

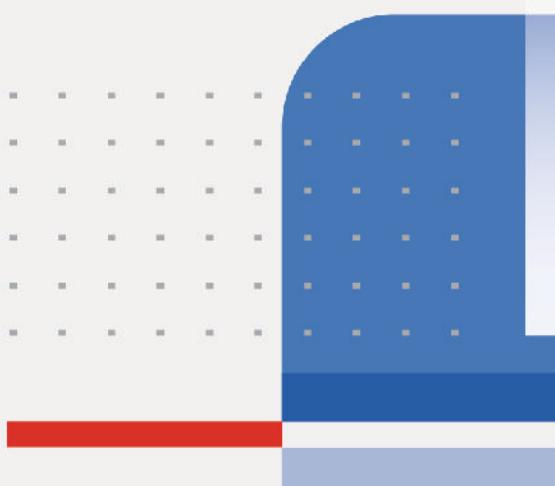
DO NOT REPRINT
© FORTINET



FortiAnalyzer Analyst 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

01 SOC Concepts and Security Fabric.....	4
02 Log Data Flow and Navigation.....	32
03 Events, Indicators, and Incidents.....	72
04 FortiAI, Threat Hunting, and Troubleshooting.....	111
05 Reports.....	152
06 Playbooks.....	193
Supplementary - FortiOS Logging.....	223

DO NOT REPRINT**© FORTINET**

FortiAnalyzer Analyst

SOC Concepts and Security Fabric

A small red square icon with a white "FA" monogram inside.

FortiAnalyzer 7.6

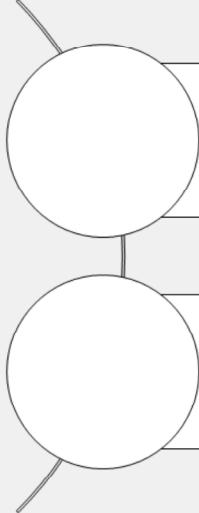
Last Modified: 16 July 2025

In this lesson, you will learn about the key features and concepts of a SOC, and the role that FortiAnalyzer plays in it. You will also learn how to initially access FortiAnalyzer.

DO NOT REPRINT

© FORTINET

Lesson Progress



SOC Concepts

Fabric Integration

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

DO NOT REPRINT**© FORTINET**

SOC Concepts

Objectives

- Describe SOC objectives
- Describe SOC responsibilities
- Describe SOC roles
- Describe the role of FortiAnalyzer in a SOC

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

By demonstrating competence in SOC features and concepts, you will be able to better understand the FortiAnalyzer features in your network.

DO NOT REPRINT**© FORTINET**

SOC Objectives



Threat identification

- Establish approach to threat intelligence
- Gain the knowledge required to recognize existing and emerging threats



Exposure and validation

- Assess your network
- Understand degree of exposure to attacks



Monitoring and detection

- Monitor the network to detect threats
- Understand detection technology



Response

- Consider impact avoidance
- Consider impact when responding

The SOC is a team that is dedicated to security operations. They are responsible for real-time security monitoring across the organization's IT infrastructure, including applications, networks, devices, and cloud environments.

The SOC has four key objectives:

- Threat identification: This includes establishing an approach to threat intelligence, so the SOC has the knowledge required to recognize existing and emerging threats.
- Exposure and validation: This involves assessing your network to understand its degree of exposure to attacks. Continuously assessing the network's exposure is important for effective monitoring and detection.
- Monitoring and detection: The SOC monitors the network to detect threats. The SOC must understand where to place detection technology and the threats they are looking for to align objectives with the organization's needs and compliance requirements.
- Response: This should be considered in terms of impact avoidance; when the attack has already occurred and been detected, the SOC must consider the impact when responding.

DO NOT REPRINT**© FORTINET**

SOC Responsibilities

Objective	Responsibility
Threat identification	<ul style="list-style-type: none"> • Threat intelligence • Compliance
Exposure and validation	<ul style="list-style-type: none"> • Continuous threat exposure management (CTEM): <ol style="list-style-type: none"> 1. Scoping 2. Discovery 3. Prioritization 4. Validation 5. Mobilization
Monitoring and detection	<ul style="list-style-type: none"> • Real-time monitoring • Threat detection
Response	<ul style="list-style-type: none"> • Incident investigation • Incident response

The SOC objectives can be further broken down into responsibilities for security operations:

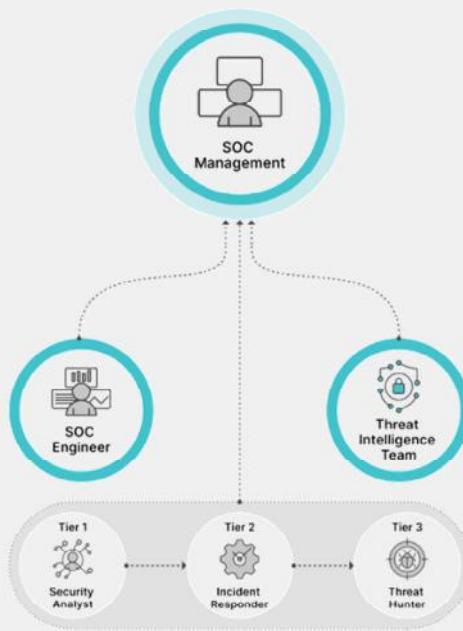
- Threat intelligence: The SOC should stay updated on the latest cyberthreats to refine detection strategies and enhance defensive capabilities. Threats are constantly evolving, so it is important for a SOC to leverage support from other resources when possible.
- Compliance: The SOC must adhere to regulatory standards for its industry and geographical location while maintaining records of threats and incident responses.
- CTEM: This methodology for scoping, prioritizing, and validating threat exposure in the network allows the SOC to plan how to best mobilize its people and processes for security operations.
- Real-time monitoring: The SOC requires access to a lot of information to monitor network activity. This is accomplished using a data lake that stores information, including logs from all devices in the Security Fabric for threat detection. Dashboards, reports, and integrated security information and event management (SIEM) features monitor the network for threats and incidents.
- Threat detection: When monitoring the network, the SOC is also responsible for detecting active and potential threats. Tools such as SIEM and extended detection and response (XDR) systems can help gather and analyze telemetry data to identify potential threats. In addition, SIEM tools and third-party services are used to quickly identify incidents and emerging outbreaks in the network.
- Incident investigation: After they identify threats, the SOC is responsible for investigating these incidents further to ensure the attack does not lead to any further risks or compromise. Implementing measures such as isolating compromised systems during investigation can neutralize the threat and minimize damage from a security incident. Incident reporting is critical to ensuring the investigation is complete, tracking all the potentially affected systems and devices.
- Incident response: As part of incident investigation, the SOC also responds to threats by blocking IP addresses, domains, or URLs and coordinating recovery efforts for affected devices.

DO NOT REPRINT

© FORTINET

SOC Roles

- Tier 1: Security Analyst
 - Triage
- Tier 2: Incident Responder
 - Investigate escalated alerts in more depth for response
- Tier 3: Threat Hunter
 - Proactively hunt complex threats



A SOC can include multiple roles that are responsible for maintaining an organization's security posture. Some roles can be organized in a tiered structure to monitor and respond to threats, while other roles are responsible for maintaining tools, processes, and strategic direction. When working with large organizations and SOCs, having multiple roles can help handle the volume or complexity of security operations.

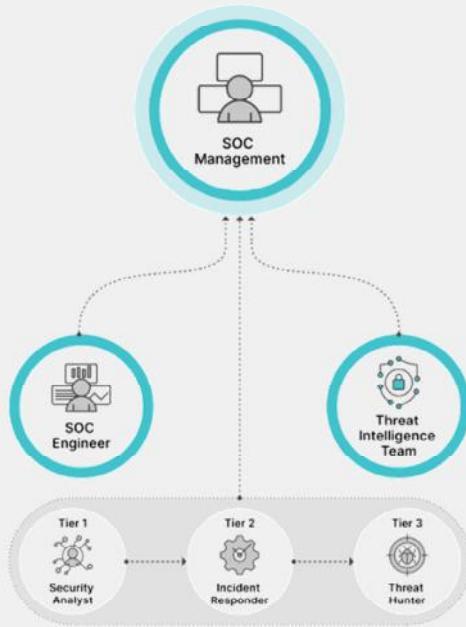
Tiered analysts are the core operational roles in the SOC for continuous monitoring and incident response. Regardless of the size of the organization and the SOC, a tiered structure can help manage threats to the network. This structure allows certain members to focus on monitoring and initial triage (tier 1) while others focus on escalated incident response for larger attacks where remediation may take more time (tier 2). In larger SOCs, a third tier is beneficial to proactively hunt larger threats by monitoring threat intelligence and testing the security posture of the network.

DO NOT REPRINT

© FORTINET

SOC Roles (Contd)

- SOC Engineer
 - Maintain the SIEM, SOAR, and other SOC tools
- Threat Intelligence Team
 - Ingest and curate threat feeds, such as IOC, TTP, and more
- SOC Management
 - Oversee the daily SOC operations



The SOC engineers are responsible for maintaining the security, orchestration, automation, and response (SOAR), SIEM, and other SOC tools and for ensuring tool uptime and performance. As part of this maintenance, they will design and plan to scale for the organization's future growth, ensuring the SOC can handle increased volume and more complex threats.

The threat intelligence team ingests and curates threat feeds, such as indicators of compromise (IOCs), tactics, techniques, and procedures (TTP), and more. They may also work with external intelligence sources, including Information Sharing and Analysis Centers (ISACs) and other vendors, to gain further insights and threat data. The team can also map threat intelligence to the MITRE ATT&CK framework, providing context to investigations and threat hunting.

SOC managers are responsible for overseeing the daily SOC operations. They can manage team schedules, develop and implement policies, and handle resource allocation. In larger SOCs, SOC team leads may be required to oversee the daily operations while managers focus on compliance, metrics, and other strategic duties to ensure a smoothly running SOC. SOC managers can also be responsible for communication and coordination with other relevant business units, such as IT.

DO NOT REPRINT
© FORTINET

Data Lake—FortiAnalyzer

- Centralized repository for structured and unstructured data in its raw format
- Ingests and stores the vast amounts of data required to maintain cybersecurity resiliency
- FortiAnalyzer acts as a data lake for security operations by ingesting and storing data from other Fabric and third-party devices



In security operations, a data lake is used to ingest and store the vast amounts of data required to maintain cybersecurity resiliency. A data lake is a centralized repository where data is stored in structured and unstructured data in its raw format. This data can come from many different sources, and it is not siloed in the data lake. Instead, the data lake can be used as a single repository to investigate and correlate the data. This makes the data lake foundational to security operations and the responsibilities of the SOC, including real-time monitoring, threat detection, and incident investigation.

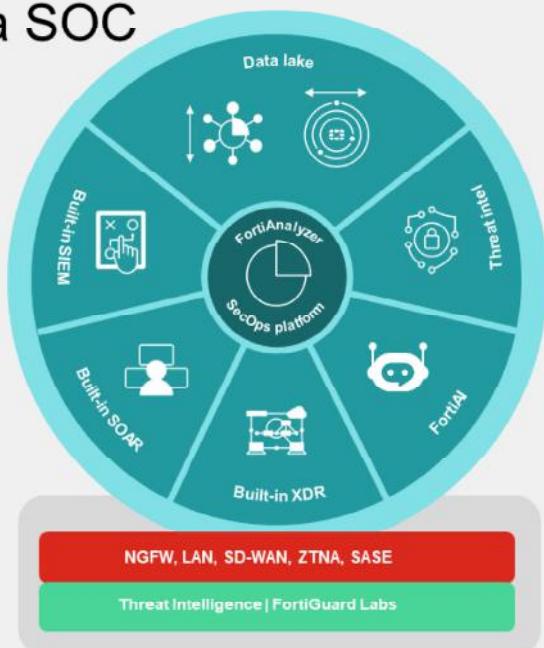
Fortinet's data lake offering is FortiAnalyzer. FortiAnalyzer acts as a data lake for security operations by ingesting and storing data from other Fortinet and third-party devices. Logs from third-party devices can be normalized for analysis and correlation using a suite of predefined log parsers, some of which are built-in with FortiAnalyzer and other premium log parsers that are available through FortiGuard licenses. Additionally, SIEM and SOAR functions are integrated in FortiAnalyzer, allowing the SOC to manage security operations efficiently.

DO NOT REPRINT

© FORTINET

Role of FortiAnalyzer Role in a SOC

- Unified data lake
 - Provides a single view of logs, incidents, configurations, and alerts
- Native threat intelligence
 - Real-time FortiGuard Labs intelligence, including outbreak detection and IOCs
- Built-in SOC automation
 - Includes SIEM, SOAR, and XDR capabilities with pre-configured content
- Embedded GenAI assistant
 - Integrates FortiAI, GenAI assistance to enhance efficiency and response
- Flexible deployments
 - Offers lightweight deployment options through horizontal big data scale with appliance, VM, or cloud deployment options
- FortiGuard SOaaS: managed attack monitoring
 - 24/7 Fortinet expert-led threat detection, investigation, and incident escalation



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

9

Over the past few years, FortiAnalyzer has been significantly enhanced, evolving from a logging and analytics tool into a comprehensive, modern security operations (SecOps) platform.

As the Fortinet Security Fabric data lake, FortiAnalyzer consolidates vast datasets and streamlines the management of logs, incidents, and reporting by unifying configurations, events, and alerts from across the Fortinet Security Fabric into a single view. With intuitive threat topologies and native intelligence from FortiGuard Labs, customers receive timely updates on the latest threats.

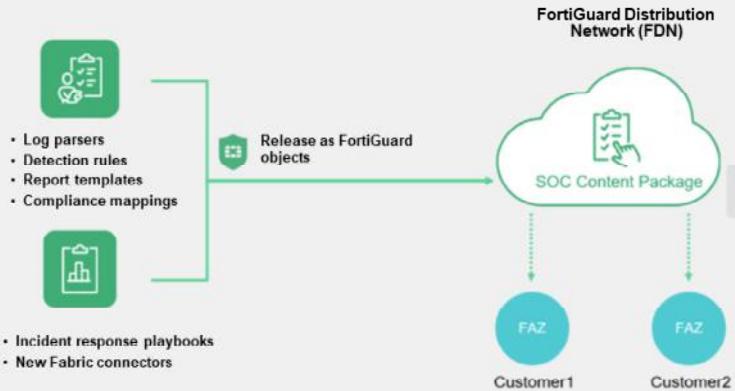
The Security Automation subscription further boosts SIEM/SOAR capabilities by providing prebuilt content packs that include event handlers, playbooks, and connectors that are updated monthly. The integration of FortiAI provides generative AI (GenAI) assistance embedded in FortiAnalyzer, enabling teams to respond quickly and effectively.

FortiAnalyzer also offers lightweight and flexible deployment options—whether as a physical appliance, a VM, or in the cloud—allowing organizations of all sizes to detect threats more intelligently, respond more swiftly, and scale horizontally using the FortiAnalyzer Fabric architecture.

DO NOT REPRINT
© FORTINET

SOC Automation Content Pack

- 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
- Separate license is required for the FortiAnalyzer SOC Automation Service content packs



The FortiAnalyzer SOC Automation Service, integrated with native SIEM and SOAR capabilities on the platform, offers a comprehensive suite of features, including third-party log parsers, advanced correlation rules, automation connectors, incident response playbooks, advanced analytics, and premium reports.

These tools empower SecOps 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**

Knowledge Check

1. Which SOC team is responsible for ingesting and curating threat feeds such as IOCs?
 - A. Threat Hunter
 - B. Threat Intelligence team

2. What is the role of FortiAnalyzer in a SOC?
 - A. Perform security orchestration, automation, and response
 - B. Ingest and store all network data

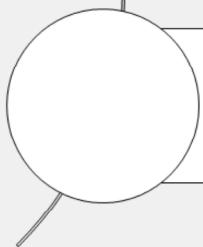
DO NOT REPRINT

© FORTINET

Lesson Progress



SOC Concepts



Fabric Integration

Good job! You now understand the SOC concepts.

Now, you will learn about FortiAnalyzer integration in the Security Fabric and FortiAnalyzer Fabric deployments.

DO NOT REPRINT**© FORTINET**

Fabric Integration

Objectives

- Describe FortiAnalyzer Security Fabric integration
- Describe how logging works in a Security Fabric
- Describe FortiAnalyzer Fabric deployments
- Describe FortiAnalyzer operating modes



© Fortinet Inc. All Rights Reserved.

13

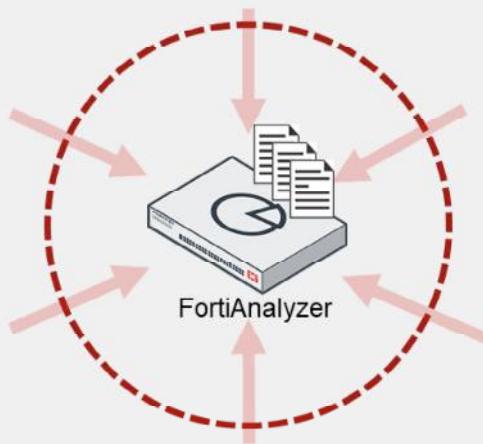
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in Security Fabric integration, you will be able to explain how FortiAnalyzer integrates into and collects and correlates logs in a Security Fabric. You will also be able to describe how FortiAnalyzer Fabric deployments work and differentiate between the FortiAnalyzer operating modes.

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

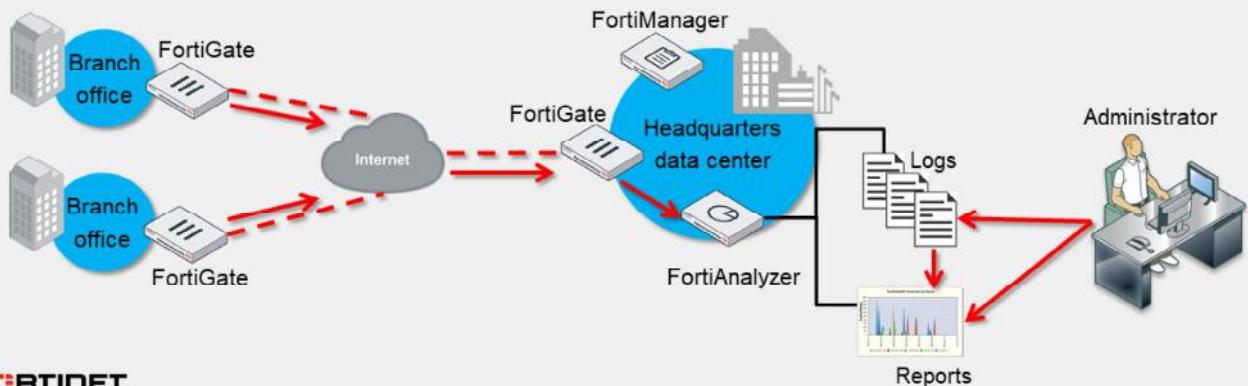
FortiAnalyzer aggregates log data from one or more Fortinet devices, thereby acting as a centralized log repository. Log aggregation provides a single channel for accessing your complete network data, so you don't need to access multiple devices, several times a day.

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



The logging and reporting workflow operates as follows:

1. Registered devices send their logs to FortiAnalyzer.
2. FortiAnalyzer collates and stores these logs in a manner that makes it easy to search and generate reports.
3. Administrators can access FortiAnalyzer using the GUI to manually view the logs or generate reports to analyze the data. They can also use the CLI for administrative tasks.

FortiAnalyzer can be easily integrated into a network, even across multiple sites. A typical topology may include several branch locations and a central headquarters. Each location's firewall is added into FortiAnalyzer, allowing the administrator to view logs and generate reports for the entire network from a single interface.

DO NOT REPRINT**© FORTINET**

Security Fabric Logging

- Store and analyze logs from devices in a Security Fabric group as if they originate from a single device
- The Security Fabric logs each session only once
 - The first FortiGate that handles a session will log it
 - No duplicate traffic logs for sessions originating from another Fabric member MAC address, except in the following cases:
 - If an upstream FortiGate performs NAT
 - If upstream FortiGate devices continue to log UTM events
- UTM and traffic logs are correlated, ensuring that session details, UTM events, reporting, and automation in the Security Fabric function correctly

Log View > FortiGate > Traffic

The screenshot shows a software interface for managing logs. At the top, there's a navigation bar with tabs for 'Traffic', 'Security', and 'Event'. Below the navigation bar, there's a search bar and some filter options. A main pane displays a list of log entries. In the bottom right corner of the main pane, there's a blue callout bubble containing the following text:

Training-Lab is the name of the Security Fabric containing two or more FortiGate devices

At the bottom left of the interface, there's a 'FORTINET Training Institute' logo. At the bottom right, there's a copyright notice: © Fortinet Inc. All Rights Reserved. 16

FortiAnalyzer supports the Security Fabric by storing and analyzing the logs from devices within a Security Fabric group as if they originate from a single device. It correlates traffic logs with corresponding unified threat management (UTM) logs, allowing it to report on sessions and bandwidth together with its UTM events.

