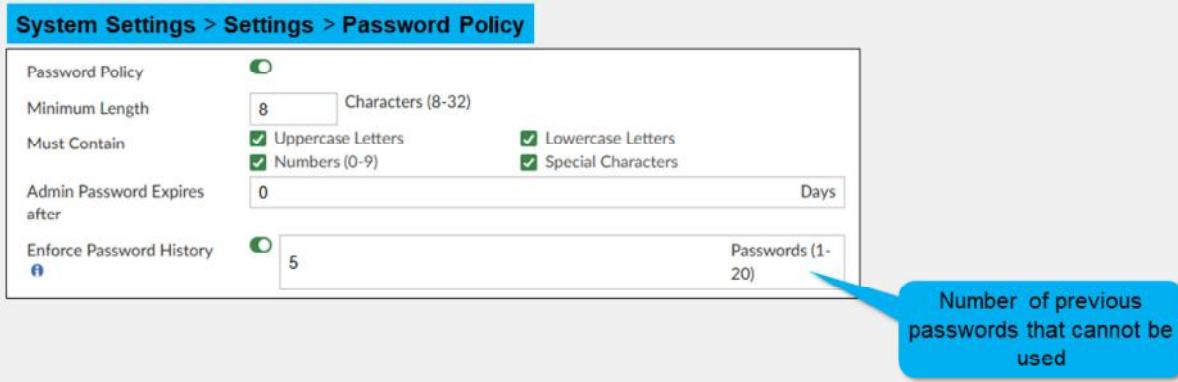
The other option is to format the flash drive and reload the image from the BIOS configuration menu. This erases the system settings, including the administrative accounts. So, make sure you remember your password or store it in a secure location.

# DO NOT REPRINT

## © FORTINET

### Increasing Account Security Through a Password Policy

- Increase administrator account security by configuring a password policy (disabled by default)
  - Global administration setting



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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Security Recommendations

- Deploy in a protected and trusted private network
- Use secure communication methods (HTTPS or SSH), even in a private network
- Configure trusted hosts
- Open only the ports necessary for your network (consult [docs.fortinet.com](https://docs.fortinet.com))
- If access from the outside is required, set up special users and use only secure protocols
- Always use secure passwords; enforce password policy
- Use the *FortiAnalyzer Best Practices* guide to help you get the most out of your FortiAnalyzer products, maximize performance, and avoid potential problems



© Fortinet Inc. All Rights Reserved.

6

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

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

# DO NOT REPRINT

## © FORTINET

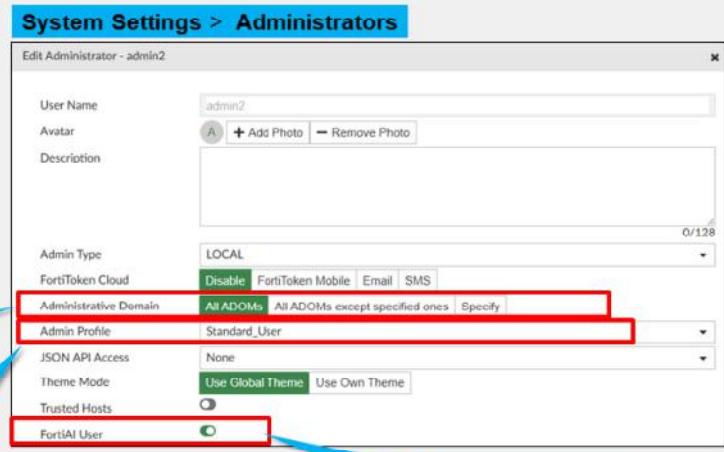
## Multiple Administrators and Security

- Divide administrative tasks by creating additional administrative accounts
- Every additional administrator causes an increase in risk
- To better protect your network, control administrator access using:
  - Administrative profiles
  - Trusted hosts
  - ADOMs

Assign one or more ADOMs to the administrator account

Administrative profile type

Enable the FortiAI feature for the administrator



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

To protect your network, you can control and restrict administrative access using the following methods:

- Administrative profiles: Determine the level of access, or privileges, granted.
- Trusted hosts: Determine from where a connection can be established.
- ADOMs: Determine to which devices the administrator will have access to view and manage logs.

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

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

**DO NOT REPRINT****© FORTINET**

## Administrative Profiles

- Never give an administrator more privileges than they require
- Assign the appropriate profile—you can modify and create profiles
  - Access profiles define administrator privileges

Profile name	Administrator privileges
Super_User	All system privileges enabled All device privileges enabled
Standard_User	No system privileges enabled Read-write access for all device privileges
Restricted_User	No system privileges enabled Read-only access for all device privileges

Standard and restricted users can't access system settings, and restricted users can't access management extensions

System Settings > Admin Profiles	
<a href="#">+ Create New</a>	<a href="#">Edit</a>
<a href="#">Name</a>	<a href="#">Type</a>
<input type="checkbox"/> Restricted_User	
<input type="checkbox"/> Standard_User	
<input type="checkbox"/> Super_User	
<input type="checkbox"/> No_Permission_User	

Create custom profiles

Modify individual privileges in profiles

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

8

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

The four default profiles are:

- Super\_User, which provides access to all device and system privileges.
- Standard\_User, which provides read and write access to device privileges, but not system privileges.
- Restricted\_User, which provides read access to only device privileges but not to system privileges, and removes all access to the management extensions.
- No\_Permission\_User, which provides no system or device privileges, and can be used for example, to temporarily remove access granted to existing admins.

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

DO NOT REPRINT  
© FORTINET

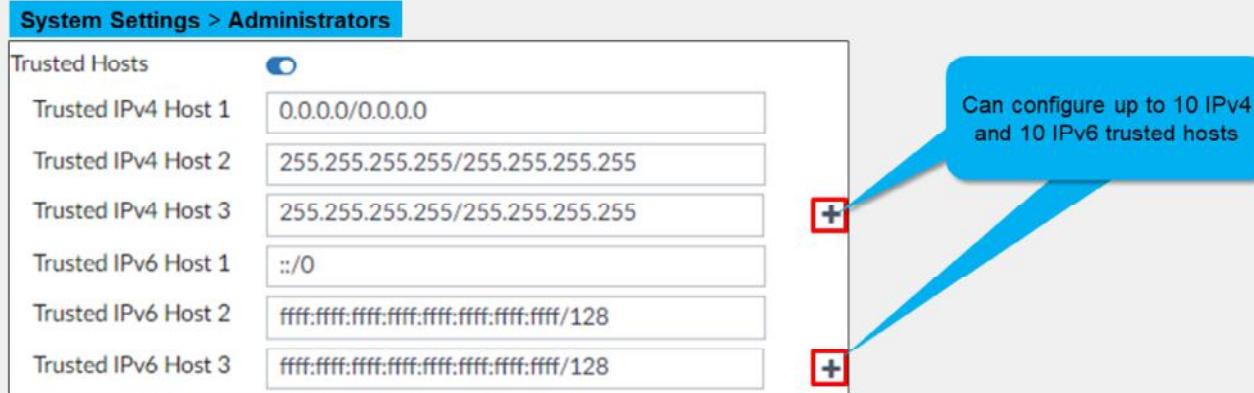
## Trusted Hosts

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

System Settings > Administrators

Trusted Hosts	
Trusted IPv4 Host 1	0.0.0.0/0.0.0.0
Trusted IPv4 Host 2	255.255.255.255/255.255.255.255
Trusted IPv4 Host 3	255.255.255.255/255.255.255.255
Trusted IPv6 Host 1	::/0
Trusted IPv6 Host 2	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
Trusted IPv6 Host 3	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128

Can configure up to 10 IPv4 and 10 IPv6 trusted hosts



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

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

DO NOT REPRINT  
© FORTINET

## Controlling Access Through ADOMs

- Monitor and manage devices in only the assigned ADOM
- Improves network security and makes device management more effective
- Administrators with the Super\_User profile have full access to system information and to all ADOMs

Assign one or more ADOMs to the administrator account

System Settings > Administrators

Edit Administrator

User Name: admin2

Avatar: A

Description:

Admin Type: LOCAL

FortiToken Cloud

Administrative Domain: **Specify**

All ADOMs

All ADOMs except specified ones

ADOM1

1 entry selected

Admin Profile: Standard\_User

JSON API Access: None

Theme Mode: Use Global Theme | Use Own Theme

© Fortinet Inc. All Rights Reserved. 10

**FORTINET.**  
Training Institute

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.

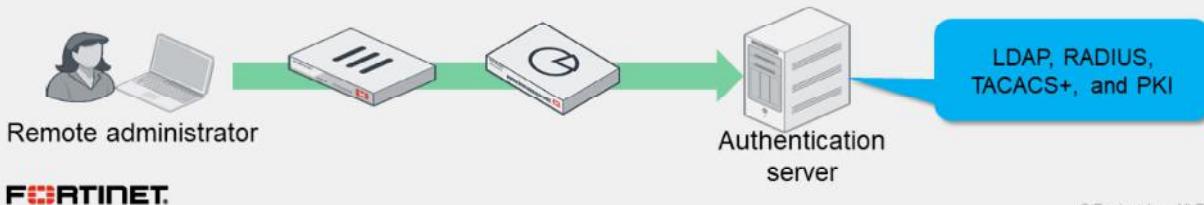
**DO NOT REPRINT**  
**© FORTINET**

## External Authentication of Administrators

- Configure external servers to validate your administrator logins (non-local users)
  - LDAP, RADIUS, TACACS+, and PKI can be used to authenticate administrators
  - Must configure server entries for each authentication server in your network

**System Settings > Remote Authentication Server**

Edit LDAP Server	
Name	External_Server
Server Name/IP	10.0.1.150
Port	389
Common Name Identifier	uid
Distinguished Name	ou=Training,dc=trainingAD,dc=training,dc=lab
Bind Type	Regular
User DN	uid=fazadmin,ou=Training,dc=trainingAD,dc=training,dc=lab
Password	*****
Secure Connection	<input checked="" type="checkbox"/>
Administrative Domain	All ADOMS    Specify



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

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

# DO NOT REPRINT

## © FORTINET

## External Authentication of Administrators (Contd)

- The wildcard feature allows you to authenticate users from one or more groups
- One user on FortiAnalyzer that points to a remote authentication server
  - No local credentials on FortiAnalyzer
- Supports LDAP, RADIUS, TACACS+, GROUP
  - Remote authentication server groups support multiple authentication server types (configured in CLI)

**System Settings > Administrators**

User Name	admin1
Avatar	
Description	
Admin Type	GROUP
GROUP	AuthServers
<input checked="" type="checkbox"/> Match all users on remote server	

**System Settings > Remote Authentication Server**

Name	Type	ADOM	Details
External_Server	LDAP	All ADOMs	10.0.1.150:389/uid: ou=Training,dc=trainingAD,dc=fr
LDAP2	LDAP	All ADOMs	10.0.1.155:389/uid: ou=training,dc=trainad,dc=fr

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.

**DO NOT REPRINT**  
**© FORTINET**

## Two-Factor Authentication

- Configure two-factor authentication
  - Something you know (password) + something you have (token)
  - Example: FortiAuthenticator and FortiToken
- FortiAnalyzer configuration:
  - Create a RADIUS server that points to FortiAuthenticator
  - Create an administrator account that points to the RADIUS server

**System Settings > Remote Authentication Server**

Name	RADIUS
Server Name/IP	10.0.1.11
Port	1812
Server Secret	*****
Test Connectivity Test User Credentials	
Secondary Server Name/IP	
Secondary Server Secret	*****
Test Connectivity Test User Credentials	
Authentication Type	ANY
Advanced Options >	

**FORTINET**  
 Training Institute

- Create an administrator account that points to the RADIUS server

**System Settings > Administrators**

Create New Administrator

User Name	2FA-Admin
Avatar	2 Add Photo Remove Photo
Description	
Admin Type	RADIUS
RADIUS Server	RADIUS1
Match all users on remote server	<input checked="" type="checkbox"/>
New Password	*****
Confirm Password	*****
FortiToken Cloud	<input type="checkbox"/> Disable <input type="checkbox"/> FortiToken Mobile <input type="checkbox"/> Email <input type="checkbox"/> SMS
Administrative Domain	All ADOMs All ADOMs except specified ones Specify

© Fortinet Inc. All Rights Reserved.

13

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

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Two-Factor Authentication (Contd)

- Use FortiToken Cloud to deliver two-factor credentials:
  - FortiToken mobile app
  - Email
  - SMS

**System Settings > Administrators**

User Name	admin-2fa
Avatar	A <input type="button" value="+ Add Photo"/> <input type="button" value="Remove Photo"/>
Description	
Admin Type	LOCAL
FortiToken Cloud	<input checked="" type="radio"/> Disable <input checked="" type="radio"/> FortiToken Mobile <input type="radio"/> Email <input type="radio"/> SMS
Email	trainingtest@fortinet.com

**FortiAnalyzer-VM64-KVM**

Please input FortiToken code:

<input type="text" value="admin-2fa"/>
<input type="password" value="*****"/>
<input type="text" value="Token Code"/>
<input type="button" value="Login"/>

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

# DO NOT REPRINT

## © FORTINET

## SAML Admin Authentication

- SAML can be enabled across all Security Fabric devices
- Allows smooth movement between devices for the administrator (SSO)
- FortiAnalyzer can be the identity provider (IdP) or the service provider (SP)

**System Settings > SAML SSO**

Single Sign-On Settings

Server Address: 10.0.13.125  
Allow admins to login with FortiCloud:

Single Sign-On Mode:  Disabled  Identity Provider (IdP)  Service Provider (SP)  Fabric SP

In Fabric SP mode, an SSO administrator is created for each Security Fabric. When a user logs in via Fabric SSO, the Fabric IdP provides the user's profile name. If this system has a profile with the matching name, the profile is assigned to the user. Otherwise, the profile of the SSO administrator is assigned to the user by default.

Default Admin Profile: Super\_User

Fabric IdPs

<input type="checkbox"/> Root Device	ADOM Name	Status	<input type="checkbox"/> IdP Settings
<input type="checkbox"/> FGVM02TM24013423	root	Enabled	Entity ID: http://10.0.11.254/saml-idp/csf_hn2irhb065hgshax61zsghraf186 Login URL: https://10.0.11.254/saml-idp/csf_hn2irhb065hgshax61zsghraf1 Logout URL: https://10.0.11.254/saml-idp/csf_hn2irhb065hgshax61zsghraf1

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 15

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. How do you restrict an administrator's access to a subset of your organization's ADOMs?
  - A. Assign the ADOMs to the administrator's account.
  - B. Configure trusted hosts.
  
2. What is the function of a wildcard administrator?
  - A. It allows administrators to log in with credentials stored locally on FortiAnalyzer.
  - B. It allows administrators to log in with credentials stored on a remote authentication server.

**DO NOT REPRINT**

**© FORTINET**

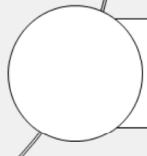
## Lesson Progress



Administrative Access Controls



Administrative and Event Task Monitoring



System Backup and Best Practices

Good job! You now understand administrative access controls.

Now, you will learn how to monitor administrative events.

DO NOT REPRINT  
© FORTINET

## Administrative and Event Task Monitoring

### Objectives

- Monitor FortiAnalyzer administrators, events, and tasks
- Monitor FortiGate administrator logins and activity



© Fortinet Inc. All Rights Reserved.

18

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.

DO NOT REPRINT  
© FORTINET

## Monitoring Administrator Login Status

- Monitor administrator accounts that are currently logged in
  - Logged in users are identified by the green check mark
  - CLI command:

```
# diagnose system admin-session status
```
- By default, the list is available only to administrators with Super\_User access

**System Settings > Administrators**

<input type="checkbox"/>	Name	Type	Profile	JSON API Access	ADOMs	Trusted IPv4 Hosts	
<b>System Administrator (2)</b>							
<input type="checkbox"/>	admin	LOCAL	Super_User	None	All ADOMs	0.0.0.0/0.0.0.0	
<input type="checkbox"/>	admin2	LOCAL	Super_User	None	All ADOMs	0.0.0.0/0.0.0.0	

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 19

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

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

**DO NOT REPRINT**  
© FORTINET

## Viewing Administrator Event Logs

- View FortiAnalyzer event logs, including administrator activity
  - By default, only available to administrators with Super\_User access

### System Settings > Event Logs

Last 1 Hour ▾ 08:16:01 To 09:16:00



#	Date/Time	Device ID	Sub Type	User	Message	Operation	Performed On
1	09:15:41	FAZ-VM0000065040	dvm	admin		Switch to new	ADOM1
2	09:15:14	FAZ-VM0000065040	system	admin	User 'admin' with	login	GUI(172.16.100.1)
3	09:15:10	FAZ-VM0000065040	system	admin	User 'admin' with	logout	GUI(172.16.100.1)

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

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

**DO NOT REPRINT**

**© FORTINET**

## Monitoring Tasks

- View the tasks FortiAnalyzer administrators have performed, including progress and status
  - By default, available only to administrators with Super\_User access

The screenshot shows the 'Task Monitor' section of the FortiAnalyzer interface. It displays a table of tasks with columns for ID, Source, Description, User, Status, Time Used, ADOM, Start Time, and End Time. Task 5, titled 'Add Multiple Devices', is highlighted with a red box and a callout. The callout shows a detailed progress report for Task 5, which has 2 subtasks: HQ-ISFW and HQ-NGFW-1, both of which are initializing configuration databases.

ID	Source	Description	User	Status	Time Used	ADOM	Start Time	End Time
4	Device Manager	dvmdb adom ADOM1 object member	A admin	Success: 1	2s	ADOM1	Tue, Mar 11, 2025 8:46 AM..	Tue, Mar 11, 2025 8:47 AM P
3	Device Manager	dvmdb adom root object member	A admin	Success: 1	2s	root	Tue, Mar 11, 2025 8:46 AM..	Tue, Mar 11, 2025 8:46 AM P
2	Device Manager	Add Multiple Devices	A admin	Success: 1	<1s	root	Mon, Mar 10, 2025 6:09 A..	Mon, Mar 10, 2025 6:09 A P
1	Device Manager	Add Multiple Devices	A admin	Success: 2	<1s	root	Thu, Mar 6, 2025 10:45 AM..	Thu, Mar 6, 2025 10:45 AM P

Task 5: Add Multiple Devices

Total: 2/2, Success: 2, Warning: 0, Error: 0

#	Name	Time Used	Status
1	HQ-ISFW	<1s	Initializing configuration database
2	HQ-NGFW-1	1s	Initializing configuration database

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 21

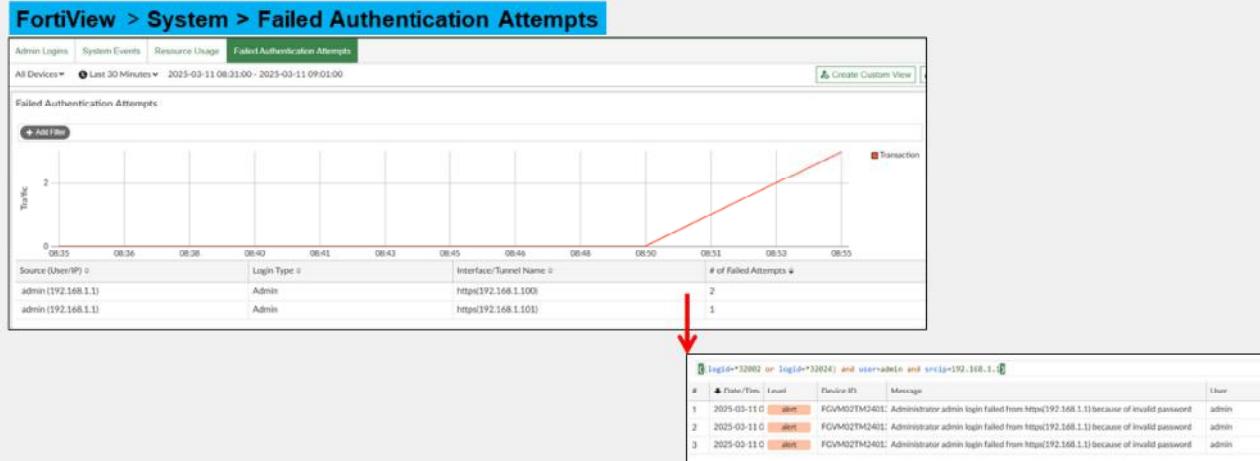
The **Task Monitor** page lets you view the progress and status of administrator tasks..