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

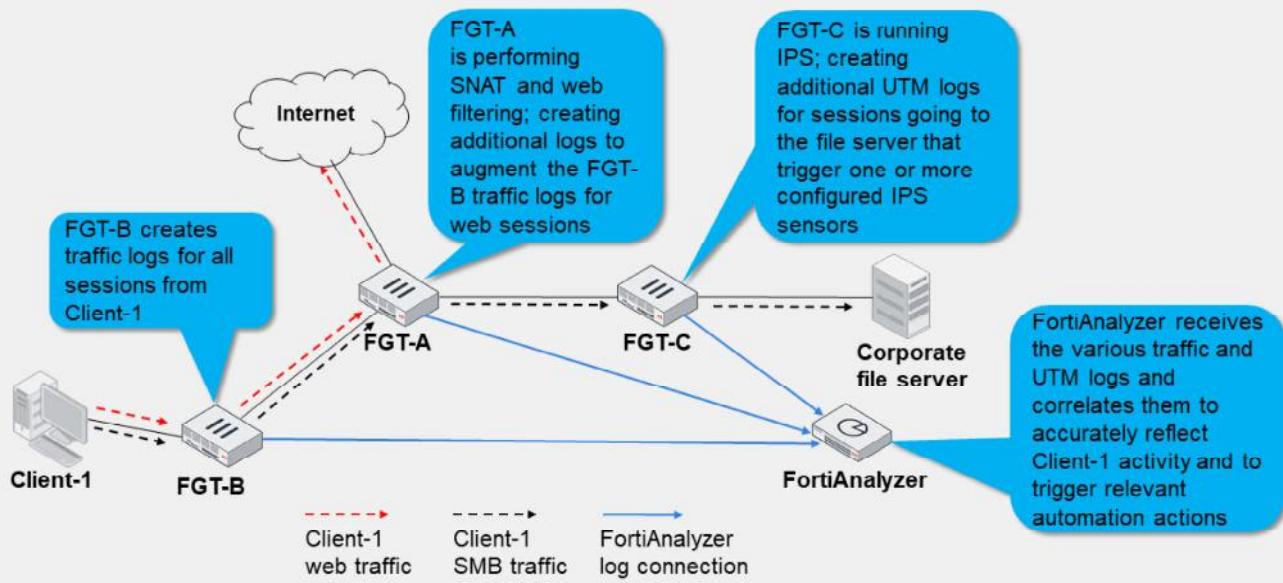
One exception to this behavior is that if the upstream FortiGate performs network address translation (NAT), then another log is generated. The additional log is needed to record NAT details, such as translated ports and addresses.

When configured, upstream devices complete UTM logging, while FortiAnalyzer automatically performs UTM and traffic log correlation for the Security Fabric. This process ensures a concise and accurate record of any UTM events that may occur, requiring no additional configuration.

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

DO NOT REPRINT
© FORTINET

Security Fabric Logging (Contd)



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

17

This slide illustrates how logging functions within the Security Fabric, ensuring full visibility while eliminating duplicate logs across the environment. Three FortiGate devices are configured in a 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 applies 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 the intrusion prevention system (IPS) for all inbound communications to the servers behind it.

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

The web session is then forwarded to FGT-A, which doesn't duplicate the initial traffic log but generates a new log due to SNAT being applied to the session. Additionally, FGT-A enforces a web filtering policy for this session and generates the relevant UTM logs as necessary.

The server message block (SMB) session is forwarded to FGT-A, which again doesn't duplicate the initial traffic log. Since FGT-A doesn't need to perform NAT or apply web filtering, it forwards the traffic to FGT-C. FGT-C also doesn't generate a duplicate traffic log, but performs IPS inspection according to its configuration. If a signature match is triggered that results in an action generating a log, it will log the event.

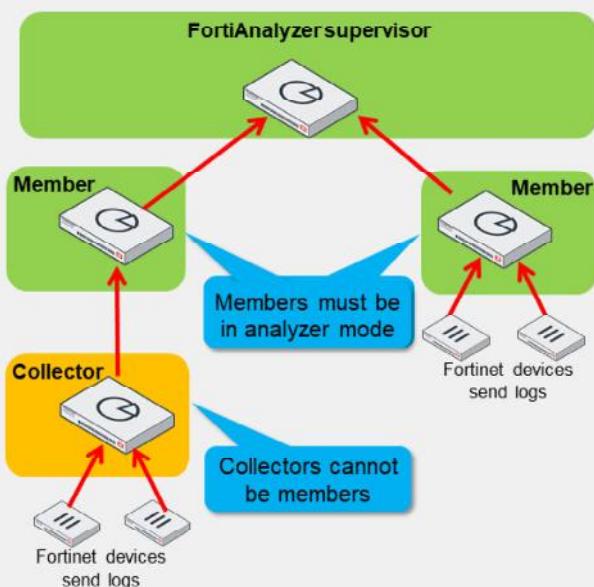
FortiAnalyzer receives the various traffic and UTM logs and automatically correlates them, ensuring they are linked for proper viewing, reporting, and automated actions.

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 Fabric operation modes:
 - Supervisor—one per fabric; acts as the root
 - Member—sends information to the supervisor
- Supervisor and members can be configured in different time zones
- Supervisor includes only the following modules:
 - Device Manager
 - Log View
 - Incident & Events
 - System Settings
 - Management Extensions
 - Report
 - FortiView
 - Threat Hunting



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

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

18

The FortiAnalyzer Fabric enables centralized monitoring of devices, incidents, and events across multiple FortiAnalyzer devices. It operates in two modes: supervisor and member.

The supervisor acts 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 generated by members. Information regarding incidents and events is synchronized from members to the supervisor through an API.

Members are FortiAnalyzer devices that send information to the supervisor for centralized monitoring. When a device is configured as a member, it retains access to the features described in the *FortiAnalyzer Administration Guide*. Each member can create or raise incidents and events.

Devices configured with high availability (HA) can act as members; however, HA is not supported for FortiAnalyzer devices serving as the Fabric supervisor.

All members of the FortiAnalyzer Fabric don't have to be in the same time zone settings as the supervisor.

DO NOT REPRINT
© FORTINET

FortiAnalyzer Operating Modes—Analyzer

Dashboard > System Information

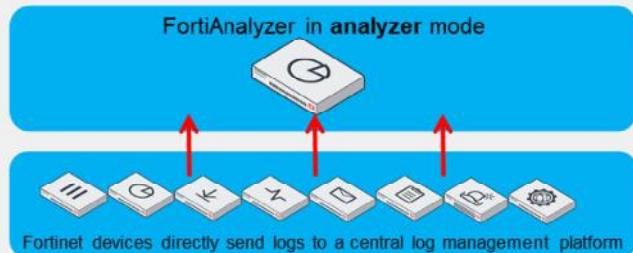
Operation Mode

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 device (or syslog or CEF server)



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

19

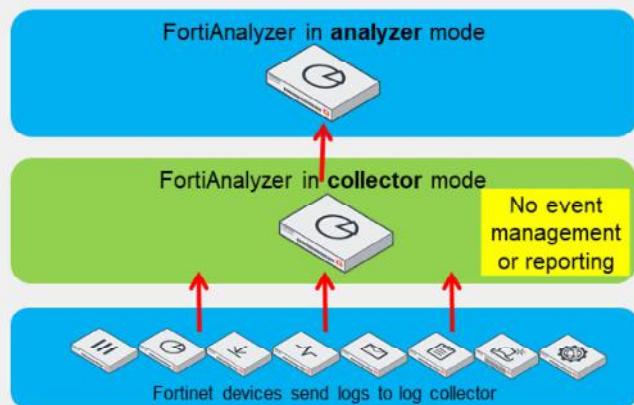
FortiAnalyzer has two modes of operation: analyzer and collector. The mode you select depends on your network topology and specific requirements. You can change the operating mode in the **System Information** widget on the dashboard.

In analyzer mode, the device acts as a central log aggregator for one or more log collectors. These could include a FortiAnalyzer operating in collector mode or any other supported device that sends logs. Analyzer is the default operating mode.

DO NOT REPRINT
© FORTINET

FortiAnalyzer Operating Modes—Collector

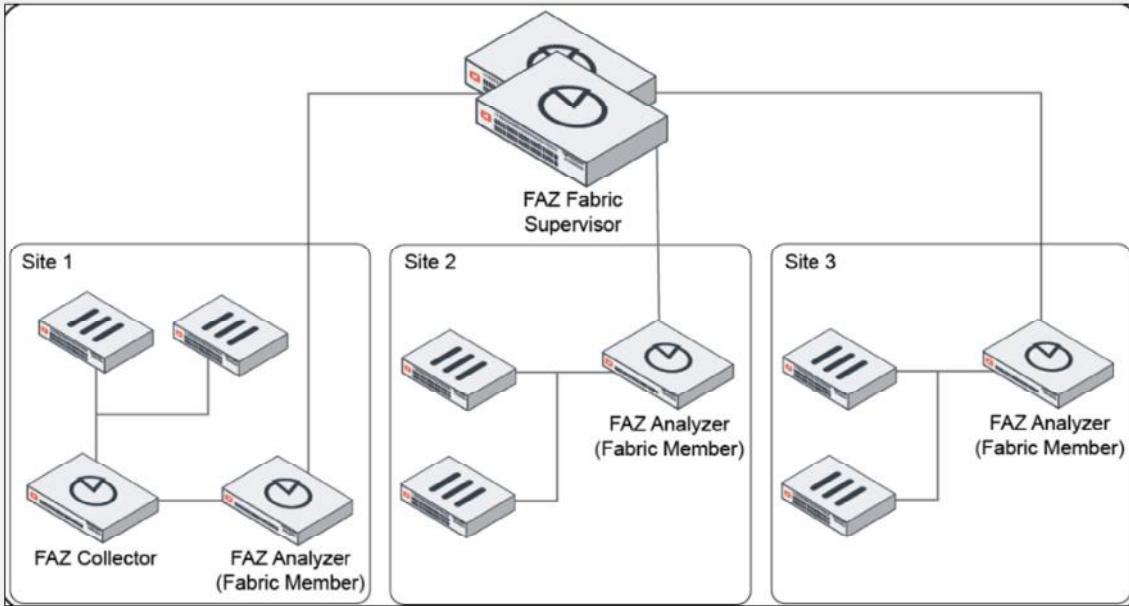
- Collects logs from multiple devices and forwards them to FortiAnalyzer in analyzer mode
 - Can aggregate logs to another FortiAnalyzer
 - However, can forward to syslog/CEF server in real-time forwarding mode only
- Not used for analytics—archiving only



When operating in collector mode, the device collects logs from multiple devices and forwards them in their original binary format to another device, such as a FortiAnalyzer in analyzer mode. It can also send the logs to a syslog server or a Common Event Format (CEF) server, depending on the forwarding mode. A collector has fewer features compared to an analyzer, because its primary function is to collect and forward logs. It does not provide capabilities for event management or reporting.

DO NOT REPRINT
© FORTINET

Use Case—FortiAnalyzer Fabric



FORTINET.
 Training Institute

© Fortinet Inc. All Rights Reserved. 21

This slide shows the use case for the FortiAnalyzer Fabric, which consists of a suitable architecture for multinational customers with subsidiaries worldwide. A multinational corporation with offices worldwide could use the Fabric Group to deploy a central analyzer at its headquarters and multiple regional collectors with their own FortiAnalyzer in analyzer mode. This architecture would give the central SOC global visibility while ensuring that log data is processed locally in each region first, thus satisfying both performance and regulatory requirements. This would make the analyzer-collector mode much more tangible.

The key differentiator here is that the regional SOC team can benefit from a fully functional analyzer, and not just have a historical log view available as on a collector. The collectors can be used to build points of presence in the different regions and forward the information to the central analyzer in the company's head office.

Advantages of this architecture are:

- Centralized visibility of managed devices, log view, incidents, and events is possible from a FortiAnalyzer supervisor.
- Single or multiple-tier deployments are supported (for example, Collector-Analyzer).

Some limitations of the FortiAnalyzer Fabric are:

- HA is not available on the supervisor.
- Scalability and redundancy are limited to each FortiAnalyzer deployment.
- You are not able to perform configuration changes or to run automation playbooks from the Fabric supervisor to members.

DO NOT REPRINT
© FORTINET

Use Case—FortiAnalyzer Fabric (Contd)

Logs > Log View

FAZ Name	Group	Event Status	Event Type	Severity	count	Device Name	Acknowledged
FAZVM-S-903	10.2.175.43		Traffic	Medium	120	FAZVMST...	No
FAZVM-S-903	10.2.126.95		Traffic	Medium	104	FAZVMST...	No
FAZVM-S-903	10.2.115.2		Traffic	Medium	103	FAZVMST...	No
FAZVM-S-903	10.2.60.111	open	IPS	High	451	FAZVMST...	No
FAZVM-S-903	10.2.60.46		Traffic	Medium	104	FAZVMST...	No
FAZVM-S-903	VAN-200289-U51	open	Traffic	High	124	FAZVMST...	No
FAZVM-S-903	10.2.60.93		Traffic	Medium	104	FAZVMST...	No
FAZVM-S-903	10.2.60.45		Traffic	Medium	86	FAZVMST...	No
FAZVM-S-903	10.2.60.121		Traffic	Medium	104	FAZVMST...	No
FAZVM-S-903	10.2.60.94		Traffic	Medium	103	FAZVMST...	No
FAZVM-S-903	10.2.175.45		Traffic	Medium	86	FAZVMST...	No
FAZVM-S-903	10.2.0.210		Traffic	Medium	176	FAZVMST...	No
FAZVM-S-903	10.2.123.9		Traffic	Medium	104	FAZVMST...	No
FAZVM-S-903	10.2.175.118		Traffic	Medium	104	FAZVMST...	No
FAZVM-S-903	10.2.175.116		Traffic	Medium	105	FAZVMST...	No
FAZVM-S-903	10.2.60.141	open	Traffic	High	283	FAZVMST...	No
FAZVM-S-903	10.2.175.46		Traffic	Medium	104	FAZVMST...	No
FAZVM-S-903	10.2.60.101		Traffic	Medium	104	FAZVMST...	No

Using FortiAnalyzer Fabric, you can view logs, reports, and events generated on Fabric members, directly on the supervisor

Reports > Report Definitions

Reports can be configured to display information from multiple FortiAnalyzer units and ADOMs.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

22

In the FortiAnalyzer Fabric supervisor, Log View displays logs collected on all FortiAnalyzer Fabric members. The logs contain the same information as displayed in the host FortiAnalyzer device they were collected on. In the example shown on this slide, the FortiAnalyzer Host Name column indicates which FortiAnalyzer the logs were collected on.

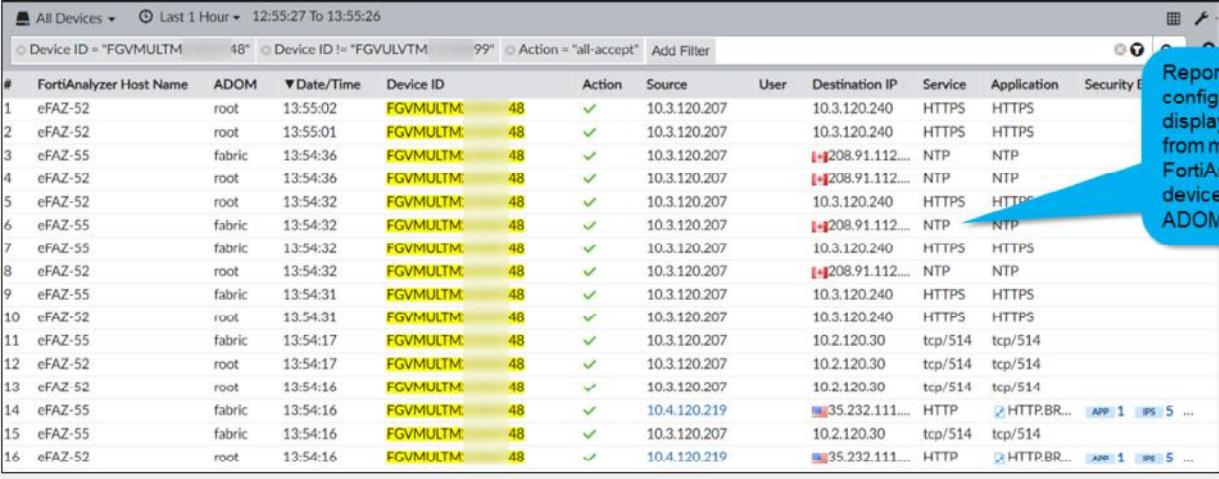
For reports, the FortiAnalyzer Fabric supervisor can fetch and aggregate data from multiple members in the FortiAnalyzer Fabric. This enables the SOC analysts at HQ to find correlations between sites and respond accordingly. In the example shown on this slide, the report can be configured to display information from multiple FortiAnalyzer devices and ADOMs.

FortiAnalyzer 7.6 Analyst Study Guide

25

DO NOT REPRINT
© FORTINET

Use Case—FortiAnalyzer Fabric (Contd)



The screenshot shows the 'Incidents & Events > Event Monitor' interface. It displays a table of log entries from 'All Devices'. The columns include: #, FortiAnalyzer Host Name, ADOM, Date/Time, Device ID, Action, Source, User, Destination IP, Service, Application, and Security Level. A blue callout bubble points to the 'Action' column, stating: 'Reports can be configured to display information from multiple FortiAnalyzer devices and ADOMs'.

#	FortiAnalyzer Host Name	ADOM	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Security Level
1	eFAZ-52	root	13:55:02	FGVMULTM:	48	✓		10.3.120.207	10.3.120.240	HTTPS	HTTPS
2	eFAZ-52	root	13:55:01	FGVMULTM:	48	✓		10.3.120.207	10.3.120.240	HTTPS	HTTPS
3	eFAZ-55	fabric	13:54:36	FGVMULTM:	48	✓		10.3.120.207	208.91.112....	NTP	NTP
4	eFAZ-52	root	13:54:36	FGVMULTM:	48	✓		10.3.120.207	208.91.112....	NTP	NTP
5	eFAZ-52	root	13:54:32	FGVMULTM:	48	✓		10.3.120.207	10.3.120.240	HTTPS	HTTPS
6	eFAZ-55	fabric	13:54:32	FGVMULTM:	48	✓		10.3.120.207	208.91.112....	NTP	NTP
7	eFAZ-55	fabric	13:54:32	FGVMULTM:	48	✓		10.3.120.207	10.3.120.240	HTTPS	HTTPS
8	eFAZ-52	root	13:54:32	FGVMULTM:	48	✓		10.3.120.207	208.91.112....	NTP	NTP
9	eFAZ-55	fabric	13:54:31	FGVMULTM:	48	✓		10.3.120.207	10.3.120.240	HTTPS	HTTPS
10	eFAZ-52	root	13:54:31	FGVMULTM:	48	✓		10.3.120.207	10.3.120.240	HTTPS	HTTPS
11	eFAZ-55	fabric	13:54:17	FGVMULTM:	48	✓		10.3.120.207	10.2.120.30	tcp/514	tcp/514
12	eFAZ-52	root	13:54:17	FGVMULTM:	48	✓		10.3.120.207	10.2.120.30	tcp/514	tcp/514
13	eFAZ-52	root	13:54:16	FGVMULTM:	48	✓		10.3.120.207	10.2.120.30	tcp/514	tcp/514
14	eFAZ-55	fabric	13:54:16	FGVMULTM:	48	✓		10.4.120.219	35.232.111....	HTTP	HTTP.BR...
15	eFAZ-55	fabric	13:54:16	FGVMULTM:	48	✓		10.3.120.207	10.2.120.30	tcp/514	tcp/514
16	eFAZ-52	root	13:54:16	FGVMULTM:	48	✓		10.4.120.219	35.232.111....	HTTP	HTTP.BR...

Using FortiAnalyzer Fabric, you can view logs, reports, and events generated on Fabric members, directly on the supervisor

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 23

Events generated by event handlers on the FortiAnalyzer Fabric members are visible on the supervisor. The SOC analysts can review these events for correlations between the members, so they can be managed together more efficiently rather than individually across the sites.

The event handlers must be configured on each of the FortiAnalyzer members; however, the related logs that trigger the event handler rules are visible from the supervisor.

DO NOT REPRINT

© FORTINET

ADOMs

- ADOMs group devices for administrators to monitor and manage
 - One or more devices can be assigned to ADOMs, and administrators can manage one or more ADOMs
- Purpose:
 - Dividing device administration and restricting access
 - Enhancing access control through VDOMs, a feature of FortiGate
 - Managing data policies and disk space allocation more efficiently
 - Settings are configured for each ADOM, rather than for each individual device

ADOMs are not enabled by default

The screenshot shows the 'System Information' section of the FortiAnalyzer dashboard. It displays various system details such as Host Name (FortiAnalyzer), Serial Number (FAZ-VMTM24012176), Platform Type (FAZVM64-KVM), HA Status (Standalone), System Time (Tue May 27 05:08:29 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), and Up Time (3 days 16 hours 49 minutes 27 seconds). A red box highlights the 'Administrative Domain' field, which is currently set to 'enable'. Below the table, there are two tabs: 'Analyzer' (selected) and 'Collector'.

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

ADOMs allow you to group devices for efficient monitoring and management. For instance, administrators can manage devices based on their geographical location or business division.

The primary purposes of ADOMs are:

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

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

All Fortinet devices that are part of a Security Fabric can be assigned to an ADOM of the Fabric type, allowing for rapid data processing and log correlation.

You will learn more about ADOMs in this course.

DO NOT REPRINT
© FORTINET

Tools for Configuring FortiAnalyzer

The screenshot shows two side-by-side interfaces. On the left is the 'FortiAnalyzer GUI' dashboard, which includes links for Device Manager, FortiView, Log View, Fabric View, Incidents & Events, Reports, and System Settings. A red 'X' icon next to 'Incidents & Events' indicates it's not available in Collector mode. On the right is the 'FortiAnalyzer CLI' interface, featuring a 'CLI Console' window showing a connection to 'FAZVM64-KVM'. A yellow callout box states: 'Can use the CLI Console widget on dashboard of GUI and terminal emulation program (for example, PuTTY)'. Below the CLI console is a 'PUTTY Configuration' dialog box. A blue callout box points to this dialog with the text: 'Requires a separate Telnet, SSH, or local console connection'. The bottom of the slide includes the Fortinet Training Institute logo and copyright information.

- 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. 25

You can use both the GUI and CLI to configure and manage FortiAnalyzer. You can use both tools locally by connecting directly to FortiAnalyzer, or remotely, based on your configured settings. You can deny or permit access based on IP addresses.

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

The FortiAnalyzer features available on the GUI and CLI depend on the profile of the administrator logged in and the operation mode of FortiAnalyzer. For instance, in collector mode, the GUI doesn't include **FortiView**, **Reports**, or **Incidents & Events**. Additionally, if you log in with the Standard_User or Restricted_User administrator profiles, you will not have full access privileges; those are reserved for the Super_User profile. The CLI also includes some settings that are not available through the GUI.

Any configuration changes you make using the GUI and CLI take effect immediately upon applying the settings, requiring a reset of FortiAnalyzer or disrupting its services.

Note that the SQL database is disabled by default when FortiAnalyzer is in collector mode. Logs that rely on the SQL database are not available in this mode unless the SQL database is enabled through the CLI.

DO NOT REPRINT

© FORTINET

Knowledge Check

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

2. What are the operation modes in a FortiAnalyzer Fabric?
 A. Supervisor and member
 B. Analyzer and collector

DO NOT REPRINT

© FORTINET

Lesson Progress



SOC Concepts



Fabric Features

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe SOC objectives
- ✓ Describe SOC responsibilities
- ✓ Describe SOC roles
- ✓ Describe the role of FortiAnalyzer in a SOC
- ✓ Describe FortiAnalyzer Security Fabric integration
- ✓ Describe how logging works in a Security Fabric
- ✓ Describe FortiAnalyzer Fabric deployments
- ✓ Describe FortiAnalyzer operating modes



© Fortinet Inc. All Rights Reserved. 28

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

DO NOT REPRINT**© FORTINET**

FortiAnalyzer Analyst

Log Data Flow and Navigation

A small red square icon containing a white square with a diagonal line, followed by the text "FortiAnalyzer 7.6".

Last Modified: 16 July 2025

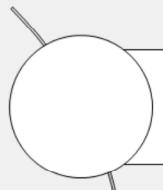
In this lesson, you will learn how to protect, view, and manage logs on FortiAnalyzer.

By understanding logging on FortiAnalyzer, you will be able to use log data to analyze network-based attacks, as well as troubleshoot and investigate network issues.

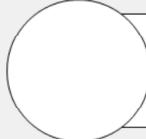
DO NOT REPRINT

© FORTINET

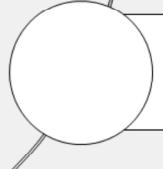
Lesson Overview



Log Data Flow



Log View



FortiView

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

DO NOT REPRINT**© FORTINET**

Log Data Flow

Objectives

- Describe how logs are collected, parsed, and indexed
- Describe how FortiAnalyzer parses and normalizes logs
- Validate log parsers
- Search logs using normalized fields

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

By demonstrating competence in understanding the purpose of log collection, log storage, and the log file workflow, you will have a better understanding of how logs are compiled and collected.

DO NOT REPRINT**© FORTINET**

Purpose of Logs

- Record information containing specific details about the network
- Troubleshoot ongoing issues with the network
- Determine load on network devices and establish baselines
- Track service use
- Support incident response and forensic analysis



Log messages help paint a picture of what is going on in your network. You can use logs for many purposes. You can use logs to troubleshoot your network, determine load on network devices, establish baselines, track service use, and support incident response and forensic analysis.

It is important to understand that logs are like a puzzle: You must put several pieces together to get a complete understanding of what is going on. You often need to review multiple log messages to determine the exact chain of events and activities that led to a breach. Examining a log in isolation often won't help you determine the best way to configure your network to prevent such breaches in the future. This is why centralized log storage is so important.

DO NOT REPRINT**© FORTINET**

Log Storage Regulations

- Regulatory requirements may mandate how logs are managed in an organization
 - Levels and analysis requirements are often defined by legislation
 - Examples: HIPAA, SOX, GDPR
 - Log and store information at the correct level to meet regulations
- Logs can provide evidence against offending parties when unauthorized activity is detected
 - Logging data must be able to stand up in court
- Additionally, NIST frameworks and ISO standards can provide guidelines on how to make your network more secure
 - Examples: NIST Cybersecurity Framework, ISO 27001/27002 standards



© Fortinet Inc. All Rights Reserved.

5

Regulations require organizations to log specific information, record data, and store it at the correct level. You must thoroughly understand the legislation that your organization must comply with, including the jurisdictions your organization falls under, and if there are any industry-specific regulations you must follow. For example, the financial and healthcare sectors may be subject to additional regulations, and certain private information may not be recorded.

You can use log entries as evidence in cases of unauthorized or illegal activity. The data you use as evidence must be able to stand up in court, so it is vital that you are able to understand and analyze your logs.

Establishing your organization's security policies can be difficult, particularly if no existing policies are in place. When developing security policies for your organization, Fortinet recommends that you consult widely recognized frameworks and standards created by organizations such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).

DO NOT REPRINT**© FORTINET**

Analyzing Your Network

- To effectively analyze your network, you must have a thorough understanding of it
- Every network and the requirements of every organization are unique; however, there are some common areas to focus on:

Areas to identify	Examples
Critical infrastructure	Servers and security devices
Types of traffic	Permitted protocols on which devices
Typical usage and peak usage	Established network baselines during all time periods
Sources of traffic bursts	Expected maintenance windows and data backups



© Fortinet Inc. All Rights Reserved.

6

To effectively analyze the traffic in your organization, you must have a deep understanding of the network and be able to identify the following:

- Critical infrastructure, such as servers and security devices. These take the highest priority in any analysis.
- Expected traffic types. This includes knowing which protocols are permitted on which devices and being able to quickly identify abnormal traffic flows.
- Typical and peak usage levels. Establishing network baselines for traffic levels at all hours will help you recognize unexpected behavior, such as a higher-than-normal amount of traffic during a certain time period.
- Sources of traffic bursts. You can use this data to create a buffer for expected maintenance windows and data backups.

DO NOT REPRINT**© FORTINET**

Logging Scope

- Depending on the size of your organization, the amount of data can vary significantly
- Balance between reducing security risks and assigning resources while adhering to regulations
 - If logging is optional for certain flows, decide whether to spend resources on it
 - Too much data can be as bad as too little
- Prioritize analysis based on
 - Source and destination
 - Type of traffic
 - Type of security event (for example, web filter or intrusion prevention)
 - Frequency
 - Time



© Fortinet Inc. All Rights Reserved. 7

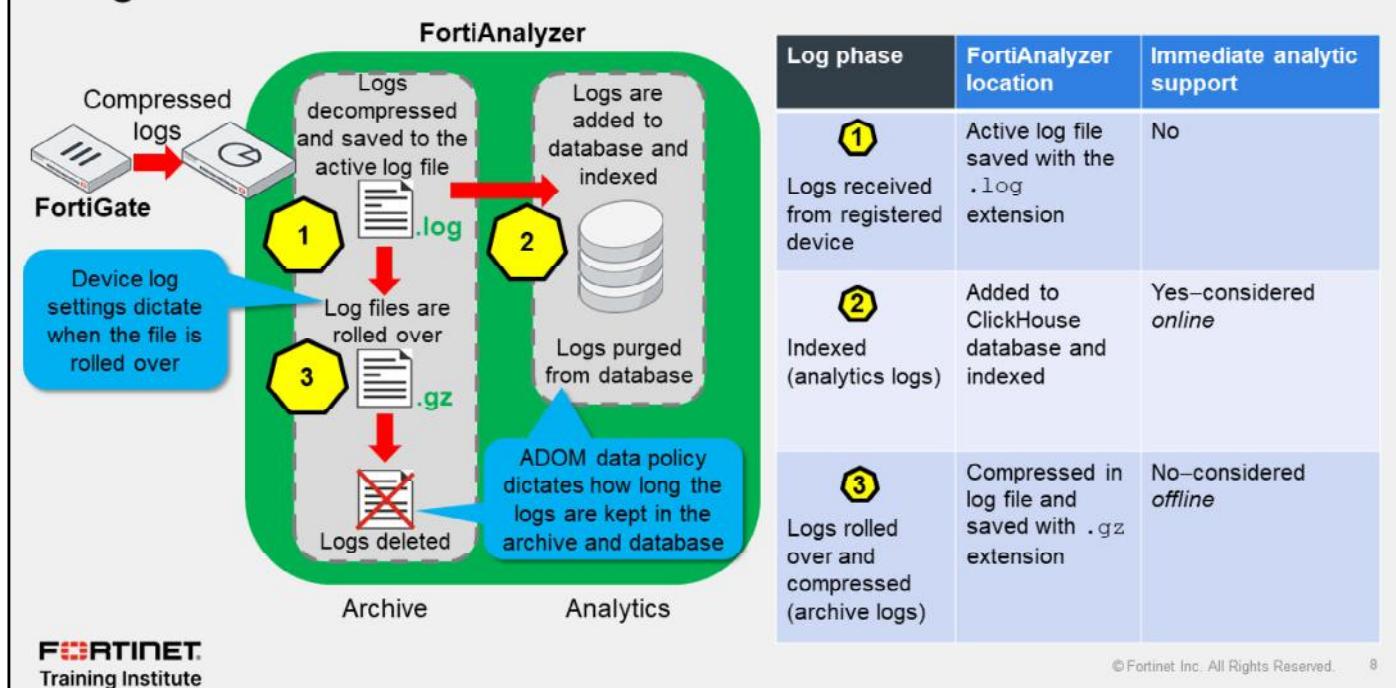
Depending on your organization's size, the amount of log data generated can become overwhelming. Logs are usually generated continuously, and one workstation can generate a large volume of logs in a short time. As an analyst, it is not practical to review every log entry. Most logs are normal: Using resources to analyze them yields no benefits.

Not everything in the network needs to be logged. For example, if your infrastructure team plans to conduct tests on an isolated network, you can work with them to disable logging beforehand. Guest devices on a restricted network also may not need to be logged.

In your analysis, prioritize factors such as the traffic type or types, the traffic sources and destinations, and if there are any security events associated with the traffic. In addition, if traffic is being sent at a frequency that is unexpected, whether you are seeing traffic more or less frequently than expected, further investigation is warranted. Knowing when your network is expected to produce traffic can also help you identify anomalous behavior, such as excessive traffic during off-hours.

DO NOT REPRINT**© FORTINET**

Log File Workflow



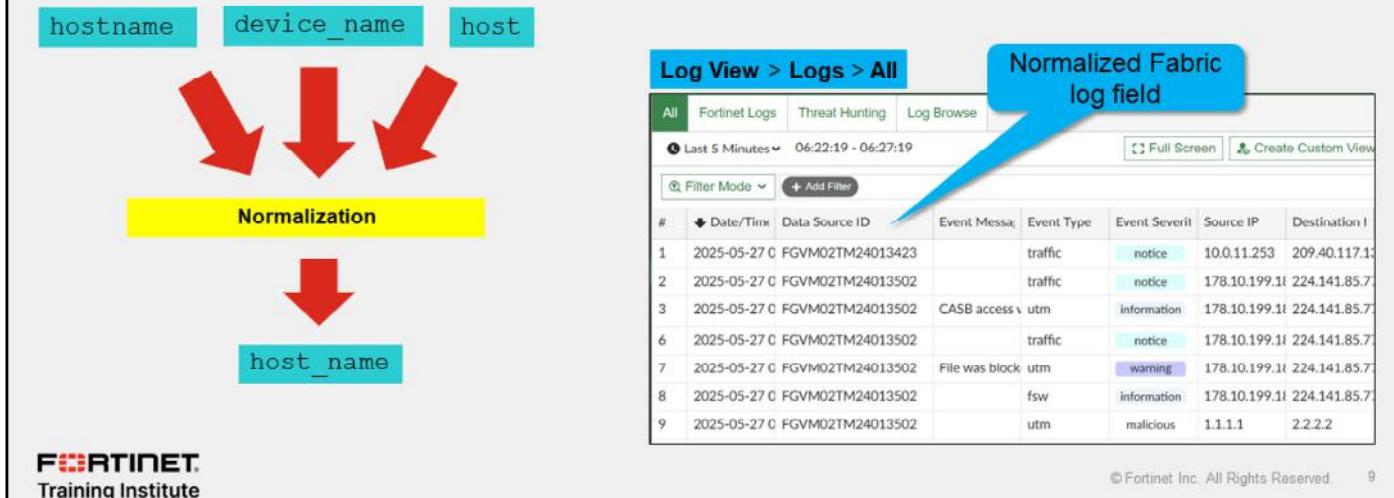
When registered devices send logs to FortiAnalyzer, logs enter the following automatic workflow:

1. Logs received are decompressed and saved in a log file on the FortiAnalyzer disk. The log file has the extension `.log`. For example, FortiAnalyzer saves FortiGate logs with the names `tlog.log` and `elog.log`, for traffic and event logs, respectively. Note that the `tlog.log` file includes FortiGate security logs.
2. At the same time, FortiAnalyzer indexes the saved logs in the SQL database to support analysis. Logs in the indexed phase are known as *analytics* logs. These logs are considered to be online and offer immediate analytic support. FortiAnalyzer purges analytics logs from the SQL database as specified in the ADOM data policy.
3. When the log file reaches a specified size, or at a set schedule, it is rolled over. The process of rolling a log file 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, archived logs count toward the archive quota and retention limits, and FortiAnalyzer deletes them based on the ADOM data policy.

DO NOT REPRINT**© FORTINET**

Normalizing Logs

- Logs from different devices are normalized on FortiAnalyzer
- View logs from Fabric devices in one place, with log fields that are consistent across all logging device



FortiAnalyzer can ingest logs from various sources. To make it easier for analysts to view and understand logs, FortiAnalyzer performs log normalization to display log fields that are consistent across all logging devices. Log normalization transforms disparate log entries into a standardized, structured format.

When FortiAnalyzer ingests logs, they are usually in their native, unstructured format. When you add a device to a Fabric ADOM, FortiAnalyzer creates a security information and event management (SIEM) database for that ADOM, where it stores all normalized logs. FortiAnalyzer uses predefined parsers to extract key fields from ingested logs and maps them to a consistent, standardized set of field names. After parsing and mapping, FortiAnalyzer inserts and indexes the log entries within the SIEM database.

Normalized logs provide a unified view and allow for easier correlation and faster investigation. For example, with standardized fields and values, FortiAnalyzer can correlate events from different devices, such as a traffic block on FortiGate and a failed login event on FortiAuthenticator. Log field correlation improves reporting accuracy and allows you to enrich log data with additional context like user identity or threat intelligence data.

The *Fabric Normalization Reference* guide provides a comprehensive list of log field correlations between Fabric devices and FortiAnalyzer.

DO NOT REPRINT

© FORTINET

Log Parsers

- Translate logs from various sources into a common format
- Identify and extract key fields from logs and map them to standard field names
- If no matching parser exists, FortiAnalyzer uses the generic syslog parser

The screenshot shows two main sections of the FortiAnalyzer interface:

Incidents & Events > Log parsers > Assigned Parsers

Device ID	Application/Vendor	Assigned Parser
FAZ-VMTM24012176	FortiAnalyzer	FortiAnalyzer Log Parser
FGVM02TM24013423	FortiGate	FortiGate Log Parser
FGVM02TM24013502	FortiGate	FortiGate Log Parser

Incidents & Events > Log parsers > Log Parsers

Name	Application	Origin	Status
Apache Log Parser	Apache	Custom	Enabled
Security Automation - Apache Log Parser	Apache	FortiGuard	Disabled
Nginx Log Parser	Nginx	Custom	Enabled
Ubuntu Syslog Parser	Ubuntu	Custom	Enabled
Windows Event Log Parser	Windows	Custom	Enabled
System Log Parser	Syslog	Custom	Enabled

A blue callout box points to the "Security Automation - Apache Log Parser" row, which is highlighted with a red border. The text inside the callout box reads: "Security Automation Service license gives access to more log parsers".

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 10

Log parsers interpret and transform raw, unstructured, or semistructured log messages into a standardized, structured format. Parsers are central to log normalization.

Parsers contain rule sets and predefined logic that FortiAnalyzer applies to incoming log data. Think of parsers as translators that convert device-specific or vendor-specific logs into a common schema on FortiAnalyzer. Parsers identify and extract key fields from log messages and map them to standardized field names. Some parsers can also standardize field values. For example, different devices may report traffic block actions differently: some might use “block” and others might use “deny”. In cases like this, parsers can convert the various values into a unified format—blocked.

FortiAnalyzer includes built-in parsers that parse, normalize, and correlate logs from Fortinet products as well as third-party applications. For example, there are built-in log parsers for Apache and Nginx web servers, and for security event logs from Windows and Linux hosts (with Fabric Agent integration). Additionally, the Security Automation Service license gives you access to even more log parsers.

DO NOT REPRINT

© FORTINET

Validating Logs Using Log Parsers

- You can validate logs using log parsers
- See how FortiAnalyzer parses logs into normalized log fields

The screenshot illustrates the process of validating a log entry using the Ubuntu Syslog Parser. On the left, under 'Incidents & Events > Log parsers > Log Parsers', the 'Log Parsers' tab is selected. A red box highlights the 'Validate' button. Another red box highlights the 'Ubuntu Syslog Parser' row, which is selected. A blue callout bubble labeled 'Normalized log fields' points to the 'Matched' section on the right. The 'Matched' section shows the raw log entry and its corresponding normalized fields.

Name	Application/Vendor	Category	Origin	Status
<input checked="" type="checkbox"/> Ubuntu Syslog Parser	Ubuntu	Endpoint Devices	Built-in	Enabled
<input type="checkbox"/> VMware Log Parser	VMware	Virtualization Platforms	Built-in	Enabled
<input type="checkbox"/> Windows Event Log Parser	Windows	Endpoint Devices	Built-in	Enabled
<input type="checkbox"/> EMS-Connector Parser	EMS-Connector	Fortinet Device	Built-in	Enabled

May 28 08:12:43 ubuntu-2204-desktop systemd[1485]: Started VTE child process 7999 launched by gnome-terminal-server process 7979.

Validate

Parse Result

Matched

Order	Parsed Log
1	adom_oid = 198 itime = 1748445618 loguid = 1714636915 epid = 0 euid = 0 data_parsername = Ubuntu Syslog Parser data_sourcename = ubuntu-2204-desktop data_sourcetype = Ubuntu Syslog data_timestamp = 1748419963 app_proc = 1485 app_service = systemd event_message ~ Started VTE child process 7999 launched by gnom ... host_name = ubuntu-2204-desktop dstepid = 0 dsteuid = 0 logflag = 0

Normalized log fields

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 11

The validate function allows you to test how a specific parser will process a raw log entry. This is useful when working with third-party logs or troubleshooting unexpected parsing issues.

This slide shows a validation example using the Ubuntu syslog parser. It shows how FortiAnalyzer takes the raw systemd log and parses and normalizes the various log fields.

DO NOT REPRINT

© FORTINET

Normalizing and Parsing Log Example

Log View > Logs > All

All	Fortinet Logs	Threat Hunting	Log Browse												
Last 1 Hour	07:36:13 - 08:36:13			<input type="button" value="Full Screen"/>	<input type="button" value="Create Custom View"/>	<input type="button" value="Refresh"/>	<input type="button" value="More"/>								
<input type="button" value="Filter Mode"/> <input type="button" value="Add Filter"/> <div style="float: right;"> <input type="button" value="Raw Log"/> <input type="button" value="Case Sensitive Search"/> <input type="button" value="Download"/> </div>															
#	Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name	Application	Category	File	File Offset	File Type	File Version	File Version
1	2025-05-27 08:35:24	FGVM02TM24013423		traffic	notice	10.0.13.125	208.91.112.63		NTP						
2	2025-05-27 08:35:19	FGVM02TM24013423		traffic	notice	10.0.11.253	96.45.45.45		DNS						

```

adom_oid=198 itime=2025-05-27 08:35:24 loguid=7509149554218893312 epid=3 euid=3 data_parseusername=FortiGate Log Parser data_sourceid=FGVM02TM24013423
data_sourcename=HQ-NGFW-1 root data_sourcetype=FortiGate data_timestamp=1748334923 app_cat=unscanned app_name=NTP app_service=NTP dst_intf=port2(undefined)
dst_ip=208.91.112.63 dst_port=123 event_action=accept event_id=13 event_policy=3 event_ref=751261e0-ce9e-51ef-f12e-a382acaf16d6 event_severity=notice
event_subtype=forward event_type=traffic host_location=Reserved host_owner=fortinet.com net_proto=17 net_rcvdpkts=1 net_recvbytes=76 net_sentbytes=76 net_sentpkts=1
net_sessionduration=180 net_sessionid=1357 src_intf=port6(undefined) src_ip=10.0.13.125 src_natip=100.65.0.101 src_natport=50403 src_port=50403 dstepid=101 dsteid=3
dst_geo_country=United States event_creation_time=27800868 event_uuid=00000000013 src_geo_country=Reserved logflag=1 data_sourcevdom=root dst_intf_role=undefined
event_policyid=3 event_policytype=policy src_intf_role=undefined itime_t=1748360124 _logMeta=undefined

```

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 12

This slide shows a FortiGate event log that has been normalized by FortiAnalyzer using the FortiGate log parser. When you change the view to raw log format, you can see that common FortiGate log fields, such as `data_sourceid`, `dst_ip`, `event_subtype`, and `event_policyid`, have been converted to normalized log fields.

FortiAnalyzer performs normalization for every supported device log that it receives. Normalization makes it easier for you to search and view logs across all the devices in your network.

DO NOT REPRINT
© FORTINET

Searching Using Normalized Fields

- It is easier to search for a corresponding log on normalized logs than on the actual device logs
- In this example, a search in the **Destination Domain** normalized field will look at the domain and hostname fields of the FortiGate log message

The screenshot shows the 'Log View > Logs > All' interface. At the top, there are tabs for 'All', 'Fortinet Logs', 'Threat Hunting', and 'Log Browse'. Below that, a search bar shows 'Last N Days' set to 90, with a date range from '02-26 12:30:45' to '05-27 12:30:45'. A 'Filter Mode' dropdown is open, showing options like 'Date/Time', 'DNS Query Type', 'Event Type', 'Event Severity', and 'Source IP'. A specific filter for 'Destination Domain' is selected. To the right of the filter, a 'Filter values' panel is open, showing suggestions like 'www.vimeo.com', 'www.dropbox.com', 'host3', '172.16.200.164', 'host', 'www.amazon.com', and 'www.youtube.com'. An 'Apply' button is at the bottom right of the filter panel.

Searching for logs using normalized fields is more efficient than sifting through raw, device-specific logs. Native device logs use inconsistent field names and varying structures, which makes recalling or discovering relevant parameters challenging and time-consuming. When FortiAnalyzer parsers standardize and map these diverse fields into a unified format, you can execute consistent, targeted queries, which streamlines investigations.