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

**DO NOT REPRINT**  
**© FORTINET**

## Monitoring FortiGate Administrator Logins

- Monitor FortiGate administrator logins, system activity, and failed authentications



You must configure FortiGate  
logging settings to log events and  
send them to FortiAnalyzer

© Fortinet Inc. All Rights Reserved. 22

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

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Monitoring FortiGate Administrator Activity

- Monitor FortiGate system activity

This entry shows that several databases were updated

#	Event Name (Description)	Severity
1	System performance statistics	Low
2	Synchronization of global object report.	Low
3	AV, IPS, GeoIP, SRC-VIS, FortiFlow, URL White-list, Certificate	Critical
4	FortiGate update succeeded	Low

View Related Logs

13:36:10	critical	FGVM01000006469	Identity	FGVM010000077446
13:36:10	critical	FGVM01000006469	Device ID	FGFW
13:36:12	critical	FGVM01000007764	Device Name	auto-script
13:36:12	critical	FGVM01000007764	User Interface	
Type				
Sub Type				
Type				
Alerts				
Action				
Level				
General				
Log Description				
AV, IPS, GeoIP, SRC-VIS, FortiFlow, URL White-list, Certificate				

© Fortinet Inc. All Rights Reserved. 23

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

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which configuration is required to view FortiGate event logs on FortiAnalyzer?
  - A. FortiGate must be registered to the root ADOM.
  - B. FortiGate logging settings must have event logging enabled.
  
2. Which administrative profile should you assign to an administrative user who needs to manage devices but not system settings?
  - A. Super\_User
  - B. Standard\_User

**DO NOT REPRINT****© FORTINET**

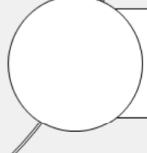
## Lesson Progress



Administrative Access Controls



Monitoring Administrative Events and Tasks



System Backup and Best Practices

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

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

**DO NOT REPRINT****© FORTINET**

## System Backup and Best Practices

### Objectives

- Perform a system configuration backup
- Describe best practices



© Fortinet Inc. All Rights Reserved. 26

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Performing a System Configuration Backup

- System configuration backups contain:
  - System information
  - Device list
  - Report configuration
- Logs and generated reports are *not included*
- You can restore a backup to only the same model and firmware version
- You must encrypt the backup file
- You can restore a system configuration from any previous backup
- If your FortiAnalyzer is a VM, you can also use VM snapshots

System Settings > Dashboard	
<b>System Information</b>	
Host Name	FortiAnalyzer
Serial Number	FAZ-VMTM24012176
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Tue Mar 11 09:05:52 2025 PDT
Firmware Version	v7.6.2 build3415 (Feature)
<b>System Configuration</b>	Last Backup: Fri Nov 22 08:28:51 2024
Current Administrators	admin / 1 in total
Up Time	4 days 21 hours 34 minutes 10 seconds
Administrative Domain	●
Operation Mode	Analyzer Collector

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

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

The system configuration backup includes the following:

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## 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

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.

**DO NOT REPRINT****© FORTINET**

## Best Practices

- Shut down FortiAnalyzer gracefully—not doing so can damage the databases  

```
# execute shutdown
```
- Run on an uninterruptable power supply (UPS)
- Enable password policy and set requirements for the administrator password
- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server

The following are some best practices for operating FortiAnalyzer:

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

**DO NOT REPRINT****© FORTINET**

## Best Practices (Contd)

- Implement a comprehensive backup plan that includes the configuration and the logs
- Increase reliability by configuring high availability (HA) and link aggregation
- Check the compatibility matrix for FortiAnalyzer and other Fortinet products
  - This includes the firmware compatibility on both ends
- Check and follow the recommended upgrade path
  - You can verify the upgrade history on your FortiAnalyzer device:

```
# diagnose cdb upgrade summary
===== New configuration database initiated =====
2024-11-10 16:28:58      v7.4.4-build2550 240916 (GA.F)
2024-10-15 16:33:21      v7.6.0-build3340 240729 (GA.F)
2024-11-22 15:05:24      v7.6.1-build3345 241023 (GA.M)
2025-01-03 06:51:29      v7.6.2-build3415 241212 (GA.F)
```

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

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

# DO NOT REPRINT

## © FORTINET

### OS Firmware Levels—Feature(F) and Mature(M)

- FortiAnalyzer 7.6.0 and later firmware images use tags to indicate firmware maturity levels:
- The Feature tag indicates that the firmware release includes new features
  - It can also include bug fixes and vulnerability patches where applicable
- The Mature tag indicates that the firmware release includes no new, major features
  - Mature firmware contains bug fixes and vulnerability patches where applicable

The screenshot shows the FortiAnalyzer interface. On the left, there is a 'System Information' table with the following data:

System Information	
Host Name	FortiAnalyzer
Serial Number	FAZ-VMTM24012176
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Mon Jun 09 15:34:43 2025 PDT
Firmware Version	v7.6.2 build3415 (Feature)
System Configuration	Last Backup: Thu Dec 5 10:17:46 2024
Current Administrators	admin / 1 in total

A red box highlights the 'Firmware Version' row. A blue arrow points from this row to a 'Confirm Upgrade' dialog box on the right. The dialog box contains the following text:

The Mature level of the currently installed firmware version is different than the Feature level of the firmware version selected. Use extra caution, as the Feature release may contain changes which impact production environments.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

A blue callout box at the bottom of the slide states: "Firmware 7.6.2 is a feature release".

At the bottom left is the Fortinet Training Institute logo. At the bottom right are copyright and page number information: © Fortinet Inc. All Rights Reserved. 31

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

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

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

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Administrative Access Controls



Administrative and Event Task Monitoring



System Backup and Best Practices

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Configure secure administrative access
- ✓ Authenticate administrators using external servers
- ✓ Configure two-factor authentication
- ✓ Monitor administrative events
- ✓ Perform a system configuration backup
- ✓ Describe best practices



© Fortinet Inc. All Rights Reserved. 34

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.

DO NOT REPRINT

© FORTINET



# FortiAnalyzer Administrator

## ADOMs and HA

 FortiAnalyzer 7.6

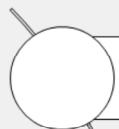
Last Modified: 16 July 2025

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

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



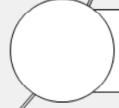
ADOMs



Disk Quota



High Availability



Firmware Upgrades

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

# DO NOT REPRINT

© FORTINET

## ADOMs

### Objectives

- Configure and create 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.

**DO NOT REPRINT****© FORTINET**

## Enabling ADOMs

- Enabled or disabled in CLI or GUI
  - Required if you want to register a non-FortiGate device on FortiAnalyzer

```
# config system global
    set adom-status {enable | disable}
end
```

- Maximum number of ADOMs depends on the FortiAnalyzer model
- Once enabled, you must select an ADOM from all the configured ADOMs

### Dashboard > System Information

System Information	
Host Name	FortiAnalyzer
Serial Number	FAZ-VMTM24012176
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Tue Mar 11 09:05:52 2025 PDT
Firmware Version	v7.6.2 build3415 (Feature)
System Configuration	Last Backup: Fri Nov 22 08:28:51 2024
Current Administrators	admin / 1 in total
Up Time	4 days 21 hours 34 m
Administrative Domain	
Operation Mode	(Analyzer) Collector

Note: ADOMs are not enabled by default

Select an ADOM

root  
Fabric

ADOM1 (1)  
FortiGate

With ADOMs enabled, you must select an ADOM after login

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

4

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## How ADOMs Operate With FortiGate VDOMs

- Global ADOM configuration can operate in normal mode (default) or advanced mode
- **Normal:** Cannot assign VDOMs from the same FortiGate to multiple FortiAnalyzer ADOMs
  - Must assign the FortiGate device and all of its VDOMs to a single ADOM
- **Advanced:** Can assign VDOMs from the same FortiGate to multiple FortiAnalyzer ADOMs
  - Can use **FortiView**, **Event Management**, and **Reports** functions to analyze data for individual VDOMs

System Settings > Advanced > Misc Settings

Log Forwarding Logging Topology Device Log Settings Mail Server Misc Settings

Advanced Settings

ADOM Mode **Normal** Advanced

```
# config system global
    set adom-mode {advanced | normal}
end
```

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

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

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

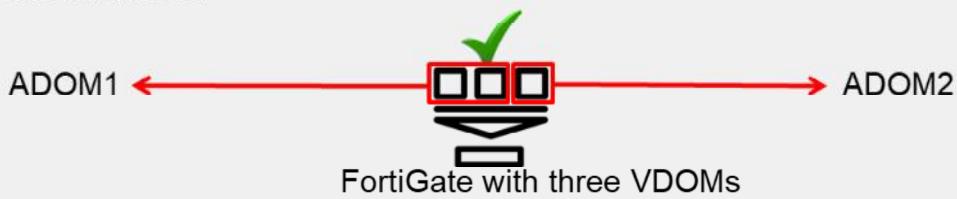
**DO NOT REPRINT****© FORTINET**

## How ADOMs Operate With FortiGate VDOMs (Contd)

- **Normal mode:**



- **Advanced mode:**



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

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

# DO NOT REPRINT

# © FORTINET

## Creating an ADOM

- Create new ADOMs if default ones do not fit your requirements
  - Devices can be registered to their *device-specific* ADOMs only
- Disk quota configured per ADOM (can be configured per device using CLI)
- Cannot delete a custom ADOM if a device is still assigned to it
- CLI command to view ADOMs:

```
# diagnose dvm adm list
```

The screenshot shows two windows from the FortiAnalyzer interface. On the left is the 'System Settings > ADOMs' page, which lists existing ADOMs like 'root' (Fabric, 1000 MB) and 'ADOM1' (Fabric, 2 GB). On the right is the 'Create ADOM' dialog. It has fields for 'Name' (set to 'ADOM1') and 'Type' (set to 'Fabric'). Below these are sections for 'Devices', 'Data Policy' (with 'Retention policy' highlighted by a blue callout), and 'Disk Utilization' (with 'Configure disk quota' highlighted by a blue callout). A red box highlights the 'Name' and 'Type' fields in the 'Create ADOM' dialog.

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Security Fabric ADOM

- Can group all devices in a Security Fabric in the same ADOM
- Security Fabric ADOM allows for:
  - Fast data processing
  - Log correlation
- Combines results to be presented in:
  - Reports
  - FortiView
  - Incidents & Events
  - Device Manager
  - LogView

System Settings > ADOMs

Create ADOM

Name	Fabric_ADOM
Type	Fabric
Time Zone	Default

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

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

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

**DO NOT REPRINT**

**© FORTINET**

## 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.

**DO NOT REPRINT**

© FORTINET

## Lesson Progress



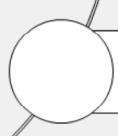
**ADOMs**



**Disk Quota**



**High Availability**



**Firmware Upgrades**

Good job! You now understand ADOMs.

Now, you will learn how to manage disk quotas.

**DO NOT REPRINT**

**© FORTINET**

## Disk Quota

### Objectives

- Describe what comprises the disk quota
- Monitor disk usage
- Modify the disk quota

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.

**DO NOT REPRINT****© FORTINET**

## Finite Disk Space

- When allotted log disk space is full:
  - An automatic alert is generated
  - The oldest logs are overwritten (default behavior)
  - To stop logging when the disk is full:
- What you need to know:
  - FortiAnalyzer disk quota and what is included in the quota
  - How the disk quota is enforced
  - What space is reserved and not available for storing logs

```
# config system locallog disk setting  
    set diskfull nolog  
end
```



© Fortinet Inc. All Rights Reserved.

12

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

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

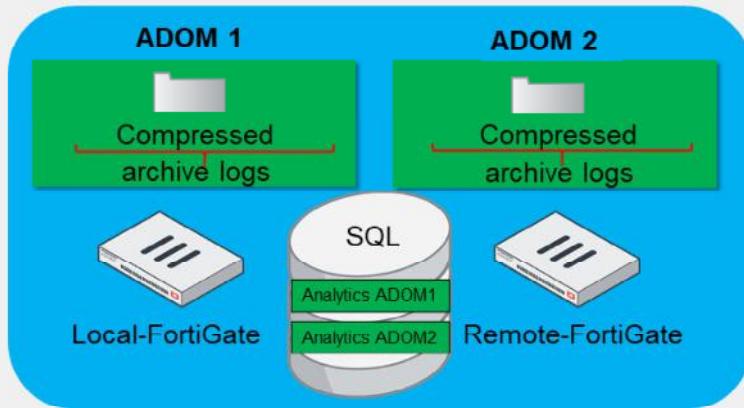
No administrator wants to lose important log data or face compliance issues regarding data retention. Therefore, it is essential to understand your FortiAnalyzer disk quota, how it is enforced, and which space is reserved and unavailable for storing logs.

# DO NOT REPRINT

## © FORTINET

### Disk Quota

- Disk quota includes:
  - Archive logs
  - Analytics logs



The FortiAnalyzer disk quota includes two types of logs:

- Archive logs: These are logs compressed on hard disks and offline.
- Analytics logs: These are the logs stored and indexed in the SQL database and online.

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

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

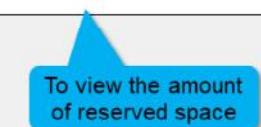
**DO NOT REPRINT****© FORTINET**

## Reserved Disk Quota

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

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

# diagnose log device

To view the amount of reserved space

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

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

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

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

# DO NOT REPRINT

## © FORTINET

### Example—Understanding Disk Quota

# diagnose log device	59.0 GB (total system storage) - 11.0 GB (reserved space) <hr/> = 48.0 GB (total quota)
Total Quota Summary: Total Quota      Allocated 48.0GB      19.5GB	Available      Allocate% 28.5GB      40.7%
System Storage Summary: Total      Used 59.0GB      4.7GB	Available      Use% 54.3GB      8.0 %
Reserved space: 11.0GB (18.6% of total space).	19.5 GB (allocated) = archive + analytics quota for all ADOMs  4.7 GB (used) = logs + all system files on mounted drive (# diagnose system print df)

AdomName	AdomOID	Type	Archive						Analytics						Database				
			[Retention	Quota	Used	Logs/	Logs/	Logs/	Logs/	Logs/	Logs/	Logs/	Logs/	Logs/	Database	Quota	Used	SiemDB/	Cache
ADOM1	185	FSF	365days	600.0MB	10.7MB(	10.7MB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	1.4GB	5.5MB(	927.4KB/	0.0KB)	0.4%
ADOM2	207	FGT	365days	300.0MB	104.0KB(	104.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	700.0MB	984.0KB(	0.0KB/	0.0KB)	0.1%
FortiAnalyzer	122	FAZ	365days	300.0MB	0.0KB(	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	700.0MB	0.0KB(	0.0KB/	0.0KB)	0.0%
FortiAuthenticator	138	FAC	365days	300.0MB	0.0KB(	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	700.0MB	0.0KB(	0.0KB/	0.0KB)	0.0%
FortiCache	126	FCH	365days	300.0MB	0.0KB(	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	700.0MB	0.0KB(	0.0KB/	0.0KB)	0.0%
FortiCarrier	118	FGT	365days	300.0MB	0.0KB(	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	700.0MB	0.0KB(	0.0KB/	0.0KB)	0.0%
... (output truncated) ...																			
root	3	FSF	365days	300.0MB	0.0KB(	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	0.0KB/	700.0MB	1.9MB(	120.2KB/	0.0KB)	0.3%
Total usage: 19 ADOMs, logs=10.9MB(10.9MB/0.0KB/0.0KB/0.0KB) database=162.6MB(ADOMs usage:8.4MB(1.0MB, 0.0KB) + Internal Usage:154.2MB)																			



© Fortinet Inc. All Rights Reserved.

15

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

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

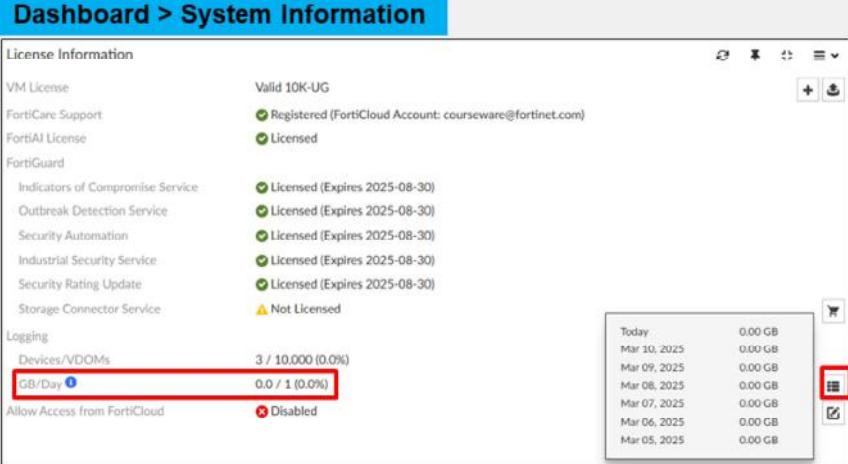
Determine the allocated space by adding the archive and analytics quota for all ADOMs.

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

**DO NOT REPRINT**  
**© FORTINET**

## Disk Quota on License Information Widget

- The **License Information** widget shows values lower than the disk quota
  - Reports only on the number of logs pushed to FortiAnalyzer *on that day*
  - Limited to statistics gathered by `fortilogd` daemon (FortiGate/FortiAnalyzer real-time forwarded logs)
    - Doesn't include log archive, FortiGate store and upload logs, FortiAnalyzer aggregated logs, or FortiClient logs
    - Doesn't include SQL tables



The screenshot shows the FortiAnalyzer dashboard under 'System Information'. The 'License Information' section lists various services and their licensing status. The 'Disk Quota' section shows a summary of log volume and a detailed history for the previous six days.

Category	Value	Unit	Percentage
Devices/VDOMs	3	10,000	(0.0%)
GB/Day	0.0	1	(0.0%)

**Show Details** icon (highlighted with a red box) is located next to the GB/Day row.

**Allow Access from FortiCloud** is set to **Disabled**.

**Detailed Log Volume History:**

Date	Log Volume
Today	0.00 GB
Mar 10, 2025	0.00 GB
Mar 09, 2025	0.00 GB
Mar 08, 2025	0.00 GB
Mar 07, 2025	0.00 GB
Mar 06, 2025	0.00 GB
Mar 05, 2025	0.00 GB

**Fortinet Training Institute** logo is at the bottom left. Copyright notice: © Fortinet Inc. All Rights Reserved. 16

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

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

**DO NOT REPRINT****© FORTINET**

## Disk Quota Enforcement

- Processes used for disk quota enforcement:

<b>logfiled</b>	<b>sqlplugind</b>	<b>oftpd</b>
Monitors log file size, SQL database size, and archive file size; sends commands to the other daemons to process	Enforces the SQL database size	Enforces the archive file size
Enforces log file size		

- The *logfiled* checks processes every 2 minutes (unless system resources are high) and estimates space used by SQL database
  - If estimated disk quota use is above 95%, FortiAnalyzer removes older files as needed down to 85%

Different processes are responsible for enforcing disk quotas:

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

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

# DO NOT REPRINT

© FORTINET

## Modify ADOM Disk Quota

- Monitor log utilization and quotas
 

```
# diagnose log device
```
- If the volume of logs is high, consider increasing the ADOM log quota to prevent the loss of the oldest logs
- Allocating an insufficient quota to an ADOM can:
  - Hinder log retention objectives
  - Consume unnecessary CPU resources while enforcing the quota with log deletion and database trims
  - Impact reporting if quota enforcement affects analytical data before a report is complete

The screenshot shows the 'System Settings > ADOMs' page. Under 'Data Policy', 'Keep Logs for Analytics' is set to 60 days and 'Keep Logs for Archive' is set to 365 days. In the 'Disk Utilization' section, the 'Allocated' quota is set to 3000 MB (Maximum Available: 30.4 GB). Below this, under 'Analytics: Archive', the 'Alert and Delete When Usage Reaches' threshold is set to 90%. A note at the bottom states: 'If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted.'

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Increasing Disk Space

- With FortiAnalyzer VMs, you can dynamically add more disk space:
  1. Power off the VM and add a new virtual disk
  2. Start the VM and enter `lvm info` to confirm the new disk was detected
    - The new disk is labeled as **Unused**
  3. Enter `execute lvm extend`
    - This command will add the space of the additional disk to the Logical Volume Manager (LVM)
  4. Reboot the VM, and then enter `get system status` to view the new amount of disk space available
- For FortiAnalyzer hardware, you must add one or more disks to the device
  - If you are using RAID, this requires you to rebuild your RAID array
- Be sure to account for future growth and size correctly from the outset!



© Fortinet Inc. All Rights Reserved. 19

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

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

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

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. By default, what happens when the allotted log disk space is full?  
 A. The oldest logs are overwritten.  
 B. Logging stops.
  
2. What is disk quota composed of?  
 A. Archive logs and analytics logs  
 B. Raw logs and archive files

DO NOT REPRINT

© FORTINET

## Lesson Progress



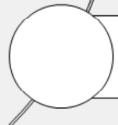
ADOMs



Disk Quota



High Availability



Firmware Upgrades

Good job! You now understand disk quotas.

Now, you will learn about FortiAnalyzer HA.

# DO NOT REPRINT

© FORTINET

## High Availability

### Objectives

- Describe FortiAnalyzer HA
- Configure HA
- Describe HA synchronization and load balancing
- Verify the regular operation of an HA cluster



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

22

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

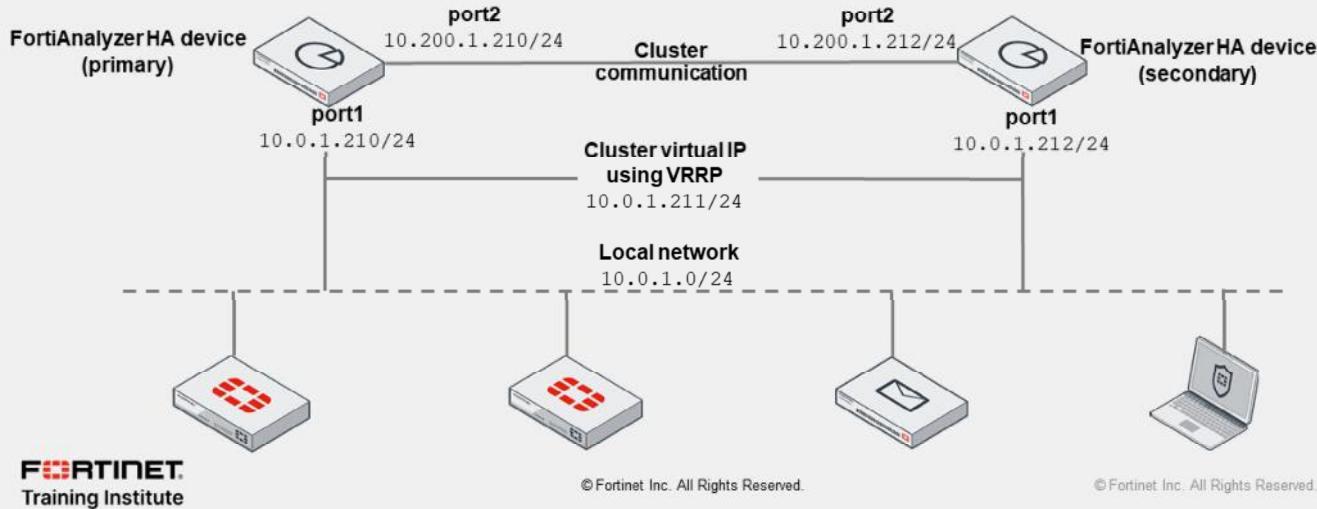
By demonstrating competence in configuring and troubleshooting high availability (HA), you can increase the availability of your FortiAnalyzer implementation.

# DO NOT REPRINT

## © FORTINET

## High Availability

- FortiAnalyzer HA offers:
  - Real-time redundancy in the event of primary device failure
  - Synchronization of logs and data among members of the HA cluster
  - Reduction of the load on the primary device by distributing some processes to secondary devices



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 23

A FortiAnalyzer HA cluster offers the following advantages:

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Active-Active HA

- FortiAnalyzer in active-passive HA mode requires layer 2 connectivity between devices to form a cluster
- However, FortiAnalyzer in active-active mode can form a cluster with devices on different subnets
  - This allows FortiAnalyzer HA to form between devices in different geographic locations
- Additional differences:

Active-passive	Active-active
Only the HA primary device can receive logs and archive files from its directly connected devices and forward them to the HA secondary devices	All HA members can receive logs and archive files from their directly connected devices and forward them to their HA peers
Only the HA primary device can forward logs and archive files to a remote server	All HA members can forward their directly received logs and archive files to a remote server

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

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

# DO NOT REPRINT

## © FORTINET

### HA Options

- FortiAnalyzer has three HA operation modes:
  - Standalone
  - Active-Passive
  - Active-Active
- Most common HA settings are available in the GUI
  - Virtual IP address
  - IP address and serial number of peer devices
  - Group name, group ID, and password must match for all cluster members
- Some options are available only on the CLI. For example:

```
# set unicast enable
```

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

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

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

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

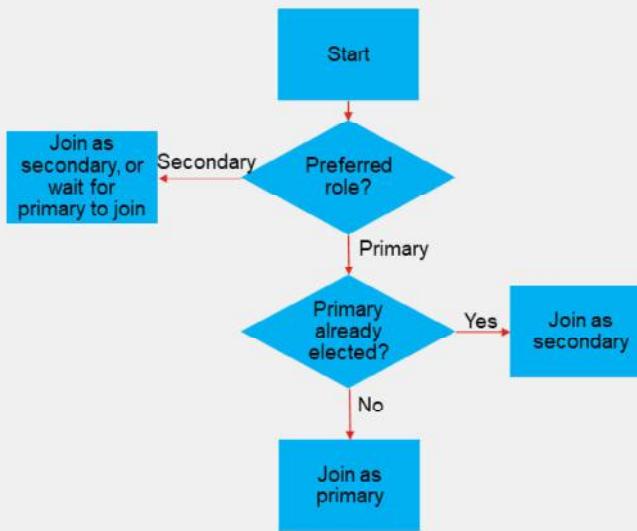
The primary device and all secondary devices must have the same **Group Name**, **Group ID**, and **Password**. The **Priority** setting is used during the selection of the primary device in the cluster. You can assign a value from 80 to 120, where a higher number has higher priority. The **Log Data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

# DO NOT REPRINT

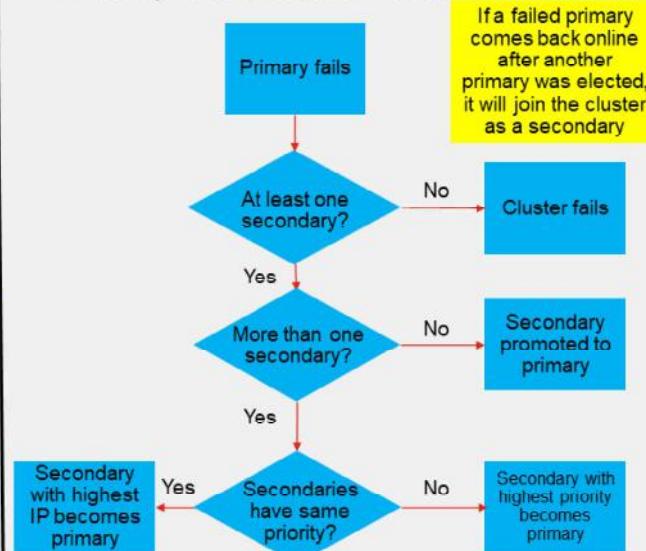
## © FORTINET

## HA Primary Election Process

- Initial primary election



- Primary election after failure



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 26

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## HA Synchronization

- FortiAnalyzer HA synchronizes logs in two states:
  - Initial synchronization (Initial Sync)
  - Real-time synchronization (Log Data Sync)
- FortiAnalyzer HA synchronizes the configuration of the following modules:
  - Device Manager, Incidents and Events, Reports, and most System Settings

System Settings	Configuration synchronized
Dashboard > System Information	ADOM widget only
All ADOMs	Yes
Admin	Yes
Certificates > CA Certificates	Yes
Certificates > CRL	Yes
Log Forwarding	Yes
Task Monitor	Yes
Advanced > Mail Server	Yes
Advanced > Syslog Server	Yes

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

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

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

Configuration synchronization provides redundancy and load balancing among the cluster devices. A FortiAnalyzer HA cluster synchronizes the configuration of the following modules to all devices in the cluster:

- Device Manager
- Incidents and Events
- Reports
- Most system settings

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

**DO NOT REPRINT****© FORTINET**

## HA Load Balancing

- FortiAnalyzer supports load balancing
- It improves the performance of the following modules:
  - Reports
  - FortiView
- When generating multiple reports, the loads are distributed to all HA cluster devices in a round-robin fashion
- For FortiView, cluster devices share some of the load when these modules generate output for their widgets



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 28

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

- Reports
- FortiView

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

**DO NOT REPRINT**  
**© FORTINET**

## HA Monitoring and Troubleshooting

- **Cluster Status** monitors the status of the FortiAnalyzer devices in an HA cluster
- Displays information about each cluster device

### System Settings > HA

Cluster Status							
<input type="checkbox"/>	Role	Serial Number	IP	Host Name	Uptime/Downtime	Initial Logs Sync	Configuration Sync
<input type="checkbox"/>	Primary	FAZ-VM0000065040	10.200.1.210	FAZ1	↑04m 13s	-	Config will be synced to secondaries
<input type="checkbox"/>	Secondary	FAZ-VMTM23008175	10.200.1.224	FAZ2	↑02m 50s	Syncing100%	In-Sync

- Use the following CLI commands to diagnose HA:

```

diagnose ha status (Shows HA status)
diagnose ha stats (Shows HA statistics)
diagnose ha dump-datalog (Dump HA data log)
diagnose ha failover (Run on master, force HA failover)
diagnose ha force-cfg-resync (Force HA to resync configuration)
diagnose ha load-balance (Shows HA load balance status)
diagnose ha restart-init-sync (Run on master, restart HA initial sync)

```

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

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

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

**DO NOT REPRINT**

**© FORTINET**

## 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 Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 30

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



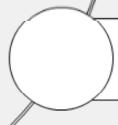
**ADOMs**



**Disk Quota**



**High Availability**



**Firmware Upgrades**

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT**

© FORTINET

## Firmware Upgrades

### Objectives

- Prepare for a firmware upgrade
- Manage a firmware upgrade
- Manage an HA upgrade



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

32

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

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

**DO NOT REPRINT****© FORTINET**

## Preparing for an Upgrade

- From the Fortinet Customer Service & Support portal:
  - Download and review the release notes
  - Download the firmware images
- Before starting an upgrade, use the **Device Manager** pane to review the status of all logging devices to ensure that no devices have **Status = Down**
- Run the `diagnose log device` command before and after the upgrade to verify that the device and ADOM disk quota are correct
- Back up the FortiAnalyzer configuration file and databases
- Back up the logs (recommended)
- Wait until all the reports that are running are finished, and make sure no reports are scheduled to run during the upgrade



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 33

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

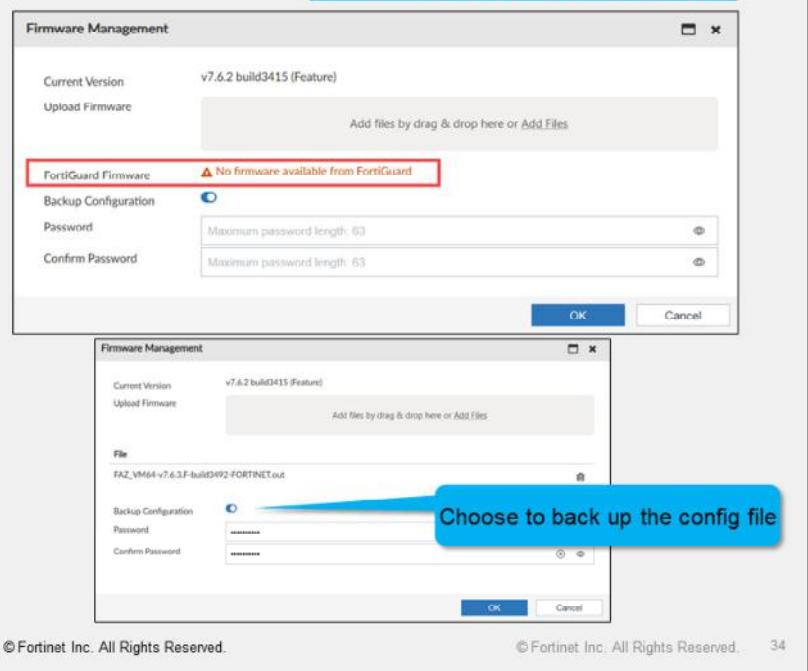
1. Review the release notes and download the firmware images from support.Fortinet.com.
2. Check the status of all logging devices to ensure that no devices have a status of **Down**.
3. Run the `diagnose log device` command and save its output.
4. After completing the upgrade, run the command again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

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

**DO NOT REPRINT**  
**© FORTINET**

## Methods of Upgrading FortiAnalyzer

- From the FortiAnalyzer GUI, download the firmware from FortiGuard and upgrade the device
- From the FortiAnalyzer GUI, upload the firmware that you previously downloaded from the Customer Service & Support portal
- Use the following CLI command to run firmware stored on an FTP or TFTP server:
  - execute restore image {ftp | tftp} <file path to server> <IP of server> <username on server> <password>



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 34

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

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

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

**DO NOT REPRINT****© FORTINET**

## Completing the Firmware Upgrade

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



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

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

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

**DO NOT REPRINT****© FORTINET**

## Upgrading an HA Cluster

- Upgrade the secondary devices
- Upgrade the primary device after you have upgraded all secondary devices and they have synchronized with the primary device
- When upgrading the primary device, one of the secondary devices is automatically selected as the primary device, following the rules configured in FortiAnalyzer
  - This allows the HA cluster to continue operating through the upgrade process with primary and secondary devices
- During the upgrade, you might see messages about firmware version mismatch. This is to be expected
  - When the upgrade is completed and all cluster members are at the same firmware version, you should not see this message
- If firmware versions between cluster members do not match, configuration synchronization is disabled. Other synchronization operations continue to function



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 36

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

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

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

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

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

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



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 37

**DO NOT REPRINT**

© FORTINET

## Lesson Progress



**ADOMs**



**Disk Quota**



**High Availability**



**Firmware Upgrades**

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT**

**© FORTINET**

## Review

- ✓ Configure and create ADOMs
- ✓ Monitor disk usage
- ✓ Modify the disk quota
- ✓ Configure HA
- ✓ Verify the regular operation of an HA cluster
- ✓ Prepare for a firmware upgrade
- ✓ Manage a firmware upgrade
- ✓ Manage an HA upgrade



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 39

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 how to use HA to make your FortiAnalyzer device more resilient against hardware failures.

DO NOT REPRINT

© FORTINET

**FORTINET**  
Training Institute

# FortiAnalyzer Administrator

## Managing Devices

 FortiAnalyzer 7.6

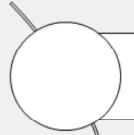
Last Modified: 16 July 2025

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.

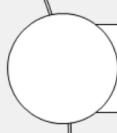
**DO NOT REPRINT**

© FORTINET

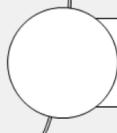
## Lesson Overview



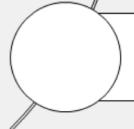
Registering Devices



Troubleshooting Communication Issues



Managing Registered Devices



Configuring connectors

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

**DO NOT REPRINT****© FORTINET**

## Registering Devices

### Objectives

- Demonstrate how to register a device on FortiAnalyzer
- Describe how device registration works with ADOMs
- View device status
- Create device groups



© Fortinet Inc. All Rights Reserved.

3

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.

**DO NOT REPRINT****© FORTINET**

## Methods of Device Registration

- Device registration states:
  - Registered: The device is authorized to store logs on FortiAnalyzer
  - Unregistered: The device is requesting permission to store logs on FortiAnalyzer
- Methods for registering a device with FortiAnalyzer:
  - Initiate registration from FortiAnalyzer or from the remote device
  - Stage devices on FortiAnalyzer by prepopulating their information
  - Add individual devices or configure a Security Fabric



© Fortinet Inc. All Rights Reserved.