DO NOT REPRINT**© FORTINET**

Log Types by Device

Device	Log type
Fabric	all
FortiGate	traffic, event, security
FortiCache	traffic, event, antivirus, web filter
FortiClient	traffic, event, vulnerability scan
FortiMail	history, event, antivirus, email filter
FortiManager	event
FortiSandbox	malware, network alerts
FortiWeb	event, intrusion prevention system (IPS), traffic
Syslog	generic (used for compatibility with older FortiGate or non-Fortinet devices)

The logs displayed on FortiAnalyzer depend on the device type logging to it and the enabled features



© Fortinet Inc. All Rights Reserved.

14

To analyze and interpret logs, you must understand the different log types and the information they contain, as well as which logs FortiAnalyzer collects from each supported device.

The logs displayed on FortiAnalyzer are dependent on the device type logging to it and the features you enabled. For example, FortiGate devices generate three log types: traffic logs, event logs, and security logs. Each log type has corresponding log subtypes.

This table lists the log types and subtypes FortiAnalyzer collects from some supported devices. For the complete list, refer to the *FortiAnalyzer Administration Guide*.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What are logs in the compressed phase called?

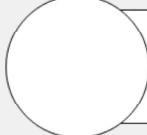
- A. Archive logs
- B. Analytics logs

DO NOT REPRINT**© FORTINET**

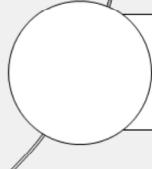
Lesson Overview



Log Data Flow



Log View



FortiView

Good job! You now understand log data flow.

Now, you will learn about ways to navigate the FortiAnalyzer GUI to view and search your logs on FortiAnalyzer.

DO NOT REPRINT**© FORTINET**

Log View

Objectives

- View and search for logs in the log view
- Differentiate between real-time views and historical views
- Create saved filters and dashboards



© Fortinet Inc. All Rights Reserved. 17

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

By demonstrating competence in viewing logs, log summaries, and dashboards, you will be able to find and view a variety of log-related information.

DO NOT REPRINT

© FORTINET

Log View

- View all logs received for each ADOM
- You can choose to view only specific devices, Fortinet logs, log browse, and log groups

The screenshot shows the FortiAnalyzer interface with the 'Log View > Logs > All' path highlighted. The 'Logs' section is selected, and the 'Fortinet Logs' tab is active. A callout bubble points to the 'Fortinet Logs' tab with the text: 'View current logs and any rolled logs, and import logs to FortiAnalyzer'. Below the interface, the Fortinet Training Institute logo is visible.

Log View > Logs > All

FortiAnalyzer

Log View > Logs > All

All Fortinet Logs Threat Hunting Log Browse

Last 1 Hour 07:25:16 - 08:25:16

Filter Mode Add Filter

#	Date/Time	Data Source	Event Message	Event Type
1	2025-05-27 0	FGVM02TM2	traffic	info
2	2025-05-27 0	FGVM02TM2	traffic	info
3	2025-05-27 0	FGVM02TM2	traffic	info

View Less ^

Log View

Logs

Log Settings

View Less ^

View current logs and any rolled logs, and import logs to FortiAnalyzer

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 18

The log view allows you to view all log types received by FortiAnalyzer in normalized log format. When you enable ADOMs, the logging information for each ADOM is displayed.

You can choose to view logs from specific devices, Fabric groups, or log groups. A log group is a group of devices placed together in a single logical object. Log groups are virtual, so they don't have SQL databases or occupy additional disk space. You can view logs generated by FortiAnalyzer, the current log files, and any rolled log files. You can also import logs from other FortiAnalyzer devices.

The options available in the log view vary, depending on the type of ADOM you create. In the example shown on this slide, the ADOM type is Fabric.

DO NOT REPRINT

© FORTINET

Viewing FortiGate Logs

- View three different types of FortiGate logs: traffic, security, and event
- Security and event logs offer a summary dashboard

Log View > Logs > Fortinet Logs

#	Date/Time	Device ID	Action	Source	Destination IP	Service	Application	Sent/Received	Security Event List
1	2025-05-27 1	FGVM02TM2401: ✓		10.0.11.253	96.45.45.45	DNS	DNS	649.0 B/2.2 KB	
2	2025-05-27 1	FGVM02TM2401: ✓		10.0.11.253	96.45.45.45	DNS	DNS	649.0 B/2.2 KB	
3	2025-05-27 1	FGVM02TM2401: ✓		168.10.199.186	224.141.85.77	other	other	0 B/0 B	
4	2025-05-27 1	FGVM02TM2401: ⚡ Deny:UTM		178.10.199.186	224.141.85.77	HTTP	HTTP	900.0 B/2.8 KB	
5	2025-05-27 1	FGVM02TM2401: ⚡ Deny:UTM		178.10.199.186	224.141.85.77	HTTP	HTTP	3.2 KB/1.3 KB	APP 1
6	2025-05-27 1	FGVM02TM2401: ⚡ Deny:UTM		178.10.199.186	224.141.85.77	HTTP	HTTP	1.8 KB/7.5 KB	EMAIL 1
7	2025-05-27 1	FGVM02TM2401: ✓		177.10.199.186	224.141.85.77	HTTP	Vimeo_Video.Play	1.4 KB/11.6 KB	APP 1
8	2025-05-27 1	FGVM02TM2401: ✓		175.10.199.186	224.141.85.77	HTTP	Dropbox_File.Upload	2.7 KB/3.4 KB	APP 1
9	2025-05-27 1	FGVM02TM2401: ✓		175.10.199.186	224.141.85.77	HTTP			
10	2025-05-27 1	FGVM02TM2401: ✓		175.10.199.186	224.141.85.77	HTTP			

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved. 19

Traffic logs allow you to see the traffic traversing the firewalls, including details such as source, destination, service, action (whether the traffic is allowed), and more. Security logs allow you to view logs related to unified threat management (UTM) inspection. Event logs are generally related to firewall system operations.

You can select the security or event log subtype you want to see or access a summary dashboard for an overview.

DO NOT REPRINT

© FORTINET

Viewing FortiGate Logs (Contd)

- View a summary of security logs or event logs to investigate

The screenshot displays two side-by-side dashboards under the heading "Log View > Logs > Fortinet Logs".

Left Dashboard (Security: Summary):

- Header: Traffic, Security, Event.
- Filter: All Devices, Last N Weeks, N = 20, 2025.
- Widget: AntiVirus (Shows Top Virus/Botnet with 9238 monitored, 8448 passthrough, virus_test3 passthrough).
- Widget: SSL (Shows Top Category with SSL connection blocked due to blocked, Logid_62305 blocked, Logid_62307 info).

Right Dashboard (Event: Summary):

- Header: Traffic, Security, Event: Summary, FortiSwitch.
- Filter: All Devices, Last N Days, N = 90, 2025-02-26 13:23:00 - 2025-05-27 13:23:00.
- Section: Total Events (A line chart showing event counts over time from 2025/02/26 21:00 to 2025/05/22 00:00. A significant peak is visible around April 16, 2025, reaching approximately 5000 events.)
- Section: System Events (Shows events like System performance statistics (notice), GUI FortiGuard resource prefetch (information), FortiGate update succeeded (notice), Test (warning)).
- Section: User Events (Shows events like FSSO authentication successful (notice), FSSO authentication failed (notice), Authentication lockout (warning), FSSO log off authentication status (notice)).

A blue callout bubble points to the left dashboard with the text: "Click any entry to drill down for more details".

Fortinet Training Institute

© Fortinet Inc. All Rights Reserved. 20

You can monitor all enabled security and event log types from their respective summary dashboards. Summary dashboards use multiple widgets to display the top logs for each subtype. You can add or remove widgets as needed.

The time filter set at the dashboard level affects the information included on all widgets simultaneously, so you must ensure that it is set correctly.

You can click the links in provided in summary dashboards to go to specific logs. Doing so takes you to the specific log subtype section with the appropriate filters applied to search for the specific log entries.

DO NOT REPRINT
© FORTINET

Logging Interface Overview

The screenshot shows the FortiAnalyzer Logging Interface Overview. At the top, there's a header with "Log View > Logs > Fortinet Logs". Below the header is a search bar with "Set device and time frame" and a "Custom view" button. A blue callout points to the "Custom view" button. To the right of the search bar is a "Create Custom View" button, which is highlighted with a red box. Another blue callout points to this button with the text "Toggle between real-time and historical logs". Further to the right are "Refresh" and "More" buttons.

The main area contains a table of log entries. The first column has a "Text Mode" dropdown set to "action=passthrough catdesc='Information Technology'". A blue callout points to this dropdown with the text "Toggle between raw or formatted logs". The table has columns for #, Date/Time, Device ID, User, Source, Destination IP, Service, Host Name, Action, URL, and several status indicators (Security, Level, General, Direction, Log ID, Message, Session ID, Virtual Domain). The last few columns show detailed log information: Device ID (FGVM02TM2401), Device Name (HQ-NGFW-1), Source Country (Reserved), Source IP (10.0.11.253), Source Interface (port4), Source Interface Role (undefined), Source Port (7962), Source UUID (7bc87d34-7916-51e7-3d5b-71812a61b98e), UEBA Endpoint ID (3), UEBA User ID (3), and Destination (Destination).

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. 21".

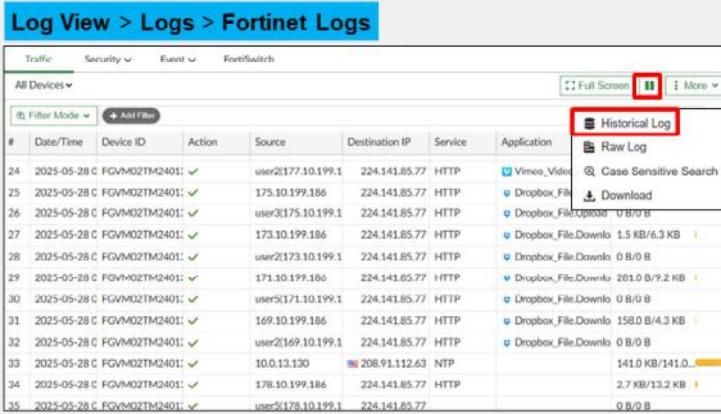
As a SOC analyst, you will frequently need to search through many logs. FortiAnalyzer makes it very easy to search based on any of the fields included in the logs.

To search for specific logs, you select the device and log type and then set the appropriate filters. You can create filters based on any available value, for example, a filter for a specific device within the ADOM and a limited time frame. You can also save a custom view, add or remove columns, view logs in real time or historically, or view logs as raw or formatted logs. To view more information about a log, double-click the log entry.

DO NOT REPRINT
© FORTINET

Real Time vs. Historical Log Views

- View historical logs with the option to specify a time period
- By default, historical logs are displayed
- When viewing logs in real time, you can pause the view to get a more detailed view of the logs



The screenshot shows the 'Log View > Logs > Fortinet Logs' interface. At the top, there are tabs for Traffic, Security, Event, and FortiSwitch. Below that, a dropdown menu shows 'All Devices'. On the right side of the header, there are buttons for 'Full Screen' (with a play/pause icon) and 'More'. A red box highlights the 'Historical Log' button. The main area is a table with columns: #, Date/Time, Device ID, Action, Source, Destination IP, Service, Application, and Raw Log. The table contains 35 rows of log entries. The 'Application' column includes links like Vimeo_Video, Dropbox_File, and Dropbox_File_Download. The 'Raw Log' column shows file sizes and download counts.

#	Date/Time	Device ID	Action	Source	Destination IP	Service	Application	Raw Log
24	2025-05-28 C	FGVM02TM2401:	✓	user2 177.10.199.1	224.141.85.77	HTTP	<input checked="" type="checkbox"/> Vimeo_Video	Case Sensitive Search
25	2025-05-28 C	FGVM02TM2401:	✓	175.10.199.186	224.141.85.77	HTTP	<input checked="" type="checkbox"/> Dropbox_File	<input checked="" type="checkbox"/> Download
26	2025-05-28 C	FGVM02TM2401:	✓	user3 175.10.199.1	224.141.85.77	HTTP	<input checked="" type="checkbox"/> Dropbox_File_Download	0 B/0 B
27	2025-05-28 C	FGVM02TM2401:	✓	173.10.199.186	224.141.85.77	HTTP	<input checked="" type="checkbox"/> Dropbox_File_Download	1.5 KB/6.3 KB
28	2025-05-28 C	FGVM02TM2401:	✓	user2 173.10.199.1	224.141.85.77	HTTP	<input checked="" type="checkbox"/> Dropbox_File_Download	0 B/0 B
29	2025-05-28 C	FGVM02TM2401:	✓	171.10.199.186	224.141.85.77	HTTP	<input checked="" type="checkbox"/> Dropbox_File_Download	201.0 B/9.2 KB
30	2025-05-28 C	FGVM02TM2401:	✓	user5 1.10.199.1	224.141.85.77	HTTP	<input checked="" type="checkbox"/> Dropbox_File_Download	0 B/0 B
31	2025-05-28 C	FGVM02TM2401:	✓	169.10.199.186	224.141.85.77	HTTP	<input checked="" type="checkbox"/> Dropbox_File_Download	158.0 B/4.3 KB
32	2025-05-28 C	FGVM02TM2401:	✓	user2 169.10.199.1	224.141.85.77	HTTP	<input checked="" type="checkbox"/> Dropbox_File_Download	0 B/0 B
33	2025-05-28 C	FGVM02TM2401:	✓	10.0.13.130	208.91.112.63	NTP		141.0 KB/141.0 KB
34	2025-05-28 C	FGVM02TM2401:	✓	178.10.199.186	224.141.85.77	HTTP		2.7 KB/13.2 KB
35	2025-05-28 C	FGVM02TM2401:	✓	user5 178.10.199.1	224.141.85.77	HTTP		0 B/0 B

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 22

You can view historical logs with the option to specify a time period. By default, historical logs are displayed. You must be using the historical log view to use the custom view or chart builder features.

You can switch from viewing historical logs to viewing logs in real time. When viewing logs in real time, you can pause the display to get a more detailed view.

DO NOT REPRINT
© FORTINET

Saving Frequent Log Searches

The screenshot illustrates the process of saving frequent log searches in FortiAnalyzer. It shows two main interfaces: 'Log View > Logs > Fortinet Logs' and 'Log View > Custom Views'.

In the 'Log View > Logs > Fortinet Logs' interface, a search filter 'action=pass appcat=Network.Service' is applied. A blue callout box points to the 'Create Custom View' button, which is highlighted with a red box. This leads to the 'Create New Custom View' dialog box, also shown with a red box around the 'Public Others can see this Custom View' checkbox.

In the 'Log View > Custom Views' interface, a blue callout box points to the 'Custom Views (1)' link under the 'Logs' section, which is highlighted with a red box. This indicates that the saved search is now available under Custom Views.

A large blue callout box at the bottom right states: 'Saved search is available under Custom Views'.

Other UI elements include 'Text Mode' dropdowns, date/time filters, and various log columns like Device ID, Source, Destination IP, Service, and Application Category.

FortiAnalyzer allows you to save searches and build a custom view that you can go to directly whenever you are looking for logs using specific search parameters. This feature is very useful when you are performing a specific search frequently and repeatedly. You can set custom views as public or private. Public custom views can be viewed by all administrators, whereas private custom views can be viewed by only the creator of that view. Users cannot make changes to custom views created by other administrators but can save a copy.

To create a custom view, you will need to add filters, specify a device, specify a time period, and give a name to the view. FortiAnalyzer pulls the time period and search filters that you specify. Custom views are available on the GUI.

This slide shows a custom view that includes all network service traffic logs received over the last 90 days.

DO NOT REPRINT
© FORTINET

Searching Logs

- Filter mode allows you to define your search criteria using the GUI
- Text mode allows you to type in your filter and conditions manually, or select a filter from history

The screenshot shows two side-by-side log views. Both views have a top navigation bar with tabs: All, Fortinet Logs, Threat Hunting, and Log Browse. Below the navigation bar, there is a search bar with a dropdown for 'Last N Days' set to 90 days, and a date range from 02-26 12:09 to 05-27 12:09:16.

Left View (Filter Mode): This view shows a 'Filter values' section with a dropdown menu open, displaying operators like '=', '<', '>', '>=', '

#	Date/Time	Data Source	Event Type	Description
1	2025-05-27 1	FGVM02TM2	traffic	notice 178.10.199.11
2	2025-05-27 1	FGVM02TM2	utm	warning 178.10.199.11
3	2025-05-27 1	FGVM02TM2	traffic	notice 178.10.199.11
4	2025-05-27 1	FGVM02TM2	utm	notice 178.10.199.11

Right View (Text Mode): This view shows a search bar with 'Text Mode' selected and the filter condition 'threat_type != "Reconnaissance"'. The results table is identical to the one on the left.

If your search filters don't return the results you expected, the filter may be poorly constructed.

There are two modes you can use when you search for logs in the log view:

- Filter mode allows you to define your search criteria using the GUI.
- Text mode allows you to type in your filter and conditions or pick a filter from history.

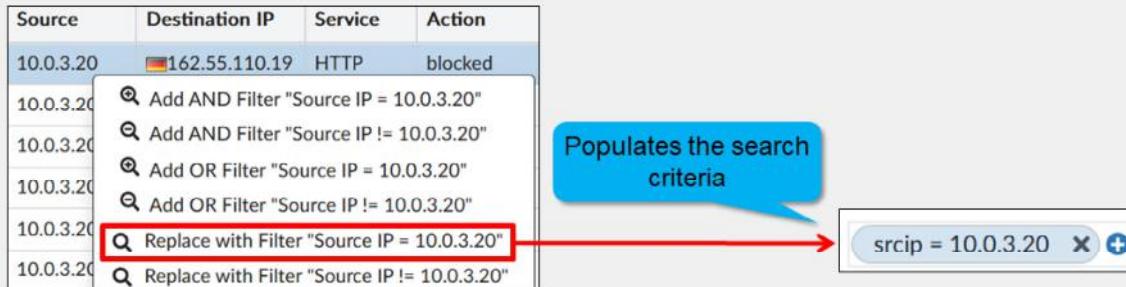
Typing in filters manually is prone to syntax errors and spelling mistakes. Using the context menus in the GUI prevents you from making those mistakes.

DO NOT REPRINT

© FORTINET

Search Tips

- Right-click the desired field value to set a filter based on that data



- Can include (=) or exclude (!=) the selected value from the search results
- Use AND logic if all conditions must be true
- Use OR logic if any of the conditions must be true
- Can also replace the current filter with your new conditions

Another useful tip is to right-click any field in the log entries to add the value to the filter. First, find a log in the log table that includes the data you want to search for. For example, if you want to search for any log entry that contains a specific IP address, right-click the desired value. A pop-up window will open, and you can inject that value into the filter.

You can include or exclude the selected value, use a single condition or multiple conditions, and use AND/OR logic to yield the desired results. You can also replace the current filter with the selected value.

DO NOT REPRINT

© FORTINET

Example of a Log Search

- You must identify the malicious websites visited by the client with IP address 10.0.3.20 for a specific time period

The screenshot shows a log search interface with the following details:

- Security subtype is Web Filter**: A blue callout points to the security type selected.
- Custom time period**: A blue callout points to the custom date range from Jun 07 To Jun 08.
- Filters applied**: The filter bar shows `srcip = 10.0.3.20` AND `Category Description = Malicious Websites`.
- Result Table Headers**: #, Date/Time, Device ID, Source, Destination IP, Service, Action, URL, Category Description.
- Result Data** (Rows 1-5):

#	Date/Time	Device ID	Source	Destination IP	Action	URL	Category Description	
1	06-08 10:37	FGVM-0000077646	10.0.3.20	64.70.19.203	HTTP	blocked	http://fb07fb6990e3b5da86d66d43b4	Malicious Websites
2	06-08 10:37	FGVM-0000077646	10.0.3.20	155.159.36.59	HTTP	blocked	http://whollyfitinc.com/	Malicious Websites
3	06-08 10:37	FGVM-0000077646	10.0.3.20	176.103.56.36	HTTP	blocked	http://176.103.56.36/	Malicious Websites
4	06-08 10:37	FGVM-0000077646	10.0.3.20	43.163.226.161	HTTP	blocked	http://234w.cc/	Malicious Websites
5	06-08 10:35	FGVM-0000077646	10.0.3.20	50.28.56.190	HTTP	blocked	http://www.xn--l3cgic6bw6ctd.com/	Malicious Websites
- Annotations**:
 - A blue callout states: "Filters are based on the client IP address as the source and the category description".
 - A blue callout states: "Fields used in the filter are highlighted".

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 26

This slide shows an example of a filter applied in the log view. You can easily add a filter by right-clicking the desired log field and selecting whether you want that value included or excluded from the logs displayed.

In the example, the following parameters were selected to display malicious websites visited by a client machine:

- The log type selected is **Security**.
- The log subtype selected is **Web Filter**.
- The time frame is **Custom**.
- A filter was applied for the source IP address **10.0.3.20**.
- A filter was applied for the category description **Malicious Websites**.

If you need more granular results, you can add more filters or edit the current filters.

DO NOT REPRINT

© FORTINET

More Tools

- Toggle between formatted logs and raw logs
- Enable or disable case-sensitive searching
- Download logs based on the current filters
- Build custom charts for each type of log message

 More

-  Real-time Log
-  Raw Log
-  Case Sensitive Search
-  Download
-  Chart Builder

Formatted

#	Date/Time	Device ID	Action	Source	Destination IP
4	14:59:50	FGVM010000064692	✓accept	10.200.1.1	208.91.112.60
5	14:59:40	FGVM010000064692	✓accept	10.200.1.1	208.91.112.61
6	14:59:30	FGVM010000064692	✓accept	10.0.1.200	208.91.112.60
7	14:59:30	FGVM010000064692	✓accept	10.0.1.200	208.91.112.63

Raw

```
date=2023-08-16 time=14:59:24 id=7268043151217000450 itime=2023-08-16 14:59:25 euid=3 epid=104
dsteuid=3 dstepid=101 type=traffic subtype=local level=notice action=accept policyid=0 sessionid=89571
srcip=10.0.1.200 dstip=208.91.112.60 srcport=123 dstport=123 transdisp=noop duration=183 proto=17
sentbyte=76 rcvbyte=76 sentpkt=1 rcvdpkt=1 logid=0001000014 service=NTP app=NTP appcat=unscanned
srcintfrole=undefined dstintfrole=undefined eventtime=1692223164328415424 srccountry=Reserved
dstcountry=Canada srcintf=root dstintf=port1 tz=-0700 devid=FGVM010000077646 vd=root
dttime=2023-08-16 14:59:24 itime_t=1692223165
```

The FortiAnalyzer GUI provides options for viewing, searching, and downloading logs.

You can toggle between viewing formatted and raw logs. You can sort formatted logs and customize the columns to meet your requirements. You can show only the data you are looking for and omit the data you do not need. Raw logs are more difficult to read but can provide syntax guidance. For example, there may be instances where you need to look up fields and values to use in text filters when configuring handlers.

To narrow down a query, you can enable or disable case-sensitive searching. You can also download logs based on the current filters as a text or CSV file.

You also use the chart builder feature to build custom charts for each type of log message.

DO NOT REPRINT
© FORTINET

FortiAnalyzer Application Logs

- FortiAnalyzer application logs:
 - Include audit logs for local, SIEM, and SOAR applications (playbooks)
 - Each ADOM has its own audit logs

The root ADOM has event and application logs, while other ADOMs only have application logs

List application log subtypes, such as automation and system, and event type

More details about the events

#	Date/Time	Device ID	User	Sub Type	Event Type	Log ID	Level	Message	Status	Incident ID
1	09:53:42	FAZ-VM0000065040	admin	playbook	cfg-change	110021	notice	Playbook 'New Playbook created from scratch - 20'	success	
2	09:51:13	FAZ-VM0000065040	admin	playbook	run-stat	110263	notice	Task 'Create_Incident' executed successfully.	success	
3	09:51:13	FAZ-VM0000065040		incident	config	100001	notice	Incident IN00000001 is created.	success	IN00000001
4	09:51:11	FAZ-VM0000065040	admin	playbook	trigger	110020	notice	Playbook 'New Playbook created from scratch - 20'	success	
5	09:50:13	FAZ-VM0000065040	admin	playbook	cfg-change	110021	notice	Playbook 'New Playbook created from scratch - 20'	success	
6	09:46:48	FAZ-VM0000065040	system	system	perf-stats	220004	notice	Adom ADOM1 performance status: lograte=0/sec		
7	08:46:48	FAZ-VM0000065040	system	system	perf-stats	220004	notice	Adom ADOM1 performance status: lograte=0/sec		

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved. 28

FortiAnalyzer applications, such as incident management, logging events, and automation playbooks, generate local audit logs accessible in **Log View** under each ADOM.

Administrators can view both local event logs and application logs in the root ADOM. FortiAnalyzer event logs show system-wide information, whereas application logs are ADOM-specific. Non-root ADOMs show only application logs.

On this slide, you can see several logs that show that multiple automation tasks have succeeded. You also see the log rates of ADOM1.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which log view includes the chart builder feature?

- A. Real-time
- B. Historical

2. Saved searches appear under which log view?

- A. Logs
- B. Custom views

DO NOT REPRINT**© FORTINET**

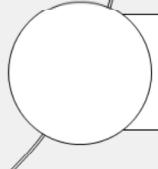
Lesson Overview



Log Data Flow



Log View



FortiView

Good job! You now understand log view navigation.

Now, you will learn how to view summary data and widgets in FortiView.

DO NOT REPRINT**© FORTINET**

FortiView

Objectives

- View summary data in FortiView
- View dashboards and widget features



© Fortinet Inc. All Rights Reserved. 31

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

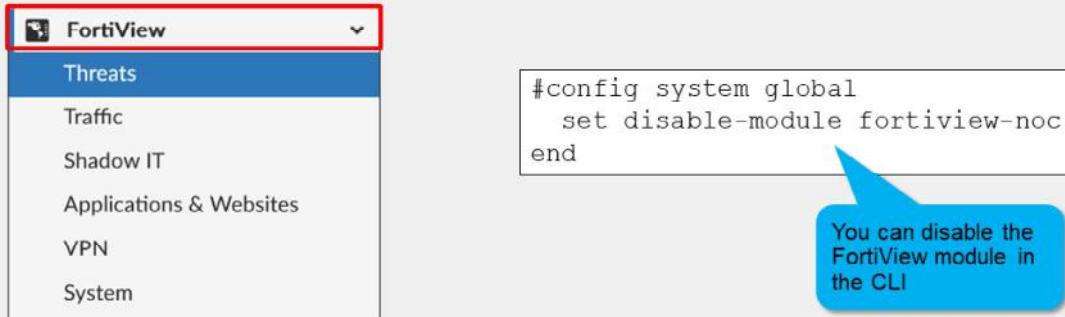
By demonstrating competence in viewing logs, log summaries, and dashboards, you will be able to find and view a variety information related to logs.

DO NOT REPRINT

© FORTINET

FortiView

- A comprehensive monitoring system that displays real-time and historical data
- Each ADOM has its own data analysis in FortiView
- Displays data from analytics logs but not from archived logs
- Offers multiple dashboards to provide summarized views of the network



FortiView displays real-time and historical data and offers multiple dashboards to provide a summarized view of the information for your network. FortiView displays data from analytics logs; however, data from archive logs is not displayed in FortiView.

Each ADOM has its own data analysis view in FortiView. When viewing ADOM data, always ensure that you are in the correct ADOM.

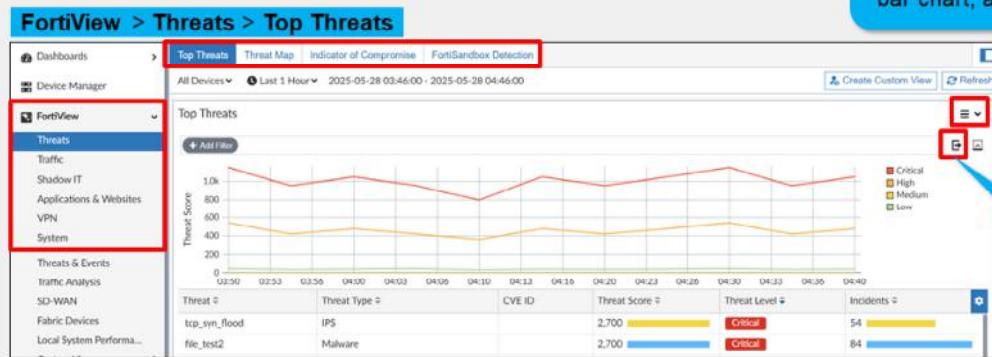
You can disable the FortiAnalyzer FortiView module when you need to for performance tuning using the commands shown on this slide. When disabled, the GUI hides FortiView and stops background processing for this feature.

DO NOT REPRINT

© FORTINET

FortiView Dashboards

- Integrates real-time and historical data into summary views
- Includes multiple predefined dashboards:
 - Threats
 - Traffic
 - Shadow IT
 - Applications & Websites
 - VPN
 - System



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 33

FortiView includes the following predefined dashboards that summarize different aspects of the network:

- Threats** shows top threats, a global map showing traffic destinations, and more.
- Traffic** shows the traffic source, destination, policy hits, and more.
- Shadow IT** shows cloud applications (such as Dropbox and YouTube) and cloud users
- Applications & Websites** shows the top applications, top domains, top website categories, and top browsing users.
- VPN** shows SSL and IPsec dial-up users and site-to-site VPN users.
- System** shows FortiAnalyzer logins, system events, and resource usage.

FortiView allows you to use multiple filters, enabling you to narrow your view to a specific time, by user ID or local IP address, by application, and more. You can also use multiple filters to investigate traffic activity, such as user uploads and downloads or videos watched on YouTube, on a network-wide user group or for individual users.

You can also export FortiView information as a PDF file or create a chart to use in reports.

DO NOT REPRINT

© FORTINET

Example of Using Information on a Widget

- Find threat details on the **Top Threats** dashboard
- Double-click any entry to drill down for more details

This screenshot shows the FortiAnalyzer Top Threats dashboard. A specific threat entry is highlighted with a red border:

Threat	Threat Type	CVE ID	Threat Score	Threat Level	Incidents
PHPBB.Viewtopic.Highlight.Remote.Code.Execution	IPS	840	High	28	
Maze.PHP.Chat.Multiple.File.Inclusion	IPS	CVE-2007-2931	360	High	12
RipeCMS.Parameter.Level.File.Inclusion	IPS	CVE-2007-3584	240	High	8
Ajax.File.Browser.approot.Parameter.File.Inclusion	IPS	CVE-2007-4921	180	High	6

A blue callout bubble points to this entry with the text: "This IPS event has a very high threat score. Double-click to investigate".

Below the main dashboard, a detailed view of the selected threat is shown in a new window:

Summary

threat: PHPBB.Viewtopic.Highlight.Remote.Code.Execution
 Threat Type: IPS
 CVE ID:
 Threat Score (Blocked/ Allowed): 840
 Threat Level: High
 Incidents (Blocked/ Allowed): 28

The detailed view includes a timeline chart showing incidents over time, and a table with source information.

Threats were blocked, but the entry should be thoroughly investigated

Fortinet Training Institute

© Fortinet Inc. All Rights Reserved. 34

From the information displayed on a widget, you can find more details about a specific entry.

On this slide, the **Top Threats** widget displays the top 100 threats. The threat at the top of the list is an IPS event with a very high threat score. If you double-click that entry, you will see more details, like the source IP addresses related to this traffic. In this example, only one IP address is listed, indicating that this host has likely been compromised, and the analyst should report the findings. The IPS threats listed in the widget also include corresponding common vulnerabilities and exposures (CVE) ID numbers with hyperlinks that you can click to read more about the attack vectors, suggested impact, vulnerable software, and more.

DO NOT REPRINT

© FORTINET

Example of Using Information on a Widget (Contd)

- Investigate the top sources displayed on the **Traffic** dashboard



You can use the information displayed on a widget to see more details about a specific entry.

In the example shown on this slide, the **Top Sources** widget was enlarged and customized to display the information in a table format and with full view. The top source on the list is a host that is accessing the network through SSL VPN, with a very high threat score. Double-clicking that host entry will provide more details, like the applications that are generating this traffic. In this example, HTTP is listed as the major source of blocked traffic from that host. More investigation is required to identify if this traffic is normal or if the client is compromised.

DO NOT REPRINT
© FORTINET

Retrieving Archived Logs Through Log Fetching

- Retrieve archive logs from *another* FortiAnalyzer and then run queries or reports on those archived logs
 - Select devices and the time period to be indexed
 - Customize log retention settings for generating reports on older logs
 - Avoid log duplication
- FortiAnalyzer fetch client queries the remote FortiAnalyzer fetch server to retrieve data

System Settings > Advanced > Log Fetch

1. On the fetch client, create a profile for the fetch server:

Create New Profile	
Name	Fetch-Profile
Server IP	10.0.1.210
User	admin
Password	*****

Must have Super_User or Standard_User profile

2. On the fetch client, send the fetch request:

+ Create New	Edit	Delete	Request Fetch
Name:		Server IP:	
<input checked="" type="checkbox"/> Fetch-Profile		10.0.1.210	

Can specify source and target ADOMs, devices, dates, and filters

3. On the fetch server, review, approve, or reject request:

Request Time	Host/Server IP	User	Status	Action
Received Request (1)				
15:20:29	FAZ2(FAZ-VMTM23008175)	admin	Waiting for approval	Review

You can use FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer and index that data. Then, you can run queries or reports for forensic analysis. Log fetching simplifies the generation of reports based on log data by:

- Allowing the administrative user to select the devices and time period to be indexed
- Allowing customized log retention settings for the indexed logs pulled into the ADOM to suit the purpose of report generation based on older logs
- Avoiding log duplication, which can occur during an import from an external backup source

The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices. A FortiAnalyzer device can perform either the fetch server or fetch client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.

You can establish only one log-fetching session at a time between two FortiAnalyzer devices.

DO NOT REPRINT**© FORTINET**

Considerations for Using Log Fetching

- Client and server should run the same firmware version to ensure all log fields match
- Select a source and destination ADOM of the same type
- The destination ADOM must have enough space allocated for the incoming logs
- Data policy on the client must retain logs from the specified time period
 - Logs outside the data policy constraints are deleted
- You must add the devices to Device Manager before you can see their logs on the client
 - You can do the log fetching before adding the devices, but you won't be able to see the logs
- During the request, you can choose filters to include:
 - Logs from specific devices
 - Logs of specific types and values
 - Logs from a specific time frame

There are a few things to consider when using log fetching:

- The client and server devices should be running the same firmware to ensure all log fields match.
- The source and destination ADOMs must be of the same type.
- Ensure the destination ADOM has enough allocated space for the incoming logs.
- Verify the data policy on the client will not delete the incoming logs because they fall outside of the configured time frame.
- The incoming logs will be visible on the client only if the corresponding devices are added to Device Manager.
- Select only the required logs using the available filters in the request window.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which logs does FortiAnalyzer use to populate FortiView data?
 A. Archive logs
 B. Analytics logs

DO NOT REPRINT**© FORTINET**

Lesson Overview



Log Data Flow



Log View



FortiView

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Describe how FortiAnalyzer parses and normalizes logs
- ✓ Validate log parsers
- ✓ Search logs using normalized fields
- ✓ View and search for logs in the log view
- ✓ Differentiate between real-time views and historical views
- ✓ Create saved filters and dashboards
- ✓ View summary data in FortiView
- ✓ View dashboards and widget features



© Fortinet Inc. All Rights Reserved. 40

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

By mastering the objectives covered in this lesson, you learned how FortiAnalyzer parses and normalizes logs. You also learned various methods of searching for logs in log view, as well as how to view summary data, dashboards, and widgets in FortiView.

DO NOT REPRINT**© FORTINET**

FortiAnalyzer Analyst

Events, Indicators, and Incidents

A small red square icon with a white "FA" monogram.

FortiAnalyzer 7.6

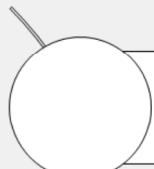
Last Modified: 16 July 2025

In this lesson, you will learn about events, indicators, and incidents on FortiAnalyzer, and how to configure them and use them to triage alerts as a SOC analyst.

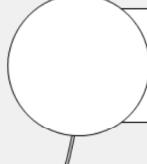
DO NOT REPRINT

© FORTINET

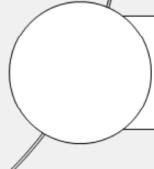
Lesson Overview



Events



Indicators



Incidents

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

DO NOT REPRINT**© FORTINET**

Events

Objectives

- Describe how events are generated
- Configure event handlers
- Manage events

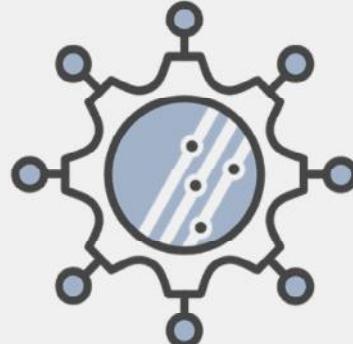
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in managing events and configuring event handlers, you will be able to handle the security events taking place in your environment.

DO NOT REPRINT
© FORTINET

Events and Event Handlers

- Events are generated by event handlers
 - FortiAnalyzer is preconfigured with many event handlers
 - You can create custom event handlers to generate events
- FortiAnalyzer filters all incoming logs using event handlers
 - If logs match the conditions configured in an event handler, FortiAnalyzer generates an event
- All the events that are generated can be viewed on the **Events Monitor** page



Note: Subscription to the Security Automation Service provides FortiAnalyzer with real-time event handlers that can help detect zero-day attacks

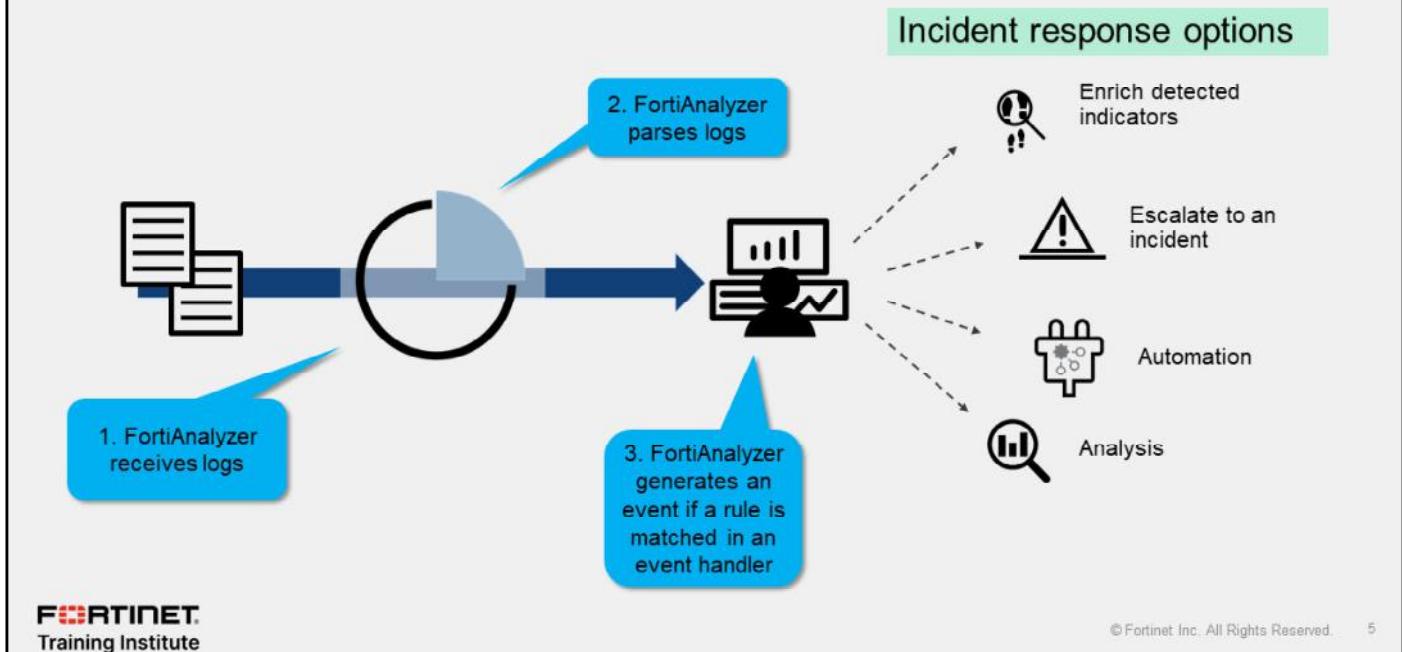
Event handlers generate events on FortiAnalyzer. FortiAnalyzer is preconfigured with many prebuilt event handlers. However, FortiAnalyzer provides analysts with the ability to custom build their own event handlers to generate events from logs that they determine are important. Subscription to the Security Automation Service provides FortiAnalyzer with real-time event handlers that can help detect zero-day attacks.

FortiAnalyzer filters the logs it receives using event handlers and, if the logs received match the conditions that are set in the event handlers, FortiAnalyzer generates an event.

You can view all generated events on the **Events Monitor** page.

DO NOT REPRINT
© FORTINET

How Are Events Generated?



After receiving logs from other devices, and based on the details included in them, FortiAnalyzer uses event handlers to determine if new events need to be generated. Event handlers identify whether the information in the logs matches a series of configurable criteria, such as threat type, device type, log type, and so on.

FortiAnalyzer comes with many predefined event handlers that you can use, clone, and customize. You can also create custom event handlers from scratch.

You can view generated events under **Event Monitor**, where you can see them combined or further divided by endpoint, threat, and system events.

If events warrant further attention and investigation, you can escalate them into incidents. From there, you can correlate logs with an incident, look at an incident timeline, assign a priority and an analyst to review an incident, and more. For a large volume of generated events, you may leverage playbooks to create, handle, and resolve incidents.

FortiAnalyzer can extract indicators such as IP addresses, domains, and URLs out of generated events and enrich them using FortiGuard and Virus Total enrichment services.

DO NOT REPRINT

© FORTINET

Managing Event Handlers

- Event handlers look for specific conditions in the logs
- FortiAnalyzer comes with many predefined event handlers
- Enable or disable them as needed
- Disabled handlers do not generate events

Incidents & Events > Event Handlers

Status	Name	Rules	Events	MITRE Tech ID
Disabled	Default-Web-Server-URL-Scanning-Detected	Rule-1 Web request to malicious destination detected Rule-2 Web request to malicious destination blocked: Rule-3 DNS request to malicious destination detected Rule-4 DNS request to malicious destination blocked: +11	33	T1112, T1595.003
Enabled	Default-Risky-Destination-Detection-By-Threat	Rule-1 Web request to malicious destination blocked: Rule-2 Web request to malicious destination detected Rule-3 Web request to suspicious destination detected Rule-4 DNS request to malicious destination detected +10	7	T1102, T1071.001, T1071.004, T1021.00
Enabled	Default-Risky-Destination-Detection-By-Endpol...			T1102, T1071.001, T1071.004, T1021.00

An event handler looks for specific conditions in the logs and, if a match exists, generates an event with details that you can configure. FortiAnalyzer includes many predefined event handlers that you can enable to generate events.

This slide shows a predefined event handler that has 15 rules and has generated over 33 events on the FortiAnalyzer device.

DO NOT REPRINT

© FORTINET

Event Handlers—Configuration

- The configuration for each event handler can include:
 - Event handler type: basic or correlation
 - MITRE attributes
 - Data selectors (exclusion filters)
 - Automation stitches
 - Notifications
 - Rules
- Rules are granular conditions
 - Event handlers can have one or more rules
 - Basic event handlers use the OR logic
 - Correlation event handlers have many operator logic options

Incidents & Events > Event Handlers

Status: Sample Handler
Name *
Description
Event Handler Type: Basic (selected) Correlation
MITRE Tech ID: HQ-NGFW-1
Data Selector
Automation Stitch
Automatically Create Incident
Rules: Rule 1 - Emergency Priority (selected)
Handler Settings
Notifications: Click to select

An event is generated when a set of rules is met in a correlation sequence

Event handlers require configuration and fine-tuning to deliver only the desired events. The main configuration page for the event handler allows you to enable the handler, assign a name, write a description, and select the type: basic or correlation. When event handler type correlation is selected, an event is generated when a set of rules is met in the correlation sequence.