4

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

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Method 1: Request From a Supported Device

1. The FortiGate administrator enables remote logging to FortiAnalyzer

2. The FortiAnalyzer administrator accepts (or rejects) the registration request
  - If ADOMs are enabled, you must add the requesting device to the desired ADOM
  - Optionally, you can assign a new name to the device (not shown in the image)

**FORTINET.**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

5

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

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

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

# DO NOT REPRINT

## © FORTINET

### Method 1: Request From a Supported Device (Contd)

- The FortiGate administrator enables the Security Fabric and enters FortiAnalyzer IP

**Security Fabric > Fabric Connectors > Logging & Analytics**

Logging Settings

FortiAnalyzer Cloud Logging

Status: Enabled (radio button selected)  Disabled

Server: 10.0.1.210 (highlighted with a red box)

Connection status: Connected (green icon)

Upload option: Real Time (radio button selected)  Every Minute  Every 5 Minutes

Allow access to FortiGate REST API:

Verify FortiAnalyzer certificate:  FAZ-VM0000065040

#### Security Fabric > Fabric Connectors > Security Fabric Setup

Security Fabric Settings

Security Fabric role: Standalone  Serve as Fabric Root (highlighted with a red box)

Join Existing Fabric:

Allow other Security Fabric devices to join: port3 (highlighted with a red box)

Fabric name: Training

Device authorization: 1 Connected / 1 Total (highlighted with a red box)

#### Device Manager

Device Manager

ADOM: root (highlighted with a red box)

2 unauthorized device(s). (highlighted with a red box)

All Logging Devices	Device Name	Platform	IP Address	Firmware Version
Unauthorized Devices	FortiFW	FortiGate-VM...	10.0.1.200	FortiGate 7.4.build2360
	Local-FortiGate	FortiGate-VM...	10.0.1.254	FortiGate 7.4.build2360

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

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

# DO NOT REPRINT

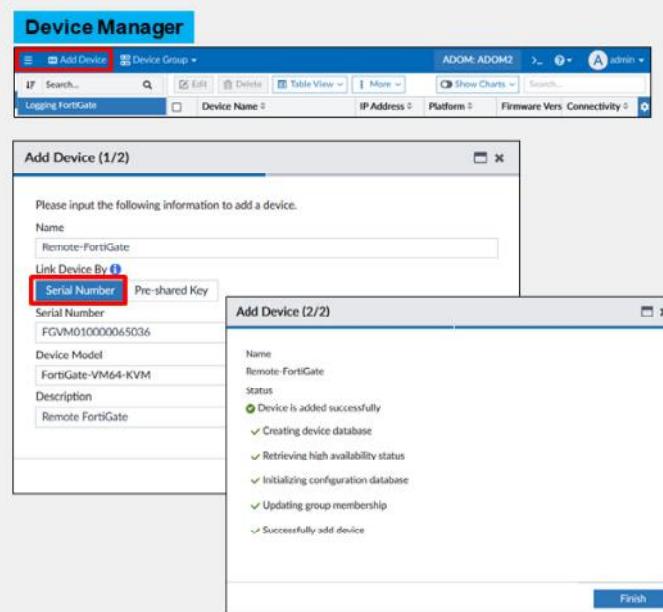
## © FORTINET

### Method 2: Add Device Wizard Using a Serial Number

- Add a device using **Device Manager**

- 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

© Fortinet Inc. All Rights Reserved.

7

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

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

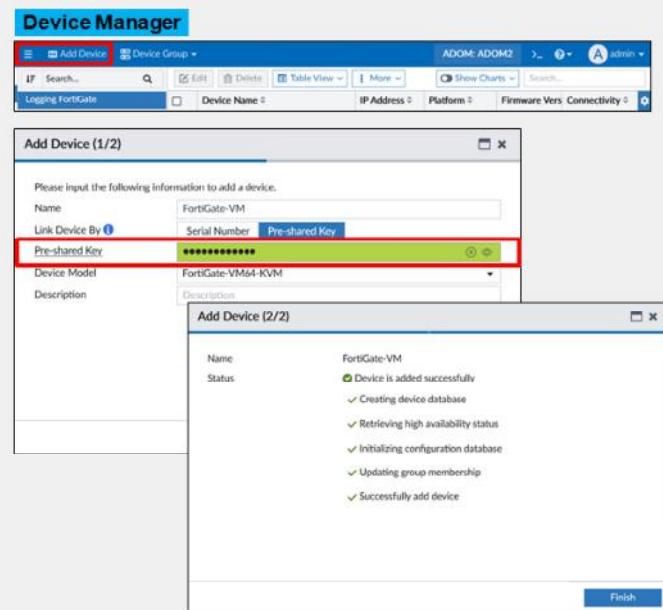
**DO NOT REPRINT**  
**© FORTINET**

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

### 1. Add a device using **Device Manager**

### 2. Select **Pre-shared Key** and complete the rest of the fields as needed

- Switch to the desired ADOM *before* adding a device using the wizard



**FORTINET.**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

8

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

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

# DO NOT REPRINT

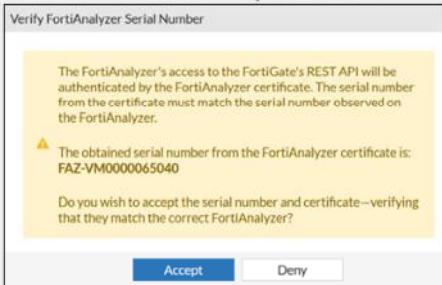
## © FORTINET

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

- Enter the pre-shared key on the FortiGate CLI

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

- Authorize FortiAnalyzer on FortiGate



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

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

# DO NOT REPRINT

## © FORTINET

### Method 4: Using Fortinet Security Fabric Authorization

1. Configure the FortiAnalyzer IP address and port that will accept authorizations through Fabric connectors
2. The FortiGate administrator enables the Security Fabric and FortiAnalyzer
3. The Fortinet administrator initiates the authorization process using valid FortiAnalyzer credentials
4. The Fortinet administrator approves the registration from the **Fortinet Security Fabric** window

The screenshot shows the 'System Settings > Settings' page under 'Fabric Authorization'. It displays the 'Authorization Address' as 10.0.1.210 and the 'Authorization Port' as 443. A yellow callout box notes: 'Note: This IP address must be reachable from the management computer because a pop-up window will open'.

The screenshot shows the 'FortiAnalyzer' status page with 'Status' set to 'Enabled' and 'Server' set to '10.0.1.210'. The 'Connection status' is 'Unauthorized'.

A 'Confirm' dialog box asks: 'FortiGate is unauthorized or denied on FortiAnalyzer. Would you like to open a window and authorize FortiGate on FortiAnalyzer?' with 'OK' and 'Cancel' buttons.

The 'Fortinet Security Fabric' window shows a list of devices. One device, 'Local-FortiGate', has an 'Approve' button highlighted with a red arrow.

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

10

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

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

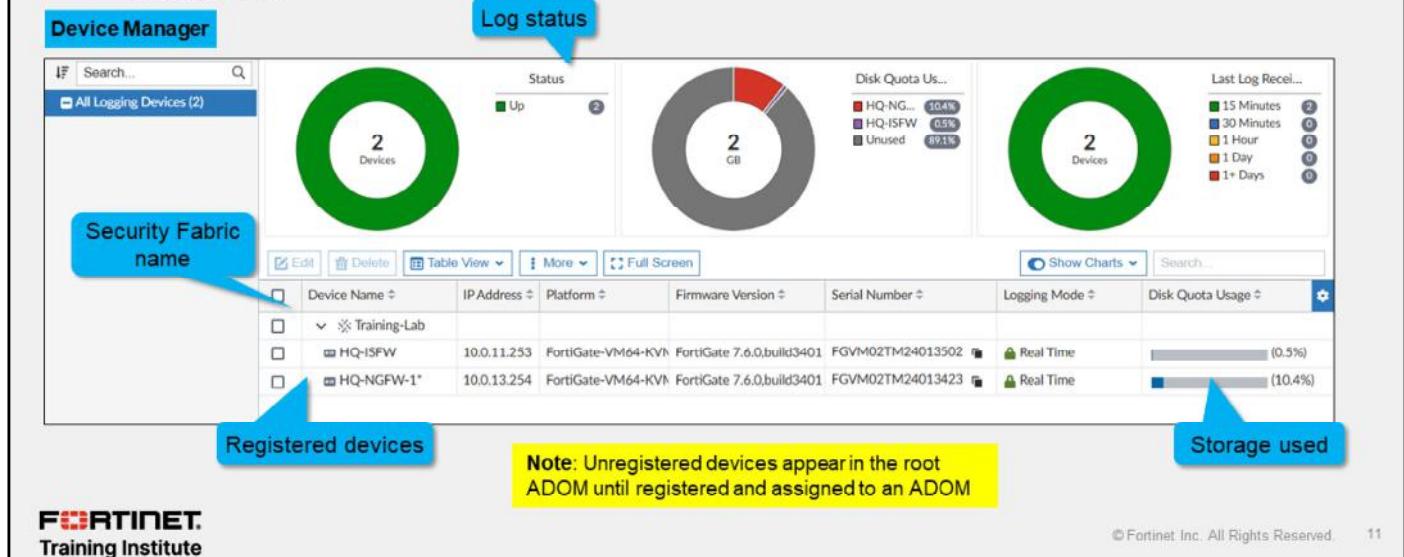
To complete the registration process, the FortiGate administrator must have valid credentials on FortiAnalyzer. To do so, click **Approve** in the **Fortinet Security Fabric** window.

# DO NOT REPRINT

## © FORTINET

## Viewing Device Status

- **Device Manager** displays all registered devices for that ADOM
  - Also shows log status (up or down)
  - Storage used



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

# DO NOT REPRINT

## © FORTINET

## Device Groups

- Create device groups to organize your devices in a logical and efficient manner

The screenshot shows two instances of the FortiAnalyzer Device Manager interface. In the top instance, the 'Device Group' dropdown is selected, revealing a list of groups: 'All Logging Devices' (selected), 'Canada\_Offices (0)', 'Ottawa\_HQ', and 'Toronto\_Branch'. A blue callout labeled 'Default group' points to 'All Logging Devices'. Another blue callout labeled 'Custom group' points to 'Canada\_Offices (0)'. A blue callout on the right states: 'Only devices from the selected group are displayed'. In the bottom instance, the 'Device Group' dropdown is also open, showing the same group structure. A yellow callout on the right states: 'Note: Device groups can be nested'.

Device Manager

Default group

All Logging Devices

Custom group

Canada\_Offices (0)

Ottawa\_HQ

Toronto\_Branch

OT

Device Manager

Note: Device groups can be nested

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

12

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

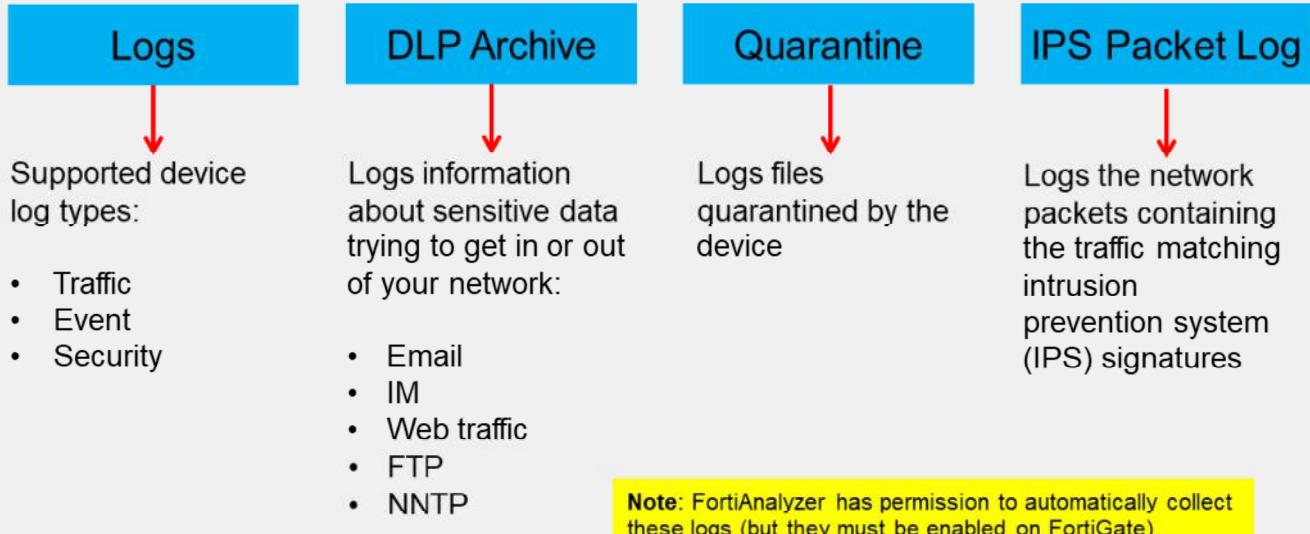
Additionally, you can nest device groups. In the example shown on this slide, a device group named **Canada\_Offices** contains a nested group with two branches.

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

# DO NOT REPRINT

## © FORTINET

### Which Logs Are Collected From FortiGate?



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

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

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

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

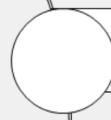
**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



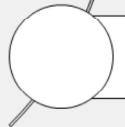
Registering Devices



Troubleshooting Communication Issues



Managing Registered Devices



Configuring connectors

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.

**DO NOT REPRINT****© FORTINET**

## Troubleshooting Communication Issues

### Objectives

- Troubleshoot device communication issues



© Fortinet Inc. All Rights Reserved.

16

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

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

**DO NOT REPRINT****© FORTINET**

## Basic CLI Commands

- Use the following FortiAnalyzer CLI commands to check system status, performance, and hardware statistics

What to investigate	CLI command to use
What is the status of FortiAnalyzer?	get system status
What are the performance statistics on FortiAnalyzer?	get system performance
What are the hardware statistics for CPU, memory, disk, and RAID?	diagnose hardware info
Which processes are using the most resources?	execute top



© Fortinet Inc. All Rights Reserved.

17

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

**DO NOT REPRINT****© FORTINET**

## Troubleshooting: get system status

```

FAZ # get system status
Platform Type : FAZVM64-KVM
Platform Full Name : FortiAnalyzer-VM64-KVM
Version : v7.6.2-build3415_241212_(GA.F)
Serial Number : FAZ-VM0000065040
BIOS version : 04000002
Hostname : FAZ
Max Number of Admin Domains : 5
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
HA Mode : Stand Alone
Branch Point : 3415
Release Version Information : GA.F
Current Time : Tue Mar 18 14:33:00 PDT 2025
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
x86-64 Applications : Yes
Disk Usage : Free 53.15GB, Total 58.99GB
File System : Ext4
License Status : Valid

```



© Fortinet Inc. All Rights Reserved.

18

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

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

# DO NOT REPRINT

## © FORTINET

### Troubleshooting: get system performance

```

FAZ # get sys performance
CPU:
Used: 37.77%
Used(Excluded NICE): 37.77%
%used %user %nice %sys %idle %iowait %irq %softirq
CPU0 42.29 18.54 0.00 22.92 57.71 0.62 0.00 0.21
CPU1 37.32 9.64 0.00 27.46 62.68 0.00 0.00 0.21
Memory:
Total: 10,264,016 KB
Used: 5,222,084 KB 50.9%
Total (Excluding Swap): 8,166,868 KB
Used (Excluding Swap): 5,222,084 KB 63.9%
Hard Disk:
Total: 61,857,580 KB
Used: 6,577,288 KB 10.6%
Inode-Total: 3,932,160
Inode-Used: 39,714 1.0%
IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
       6.4   0.2   6.3     4.6    115.0    0.0    1.7    0.0    0.0    0.0    580831.56
Flash Disk:
Total: 1,007,512 KB
Used: 416,460 KB 41.3%
Inode-Total: 65,536
Inode-Used: 43 0.1%
IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
       0.0   0.0   0.0     0.7    0.0    0.0    0.7    0.1    0.0    0.0    580831.57

```

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

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

# DO NOT REPRINT

## © FORTINET

### Troubleshooting: diagnose hardware info

FAZ # diagnose hardware info		### Memory info	### Disk info
<b>### CPU info</b>			
processor	: 0	MemTotal:	16412084 kB
vendor_id	: GenuineIntel	MemFree:	7129748 kB
cpu family	: 6	MemAvailable:	9675996 kB
model	: 63	Buffers:	82232 kB
model name	: Intel(R) Xeon(R) CPU E5-2680 v3 @ 2.50GHz	Cached:	4421640 kB
stepping	: 0	SwapCached:	0 kB
microcode	: 0x1	Active:	5799316 kB
cpu MHz	: 2500.000	Inactive:	2726196 kB
cache size	: 16384 KB	Active(anon):	5303000 kB
physical id	: 0	Inactive(anon):	640792 kB
siblings	: 1	Active(file):	496316 kB
core id	: 0	Inactive(file):	2085404 kB
cpu cores	: 1	Unevictable:	417692 kB
apicid	: 0	Mlocked:	417692 kB
initial apicid	: 0	SwapTotal:	2097148 kB
fpu	: yes	SwapFree:	2097148 kB
fpu_exception	: yes	AnonPages:	4439328 kB
cpuid level	: 13	Mapped:	698592 kB
wp	: yes	Shmem:	1930156 kB
flags	: fpu vme de pse tsc msr pae mce cx8	PageTables:	101480 kB
bugs	: cpu_meltdown spectre_v1 spectre_v2	CommitLimit:	10303188 kB
spec_store_bypass_l1tf l1tf mds swapgs itlb_multihit		Committed_AS:	46446328 kB
		VmallocTotal:	34359738367 kB

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

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

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

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

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

**DO NOT REPRINT**

**© FORTINET**

## Troubleshooting: execute top

top - 11:03:59 up 19:30, 0 users, load average: 0.29, 0.27, 0.22								
Tasks: 245 total, 1 running, 244 sleeping, 0 stopped, 0 zombie								
%Cpu(s): 1.8/1.0 3[   ]								
FID	USER	PR	NI	VIRT	RES	%CPU	%MEM	TIME+ S COMMAND
2585	root	20	0	165.3m	133.2m	2.6	0.8	34:19.03 S /bin/python /u
1025	root	20	0	97.6m	39.0m	1.3	0.2	11:04.17 S forticlidd.main
1032	root	20	0	833.3m	105.2m	1.3	0.7	12:36.29 S oftpd
3486	postgres	20	0	2844.2m	30.5m	1.0	0.2	0:20.11 S postgres
249	root	20	0	87.6m	35.1m	0.7	0.2	5:06.77 S cmdbsvr
1028	root	20	0	395.1m	39.2m	0.7	0.2	10:54.60 S logfwd.main
2607	root	20	0	158.6m	128.2m	0.7	0.8	7:22.42 S airflow schedul
8	root	20	0	0.0m	0.0m	0.3	0.0	1:27.66 I rcu_sched

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

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

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

**DO NOT REPRINT**  
© FORTINET

## Device and ADOM Status Check

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

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



© Fortinet Inc. All Rights Reserved. 22

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

**DO NOT REPRINT**  
**© FORTINET**

## Troubleshooting Communication Issues

- Use the following CLI commands to troubleshoot communication issues:

What to investigate	CLI command to use
Can the devices contact each other?	execute ping
Is FortiAnalyzer receiving logs?	diagnose debug application oftpd 8
Is FortiGate configured for remote logging to FortiAnalyzer?	FortiGate: show log fortianalyzer setting
Is the FortiAnalyzer source IP address set on FortiGate?	
Are the logging filters for logs sent to FortiAnalyzer on FortiGate enabled?	FortiGate: show log fortianalyzer filter
Is FortiGate capable of generating logs?	FortiGate: diagnose log test

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

Other questions to ask:

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

# DO NOT REPRINT

## © FORTINET

### Troubleshooting Communication Issues (Contd)

What to investigate	CLI command to use
Are packets leaving FortiGate, but not reaching FortiAnalyzer? Is traffic blocked? Is there a routing issue?	diagnose sniff packet <interface> <filter> <level> <count> <timestamp>

- Example output

```
FAZ# diag sniffer packet port1 'udp and port 53' 1 4 1
interfaces=[port1]
filters=[udp and port 53]
2025-02-28 16:29:17.741947 192.168.42.210.14610 -> 208.91.112.52.53: udp 27
2025-02-28 16:29:17.742016 192.168.42.210.14610 -> 208.91.112.52.53: udp 27
2025-02-28 16:29:17.745001 208.91.112.52.53 -> 192.168.42.210.14610: udp 155
2025-02-28 16:29:17.745047 208.91.112.52.53 -> 192.168.42.210.14610: udp 195
```

**System Settings > Network**

Network Sniffers						Search...
	+ Create New	Edit	Delete			
	Interface	Filter Criteria	# Packets	Max Packet Count	Progress	Actions
	port1	port=53	4	4000	(4/4000)	

Can also capture using the GUI

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 24

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

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

In the CLI example shown on this slide, the capture has the following characteristics:

- Traffic on port1
- UDP port 53 (DNS traffic)
- Level 1 verbosity
- Capture limit of four packets
- Local time

For more syntax information, consult the *CLI Reference* guide for FortiAnalyzer on [docs.fortinet.com](http://docs.fortinet.com).