You can also choose which MITRE domain the event handler falls under, and then select from a list of tech IDs that correspond to the handler. Many predefined event handlers already have the MITRE attributes configured. You can view the MITRE ATT&CK framework matrices under **Incidents & Events**.

You can also add a data selector, which is a common filter that is applied before every rule configured in the event handler. Because of that, they are also known as *exclusion filters*.

When a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification to the FortiGate automation framework, which then checks if there is a corresponding automation stitch in FortiOS. If there is one, the configured action is triggered.

The **Rules** section contains the fields that must match logs in order to generate events. You can disable, edit, or delete rules for the handler. The basic handler type uses OR logic when evaluating multiple rules. The correlation handler type has many more operator logic choices.

You can select a notification profile to send alerts whenever an event is generated by the handler.

DO NOT REPRINT
© FORTINET

Event Handlers—Rule Configuration

- Rules have many customizable fields
 - Not every field is required

Incidents & Events > Event Handlers

Status	Rule 1 - Emergency Priority
Name	Medium
Event Severity	
Choose Your Logs	
Start by selecting the device and log type that you want to monitor for events.	
Log Device Type	FortiGate
Log Type	Traffic Log (traffic)
Log Subtype	Any
The system will categorize logs into smaller groups based on the chosen log fields.	
Log Field	Device ID (devid)
	Not in use
	Not in use
Refine Your Logs	
Once logs are grouped, you can refine the data within each group by applying filter with other log fields. Logs that match the filters will be retained within each group.	
Log Filters	All Filters
Log Field	Any One of the Filters
Match Criteria	
Value	
Action	
Level (pri)	Equal To
	(Emergency)
Log Filter by Text	

Note: The fields available in the rules depend on the selected device type

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved. 8

This slide shows the fields available for configuration inside a rule, including the log device type, log type, and log subtype. Note that within rules themselves both AND and OR logic are supported if there are multiple conditions. You can select common criteria to include in the filter in the **Log Field**. Alternatively, you can use generic text filters if you require precise filtering.

DO NOT REPRINT
© FORTINET

Event Handlers—Rule Configuration (Contd)

- You can define event conditions to reduce the number of generated events
 - Event triggering thresholds can be set based on minimum total matches, field matches, duration, size, and other totals

The screenshot shows the FortiAnalyzer interface for defining event handlers. The 'Define Event Conditions' section is highlighted with a red box. It includes options for triggering an event based on log counts, field values, or duration. Below this is the 'Advanced Settings' section with tabs for Event Type Override, Event Message, Event Status, Tags, Indicators, and Additional Info. The 'Indicators' tab shows a table mapping log fields to indicator types and counts.

Log Field	Indicator Type	Count	Action
Destination IP (dstip)	IP	2	X +
Host Name (hostname)	Domain	2	X +

© Fortinet Inc. All Rights Reserved. 9

If an event handler is generating too many events in your environment, you can configure aggregation expression and aggregation duration settings.

The **Trigger an event when** section contains three options:

- You can set a threshold based on count, or the minimum number of matching logs.
- You can set a threshold based on a distinct field, such as a distinct source IP address or application.
- You can also set a threshold based on duration, sent/received bytes, and sent/received packets.

Duration is the minimum threshold in minutes to generate events. The duration and minimum threshold settings work together. To generate an event, the minimum number of matching logs (expression) must occur in the specified time period (duration).

You can also specify event type, message, status, and severity for events.

DO NOT REPRINT

© FORTINET

Event Handlers—Data Selectors

- Data selectors help narrow down events generated by devices, subnets, and filters:
 - Devices (by name)
 - Subnets (created in Fabric view)
 - Filters (OR logic)
- Filters are granular conditions within data selectors:
 - Log device type
 - Log type/subtype
 - Matching logic (AND/OR logic)
 - Generic text filter (for more precise filtering)

Incidents & Events > Data Selectors

Add New Data Selector

Name * Sample Data Selector

Devices All Devices Specify

Subnets All Subnets Specify

Filters Any of the following conditions

Traffic to Sample IP

Name Traffic to Sample IP

Log Device Type FortiGate

Log Type Traffic Log (traffic)

Log Subtype Any

Logs match All Any of the following conditions

Log Field Destination IP (dstip) **Match Criteria** Equal To **Value** 10.0.0.254

Generic Text Filter

0/1023

Note: The fields available in the filters depend on the selected device type

Data selectors help narrow down the events you see generated in event handlers. You can specify various criteria within the data selector, including devices, subnets, and filters. You must configure a data selector first before you can apply it to an event handler.

Filters are granular rules that filter which types of logs match the data selector. You can create multiple filters per data selector. The data selector matches filters using OR logic.

This slide shows the fields that you can configure for a filter, including the log device type, log type, and log subtype. Note that filters support both AND and OR logic. When configuring a filter, you can select from common criteria on the GUI, or you can use generic text filters if you require precise filtering.

DO NOT REPRINT

© FORTINET

Event Status

- Events can have one of four statuses

Incidents & Events > Event Monitor		Event status	Description
10.0.3.20 (115)	Unhandled	Unhandled	The security event risk is not mitigated or contained, so it is considered open
Compromised host detected	Unhandled	Contained	The risk source is isolated
Web request to Unrated detected	Unhandled	Mitigated	The security risk is mitigated by being blocked or dropped
Web request to Malicious Websites blocked	Mitigated	Blank	Other scenarios
Compromised host detected	Unhandled		
Compromised host detected	Unhandled		
Web request to Malicious Websites blocked	Mitigated		

Note: You can configure the desired event status manually in the handler settings, or let FortiAnalyzer choose it automatically

Events in FortiAnalyzer can have one of four statuses. The current status of an event determines if the security team needs to take further action or not.

The possible statuses are:

- Unhandled:** The security event risk is not mitigated or contained, so it is considered open. For example, an IPS/AV log with `action=pass` will have the event status **Unhandled**. Botnet and IoC events are also considered **Unhandled**.
- Contained:** The risk source is isolated. For example, an antivirus log with quarantine `action` will have the event status **Contained**.
- Mitigated:** The security risk is mitigated by being blocked or dropped. For example, an intrusion prevention system (IPS) or antivirus log with a block/drop `action` will have the event status **Mitigated**.
- (Blank):** A blank status indicates a state that the risk is state is something other than unhandled, contained, or mitigated. For example, both allow and block actions can be seen in logs associated with the event.

DO NOT REPRINT

© FORTINET

Event Handlers—Log Filter by Text

- Log filtering by text (generic text filters) allows you to have more precise and flexible control over which logs trigger an event
 - Multiple operators and logic are supported
 - Operators based on regex and POSIX

Operator	Meaning
<code>==</code>	Equal (Exact match)
<code>!=</code>	Not equal (Not matching)
<code><</code>	Smaller than
<code><=</code>	Smaller than or equal
<code>></code>	Greater than
<code>>=</code>	Greater than or equal
<code>~</code>	Contained (included somewhere in the string)
<code>!~</code>	Not contained (not included)

Generic text format:

- Tokens: `'('`, `')'`, `'&'`, `'|'`, `'and'`, `'or'`, `'not'`
- Operators: `'=='`, `'!='`, `'<'`, `'<='`, `'>'`, `'>='`, `'<='`, `'>='`, `'~'`, `'!~'`

Examples:

```
dstip==192.168.1.168 and hostname ~ "facebook" dstip==192.168.1.168 and ( dstport == 514 or dstport == 515 )
```

These syntax examples
are available on the GUI

- Supported tokens: `'('`, `')'`, `'&'`, `'|'`, `'and'`, `'or'`, `'not'`

Tip: Search the logs for the string that you want to generate an event for, and copy the strings you want to match from the raw log

© Fortinet Inc. All Rights Reserved. 12

FORTINET
Training Institute

When you configure an event handler, you can use generic text filters for more precise and flexible control over which logs trigger an event. Text filters use operators based on regex and the Portable Operating System Interface (POSIX) standard.

Event handlers support multiple operators and logic. You can hover your cursor over the question mark next to **Generic Text Filter** to display an example.

Example: `dstip==192.168.1.168 & hostname ~ "facebook"` matches all logs with a destination IP address field equal to 192.168.1.168 and a hostname field containing the string facebook.

You must use the escape character `\` if you need to include a reserved character in your filter.

To avoid syntax errors, search your raw logs for the log file for which you want to add an event handler and copy and paste the string you want to match.

DO NOT REPRINT**© FORTINET**

Event Handlers—Log Filter by Text (Cont'd)

- A generic filter can be used to exclude or include subnets as a source and/or destination address.
- In this example, the goal is to exclude the following as source IP subnets:
10.0.0.0/8, 192.168.0.0/16, and range: 172.[20-21].[0-255].[0-255].
- POSIX syntax can be used to represent the subnets and ranges
 - 10.0.0.0/8 as 10\.[0-9]+\.[0-9]+\.[0-9]+.
 - 192.168.0.0/16 as 192\.168\.[0-9]+\.[0-9]+.
 - 172.[20-21].[0-255].[0-255] as 172\.[2[0-1]\.[0-9]+\.[0-9]+.
- The generic text filter expression will be:
`srcip!~"10\.[0-9]+\.[0-9]+\.[0-9]+" and srcip!~"192\.168\.[0-9]+\.[0-9]+" and
srcip!~"172\.[2[0-1]\.[0-9]+\.[0-9]+"`



© Fortinet Inc. All Rights Reserved. 13

In the example shown on this slide, the goal is to exclude the following as source IP subnets: 10.0.0.0/8, 192.168.0.0/16, and range: 172.[20-21].[0-255].[0-255].

We see how the POSIX syntax will look like for each of the IP address subnets.

In the POSIX syntax:

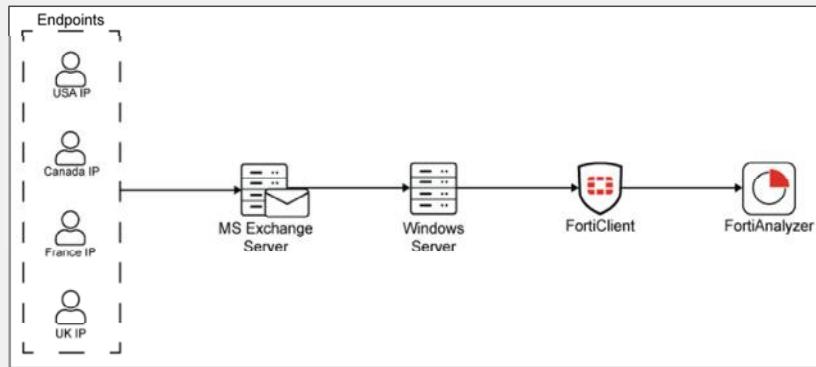
- Slash '\' is needed to escape a period to include it as a valid character.
- [0-9] means any single digit between 0 and 9, and the plus '+' allows more digits.
- The syntax will also match octet '999', which would be wrong, but since it is already known that the logs include only valid IP addresses, it is not necessary to make the filter incredibly precise. The firewall already filters out these results when forming log messages.
- 2[0-1] - means: starting with 2 and the next digit is 0 or 1.

We then combine the three POSIX syntax subnets in and statements to form the expression that will be used in the generic text filter.

DO NOT REPRINT**© FORTINET**

Predefined Event Handlers

- Predefined event handlers are available to detect suspicious activities in the MS Exchange Server
 - MS Exchange—Large Email
 - MS Exchange—Multiple Failed Deliveries
 - MS Exchange—Suspicious Email Activity



FortiAnalyzer comes with predefined event handlers that provide a starting point. You can quickly deploy the predefined event handlers for essential monitoring capabilities, especially in new deployments.

Since the predefined event handlers are configured following Fortinet's recommended best practices, they also serve as an essential learning tool. You can examine the filters and conditions and follow the same guidelines when configuring new handlers.

DO NOT REPRINT

© FORTINET

Use Case: MS Exchange—Large Email Event Handler

- Predefined event handler that uses MS Exchange Server logs to detect large email attachments (greater than 10485760 net sent bytes)

The screenshot shows two windows side-by-side. On the left is the 'Incidents & Events > Event Handlers' window, where a new event handler named 'MS Exchange - Large Email' is being created. It uses the 'Default Microsoft Exchange Transport Log' data selector and has a rule named 'Large Email Attachment Detected'. On the right is the 'Incidents & Events > Data Selectors' window, which shows the configuration of the 'Default Microsoft Exchange Transport Log'. It includes log fields like 'Data Source Type' (Equal To Windows) and 'Application No.' (Equal To Microsoft Exchange Mail). Below this is another 'Choose Your Logs' window, which also shows log fields and filters, including one for 'Net Sent Bytes (Int)' greater than or equal to 10485760.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

15

MS Exchange - Large Email is a predefined event handler that uses MS Exchange server logs to detect large email attachments (greater than 10485760 net sent bytes) being transported in the Microsoft Exchange server.

This event handler uses the predefined data selector, **Default Microsoft Exchange Transport Log**, to ensure the proper devices and logs are used to trigger events.

DO NOT REPRINT

© FORTINET

Use Case: Sensitive Keyword Detection for Safeguarding

- Predefined event handler available to detect safeguarding keywords
 - Web traffic
 - Application traffic (social media)
 - Email

The screenshot shows the FortiAnalyzer interface with two main windows:

- Incidents & Events > Event Handlers**: This window lists event handlers. One entry, "Sensitive Keyword Detection for Safeguarding", is highlighted with a red box. A red arrow points from this entry to the "Define Event Conditions" section in the adjacent window.
- Incidents & Events > Safeguarding**: This window displays a table of keywords and their details. A red box highlights the "Risk Score" column, which contains values like 0.6 and 0.8. Another red arrow points from the "Safeguard Risk Score is more than 0.8" setting in the configuration window to this column.

Incidents & Events > Event Handlers

Status	Name
<input checked="" type="checkbox"/>	Sensitive Keyword Detection for Safeguarding

Define Event Conditions

Once you have organized and filtered the logs, set up criteria that enable the system to automatically initiate events when log records reoccur within each group.

Trigger an event when:

- A group contains or more log occurrences
- Within a group, the log field has or more unique values
- The sum of is greater than or equal to
- Safeguard Risk Score is more than

When "Safeguard" is used, log categorization options may become more limited.
Please review the log categorization selections.

All logs were generated within minutes

Incidents & Events > Safeguarding

Keywords	Origin	Category	Risk Score
Cyber Bullying (2148)			
parent	FortiGuard	Cyber Bullying	0.6
explosive	FortiGuard	Cyber Bullying	0.6
tell adult	FortiGuard	Cyber Bullying	0.6
innocent	FortiGuard	Cyber Bullying	0.6
jumpy	FortiGuard	Cyber Bullying	0.6
braggart	FortiGuard	Cyber Bullying	0.6

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 16

A predefined event handler is available to detect safeguarding keywords in logs for web traffic, application traffic (social media), and email. This event handler supports consistent monitoring for harmful content, allowing timely intervention.

When the rule has a log type of web filter, application control, and email filter, you can trigger an event when the safeguard risk score is more than a specified value. You can view the safeguard keywords and their associated risk scores on the **Safeguarding** page. For all rules in the **Sensitive Keyword Detection for Safeguarding** event handler, FortiAnalyzer triggers events when the safeguard risk score is more than 0.8.

The **Sensitive Keyword Detection for Safeguarding** event handler includes a separate rule for each of the log types that allow for this new trigger (web filter, application control, and email filter).

DO NOT REPRINT
© FORTINET

Exporting and Importing Event Handlers

- Event handlers are configured per ADOM
- To reuse existing event handlers, export them from one ADOM and import them into a different ADOM

The screenshot shows the 'Incidents & Events > Event Handlers' page. In the center, there's a table listing two event handlers: 'Outbreak Alert - Microsoft Outlook' and 'Outbreak Alert - MSDT DogWalk V'. On the right side of the table, there's a context menu with options: 'Enable', 'Disable', 'Show Predefined', 'Show Custom', 'Import' (highlighted with a red box), 'Export' (highlighted with a red box), and 'Factory Reset'. Below the table, there are two dialog boxes: 'Export Event Handler' on the left and 'Import Event Handler' on the right. The 'Export Event Handler' dialog has checkboxes for 'Include Data Selectors' and 'Include Notification Profiles', and a 'Select Export Data Type' dropdown with 'Zipped' selected. The 'Import Event Handler' dialog has a text input field with the placeholder 'Drag & Drop your files or Browse'. Red arrows point from the 'Import' and 'Export' menu items to their respective dialog boxes.

By default, event handlers are restricted to the ADOM where they were created. If you need to use the same settings in a different ADOM, exporting the event handlers saves you the time of creating them again.

To export an event handler, in the **Event Handler** list, select one or more handlers, right-click, and then select **Export**.

A new window opens where you must choose if you want to include data selectors, notification profiles, and the type of file you want to create, whether zipped, text, or CLI configuration. Click **OK** to finish and save the file.

You can create subnets and subnet groups in the Fabric view and use them as filters in event handlers and reports.

To import an event handler, in **Handlers**, right-click, and then select **Import**. You can drag and drop the file, or use the file browser to find the file.

If the imported handler name already exists, you can rename, replace, or skip the import.

DO NOT REPRINT**© FORTINET**

Managing Events

- **Event Monitor** displays events generated by the configured event handlers

Incidents & Events > Event Monitor

Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler
66.199.231.77 (1)	Mitigated	Web Filter	1	Medium	21 hours ago	21 hours ago	Default-Risky-Destination-Detection-By-Threat
66.45.245.150 (2)	Unhandled	Traffic	2	Critical	a day ago	a day ago	Default-Compromised-Host-Detection-IOC-By-Threat
Traffic to C&C from 10.0.1.200 detected	Unhandled	Traffic	1	Critical	2023-09-05 19:05:42	2023-09-05 19:06:05	Default-Compromised-Host-Detection-IOC-By-Threat

Critical severity and marked as unhandled
Double-click to see the originating log

This is the event handler that generated this event

Search or type filters...

#	Date/Time	Device ID	Action	Source	Destination IP	Service	Application	Sent/Received	Security Event List
1	09-05 19:05	FGVM010000064692	✓ close	10.0.1.200	66.45.245.150	HTTP	HTTP.BROWSER	464.0 B / 1.1 KB	1

Note: If FortiAnalyzer is creating unexpected events, you need to check the handler configuration

© Fortinet Inc. All Rights Reserved. 18

After event handlers start generating events, you can view and examine them combined or divided by endpoint, threat, or system events.

You can double-click an event to see more details about it, including the information from the associated logs. Generally, you should give priority to events with an unhandled status or critical severity.

DO NOT REPRINT
© FORTINET

Available Management Actions for Events

- You can acknowledge an event, add a comment, assign it to an administrator, or create an incident from it

The screenshot shows the 'Incidents & Events > Event Monitor' page. At the top, there are filters for 'All Events', 'By Endpoint', 'By Threat', 'System Events', and 'Toggle Views'. A red box highlights the 'Show Acknowledged' checkbox, which is unchecked. A blue callout bubble says 'Acknowledged events are not shown by default'. Below the filters is a table with columns: Event, Handler, Event Type, Count, and Severity. The table lists various events like 'Intrusion from 100.65.0.254 detected' and 'Default-Botnet-Communication-Detection-By-Threat'. A red box highlights the right-click context menu for an event row. The menu options include 'Acknowledge', 'Comment', 'Assign To', 'View Logs', 'Search in Log View', 'Create New Incident', and 'Add to Existing Incident'. A blue callout bubble for this menu says 'Right-click an event to see the list of available actions'. Another blue callout bubble says 'Create incidents from events that require further investigation'. A red box highlights the filter bar at the bottom of the table, which includes dropdowns for 'All' and 'IPS' and a search bar. A blue callout bubble says 'Filter based on the column values to narrow the search'. The Fortinet Training Institute logo is in the bottom left, and the copyright notice '© Fortinet Inc. All Rights Reserved.' is in the bottom right.

You can right-click an event to leave a comment for your records, acknowledge the event, assign it to an administrator (or yourself) for further investigation, or create an incident from it. You will learn about incidents in this lesson.

Acknowledging an event removes it from the event list, but you can display it again by clicking **Show Acknowledged**. Generally, you can acknowledge mitigated events because the related traffic was blocked by the firewall. The exception could be an excessive number of mitigated events, which, despite being blocked, may indicate a compromised device. Additionally, if an event was used to generate an incident, you should also acknowledge it after you mark it as resolved.

You can use filters to display only the events of interest. For example, you may need to display only events related to IPS.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What are event handlers?
 - A. Threats identified by FortiGuard that generate events
 - B. A set of matching conditions in the logs that generate events

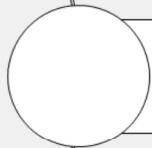
2. How do you create event handlers for all ADOMs?
 - A. Create the event handlers in the root ADOM.
 - B. Export handlers and then import them into the appropriate ADOMs.

DO NOT REPRINT**© FORTINET**

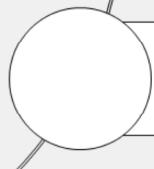
Lesson Overview



Events



Indicators



Incidents

Good job! You now know how to manage events and configure event handlers.

Now, you will learn about indicators.

DO NOT REPRINT**© FORTINET**

Indicators

Objectives

- Configure indicators

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

By demonstrating competence in configuring indicators, you will be able to add more context and threat intelligence about suspicious artifacts when investigating security incidents.

DO NOT REPRINT

© FORTINET

What Are Indicators?

- Data extracted by FortiAnalyzer from events that could be harmful or malicious
- You can choose what type of data to extract from which events
- Indicator types
 - IP address
 - URL
 - Domain
- Indicator reputation
 - Malicious
 - Suspicious
 - Harmless
 - Undetected

Extract indicators such as IP addresses, domains, and URLs out of the events

Indicators	Log Field	Indicator Type	Count	Action
Destination IP (dstip)	A	IP	2	x +
Host Name (hostname)	A	Domain	2	x +

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 23

Indicators are data extracted by FortiAnalyzer from events that could be harmful or malicious. On FortiAnalyzer, you can choose which type of data to extract from which events by filtering while configuring the rules in event handlers. You can also manually create indicators on the **Indicator** page.

There are three types of indicators: IP addresses, URLs, and domains.

Also, after their enrichment, indicators can have one of four reputation types: malicious, suspicious, harmless, or undetected.