**DO NOT REPRINT**  
**© FORTINET**

## Troubleshooting Communication Steps

### 1. Debug the oftpd process

```
FortiAnalyzer # diagnose debug application oftpd 8  
  
OFTP_destroy_SSL_context:1898 FGVM010000064692] SSL socket[24] pid[988] ssl[0x162d260]  
destroy_SSL_context  
[OFTP_recv_SSL_packet:1792 FGVM010000064692] SSL socket[27] pid[988] ssl[0x1d60b30] received [12] bytes:  
[oftpd_handle_session:3656 FGVM010000064692] handle KEEPALIVE (11)  
[OFTP_send_SSL_packet:1852 FGVM010000064692] SSL socket[27] pid[988] ssl[0x1d60b30] sent [21] bytes:
```

### 2. Generate test logs on FortiGate

```
Local-FortiGate # diagnose log test  
generating a system event message with level - warning  
generating an infected virus message with level - warning  
generating a blocked virus message with level - warning  
generating a URL block message with level - warning  
generating a DLP message with level - warning  
generating an IPS log message  
generating an botnet log message
```

Verify that FortiAnalyzer  
received logs

### 3. Verify that logs are received

**Note:** The debug command in FortiAnalyzer must be running before you generate the test logs in FortiGate

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 25

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

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

# DO NOT REPRINT

## © FORTINET

### FortiAnalyzer Temporarily Unavailable

- The FortiGate `miglogd` process caches logs on FortiGate when FortiAnalyzer is not reachable
- When the maximum cached value is reached, `miglogd` drops cached logs (oldest first)
- When the FortiAnalyzer connection is restored, `miglogd` sends the cached logs
  - FortiGate buffer keeps logs long enough to sustain a reboot of FortiAnalyzer. This is not intended for lengthy outages
- FortiGate devices with an SSD have a configurable log buffer

#### FortiGate CLI Commands

```
Remote-FortiGate # diagnose test application miglogd 6
mem=0, disk=9036, alert=0, alarm=0, sys=0, faz=3113, faz-cloud=0, webt=0, fds=0
interface-missed=170
Remote-FortiGate # diagnose test application fgtlogd 4
Queues in all miglogds: cur:0 total-so-far:23437
global log dev statistics:
faz=3115, faz_cloud=0, fds_log=0
faz 0: sent=3087, failed=0, cached=0 dropped=0

Remote-FortiGate # diagnose log kernel-stats
fgtlog: 1
fgtlog 0: total-log=16838, failed-log=0 log-in-queue=0
```

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

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

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

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

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

To change the buffer size, use the following commands:

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

**DO NOT REPRINT**  
© FORTINET

## Troubleshooting Logging Issues

What to Investigate	CLI Command to Use
What is the current log rate on FortiAnalyzer?	diagnose fortilogd lograte
What is the log rate per ADOM?	diagnose fortilogd lograte-adom
What is the log rate per device?	diagnose fortilogd lograte-device [filter]
What is the log message rate ?	diagnose fortilogd msgrate
What is the status of the FortiLog daemon?	diagnose fortilogd status



© Fortinet Inc. All Rights Reserved. 27

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

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

**DO NOT REPRINT****© FORTINET**

## 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

**DO NOT REPRINT**

© FORTINET

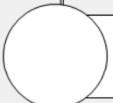
## Lesson Progress



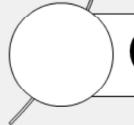
Registering Devices



Troubleshooting Communication Issues



Managing Registered Devices



Configuring connectors

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

Now, you will learn how to manage registered devices.

**DO NOT REPRINT****© FORTINET**

## Managing Registered Devices

### Objectives

- Move registered devices between ADOMs
- Add FortiGate devices in a high availability (HA) cluster to FortiAnalyzer



© Fortinet Inc. All Rights Reserved. 30

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.

**DO NOT REPRINT****© FORTINET**

## Managed Devices

- Use the **Device Manager** window to add, configure, and manage devices and VDOMs
- FortiAnalyzer begins collecting logs from a device or VDOM after you add and authorize it

The screenshot shows the FortiAnalyzer Device Manager interface. At the top, there are three donut charts: one for device status (7 devices, 1 Down, 6 Up), one for disk quota usage (32 GB, 0.2% Enterprise, 0.9% Enterprise, 0.1% Enterprise, 1.1% Others, 94.4% Unused), and one for last log reception (7 devices, 15 Minutes, 30 Minutes, 1 Hour, 1 Day, 1+ Days). Below the charts is a search bar and a table of managed devices.

Device Name	IP Address	Platform	HA Status	Description	Firmware Version	Last Log Time
Enterprise_FortiMail	10.100.88.4	FortiMail-VM			FortiMail 6.6	N/A
Enterprise_FortiSandbox	10.100.88.19	FortiSandbox-VM			FortiSandbox 6.6	4/4/2024, 11:23:12 AM PDT
Branch_Office_01	10.1.0.1	FortiGate-VM64...			FortiGate 7.4.0.build2360 (GA)	4/4/2024, 11:26:18 AM PDT
Branch_Office_02	10.2.0.1	FortiGate-VM64...			FortiGate 7.4.0.build2360 (GA)	4/4/2024, 11:26:18 AM PDT
Enterprise_Core	10.100.88.1	FortiGate-VM64...			FortiGate 7.4.0.build2360 (GA)	4/4/2024, 11:26:19 AM PDT
Enterprise_First_Floor	10.100.88.101	FortiGate-VM64...			FortiGate 7.4.0.build2360 (GA)	4/4/2024, 11:26:19 AM PDT
Enterprise_Second_Floor	10.100.88.102	FortiGate-VM64...			FortiGate 7.4.0.build2360 (GA)	4/4/2024, 11:26:19 AM PDT

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 31

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

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

FortiAnalyzer supports collection and analysis of logs from almost all Fortinet devices. Go to [docs.fortinet.com](https://docs.fortinet.com) for a complete list of all the devices that FortiAnalyzer supports.

**DO NOT REPRINT**  
© FORTINET

## Moving Registered Devices Between ADOMs

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

Name	Version	From ADOM
Remote-FortiGate	7.4	
FortiGate-VM64-KVM, 10.200.3.1	7.4	ADOM2

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Considerations Before Moving Devices

- What is the disk quota of the new ADOM? Ensure it has enough space
- Are the device analytics logs required for reports in the *new* ADOM? If so, rebuild the database to rebuild all ADOMs:

```
# execute sql-local rebuild-db
```

Reboots FortiAnalyzer

- To view the rebuild status while the database is being rebuilt, enter the following command:

```
# diagnose sql status rebuild-db
```

- When you move a device, only the archive (compressed) logs are migrated to the new ADOM. The analytics (indexed) logs stay in the old ADOM until you rebuild the database

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

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

# DO NOT REPRINT

## © FORTINET

### Adding a FortiGate HA Cluster

- FortiAnalyzer automatically discovers if a FortiGate device is in an HA cluster
  - If devices were registered to FortiAnalyzer before forming a cluster, you can manually add them together
- In an HA cluster, each device generates its own logs (separate serial number in logs)
  - The primary device is responsible for sending all logs from the other devices to FortiAnalyzer
- FortiAnalyzer distinguishes different devices by their serial number
  - Serial numbers are in log message headers

System Settings > HA

HA	From Existing Devices	HA Member	Action
HA Cluster HA Cluster List		Local-FortiGate (FGVM010000064692)	<input type="button" value="+"/>
		Remote-FortiGate (FGVM010000065036)	<input type="button" value="x"/> <input type="button" value="+"/>

Edit in Device Manager

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

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

**DO NOT REPRINT**

© FORTINET

## Lesson Progress



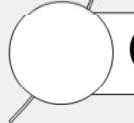
Registering Devices



Troubleshooting Communication Issues



Managing Registered Devices



Configuring connectors

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

Now, you will learn about connectors.

**DO NOT REPRINT**

**© FORTINET**

## Configuring Connectors

### Objectives

- Describe connector types
- Configure connector actions



© Fortinet Inc. All Rights Reserved. 37

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

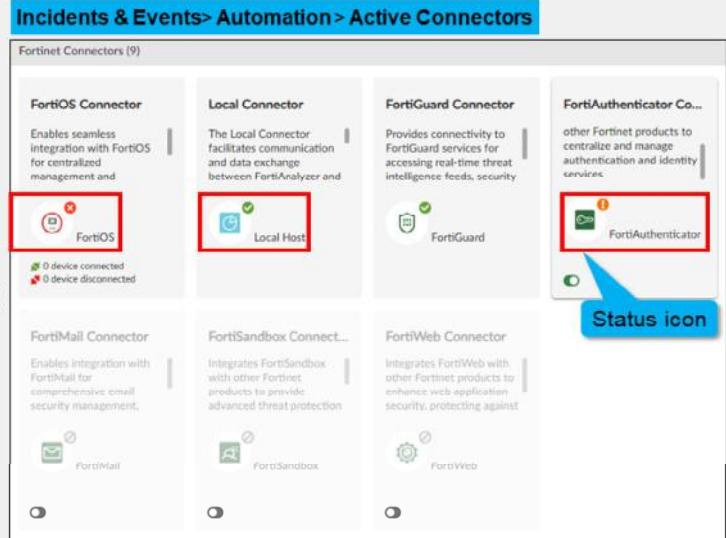
By demonstrating competence in configuring connectors, you will understand how FortiAnalyzer uses connectors to automate actions to be performed on other Fortinet devices.

# DO NOT REPRINT

## © FORTINET

## Connectors

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



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

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

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

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

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

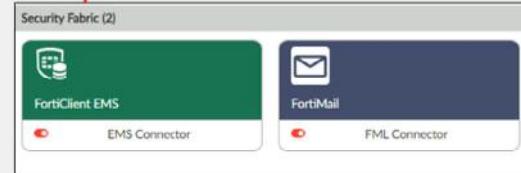
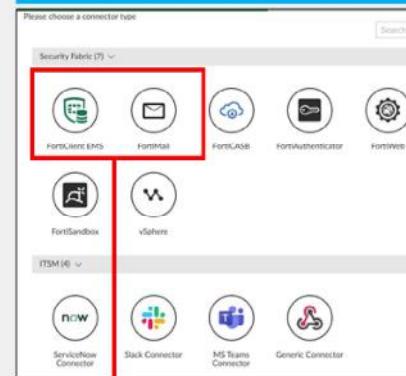
**DO NOT REPRINT**

© FORTINET

## Connector Types

- Two types of connectors
  - Security Fabric
  - ITSM
- Security Fabric connectors:
  - FortiClient EMS
  - FortiMail
  - FortiCASB
  - FortiAuthenticator
  - FortiWeb
  - FortiSandbox
  - vSphere
- ITSM connectors:
  - Service Now
  - Slack
  - MS Teams
  - Generic: Support additional third-party ticketing platforms

### Incidents & Events > Automation > Active Connectors



© Fortinet Inc. All Rights Reserved.

39

**FORTINET.**  
Training Institute

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

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

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

# DO NOT REPRINT

## © FORTINET

## Connector Actions

- Automated
- Predefined
- Set of actions for each connector

**Incidents & Events > Automation > Active Connectors**

Status	Name	Description	Filters/Parameters
Enabled	AV_FULL_SCAN	run full av scan on endpoints	id: cmd: av_full_scan
Enabled	AV_QUICK_SCAN	run quick av scan on endpoints	id: cmd: av_quick_scan
Enabled	GET_ENDPOINTS	retrieve list of endpoints and all of th...	filter: ip: filter group:
Enabled	GET PROCESSES	retrieve list of running process on en...	id: cmd:
Enabled	GET_SOFTWARE_INVENTORY	retrieve list of software and apps inst...	id: cmd:
Enabled	QUARANTINE	quarantine endpoints	id: cmd:
Enabled	TAG_ENDPOINTS	tag endpoints on EMS	id: cmd:
Enabled	UNQUARANTINE	unquarantine endpoints	id: cmd:
Enabled	UNTAG_ENDPOINTS	untag endpoints on EMS	id: cmd:
Enabled	VULN_SCAN	run vulnerability scan on endpoints	cmd: vuln_scan

Status	Name	Description	Filters/Parameters
Enabled	GET_EMAIL_STATISTICS	retrieve information of e...	id: cmd:
Enabled	GET_SENDER_REPUTATION	retrieve information suc...	id: cmd:
Enabled	ADD_SENDER_TO_BLOCKLIST	discard email received fro...	id: cmd:

FortiClient EMS  
connector actions

FortiMail  
connector actions

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 40

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

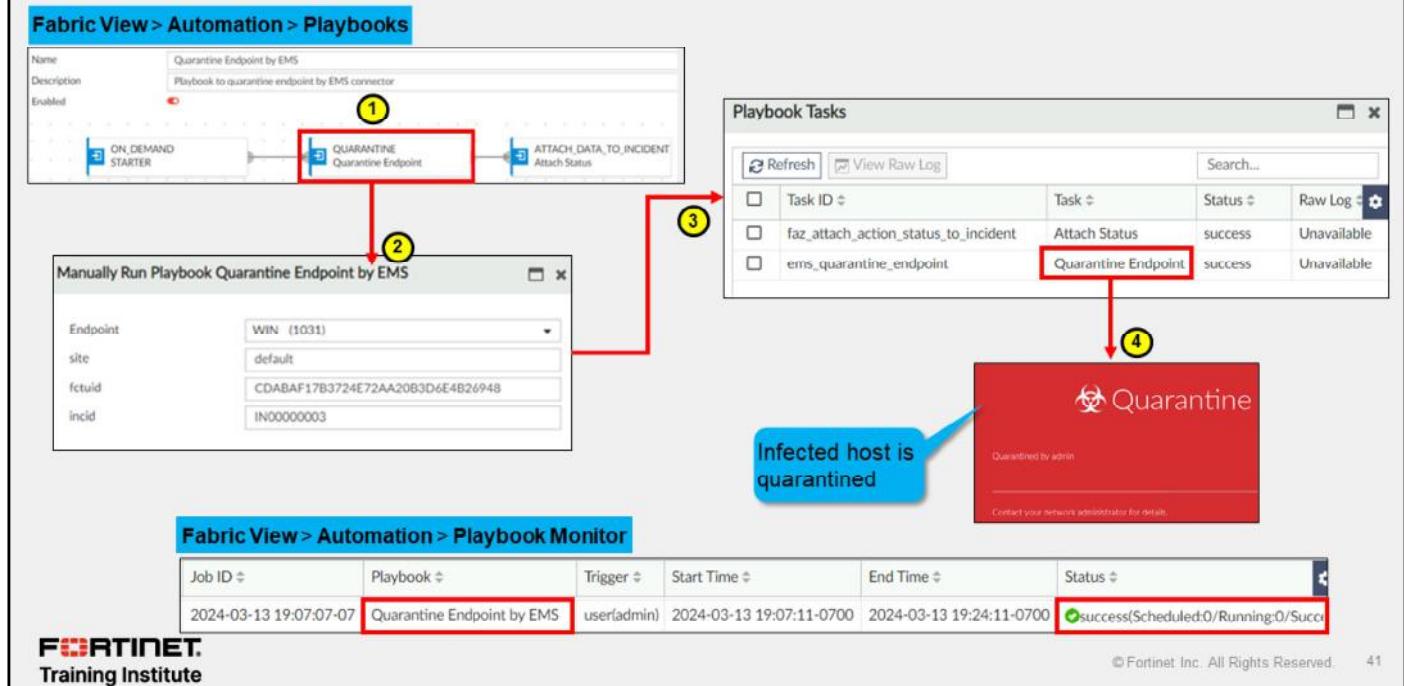
An example of when you might use a connector action in your network is to have a FortiClient EMS connector regularly retrieve a list of endpoints or perform quarantine actions on compromised endpoints.

All connector actions are predefined and cannot be modified.

# DO NOT REPRINT

## © FORTINET

### Use Case



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

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

The analyst performs the following actions:

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

The playbook automates the following actions:

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

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. Which color indicates an unknown connection status on FortiAnalyzer?

- A. Green
- B. Orange
- C. Black
- D. Red

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Registering Devices



Troubleshooting Communication Issues



Managing Registered Devices



Configuring connectors

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Register a device
- ✓ Describe how device registration works with ADOMs
- ✓ View device status
- ✓ Create device groups
- ✓ Troubleshoot device communication issues
- ✓ Move registered devices between ADOMs
- ✓ Add devices in an HA cluster to FortiAnalyzer
- ✓ Configure connector actions

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.

**DO NOT REPRINT****© FORTINET****FORTINET**  
Training Institute

# FortiAnalyzer Administrator

## Logs and Reports Management

 FortiAnalyzer 7.6

Last Modified: 16 July 2025

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.