DO NOT REPRINT

© FORTINET

Managing Indicators

Indicator ...

- Domain 2
- IP 1
- URL 1

Reputation

- TBD 4
- Malici... 0
- Suspici... 0
- NoRe... 0
- Failed 0

Enrichme...

- None 4
- InProc... 0
- Compl... 0
- Failed 0

Block Sta...

- None 4

Create New **Edit** **Clone** **Delete** **Enrich** **Block** **Show Charts** **Search...**

Type	Block Status	Rating Confidence	Reputation	Enrichment Status
Domain	Domain			
IP				
URL				
Domain				

Select a value on the chart to see items from that section

Actions that can be performed on the Indicators

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

The **Indicators** chart consolidates all detected indicators for centralized analysis. This streamlines threat evaluation and enables SOC analysts to take swift action to mitigate risks. The indicators page allows you to view details about the indicators in a pie chart and tabular form. Select a value in any of the charts to apply the filter to all charts and the table view. To remove the filter, click the chart title.

DO NOT REPRINT**© FORTINET**

Enriching Indicators

The screenshot illustrates the FortiAnalyzer interface for enriching indicators. On the left, the 'Incidents & Events > Indicators' screen shows two entries: '99.goodyouxi.com' (Domain) and '55.184.85.99' (IP). The 'Enrich' button is highlighted with a red box. An arrow points from this button to the right-hand enrichment details window. The enrichment details window for '99.goodyouxi.com' displays various threat intelligence feeds and vendor analysis. It includes sections for 'Forticloud CTS', 'Confidence IOC Category IOC Tags', 'VirusTotal Summary', and a large table titled 'Security Vendors' Analysis' containing 94 rows of data from various security vendors like Kaspersky, BitDefender, and ESET, each with a status column (e.g., Malicious, Harmless, Acronis, etc.). Below the enrichment details window, a 'Whois Lookup' panel provides detailed WHOIS information for the domain.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

25

The indicator enrichment feature provides security analysts with comprehensive threat intelligence about identified IP addresses, domains, and URLs. Enriched context gives analysts an opportunity for a deeper understanding of security incidents, empowering them to make more informed and effective decisions. When you save an enrichment, it updates the existing entry in the history. A new entry will only be created when there are changes in the enrichment.

DO NOT REPRINT
© FORTINET

Connectors for Indicator Enrichment

- FortiAnalyzer uses FortiGuard and VirusTotal enrichment services to evaluate the risk posed by the indicators

The screenshot displays the FortiAnalyzer interface with two main sections:

- Incidents & Events > Automation > Active Connectors:** Shows the configuration for the VirusTotal Connector. A callout notes: "VirusTotal requires an API Key in the Fabric Connectors".
- Incidents & Events > Automation > Playbooks:** Shows a playbook named "Indicator Enrichment" which "Enrich indicator with different connectors". The playbook flowchart includes steps: ON DEMAND STARTER → ENRICH_START → ENRICH_VirusTotal_enrichment → ENRICH_FortiGuard_enrichment → ENRICH_AGGREGATE. A callout notes: "Playbook is executed every time an indicator is enriched".

Fortinet Training Institute

FortiAnalyzer uses FortiGuard and VirusTotal enrichment services to evaluate the risk posed by the indicators. FortiGuard is built in and ready to use, and VirusTotal requires you to configure an API key in the Fabric connectors.

FortiAnalyzer now offers a new predefined playbook called Indicator Enrichment. This playbook is read-only and enabled by default. It is executed every time an indicator is enriched.

DO NOT REPRINT

© FORTINET

Blocking Indicators

- To use this feature, you must configure an authorized FortiManager connector for FortiAnalyzer

The screenshot shows two interface windows side-by-side. On the left, the 'FortiAnalyzer Incidents & Events > Indicators' window displays a list of suspicious indicators. One indicator, 'secure-sys-update.com', is selected and highlighted in green. On the right, the 'FortiManager: FortiGuard > External Resource' window shows the 'Edit External Resource File "root_BLKIP"' dialog. This dialog lists three files: 'root_BLKURL', 'root_BLKIP' (which is checked), and 'root_BLKDOM'. The 'Content' pane displays a list of IP addresses: 104.16.63.16, 104.20.175.46, 104.26.6.17, 13.224.14.35, 149.202.98.191, 162.159.136.10, 162.159.136.11, 162.159.136.15, 162.159.136.16, 192.95.4.124, 195.201.58.253, 213.95.36.8, 23.26.60.198, and 25.36.59.17. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

You can block suspicious indicators directly from FortiAnalyzer. This can help you reduce potential risks and quickly respond to known threats by blocking suspicious IP addresses, URLs, or domains. To use this feature, you must set up an authorized FortiManager connector for the FortiAnalyzer on the **Fabric Connector** page of FortiAnalyzer.

In the back end, a playbook called `Block_indicator` runs every 5 minutes to send the information to FortiManager. After the playbook is run, the indicator's status changes to **Blocked**. The **Blocked** status on FortiAnalyzer confirms that the list is updated on FortiManager, but it is not synced to FortiGate.

When the playbook runs successfully, the blocked indicator is pushed to the FortiManager **External Resource** list. Using this list in FortiManager, you can create threat feeds, security profiles, and policy blocks to push the policies to the identified FortiGate. You can also use this list to update all FortiGate devices to block the suspicious indicators.

The FortiManager firmware version must be the same as FortiAnalyzer for the blocklist to be pushed to FortiGate devices.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. How does FortiAnalyzer create indicators?

- A. FortiAnalyzer extracts data from incidents.
- B. FortiAnalyzer extracts data from events.

DO NOT REPRINT**© FORTINET**

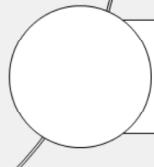
Lesson Overview



Events



Indicators



Incidents

Good job! You now know how to manage and enrich indicators.

Now, you will learn about incidents.

DO NOT REPRINT**© FORTINET**

Incidents

Objectives

- Create incidents
- Analyze incidents
- Configure incident settings

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

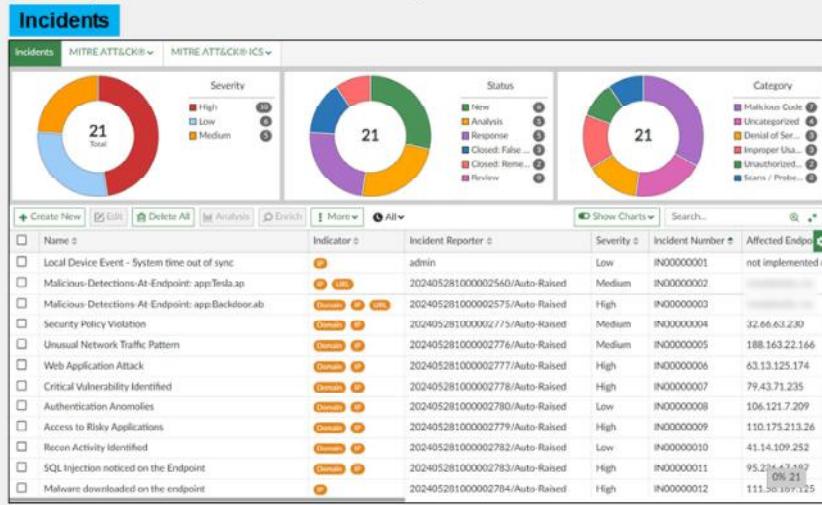
By demonstrating competence in creating and analyzing incidents, you will be able to investigate security incidents more efficiently in your organization.

DO NOT REPRINT

© FORTINET

Incidents

- The central command center for SOC analysts
- Monitor, investigate, and take action from a single interface
- Interactive charts provide immediate insights



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

31

The **Incidents** page is the central command center that allows security teams to manage, investigate, and respond to security threats efficiently.

An incident on FortiAnalyzer is a container for related security events. Key features of the **Incidents** page include prioritization at a glance, where interactive charts at the top provide immediate insights, allowing analysts to prioritize and filter incidents with ease.

The page also provides actionable intelligence, including the incident table, which places vital information, including columns like **Incident Name**, **Indicators**, and **Incident Reporter**, front and center for efficient decision-making.

DO NOT REPRINT**© FORTINET**

Creating an Incident

- An incident should be created when an event needs further analysis
- Can create manually or automatically (playbooks)

The screenshot shows the FortiAnalyzer interface. On the left, the 'Incidents & Events > Event Monitor' page is displayed, showing a list of events. One event, 'Insecure SSL connection blocked' (ID IN00000002), is selected. A context menu is open over this event, with the 'Create New Incident' option highlighted and a red arrow pointing to it. To the right, a 'Create New Incident' dialog box is open. It contains fields for 'Incident Category' (set to 'Unauthorized Access'), 'MITRE Domain' (set to 'Enterprise ICS'), 'MITRE Tech ID' (dropdown menu showing T1021.004 SSH, T1071.001 Web Protocols, T1071.004 DNS, and T1102 Web Service), 'Severity' (set to 'Low'), 'Status' (set to 'New'), 'Affected Endpoint' (set to '10.0.1.10'), 'Description' (set to 'Default-Risky-Destination-Detection-By-Endpoint'), and 'Assigned To' (set to 'admin (Super_User)'). A blue callout bubble points to the 'Assigned To' field with the text: 'Must create accounts for the party responsible for handling incidents'. At the bottom of the interface, the 'Incidents & Events > Incidents' page is visible, showing the newly created incident.

Not all events have the same impact on or importance in your network. Some events might need further analysis to prevent or mitigate security breaches. When you find an event that requires further scrutiny, you should create a new incident from that event. You can think of an incident as an event that could have negative consequences in your everyday operations.

You can create incidents manually or, preferably, automatically using playbooks, taking advantage of FortiAnalyzer automation capabilities.

In FortiAnalyzer, you create incidents manually by right-clicking the desired event and selecting the corresponding option.

Every incident includes a category, severity, status, affected endpoint, and, optionally, a description, MITRE attributes, and an assigned analyst.

Once created, you can view incidents on the **Incidents** page.

DO NOT REPRINT**© FORTINET**

Incident Analysis

- From the incident page, you can perform the following analysis tasks:
 - Export incident
 - Enrich incident indicators
 - Execute playbooks
 - Run report
 - Quarantine endpoints
- Key benefits:
 - Immediate insights: Essential functionalities are readily available, eliminating the need for multiple clicks or navigation
 - Personalized workspace: Analysts have the flexibility to arrange, resize, and customize individual widgets to tailor their incident analysis view precisely to their preferences



© Fortinet Inc. All Rights Reserved. 33

Leveraging a customizable widget layout, you can now access all critical information and actions directly from a single, personalized dashboard.

From the incident page, you can perform the following analysis tasks: Export incident, enrich incident indicators, execute playbooks, run a report on the incident, and quarantine endpoints.

Key benefits include:

- Immediate insights: Essential functionalities are readily available, eliminating the need for multiple clicks or navigation. This translates to faster response times and improved efficiency.
- Personalized workspace: Analysts have the flexibility to arrange, resize, and customize individual widgets to tailor their incident analysis view precisely to their preferences.

DO NOT REPRINT

© FORTINET

Analyzing an Incident

Incident number, description, category, and incident status

You can perform these actions

Important details to help you investigate the threat, with the option to add or delete entries

Reports

Add	Delete	Search
<input type="checkbox"/> Report Name	Format	Time Range
<input type="checkbox"/> Daily Summary Report-2025-05-28-030...	PDF	2025/05/27 - 2025/05/27
<input type="checkbox"/> Daily Summary Report-2025-05-29-030...	PDF	2025/05/28 - 2025/05/28

To view the details of an incident, go to **Incidents** and double-click the incident you want. You can also select an incident and then click **Analysis**.

The **Analysis** page provides all the relevant information and access to the tools an administrator needs to perform a full investigation of the incident. Some of the details shown on this page include: the affected endpoint and user (if available), the incident's timeline, the option to execute a playbook, audit history with any attached events and reports, and several more.

You can enrich indicators tied to the incident, block such indicators on FortiManager, and quarantine endpoints directly from the incident page.

The list of events associated with the incident is also available under the tab with that name. From here, you can access the related logs by right-clicking the event of interest.

DO NOT REPRINT**© FORTINET**

Editing an Incident

- Update each incident setting while working in it
- Close any solved incident
- Once closed, you can delete the incident from the list
- Notifications can be configured for each status change

Incidents & Events > Incidents

The screenshot shows the 'Edit Incident' form with various fields filled out. The 'Status' field is highlighted with a red border and has a dropdown menu open, displaying five options: 'New', 'Analysis', 'Response', 'Closed: Remediated', and 'Closed: False Positive'. Other visible fields include 'Incident Number' (IN0000001), 'Incident Name' (Default-Malicious-Code-Detection-By-Threat happened at 100.65.0.254), 'Incident Date / Time' (2025-05-29 12:19:28), 'Incident Update Date / Time' (2025-05-29 12:22:02), 'Incident Category' (Uncategorized), 'MITRE Tech ID' (Click to select), 'Severity' (High), 'Affected Endpoint' (100.65.0.254), and 'Description' (Default-Malicious-Code-Detection-By-Threat happened at 100.65.0.254). The 'Assigned To' field shows 'admin (Super_User)'.

Note: You must update incident details according to the progress of the investigation. Every incident must reach the **Closed** status

It is important to keep all incident settings up to date. This allows you to keep track of the work being done to solve them.

When an incident is considered closed, you should change its status accordingly. Additionally, you can delete resolved incidents from the list.

You can configure FortiAnalyzer to send notifications after any changes to an incident status.

DO NOT REPRINT
© FORTINET

Configure Incident Settings

The screenshot shows the FortiAnalyzer interface for managing incidents. At the top, there's a table of incidents with columns for Name, Severity, Indicator, and Affected Endpoint. A red box highlights the 'Export' button, with a callout 'Export incidents for compliance'. Below the table is a 'Notifications' section. It includes a 'Create New' button and two connector configurations: 'Fabric Connector 1' (MS_Teams_Connect) and 'Fabric Connector 2' (ServiceNow_Connect). Each connector has checkboxes for sending notifications on creation, update, or deletion. A blue arrow points from the 'Notifications' section to a callout 'First create the connectors in Fabric View'. To the right, a detailed view of a notification message titled 'FAZ_Notification 1:23 PM' is shown, containing JSON-like data about an incident update. A red box highlights the 'incid' field. A callout 'Notification example' points to this message. At the bottom left is the Fortinet Training Institute logo, and at the bottom right are copyright and page number information.

Note: Different connectors can have different settings

© Fortinet Inc. All Rights Reserved. 36

Incidents usually undergo several stages during the analysis process. In most cases, it is important to notify all parties involved when the incident status changes.

You can configure FortiAnalyzer to send a notification to external platforms using preconfigured Fabric connectors.

To configure notifications, in **Settings**, select a Fabric connector from the drop-down field, and then choose the incident activity for which you want to send notifications.

You can add more than one Fabric connector, each with the same or different notification settings. For the notifications to be sent successfully, you must configure the receiving side of the connector. This slide shows a notification received in Teams for an updated incident.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. When would you raise an incident?
 A. To change the status of an incident to **Unhandled**
 B. To further analyze events of interest

2. What is required to send notifications about incident updates?
 A. Existing Fabric connectors
 B. Attaching a report to an incident

DO NOT REPRINT**© FORTINET**

Lesson Overview



Events



Indicators



Incidents

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Describe how events are generated
- ✓ Configure event handlers
- ✓ Manage events
- ✓ Configure indicators
- ✓ Create incidents
- ✓ Analyze incidents
- ✓ Configure incident settings

© Fortinet Inc. All Rights Reserved.

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

By mastering the objectives covered in this lesson, you learned about how to manage the various events, indicators, and incidents on FortiAnalyzer.

DO NOT REPRINT

© FORTINET



FortiAnalyzer Analyst

FortiAI, Threat Hunting, and Troubleshooting

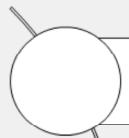
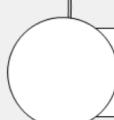
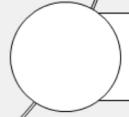
 FortiAnalyzer 7.6

Last Modified: 16 July 2025

In this lesson, you will learn how to use FortiAI and other threat hunting tools on FortiAnalyzer.

DO NOT REPRINT**© FORTINET**

Lesson Overview

**FortiAI****Threat Hunting****Troubleshooting****Automation Stitches**

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

DO NOT REPRINT**© FORTINET****FortiAI****Objectives**

- Describe FortiAI operations
- Describe FortiAI use cases



© Fortinet Inc. All Rights Reserved.

3

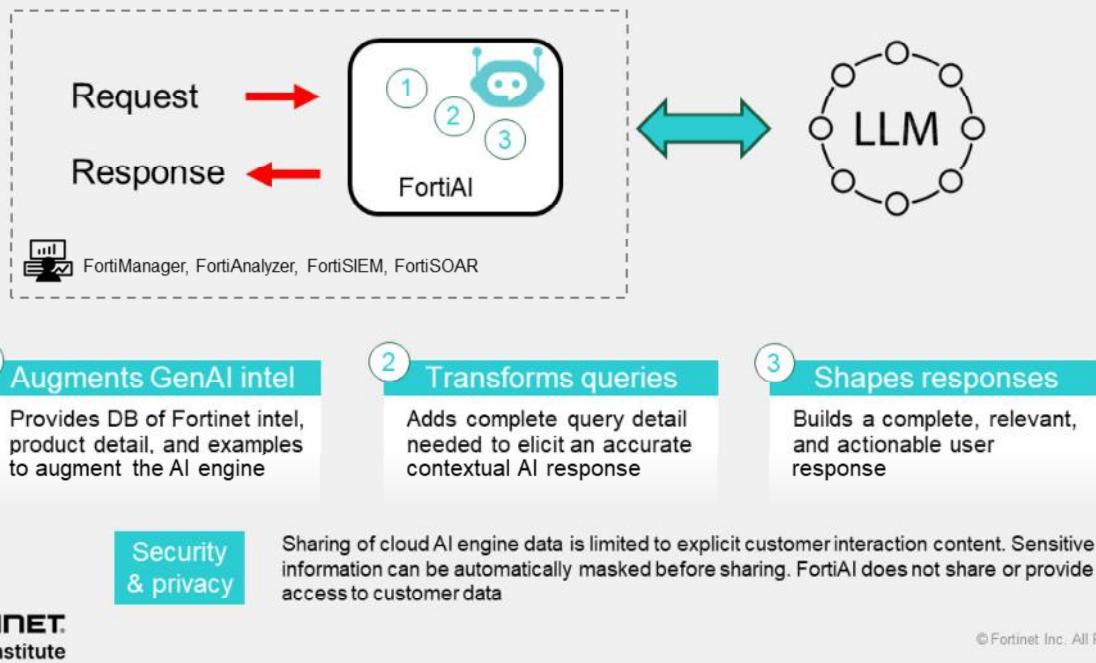
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in describing FortiAI, you will be able to incorporate it into your workflow and automate many of your day-to-day activities.

DO NOT REPRINT

© FORTINET

FortiAI—How Does it Work?



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

4

FortiAI is not just a direct call to public generative AI (GenAI) services. Fortinet AI and product specialists continuously curate a database of proprietary threat intelligence, product-specific knowledge, use case examples, and more, serving as a supplemental data source to the GenAI model. When a user submits a prompt, relevant data from this database is also sent to the GenAI engine to provide a fully relevant contextual response. This process is known as retrieval-augmented generation (RAG).

However, producing an optimal response involves more than RAG. FortiAI converts simple natural language user prompts into precise queries that accurately reflect user intent and generate a contextual response. FortiAI then refines the received response to create a complete, relevant, and product-actionable user reply.

DO NOT REPRINT
© FORTINET

FortiAI Data Protection for FortiAnalyzer

Data protection	
Function callback	<ul style="list-style-type: none"> Sends questions to the public LLM to generate a product-understandable query Processes the query and the results locally
Data masking	<ul style="list-style-type: none"> Masks IP addresses, MAC addresses, and usernames before sending to the public LLM Unmasks data locally after the function callback
Secure proxy	<ul style="list-style-type: none"> Passes all AI interactions through Fortinet proxies Performs additional checks for data protection
Data privacy warnings	<ul style="list-style-type: none"> Generates a warning prompt if data cannot be masked Requires user confirmation before uploading to the public LLM



AI guardrails	
Defined boundaries	<ul style="list-style-type: none"> Clear limits on AI capabilities Unsupported queries generate "I'm not sure" or "I don't know" responses
Retrieval Augmented Generation	<ul style="list-style-type: none"> Improves response accuracy by retrieving only relevant information Provides references to support FortiAI responses

Fortinet takes a multilayered approach to data protection.

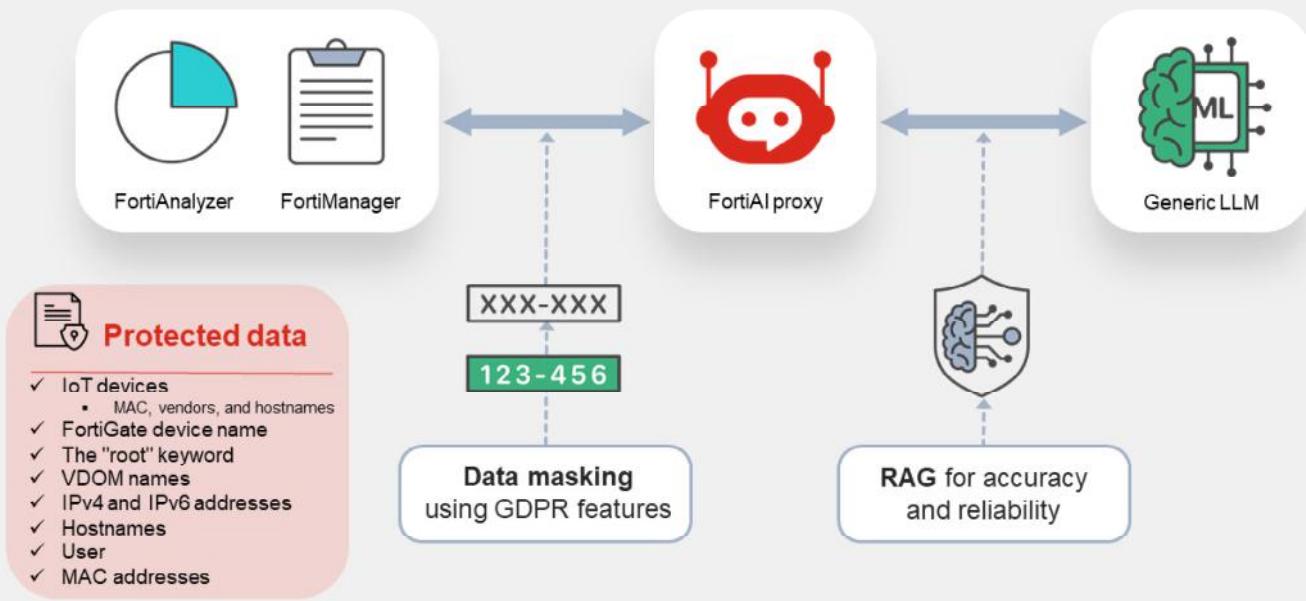
Your query first goes to a public large language model (LLM). The LLM generates a product-specific query that the device can understand. Your local host then executes this generated query. This ensures that all results are processed directly on your premises. FortiAI automatically masks all sensitive information in queries—IP addresses, MAC addresses, and usernames. The LLM doesn't require this specific data to form the query. Once the function calls back to your local device, FortiAI unmasks the data locally, making it available on your system without ever exposing it to the cloud-based LLM in its original form.