**DO NOT REPRINT****© FORTINET**

## Lesson Overview

**Log Data Management****Report Management****System Performance Monitoring and Debugging****SOC Automation**

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

**DO NOT REPRINT****© FORTINET**

## Log Data Management

### Objectives

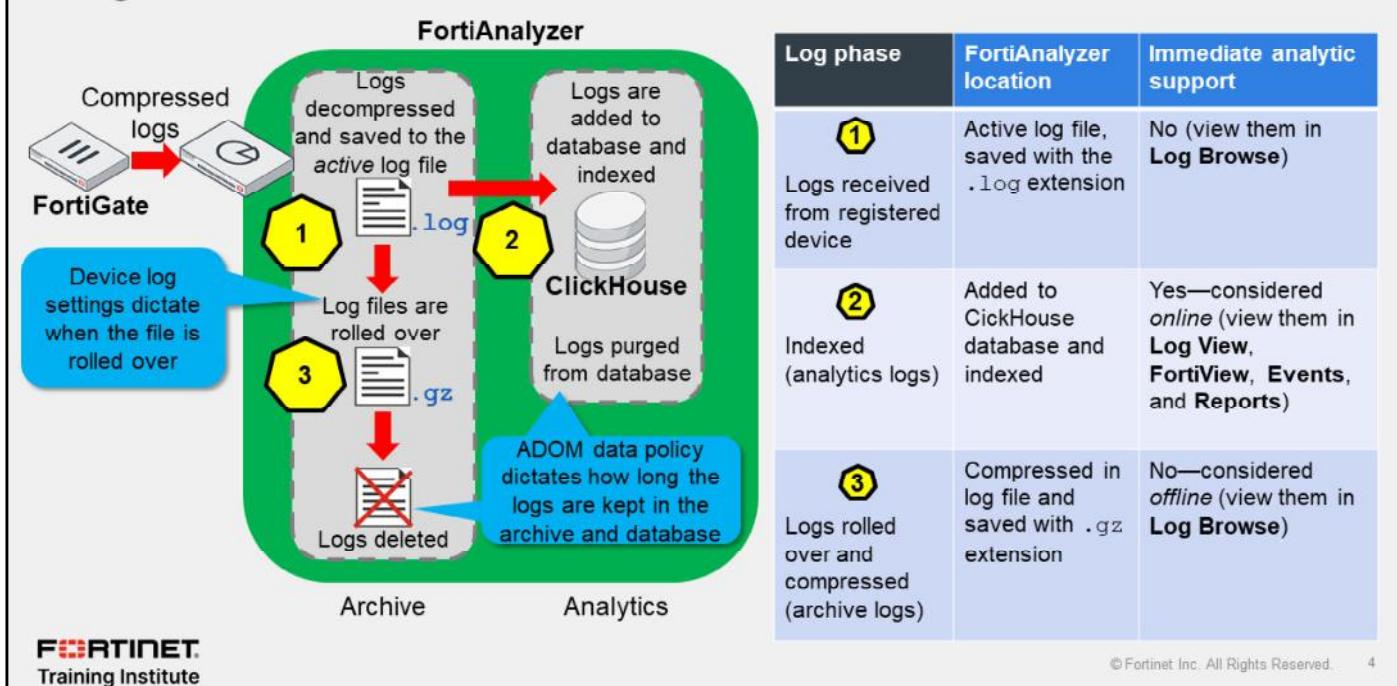
- Describe the log file workflow
- Perform log backups
- Describe Fabric connectors
- Configure log redundancy
- Configure log encryption
- Configure a log rollover and retention policy

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.

**DO NOT REPRINT**  
**© FORTINET**

## Log File Workflow



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

1. FortiAnalyzer decompresses all received logs and saves them in a log file on the FortiAnalyzer disk. The log file has the extension `.log`. For example, FortiAnalyzer saves FortiGate logs with the names `tlog.log` and `elog.log` for traffic and event logs, respectively. Note that the `tlog.log` file includes FortiGate security logs.
2. At the same time, FortiAnalyzer indexes the saved logs in the ClickHouse database to support analysis. Logs in the indexed phase are known as *analytics* logs. These logs are considered *online* and offer immediate analytic support. FortiAnalyzer purges analytics logs from the SQL database according to the ADOM data policy.
3. Eventually, when the log file reaches a configured size or a set schedule, FortiAnalyzer rolls over the log file. The process of rolling over consists of renaming the file, adding a timestamp, and then compressing it, which adds the `.gz` extension. These files are known as *archive* logs and are considered *offline*, so they don't offer immediate analytic support. Combined, they count toward the archive quota and retention limits, and FortiAnalyzer deletes them based on the ADOM data policy.

# DO NOT REPRINT

## © FORTINET

### Log Backup

- Protect log data from disk failure, deletion, or corruption
- Backup mechanisms include:
  - Using the GUI or CLI
    - GUI (**Fortinet Logs**) provides control to download a specific filtered view
    - GUI (**Log Browse**) provides rolled log download (can schedule upload of logs through **System Settings > Advanced > Device Log Settings**)

The screenshot shows the FortiAnalyzer Log View interface. On the left, a sidebar titled "Log View > Logs > Log Browse" lists "All Devices", "Last 1 Day", and "Mar 23 To Mar 24". It includes "Filter Mode" and "Add Filter" buttons. A table displays log entries for two devices: HO-NGFW-1 and FAZ-VMTM24012176. The table columns are: #, Device Name, Device ID, VDOM Name, Type, and File Name. HO-NGFW-1 has entries for elog.log and elog. FAZ-VMTM24012176 has an entry for \_self\_locallog\_. On the right, a modal window titled "Log View > Fortinet Logs <log type>" shows options: Real-time Log, Raw Log, Case Sensitive Search, Download (highlighted with a red box), and Chart Builder. A blue callout points to the "Download" button with the text "Text or CSV format". Below the table, a command line interface (CLI) example is shown: "# execute backup logs <device name|all> <ftp|sftp|scp> <server IP> <user> <password> <file path>". A blue callout points to this line with the text "Includes logs, archives, and quarantine (use logs-only if only log files are needed)".

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

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

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

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

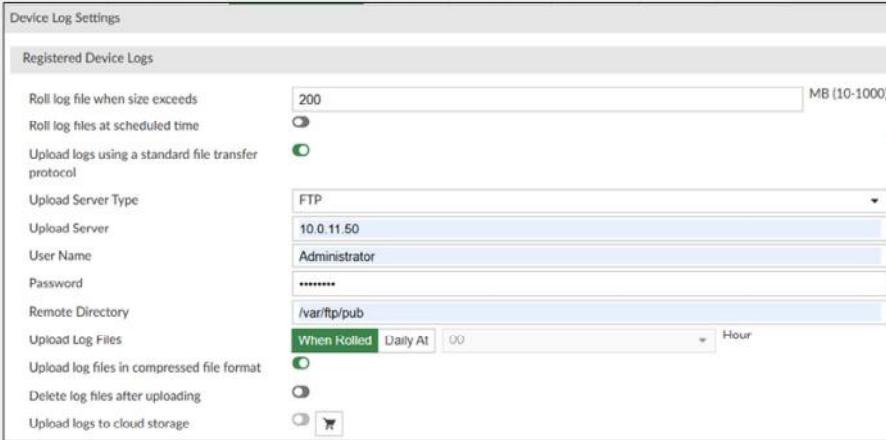
Use **LogView** when downloading a smaller subset of data. To download a large volume of data, use the **LogBrowse** page.

**DO NOT REPRINT**  
**© FORTINET**

## Log Backup (Contd)

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

### System Settings > Advanced > Device Log Settings



The screenshot shows the 'Device Log Settings' page under 'System Settings > Advanced > Device Log Settings'. It includes fields for 'Roll log file when size exceeds' (set to 200 MB), 'Upload Server Type' (set to FTP), 'Upload Server' (IP address 10.0.11.50), 'User Name' (Administrator), 'Password' (redacted), 'Remote Directory' (/var/ftp/pub), and 'When Rolled' (set to 'Daily At 00:00'). There are also options for 'Delete log files after uploading' and 'Upload logs to cloud storage'.

FortiAnalyzer supports  
FTP, SFTP, and SCP

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

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

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

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

**DO NOT REPRINT**

© FORTINET

## Fabric Connectors

- Configure FortiAnalyzer to send logs or notification events to:
  - Security Fabric: FortiClient EMS, FortiMail, FortiCASB, FortiAuthenticator, FortiWeb, FortiSandbox, vSphere
  - ITSM: ServiceNow, Slack, MS Teams, Generic Connector
- Improve data redundancy
- Reduce performance degradation
- Enrich incident response actions

The screenshot shows the 'Incidents & Events > Automation' page. At the top, there's a search bar and a 'Please choose a connector type:' dropdown set to 'Security Fabric'. Below this are two rows of icons: 'Security Fabric (7)' and 'ITSM (4)'. The 'ITSM (4)' row includes icons for 'now', 'ServiceNow', 'Slack', 'MS Teams', and 'Generic Connector'. The 'MS Teams' icon is highlighted with a red box and a red arrow pointing to it from the bottom left. A modal window titled 'Create New Fabric Connector - MS Teams Connector (2/2)' is open, showing 'Connector Settings' with a name of 'Connector' and a 'Description' field. Under 'Microsoft Teams', it shows 'Protocol: HTTPS', 'Method: POST', and a 'Teams Webhook URL' input field. The bottom right corner of the modal has a status bar with '© Fortinet Inc. All Rights Reserved.' and the number '7'.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

7

FortiAnalyzer supports integration with other products through Fabric connectors.

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Storage Connector Service

- Requires separate license for storage connector
- License includes storage limitation and expiration date

The screenshot shows the FortiAnalyzer interface. In the 'License Information' section, it says 'VM License: Valid 10K-UG'. Below that, under 'FortiGuard', there are several items listed as licensed, each with an expiry date of 'Expires 2024-06-04'. In the 'Storage Connector Service' section, there is a table with one row: 'Cloud' with '37.1 GB / 10.0 TB (0.0%)'. A red box highlights this row.

```
# diagnose fmupdate dbcontract
FAZ-VMTM23008175 [SERIAL_NO]
AccountID: *****@fortinet.com
Industry: Technology
Company: Fortinet
Contract: 10
ENHN-1-10-20240604
FGSA-1-06-20240604
FMWR-1-06-20240604
FOAS-1-06-20240604
FRVS-1-06-20240604
ISSS-1-06-20240604
PBDS-1-06-20240604
SCPC-1-06-20230912
SOAR-1-06-20240604
SPRT-1-10-20240604
```

The screenshot shows the 'Cloud Storage Usage' section. It displays usage statistics: Total Gigabytes Uploaded: 37 GB, Number of Files Uploaded: 10226 Files, Quota: 10 TB, and Number of Upload Requests Dropped: 0 Requests. A red box highlights the 'Cloud Storage Usage' section.

**Training Institute**

© Fortinet Inc. All Rights Reserved.

8

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

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

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

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

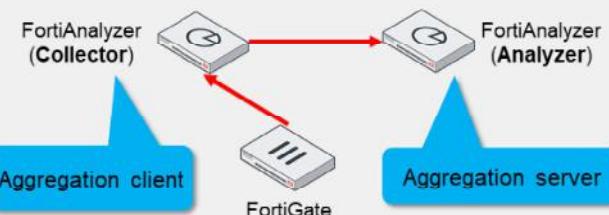
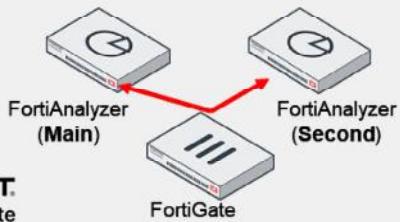
The `diagnose test application uploadd 63` command provides details, such as usage quota, total data upload in GB, total number of files uploaded, number of days remaining until license expiry, and number of uploaded requests that were dropped.

# DO NOT REPRINT

## © FORTINET

## Log Redundancy Options

- FortiAnalyzer HA cluster
  - Real-time redundancy when the primary fails
  - Log and configuration synchronization
- Send identical logs to a second logging server
  - FortiAnalyzer or Syslog
- CPU, RAM load is higher on FortiGate (more if SSL is enabled)
  - Log daemon must handle an additional TCP connection to a second log device
  - If the system is sized properly, the extra load is not a factor
- Log forwarding in aggregation mode
  - Collector sends incremental changes of logs, quarantined files, and archives to an aggregation server
  - Sends only what the analyzer doesn't have
  - If the analyzer fails, the collector sends all the data and repopulates the analyzer automatically
  - Can use aggregation mode only between two FortiAnalyzer devices



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

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

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

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

# DO NOT REPRINT

## © FORTINET

## Log Forwarding

- Forward logs to another FortiAnalyzer, syslog, or CEF
  - Supports two forwarding modes: aggregation and forwarding

### 1. Set log forwarding mode

```
# config system log-forward
  edit <log forwarding ID>
    set mode <aggregation, forwarding, disable>
  end
```

- aggregation:** Logs and content files stored and uploaded at scheduled time
- forwarding:** Real-time or near real-time forwarding logs to servers

### 2. Configure the server (FortiAnalyzer or syslog/CEF that receives logs)

```
# config system log-forward-service
  set accept-aggregation enable
end
```

### 3. Configure the client (FortiAnalyzer forwarding the logs)

- System Settings > Log Forwarding**

Specify which device logs to forward and set log filters to only send logs that match filter criteria

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

To configure log forwarding, you must complete the following:

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Encrypted Log Communication: OFTPS

- OFTP is used over SSL when information is synchronized between FortiAnalyzer and FortiGate
  - OFTP listens on port TCP/514
- Default setting
  - Auto-negotiated, so the OFTP server uses the OFTPS protocol only if the connecting FortiGate requests it

FortiGate:

```
# config log fortianalyzer setting
  set enc-algorithm {high-medium | high* | low}
end
```

FortiAnalyzer:

```
# config system global
  set enc-algorithm {high* | medium | low | custom}
end
```

FortiGate:

```
#config log fortianalyzer setting
  set reliable enable
end
```

Logs also use TCP/514 once enabled

FortiGate default encryption level is high (low encryption models can do only the low level)

FortiAnalyzer default encryption level is high. This encryption level must be equal to, or less than, the FortiGate device.



© Fortinet Inc. All Rights Reserved.

11

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

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

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

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

**DO NOT REPRINT****© FORTINET**

## Preventing Log Modification

- To prevent log modification, you can add a log checksum
- Configure FortiAnalyzer to record log file hash value, timestamp, and authentication code at transmission or rolling. Options include:
  - md5: Record the log file MD5 hash value only
  - md5-auth: Record the log file MD5 hash value and authentication code
  - none: Do not record the log file checksum

```
# config system global
    set log-checksum md5-auth {md5|md5-auth|none}
end
```

- You can also change the OFTP certificate to a custom one

```
# config system certificate oftp
    set mode custom
    set certificate <your PEM format certificate>
    set private-key <your PEM format private key>
end
```

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

The following log checksums are available:

- md5: Record log file MD5 hash value only.
- md5-auth: Record log file MD5 hash value and authentication code.
- none: Do not record the log file checksum.

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

**DO NOT REPRINT**  
**© FORTINET**

## Rolling Logs and Auto-Deleting Old Logs

- How can you better manage your logs on disk?

The screenshot shows the 'System Settings > Advanced > Device Log Settings' page. It is divided into two main sections: 'Registered Device Logs' and 'Automatically Delete'.

**Registered Device Logs:**

- 'Roll log file when size exceeds' is set to 200 MB (10-1000).
- 'Roll log files at scheduled time' is enabled, with a schedule of 'Weekly' every Sunday at 00:00.
- 'Upload logs using a standard file transfer protocol' is disabled.
- 'Upload logs to cloud storage' is disabled.

**Automatically Delete:**

- 'Device log files older than' is set to 365 days, scheduled daily at 00:00.
- 'Reports older than' is set to 365 days, scheduled daily at 00:00.
- 'Content archive files older than' is set to 365 days, scheduled daily at 00:00.
- 'Quarantined files older than' is set to 365 days, scheduled daily at 00:00.

Annotations with callouts point to these settings:

- A blue callout points to the 'Roll log file when size exceeds' section with the text: 'Roll log files when the size exceeds a set threshold'.
- A blue callout points to the 'Automatically Delete' section with the text: 'Automatically delete logs of a specified age'.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 13

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

You can configure the following:

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

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

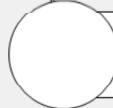
1. Which log forwarding mode stores logs and content files, and uploads them to another FortiAnalyzer server at a scheduled time?  
 A. Forwarding mode  
 B. Aggregation mode
  
2. Compressed logs on FortiAnalyzer are known as \_\_\_\_\_ logs.  
 A. archive logs  
 B. analytics logs

**DO NOT REPRINT****© FORTINET**

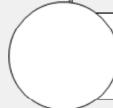
## Lesson Overview



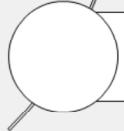
**Log Data Management**



**Report Management**



**System Performance Monitoring and Debugging**



**SOC Automation**

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

Now you will learn about managing reports.

**DO NOT REPRINT****© FORTINET**

## Report Management

### Objectives

- Describe the elements that constitute a report
- Describe how reports function within ADOMs
- Configure external storage for reports
- Enable auto-cache

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Purpose of Reports

- Reports summarize a large amount of log (text) data
- FortiAnalyzer retrieves the information collected from the log files of managed devices and presents it in tabular and graphical reports
- Reports provide a quick and detailed analysis of activity on your network

Reports > Report Definition > All Reports

Default reports categories

Application Reports
Asset and User Reports
Compliance Reports
Fabric Reports
FortiCache Reports
FortiClient Reports
FortiDDoS Reports
FortiDeceptor Reports
FortiFirewall Reports
FortiGate Reports
FortiMail Reports
FortiNAC Reports
FortiNDR Reports
FortiProxy Reports
FortiSandbox Reports
FortiWeb Reports
Network Reports
Outbreak Alert Reports
SOC Reports
Daily Summary Report

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 17

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

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

DO NOT REPRINT  
© FORTINET

## Elements That Comprise a Report

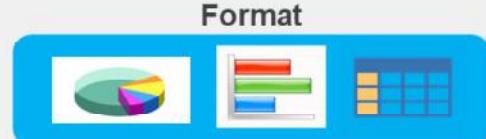
- A FortiAnalyzer report is a set of data in organized charts



- Which **data** from the ClickHouse database is displayed
- Which **format** the data is displayed in



Datasets are specific ClickHouse SQL SELECT queries



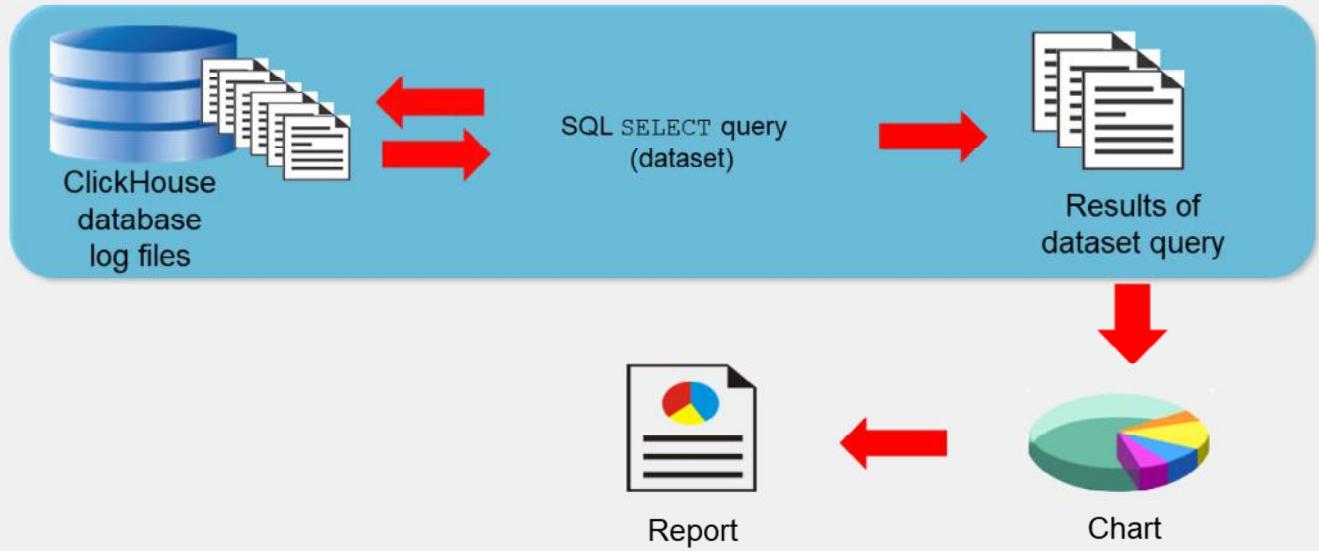
Format options include:  
pie charts, bar charts, or tables

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

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

**DO NOT REPRINT****© FORTINET**

## Report Workflow



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

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

**DO NOT REPRINT****© FORTINET**

## Reports and ADOMs

- Each ADOM has its own reports, libraries, and advanced settings
- Additional reports are available when you enable specific ADOMs
- Verify you are in the correct ADOM when creating reports

Reports > Report Definition > All Reports

<input type="checkbox"/>	Title
<input type="checkbox"/>	Application Reports
<input type="checkbox"/>	Asset and User Reports
<input type="checkbox"/>	Compliance Reports
<input type="checkbox"/>	Fabric Reports
<input type="checkbox"/>	FortiCache Reports
<input type="checkbox"/>	FortiClient Reports
<input type="checkbox"/>	FortiDDoS Reports
<input type="checkbox"/>	FortiDeceptor Reports
<input type="checkbox"/>	FortiFirewall Reports
<input type="checkbox"/>	FortiGate Reports

**Note:** A Fabric ADOM has default reports for multiple device types

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

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

**DO NOT REPRINT**  
© FORTINET

## Configure External Storage for Reports

- Send or store reports externally for backup purposes
- Requires configuration of a mail server to email reports
- Can also upload generated reports to a server (FTP/SFTP/SCP)

### System Settings > Advanced > Mail Server

Edit Mail Server Settings	
SMTP Server Name	Mail_Server
Mail Server	10.200.1.254
SMTP Server Port	25
Enable Authentication	<input checked="" type="checkbox"/>
E-Mail Account	admin@training.lab
Password	*****
From (Optional)	

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Configure External Storage for Reports (Contd)

- Configure output profiles for each ADOM
- Email reports or upload to server (HTML, PDF, XML, CSV, and JSON)
- First configure an output profile, then enable notifications for each report

### Reports > Report Definitions > All Reports

Enable Notification <input checked="" type="checkbox"/>
Output Profile Email Profile

### Reports > Advanced Settings > Output Profile

Name Email Profile	Comments
Output Format <input type="checkbox"/> HTML <input checked="" type="checkbox"/> PDF <input type="checkbox"/> XML <input type="checkbox"/> CSV <input type="checkbox"/> JSON	Subject Generated Reports
Body Please review these reports 27/1023	
Recipients Email Server	From To Action
Mail_Server: 10.200.1.254	admin@training.lab admin@training.lab x +
<input checked="" type="checkbox"/> Upload Report to Server	
Server Type FTP	FTP server
Server 10.1.1.1	
User user	
Password *****	
Directory reports	
<input checked="" type="checkbox"/> Delete file(s) after uploading	

Preconfigured mail server

FTP server

Option to delete reports locally after uploading to server

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

22

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

An output profile specifies the following:

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

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

**DO NOT REPRINT**

© FORTINET

## SQL Hard Cache (hcache) Data

- FortiAnalyzer must build the hcache before building the report
  - Increases report generation time
  - If no new logs are received for the reporting period, the hcache doesn't need to rebuild
  - If new logs come in, the hcache needs to rebuild
- To reduce report generation time, enable auto-cache
  - The hcache automatically updates when new logs come in, and FortiAnalyzer generates new log tables
- Enable hcache for most reports to ensure they are generated efficiently
  - Note that the hcache uses system resources (especially for reports that take a long time to generate datasets)

Reports > Report Definitions > All Reports

Generated Reports Settings Editor

Enable Auto-cache

Extended Log Filtering

Default Filtering  Device  Source IP  Destination IP  Endpoint ID  Source End User ID

Additional Log Fields

Policy Name (policyname)

1 entry selected

Enable **Extended Log Filtering** to cache specific log fields for faster filtering

**Note:** Hcache is automatically enabled for scheduled reports

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

23

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

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

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

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

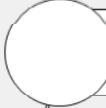
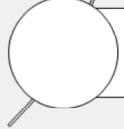
**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. On FortiAnalyzer, what is a dataset?
  - A. The database schema available to perform queries
  - B. A specific SQL SELECT query that retrieves data from the database
  
2. What is a benefit of enabling hcache in FortiAnalyzer reports?
  - A. It increases the efficiency of the storage used by reports.
  - B. It reduces the time required to generate reports.

**DO NOT REPRINT****© FORTINET**

## Lesson Overview

**Log Data Management****Report Management****System Performance Monitoring and Debugging****SOC Automation**

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

Now you will learn about system performance monitoring.

**DO NOT REPRINT****© FORTINET**

## System Performance Monitoring and Debugging

### Objectives

- Use common debugging commands



© Fortinet Inc. All Rights Reserved.

26

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

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

# DO NOT REPRINT

## © FORTINET

## Debugging

- To enable/disable debug on the CLI:
  - diagnose debug enable/disable
- Debug levels
  - From 0 to 255 (-1)
  - Level 8 provides the most detailed output
- Application debugs:
  - diagnose debug application <process> <level>
- Diagnose summary:
  - diagnose debug info
- Complete CLI dump of diagnostic commands:
  - execute tac report
- To add a timestamp:
  - diagnose debug timestamp enable

```
FortiAnalyzer # diagnose debug info
General
    cli debug level:          3
    console debug output:    enable
    debug timestamps:        disable
    terminal session debug output: disable
    terminal session data masking: disable

Application
    ddmd debug filter:       disable
    fazmaild debug level:    8
    fgfmsd debug filter:     disable

FortiAnalyzer #
```

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

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

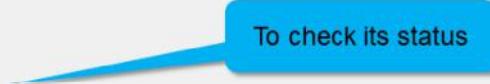
The `diagnose debug info` command shows which level the debug is currently at.

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

**DO NOT REPRINT****© FORTINET**

## Report Debugging

- `sqlreportd`
- Process responsible for report generation
- Will send queries of `sqlpuginnd`
- To check its status
  - diagnose sql status `sqlreportd`
- List generated reports
  - execute `sql-report list <ADOM>`


 To check its status

```
FortiAnalyzer # exec sql-report list ADOM1
No <days-range> input, search for recent 7 days's reports.
"Security Analysis-2025-06-06-0800-0700_f6f85be6-4320-41a1-89cd-02d634d5e06f_117"
"Daily Summary Report-2025-06-06-0300-0700_f6f85be6-4320-41a1-89cd-02d634d5e06f_113"
"Daily Summary Report-2025-06-05-0300-0700_f6f85be6-4320-41a1-89cd-02d634d5e06f_103"
"Daily Summary Report-2025-06-04-0300-0700_f6f85be6-4320-41a1-89cd-02d634d5e06f_97"
"Daily Summary Report-2025-06-03-0300-0700_f6f85be6-4320-41a1-89cd-02d634d5e06f_89"
"Daily Summary Report-2025-06-02-0300-0700_f6f85be6-4320-41a1-89cd-02d634d5e06f_81"
"Daily Summary Report-2025-06-01-0300-0700_f6f85be6-4320-41a1-89cd-02d634d5e06f_75"
"Daily Summary Report-2025-05-31-0300-0700_f6f85be6-4320-41a1-89cd-02d634d5e06f_67"
```



- View report content:
  - Execute `sql-report view report-data ADOM1 "Security Analysis-2025-06-06-0800-0700_f6f85be6-4320-41a1-89cd-02d634d5e06f_117"`

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

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

**DO NOT REPRINT****© FORTINET**

## Report Debugging (Contd)

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

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

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

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

```
FortiAnalyzer # exec sql-report run ADOM1
<name/title>  Please select one of the available SQL report schedule names or titles:
ADOM: ADOM1
NAME   TITLE
1      - Security Analysis
10000 - User Security Analysis
10002 - Bandwidth and Applications Report
10003 - Email Report
10004 - Admin and System Events Report
10006 - Threat Report
10007 - IPS Report
10008 - Detailed Application Usage and Risk
10009 - Top 20 Categories and Applications (Bandwidth)
10010 - Top 20 Categories and Applications (Session)
10011 - Top Allowed and Blocked with Timestamps
10012 - User Detailed Browsing Log
10013 - Hourly Website Hits
10014 - Top 20 Category and Websites (Bandwidth)
10015 - Top 20 Category and Websites (Session)
10016 - Top 500 Sessions by Bandwidth
10017 - User Top 500 Websites by Bandwidth
```



© Fortinet Inc. All Rights Reserved. 29

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

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

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

**DO NOT REPRINT****© FORTINET**

## Alert Email Debugging

- fazmaild process
- Daemon that handles all the email sending tasks
  - Report
  - Event Management mails
  - diagnose debug application fazmaild 8
- Test connection to specific mail server:
  - diagnose test connection mailserver "Mailserver:10.0.2.254"

- Alert email statistics

- diagnose test application fazmaild 0
- diagnose test application fazmaild 1
- diagnose test application fazmaild 2

```
FortiAnalyzer # diagnose test application fazmaild 2
total sent mail count: 0
total failed sendmail count: 0
total discard mail count: 0
last sendmail time: Wed Dec 31 16:00:00 1969
last request time: Fri Oct 11 12:56:20 2024
queue: 0/5000
queue timeout: 1800 seconds
```

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

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

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Upload Process Debugging

- `uploadadd process`
- Process responsible for uploading logs/reports to remote server
- To debug:
  - `diagnose debug application uploadadd 8`
- Command to see report queue:
  - `diagnose upload status`
- Queue operations:
  - `diagnose upload status`
  - `diagnose upload clear`

You can debug the upload of  
rolled logs or failed FTP  
uploads

```
FortiAnalyzer # diagnose upload status
-----upload log file stats-----
upload mode: BACKUP, schedule: 23 hours 46 minutes 43 seconds later,
queue: Log[0] / bkp[0] / m1[0] / m2[0] / m3[0]
prepare: done[53] / failed[0] / locate err[0] / time: total[0s], per file[0ms]
dispatch: done[53] / failed[0]
reprepare: done[0] / failed[0] / locate err[0]
-----upload rpt file stats-----
rptfiles: queue[0] / done[0] / abandoned[0] / retry[0]
cloud storage: upload[0], retry[0]
```

```
FortiAnalyzer # diagnose upload
clear           Clear uploading request.
status          Running status.
```

An issue where 10000 log files had to be  
converted into CSV and then uploaded.  
The process was taking a long time, so it  
was easier to clear the queue

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 31

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

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

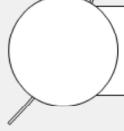
**DO NOT REPRINT****© FORTINET**

## Knowledge Check

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

**DO NOT REPRINT****© FORTINET**

## Lesson Overview

**Log Data Management****Report Management****System Performance Monitoring and Debugging****SOC Automation**

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

Now, you will learn SOC automation.

**DO NOT REPRINT****© FORTINET**

## SOC Automation

### Objectives

- Describe SOC automation content packs
- Describe log parsers
- Describe safeguarding



© Fortinet Inc. All Rights Reserved. 34

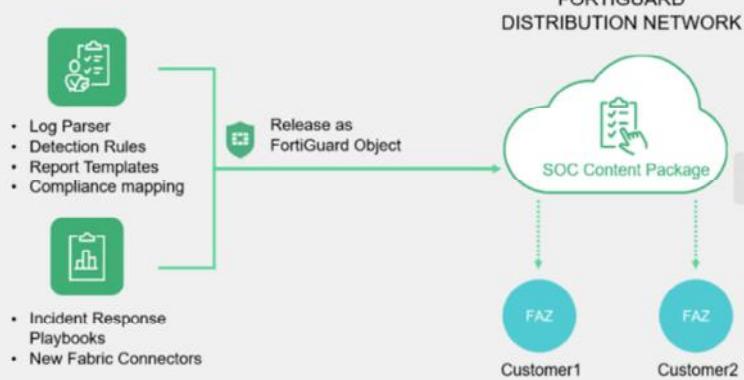
After completing this section, you should be able to achieve the objectives shown on this slide.

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

**DO NOT REPRINT**  
**© FORTINET**

## Security Automation Content Packs

- Get the latest detection rules (handlers), playbooks, compliance mapping, report templates, connectors, and log parsers from FortiGuard
  - Decouple security content release from the OS release
  - Automated content distribution similar to an outbreak package update



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

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

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

# DO NOT REPRINT

## © FORTINET

## Security Automation Content Packs (Contd)

- Details of the content pack released every month are available at <https://www.fortiguard.com>

The screenshot shows two parts of the FortiGuard Labs website. The top part is a table titled "Version Updates" with columns for "Version", "Last Update", and "Age". It lists several versions from 25.02004 to 24.10004. The bottom part is a detailed view of the "Version 25.03004" page, which includes a table of log parsers and their details.

Name	Application/Vendor	Category	Origin
Zscaler Firewall Log Parser	Zscaler	Network Devices	FortiGuard
Cisco Meraki Firewall Log Parser	Cisco	Network Devices	FortiGuard
<b>New</b> Office 365 Management Activity Log Parser	Office365	Audit and Compliance	FortiGuard
<b>New</b> Okta Log Parser	Okta	Cloud Services	FortiGuard
Juniper Firewalls Log Parser	Juniper	Network Devices	FortiGuard
Aruba CX Log Parser	Aruba	Network Devices	FortiGuard
Nozomi Networks Log Parser	Nozomi	Operational Technology	FortiGuard
Barracuda Firewall Log Parser	Barracuda	Network Devices	FortiGuard
Generic CEF Log Parser	CEF	Generic System	FortiGuard
Clavister Firewall Log Parser	Clavister	Network Devices	FortiGuard
McAfee Anti-Virus Log Parser	McAfee	Security Solutions	FortiGuard
Linux DHCP Log Parser	DHCP	Network Devices	FortiGuard

**FORTINET**  
Training Institute

The screenshot shows a list of log parsers under "Incident & Events > Log Parsers > Log Parsers". A blue callout bubble points to the "Origin" column, which is highlighted with a red box. Most entries have "FortiGuard" listed under "Origin".

Log parsers received  
from FDN

© Fortinet Inc. All Rights Reserved. 36

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

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

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

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

# DO NOT REPRINT

## © FORTINET

### Log Parsers

- Built-in log parsers have SIEM capabilities that parse, normalize, and correlate logs from
  - Fortinet products
  - Apache and Nginx web servers
  - Security event logs of Windows and Linux hosts
- Log parsers also help with integrating third-party device logs into FortiAnalyzer for analysis and log storage
- You can import new or custom log parsers into the FortiAnalyzer

#### Incident & Events > Log Parsers > Log Parsers

Name	Application/Vendor	Category	Origin
Zscaler Firewall Log Parser	Zscaler	Network Devices	FortiGuard
Cisco Meraki Firewall Log Parser	Cisco	Network Devices	FortiGuard
Office 365 Management Activity Log Parser	Office365	Audit and Compliance	FortiGuard
Okta Log Parser	Okta	Cloud Services	FortiGuard
Juniper Firewall Log Parser	Juniper	Network Devices	FortiGuard
Aruba CX Log Parser	Aruba	Network Devices	FortiGuard
Nozomi Networks Log Parser	Nozomi	Operational Technology	FortiGuard
Barracuda Firewall Log Parser	Barracuda	Network Devices	FortiGuard
Generic CEF Log Parser	CEF	Generic System	FortiGuard
Clavister Firewall Log Parser	Clavister	Network Devices	FortiGuard
McAfee Anti-Virus Log Parser	McAfee	Security Solutions	FortiGuard
Linux DHCP Log Parser	DHCP	Network Devices	FortiGuard

Helps integrate third-party device logs for analysis and storage

Log parsers received from FDN

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

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

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

**DO NOT REPRINT****© FORTINET**

## Assigned Parsers

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

Assigned Parsers > Log Parsers > Assigned Parsers			
Assigned Parsers		Log Parsers	
<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a> <input checked="" type="checkbox"/> Show Fortinet Device Parsers		Search...	
Device ID	Application	Assigned Parser	
FAZVMSTM23	FortiAnalyzer	FortiAnalyzer Log Parser	
FAZVMSTM23	FortiGate	FortiGate Log Parser	
FGVM02TM24	FortiAnalyzer	FortiAnalyzer Log Parser	
FGVM02TM24	FortiGate	FortiGate Log Parser	
FGVM02TM24	FortiGate	FortiGate Log Parser	
FGVM02TM24	FortiGate	FortiGate Log Parser	
FSAVMOTM24	FortiSandbox	FortiSandbox Log Parser	
FSAVMOTM24			

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

# DO NOT REPRINT

## © FORTINET

## Safeguarding

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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 39

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

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

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

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which feature allows you to integrate third-party devices with FortiAnalyzer for log analysis and storage?  
 A. Log parser  
 B. Safeguarding

**DO NOT REPRINT****© FORTINET**

## Lesson Overview

**Log Data Management****Report Management****System Performance Monitoring and Debugging****SOC Automation**

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Perform log backups
- ✓ Configure Fabric connectors
- ✓ Configure log redundancy and encryption
- ✓ Configure a log rollover and retention policy
- ✓ Configure and generate reports
- ✓ Configure external storage for reports
- ✓ Use common debugging commands
- ✓ Describe log parsers
- ✓ Describe safeguarding



© Fortinet Inc. All Rights Reserved. 42

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.

DO NOT REPRINT

© FORTINET



# FortiAnalyzer Administrator

## SQL and Datasets

 FortiAnalyzer 7.6

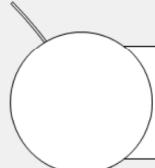
Last Modified: 16 July 2025

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.

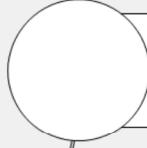
DO NOT REPRINT

© FORTINET

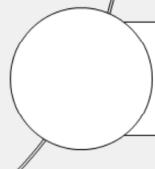
## Lesson Overview



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

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

**DO NOT REPRINT**

**© FORTINET**

## Datasets and SQL

### Objectives

- Describe datasets
- Understand SQL basics



© Fortinet Inc. All Rights Reserved.

3

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.

# DO NOT REPRINT

## © FORTINET

### Datasets

- Datasets are SQL SELECT queries to the database
  - Data populates a chart

ADOM specific

The screenshot shows the 'Reports > Report Definitions > Datasets' section of the FortiAnalyzer interface. On the left, a sidebar lists various navigation options like Dashboard, Device Manager, and Reports. The 'Reports' section is expanded, showing 'Report Definitions' which is also selected. A blue callout box highlights the 'App-Sessions-By-Category' dataset. To the right, a table lists several predefined datasets with columns for Name, Device Type, and Log Type. The 'App-Sessions-By-Category' dataset is selected, and its SQL query is displayed in a code box at the bottom right:

```
select appcat, count(*) as sessions from
$log where $filter and (logflag&1>0) and
nullifna(appcat) is not null group by
appcat order by sessions desc
```

**Dataset (example App-Sessions-By Category)**

© Fortinet Inc. All Rights Reserved. 4

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.

# DO NOT REPRINT

## © FORTINET

## Designing SQL Queries

- FortiAnalyzer uses SQL as the local database
- Proper query syntax required

**Reports > Report Definitions > Datasets**

The screenshot shows the 'Report Definitions > Datasets' page. On the left, there's a sidebar with 'Name', 'Log Type', and 'Query' sections. The 'Query' section contains an SQL query for 'App Sessions By Category' under the 'Traffic' tab:

```

1 SELECT
2     appcat,
3     count(*) AS sessions
4 FROM
5     $log
6 WHERE
7     $filter
8     AND (logflag & 1 > 0)
9     AND nullifna(appcat) IS NOT NULL
10 GROUP BY
11     appcat
12 ORDER BY
13     sessions DESC
  
```

Below the query are buttons for 'Recommendations', 'Validate', 'Analyze Query', and 'Format'. A blue callout box points to the 'Format' button with the text 'SQL queries are not case sensitive'.

On the right, there's a results table with columns 'Devices' and 'Sessions'. The table shows session counts for various categories. A red box highlights the 'Go' button at the top of the results table, and a blue callout box points to it with the text 'Test that queries are well-formed and contain keywords that are spelled correctly'.

Devices	Sessions
appcat	189
unscanned	166
Web.Client	56
Storage.Backup	32
Social.Media	21
Video/Audio	15
Collaboration	8
im	

© Fortinet Inc. All Rights Reserved. 5

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.

**DO NOT REPRINT****© FORTINET**

## SQL—The Declarative Language

```
SELECT dstip as destination_ip, count(*) as Session  
FROM $log WHERE $filter and dstip is not null GROUP BY  
dstip ORDER BY session desc LIMIT 7
```

- Declarative language: describes *what* needs to be done rather than *how* to do it
- All information in the database is represented as tables
  - Each table consists of a set of rows and columns
  - Two types of tables: user tables and system tables



© Fortinet Inc. All Rights Reserved.

6

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

**DO NOT REPRINT****© FORTINET**

## Basic Data Manipulation Constructs

- **SELECT**
  - Retrieve and display data from one or more database tables (read-only query)
  - `SELECT ... FROM ... WHERE`
- **INSERT**
  - Add new rows of data into a table
  - `INSERT INTO ... VALUES ...`
- **UPDATE**
  - Modify existing data in a table
  - `UPDATE ... SET ... WHERE`
- **DELETE**
  - Remove rows of data from a table
  - `DELETE FROM ... WHERE`

This is the only query statement used by FortiAnalyzer for reports



© Fortinet Inc. All Rights Reserved. 7

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.

**DO NOT REPRINT****© FORTINET**

## SELECT Statement

- The SELECT statement retrieves the log data you want from the database
- Must specify criteria using a recognized/supported clause

Clauses must be coded in a specific sequence

Clause	Definition
FROM	Selects the table or views
WHERE	Sets the conditions (all rows that do not satisfy the condition are eliminated)
GROUP BY	Collects data across multiple records and groups the results by one or more columns
ORDER BY	Orders the results by rows
LIMIT	Limits the number of records returned based on a limit value. OFFSET clause can be used with the LIMIT clause to offset the results by a set value

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.

**DO NOT REPRINT****© FORTINET**

## SELECT and FROM

- Use the SELECT query to ask specific questions of the database

```
SELECT column FROM log_type
```

Column from database that contains  
the value(s) you want to retrieve

The log type under which the data is contained  
(for example, traffic, web filter, and so on)

- When designing queries for SQL reports on the FortiAnalyzer device, the log type is assigned to a variable called \$log

```
SELECT dstip as destination_ip FROM $log
```

```
SELECT *
returns all
data
```

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.

**DO NOT REPRINT****© FORTINET**

## Multiple Log Types

- Search multiple log types
  - Combine the data so that you can compare and contrast information

```
SELECT dstip, hostname FROM $log-traffic, $log-webfilter
```

Log type syntax	Log type
\$log-attack	Attack log
\$log-dlp	DLP log
\$log-event	Event log
\$log-netscan	NetScan log
\$log-app-ctrl	Application control log
\$log-emailfilter	Email filter log
\$log-traffic	Traffic log
\$log-virus	Antivirus log
\$log-webfilter	Web filter log

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
```

# DO NOT REPRINT

## © FORTINET

### WHERE

- The WHERE clause requests data with certain characteristics
  - The expression specifies a stored value in the database

```
SELECT column FROM log_type WHERE expression1 and expression2 not in
expression3
```

Criteria you want to specify

Can use multiple expressions separated by AND/OR/NOT statements

```
SELECT dstip as destination_ip FROM $log WHERE $filter and dstip is
not null
```

#### Reports > Report Definitions > Datasets

Name	Example Dataset
Log Type	Traffic
Query	1 SELECT dstip as Destination_IP FROM \$log WHERE \$filter and dstip is not null

Go   Stop	Time Period	Today
Devices:	All Devices	▼
destination_ip		
1.1.1.2		
94.229.20.61		
54.83.43.69		
175.126.123.219		
224.141.85.77		

© Fortinet Inc. All Rights Reserved.

11

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.

**DO NOT REPRINT****© FORTINET**

## GROUP BY

- GROUP BY statement is usually used in conjunction with aggregate functions to group data by one or more columns.
- Returns one output row for each group
  - Can form groups within groups
- Each item in the SELECT list produces a single value per set

```
SELECT column, aggregate_function FROM log_type WHERE
expression1 and expression2 not in expression3 GROUP BY column
```

If GROUP BY is used without aggregates,  
it is similar to the DISTINCT clause

```
SELECT dstip as destination_ip, count(*) as session FROM $log
WHERE $filter and dstip is not null GROUP BY dstip
```

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 used 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).

**DO NOT REPRINT****© FORTINET**

## ORDER BY

- By default, rows of an SQL query result table are not arranged in a particular order

```
SELECT column, aggregate_function FROM log_type WHERE expression1  
and expression2 not in expression3 GROUP BY column ORDER BY  
column_name | column_number asc|desc
```

Can sort data by  
column name or  
column number

Can sort data in ascending (asc)  
or descending (desc) order. By  
default, sorts in ascending order

```
SELECT dstip as destination_ip, count(*) as session FROM $log WHERE  
$filter and dstip is not null GROUP BY dstip ORDER BY session desc
```

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.

**DO NOT REPRINT****© FORTINET**

## LIMIT and OFFSET

- The **LIMIT** clause limits the number of records retrieved from the query result
  - Useful in large deployments to help limit the CPU/memory usage for reports
  - Can be combined with **ORDER BY asc** to get the “top <x> results”

```
SELECT column, aggregate_function FROM log_type WHERE expression1  
and expression2 not in expression3 GROUP BY column ORDER BY  
column_name|column_number asc|desc LIMIT number OFFSET number
```

Specify how many records to return

Specify how many records to skip

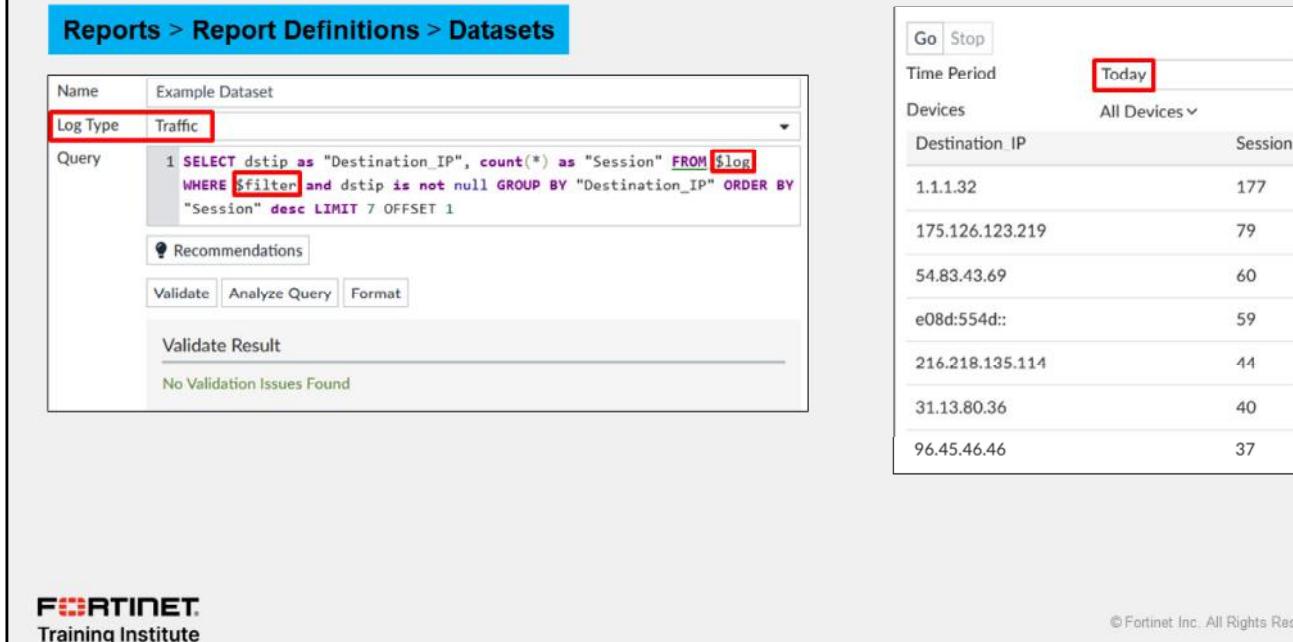
```
SELECT dstip as destination_ip, count(*) as session FROM $log WHERE  
$filter and dstip is not null GROUP BY dstip ORDER BY session desc  
LIMIT 7 OFFSET 1
```

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.

**DO NOT REPRINT**  
**© FORTINET**

## Creating a Dataset in FortiAnalyzer



The screenshot shows the FortiAnalyzer interface for creating a dataset. On the left, under 'Reports > Report Definitions > Datasets', a new dataset named 'Example Dataset' is being configured. The 'Log Type' is set to 'Traffic'. The 'Query' field contains the following SQL-like code:

```
1 SELECT dstip as "Destination_IP", count(*) as "Session" FROM $log
WHERE $filter and dstip is not null GROUP BY "Destination_IP" ORDER BY
"Session" desc LIMIT 7 OFFSET 1
```

Below the query, there are buttons for 'Recommendations', 'Validate', 'Analyze Query', and 'Format'. The 'Validate Result' section below says 'No Validation Issues Found'.

On the right, the results of the query are displayed in a table. The table has columns for 'Destination IP' and 'Session'. The data is as follows:

Destination IP	Session
1.1.1.32	177
175.126.123.219	79
54.83.43.69	60
e08d:554d::	59
216.218.135.114	44
31.13.80.36	40
96.45.46.46	37

At the bottom left is the Fortinet Training Institute logo, and at the bottom right are copyright and page number information: © Fortinet Inc. All Rights Reserved. 15.

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.

**DO NOT REPRINT**  
**© FORTINET**

## Analyzing a Dataset in FortiAnalyzer

The screenshot shows the FortiAnalyzer interface. On the left, under 'Reports > Report Definitions > Datasets', a configuration window is open for 'Example Dataset'. It has fields for 'Name' (Example Dataset), 'Log Type' (Traffic), and a 'Query' editor containing the following SQL-like query:

```
1 SELECT dstip as "Destination IP", count(*) as "Session" FROM $log
WHERE $filter and dstip is not null GROUP BY "Destination IP" ORDER BY
"Session" desc LIMIT 7 OFFSET 1
```

Below the query are buttons for 'Recommendations', 'Validate', 'Analyze Query', and 'Format'. A 'Validate Result' section below says 'No Validation Issues Found'.

On the right, the results are displayed in a table titled 'Destination IP' with a column 'Session'. The table shows the following data:

Destination IP	Session
1.1.1.32	177
175.126.123.219	79
54.83.43.69	60
e08d:554d::	59
216.218.135.114	44
31.13.80.36	40
96.45.46.46	37

At the bottom left is the Fortinet Training Institute logo, and at the bottom right is the copyright notice '© Fortinet Inc. All Rights Reserved. 16'.

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).

DO NOT REPRINT

© FORTINET

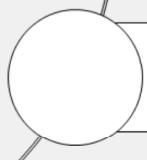
## Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

Good job! You now understand datasets and SQL.

Now, you will learn about SQL functions and operators.

**DO NOT REPRINT**

**© FORTINET**

## SQL Functions and Operators

### Objectives

- Understand SQL functions
- Understand operators



© Fortinet Inc. All Rights Reserved.

18

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.

**DO NOT REPRINT****© FORTINET**

## Aggregate Functions vs “Normal” Functions

Aggregate Functions	“Normal” Functions
Use the entire column of data as their input and produce a single output	Operate on each element in the column of data



© Fortinet Inc. All Rights Reserved.

19

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.

**DO NOT REPRINT**

**© FORTINET**

## NULLIF

- NULLIF function takes two arguments: if the first two arguments are equal, then NULL is returned; otherwise, the first argument is returned.

```
SELECT NULLIF(expression1, expression2)
```

Must be values that are of the same datatype

- NULL represents unknown data—it is not equal to zero

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.

**DO NOT REPRINT****© FORTINET**

## COALESCE

- Returns the first of its arguments that is not NULL. NULL is returned only if all arguments are NULL

```
SELECT coalesce(catdesc, 'unknown') as category,
coalesce(root_domain(hostname), 'unknown') as domain FROM $log
GROUP BY category, domain
```

category	domain
Malicious Websites	xnwipt.com
unknown	corolbugan.com
Unrated	agoinside.gq
Malicious Websites	40thousandwords.com
Malicious Websites	apple-ituncs-ios.com
Unrated	repeat-chief.ru
Malicious Websites	kir22.ru
Malicious Websites	blissyogawithannu.com
Unrated	ichiventures.com

Another common function used in FortiAnalyzer datasets is COALESCE. 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, ...)

**DO NOT REPRINT****© FORTINET**

## Aggregate Functions

- Aggregate functions perform a calculation on a set of values in a column and return a single value

### Aggregate Functions

AVG(expression)	Returns the average value
COUNT(expression)	Returns the number of rows
COUNT(*)	Returns all rows, even if some columns contain a NULL value
FIRST(expression)	Returns the first value
LAST(expression)	Returns the last value
MAX(expression)	Returns the largest value
MIN(expression)	Returns the smallest value
SUM(expression)	Returns the sum

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.

**DO NOT REPRINT**

**© FORTINET**

## Operators

- Reserved word or character used primarily in the WHERE clause to perform various operations
  - Arithmetic operators
  - Comparison operators
  - Logical operators



© Fortinet Inc. All Rights Reserved.

23

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

**DO NOT REPRINT****© FORTINET**

## 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

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.

**DO NOT REPRINT****© FORTINET**

## 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)

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.

**DO NOT REPRINT****© FORTINET**

## Logical Operators

- Test for the truth of some condition
  - Return a Boolean data type with a value of TRUE, FALSE, or UNKNOWN

Operator	Description
ALL	TRUE if all of a set of comparisons are TRUE
AND	TRUE if both Boolean expressions are TRUE
ANY	TRUE if any one of a set of comparisons are TRUE
BETWEEN	TRUE if the operand is within a range
EXISTS	TRUE if a subquery contains any rows
IN	TRUE if the operand is equal to one of a list of expressions
LIKE	TRUE if the operand matches a pattern
NOT	Reverses the value of any other Boolean operator
OR	TRUE if either Boolean expression is TRUE
SOME	TRUE if some of a set of comparisons are TRUE

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.

DO NOT REPRINT

© FORTINET

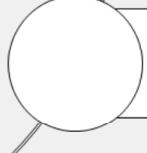
## Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

Good job! You now understand SQL functions and operators.

Now, you will learn about FortiAnalyzer functions and macros.

**DO NOT REPRINT****© FORTINET**

## FortiAnalyzer Functions and Macros

### Objectives

- Understand FortiAnalyzer functions
- Understand macros



© Fortinet Inc. All Rights Reserved.

28

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.

# DO NOT REPRINT

© FORTINET

## root\_domain

- `root_domain(hostname)`
  - Retrieves the root domain of the fully qualified domain name (FQDN)

```
SELECT devid, root_domain(hostname) as website FROM
$log WHERE 'user'='USER01' GROUP BY devid, hostname
ORDER BY hostname LIMIT 7
```

devid	website
FGVM010000064692	01gtf.org
FGVM010000064692	024student.com
FGVM010000064692	0306737775.win
FGVM010000064692	0452luntan.com
FGVM010000064692	10yi6bh1fvlx3mt260kix2924l.net
FGVM010000064692	118.171.94.192
FGVM010000064692	132r4zp18tqz1ktk0yg6kj4y2p.org

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.

# DO NOT REPRINT

## © FORTINET

### nullifna

- nullifna (expression)
  - Inverse operation of COALESCE
  - Can be used to filter out values with N/A and n/a from logs
- SQL syntax → SELECT NULLIF(NULLIF(<value>, 'N/A'), 'n/a')

```
SELECT coalesce(nullifna('user'), 'srcip') as user src,
coalesce(nullifna(root_domain(hostname)), 'unknown') as domain FROM
$log WHERE dstport='80' GROUP BY user src, domain ORDER BY
user_src LIMIT 7
```

user_src	domain
user	fgtk77.club
user	itourongbao.com
user	yuamyyimgxh.com.ve
user	144.76.106.114
user	envelopeson.com
user	tritonship.com
user	10yi6bh1fvlx3mt260kix2924l.net

If user is n/a, the source IP is displayed; otherwise, it returns the user name

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.

# DO NOT REPRINT

© FORTINET

## FortiAnalyzer Functions: email\_domain, email\_user

- **email\_domain:** Retrieves anything after the @ symbol in an email address
- **email\_user:** Retrieves anything before the @ symbol in an email address

```
SELECT 'from' as source, email user('from') as e_user,
email domain('from') as e_domain FROM $log LIMIT 5 OFFSET 10
```

Source	e_user	e_domain
user11@example.com	user11	example.com
user12@hostname.com	user12	hostname.com
user13@exampleXYZ.com	user13	exampleXYZ.com
user14@hostnameXYZ.com	user14	hostnameXYZ.com
user15@example.com	user15	example.com

`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**.

**DO NOT REPRINT**

**© FORTINET**

## FortiAnalyzer Functions: `from_dtime`, `from_itime`

- `from_dtime(bigint)`: Returns device timestamp without time zone
- `from_itime(bigint)`: Returns FortiAnalyzer timestamp without time zone

```
SELECT itime, from_itime(itime) as faz_local_time, dtime,
       from_dtime(dtime) as dev_local_time FROM $log LIMIT 3
```

itime	faz_local_time	dtime	dev_local_time
1699305243	2023-11-06 13:14:03	1699276391	2023-11-06 13:13:11
1699305243	2023-11-06 13:14:03	1699276391	2023-11-06 13:13:11
1699305243	2023-11-06 13:14:03	1699276399	2023-11-06 13:13:19

`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**.

**DO NOT REPRINT****© FORTINET**

## Macros

- FortiAnalyzer date and time macros

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

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.

DO NOT REPRINT

© FORTINET

## Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

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

**DO NOT REPRINT**  
**© FORTINET**



**FORTINET®**



**No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.**

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.