FortiAI routes all AI interactions through Fortinet proxies before they reach the LLM. The proxy performs additional security checks to ensure your data remains protected as it traverses the network. In scenarios where sensitive data, particularly in visual formats like images of network topologies, cannot be reasonably masked, FortiAI triggers a data privacy warning. This step gives you the option to confirm or cancel the upload before it's sent to the LLM.

The FortiAI assistant operates within explicitly defined boundaries. If an unsupported query is made (for instance, asking about weather, stock prices, or recipes), the AI will respond with "*I'm not sure*" or "*I don't know*". This mechanism prevents the AI from venturing into unrelated topics and helps maintain focus and security. RAG ensures the accuracy and relevance of the responses. This technology allows the AI to retrieve relevant information and provide references to support its answers.

DO NOT REPRINT
© FORTINET

FortiAI Data Protection Flow Visualized



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

6

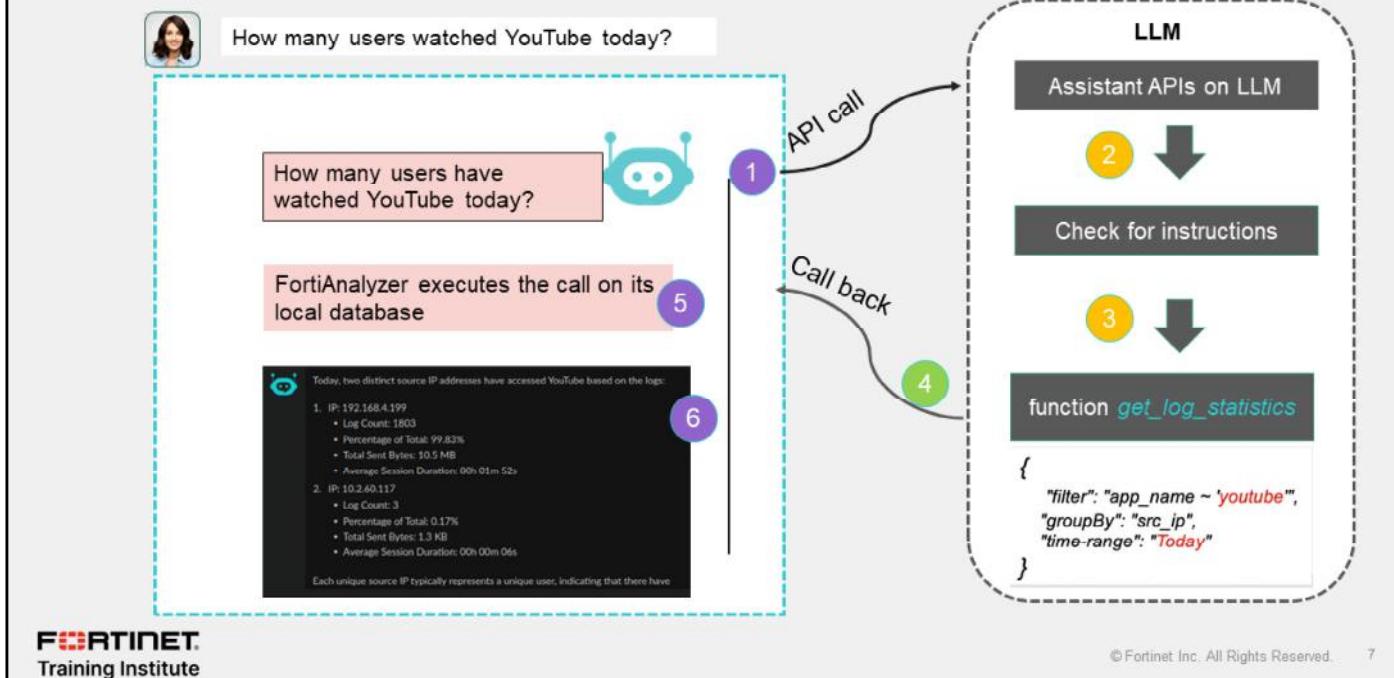
This slide shows the flow of the proxied LLM connection from FortiAnalyzer. Requests are scrubbed with data masking on their way to the FortiAI proxy, which is hosted by Fortinet. The specific types of data that are protected are shown at the bottom left. These are examples and do not constitute the full list.

RAG, which is implemented between the proxy and the LLM, embeds several pieces of knowledge about FortiAnalyzer, such as the administrator guides, supporting documentation, Fortinet knowledge base, and others. This allows Fortinet to help restrict the answers and proposed actions by the FortiAI assistant to ensure they are relevant to the product, that the data supporting the AI response is from approved sources only, and minimize the chance of any irrelevant responses or unsupported actions.

DO NOT REPRINT

© FORTINET

Example of Data Protection



This slide shows an example of data protection when using the FortiAI assistant on FortiAnalyzer. In this case, the user asks how many people have watched YouTube today. If you are the developer of an app that holds sensitive data, you could give the LLM access to the underlying logs, or you could send the relevant logs to the LLM to achieve a direct answer. However, this is neither safe nor desirable for data security reasons.

Instead, first, the FortiAI assistant determines if any of that sensitive information is needed to answer the query. FortiAnalyzer knows how to search for relevant logs and can be directed to do so with the appropriate query. It is not necessary to transmit any data about the logs themselves to answer the question. Instead, you need to know only the necessary query. The AI assistant hands this query to FortiAnalyzer, which conducts the search locally and provides the answer without the information ever having to leave FortiAnalyzer.

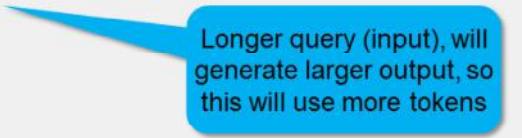
Now, suppose you make a query that does contain sensitive information, such as “*Show me how often the user at IP address 10.10.10.209 accessed YouTube today*”. To form the query, you must send a value for the IP address to the proxy and then on to the LLM. The data scrubbing must replace the IP address 10.10.10.209 with something meaningless and irrelevant, such as 169.254.0.1, and then ask the LLM to come back with the query. What is returned is a query that is formed to look for all instances of IP 169.254.0.1 accessing YouTube. The FortiAI assistant will simply replace the *dummy* value with the real IP address locally and run the query, which now gives you accurate results, without any sensitive information leaving the application.

DO NOT REPRINT

© FORTINET

Token Usage

- FortiAI license includes a monthly entitlement of tokens that all FortiAI users share
- LLMs use tokens to process text and quantify usage
- Token usage is calculated according to these guidelines:
 - On the FortiAI assistant, the text in both the prompt (input) and the response (output) are processed as tokens
 - In general, more text in the query and response results in using more tokens
 - Queries during a long session will consume more tokens than new conversations
- Consider the following two queries:
 - Can you show me all the log entries for the endpoint 10.10.10.10?
 - Show logs for 10.10.10.10 (past week)



Longer query (input), will generate larger output, so this will use more tokens

The FortiAI license for FortiAnalyzer includes a monthly entitlement of tokens that all FortiAI users share.

LLMs use tokens to process text and measure usage. Token usage is calculated according to these guidelines:

- When you use the FortiAI assistant, both the prompt (input) and the response (output) are processed as tokens.
- While there isn't a strict one-to-one link between words or characters and tokens, generally, more text in the query and response results in using more tokens.
- Because the FortiAI assistant relies on session history to generate responses, queries during a long session will consume more tokens than those in new conversations.

Consider the following two queries:

- Can you show me all the log entries for the endpoint 10.10.10.10?
- Show logs for 10.10.10.10 (past week).

The total number of tokens used in the examples above depends on both the input (prompt) and the output (response). The first prompt contains more text, so it will use more tokens in the input. It also generates a larger response from FortiAI because it requests all log entries instead of just limiting the response to logs from the past week. Therefore, the first prompt will also use more tokens in the output.

DO NOT REPRINT**© FORTINET**

Managing Monthly Tokens—Best Practices

- Make your prompts concise and specific—wordy queries use more text and therefore more tokens
 - Example: "Show recent logs for 10.10.10.10 (past week)" rather than "Can you show me all the log entries from endpoint 10.10.10.10 from the past week?"
- Use filters in your prompts to receive concise and specific responses
 - Include time ranges or specify limits for the number of results
- Use words that relate to FortiAnalyzer functions to specifically direct FortiAI
 - Example: "Apply filter", "Generate report", or "Generate script"
- Leverage predefined datasets, charts, reports, and event handlers whenever possible
- Include details in the existing thread whenever possible
 - Note that FortiAI does not retain previous threads
- Restart the FortiAI assistant after 10 conversations if you don't need to keep the historical context



© Fortinet Inc. All Rights Reserved.

9

When using FortiAI, your prompts should be directly related to the information the assistant is programmed to access, enabling efficient and effective data retrieval.

A valid prompt is a clear, well-defined question that the FortiAI assistant can easily interpret and process. It should be specific and relevant to the data or queries the FortiAI assistant is designed to handle. A valid prompt can be translated into precise SQL queries to retrieve accurate results on FortiAnalyzer.

An invalid prompt is one that cannot be easily interpreted or processed by the FortiAI assistant. This typically includes prompts that are ambiguous, lack sufficient detail, or are outside the scope of the FortiAI assistant's capabilities.

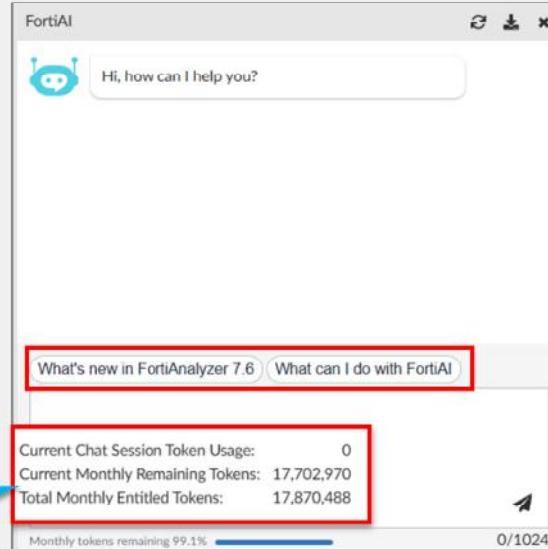
Restarting the FortiAI assistant and eliminating the historical context is important for conserving tokens, so you should do this unless you really need to reference the chat's historical context to continue processing.

DO NOT REPRINT**© FORTINET**

FortiAI Use Cases

- Perform incident investigation and response
- Perform threat hunting
- Interpret security events
- Generate detailed summaries
- Identify potential impacts and recommend remediation
- Simplify platform usage with natural language prompts
 - Create complex database queries, generate reports, write event handlers and correlation rules, and execute many other FortiAnalyzer functions during a typical workflow

Hover the mouse over **Monthly tokens remaining** to view information on the monthly token usage



FORTINET
Training Institute

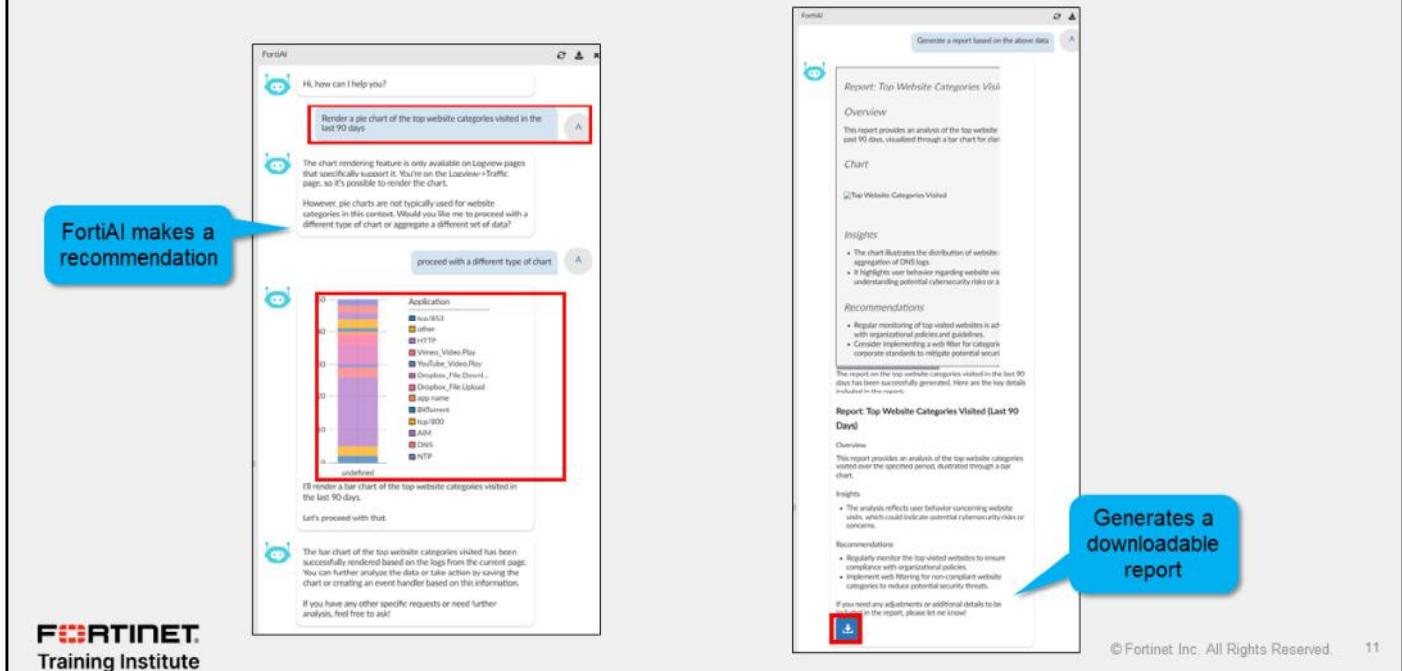
© Fortinet Inc. All Rights Reserved. 10

FortiAI can be used in FortiAnalyzer for incident investigation, response, and threat hunting. The assistant can interpret security events, generate detailed summaries, identify potential impacts, and make remediation recommendations.

FortiAI can also simplify platform usage with natural language prompts. For example, the assistant can create complex database queries, generate reports, write event handlers and correlation rules, and execute many other FortiAnalyzer functions during a typical workflow.

**DO NOT REPRINT
© FORTINET**

Use Case—Graphical Representation and Reporting

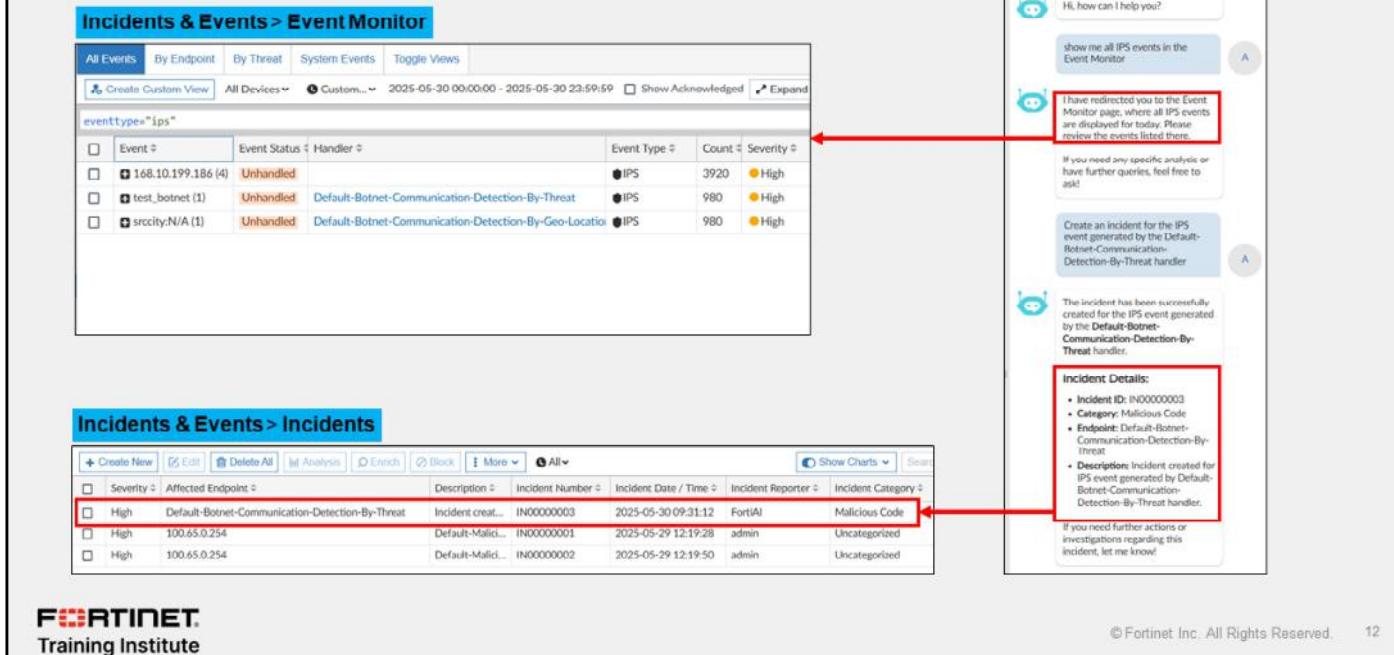


This slide shows how you can use FortiAI to generate a chart of the top website categories by application to make it easier to understand.

The image on the right shows how you can use FortiAI to generate a report based on the chart. FortiAI provides an action button to download the report.

DO NOT REPRINT
© FORTINET

Use Case—Threat Hunting



The screenshot illustrates the integration between FortiAnalyzer and FortiAI. On the left, the 'Incidents & Events > Event Monitor' page shows a list of events, with one specific event from the 'Default-Botnet-Communication-Detection-By-Threat' handler highlighted. A red arrow points from this event to the right-hand 'FortiAI' interface. The FortiAI window displays a chatbot interaction where the user asks to show all IPS events, and the bot responds by redirecting them to the Event Monitor page. Below this, another red arrow points from the event details in the FortiAnalyzer interface to a 'Incident Details' box in the FortiAI interface, which provides specific incident information.

Event #	Event Status	Handler	Event Type	Count	Severity
168.10.199.186 (4)	Unhandled		IPS	3920	High
test_botnet (1)	Unhandled	Default-Botnet-Communication-Detection-By-Threat	IPS	980	High
srccity:N/A (1)	Unhandled	Default-Botnet-Communication-Detection-By-Geo-Locatio	IPS	980	High

Affected Endpoint	Description	Incident Number	Incident Date / Time	Incident Reporter	Incident Category
Default-Botnet-Communication-Detection-By-Threat	Incident creat...	IN00000003	2025-05-30 09:31:12	FortiAI	Malicious Code
100.65.0.254	Default-Malici...	IN00000001	2025-05-29 12:19:28	admin	Uncategorized
100.65.0.254	Default-Malici...	IN00000002	2025-05-29 12:19:50	admin	Uncategorized

Incident Details:

- Incident ID: IN00000003
- Category: Malicious Code
- Endpoint: Default-Botnet-Communication-Detection-By-Threat
- Description: Incident created for IPS event generated by Default-Botnet-Communication-Detection-By-Threat handler.

This slide's example shows how you can use FortiAI to check for all intrusion prevention system (IPS) events generated in the event monitor. FortiAI redirects your FortiAnalyzer GUI page to the **Event Monitor** page.

Notice that the event handler **Default-Botnet-Communication-Detection-By-Threat** has generated an IPS event. This handler does not automatically create incidents when it generates an event, but you can ask FortiAI to create an incident based on this event.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which standard does FortiAI use when masking data for privacy and protection?
 A. RAG
 B. GDPR

2. What is the purpose of retrieval-augmented generation (RAG) in FortiAI functionality?
 A. Provides references to support FortiAI responses.
 B. Generates a warning prompt if sensitive data cannot be masked.

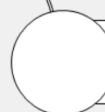
DO NOT REPRINT

© FORTINET

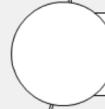
Lesson Progress



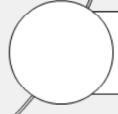
FortiAI



Threat Hunting



Troubleshooting



Automation Stitches

Good job! You now understand FortiAI.

Now, you will learn about FortiAnalyzer threat hunting.

DO NOT REPRINT**© FORTINET**

Threat Hunting and Outbreak Alerts

Objectives

- Describe threat hunting
- Use the log count chart
- Use the SIEM log analytics table
- Describe outbreak alerts



© Fortinet Inc. All Rights Reserved.

15

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

By understanding how to use the threat hunting and outbreak alert tools, you will be able to take a more proactive approach in your SOC duties and keep your FortiAnalyzer updated with the latest outbreak information provided by FortiGuard.

DO NOT REPRINT

© FORTINET

Threat Hunting

- Proactively search for suspicious or risky network activity that may have gone undetected
- The process usually begins with a question:
 - Is an advanced persistent threat currently active in our network?
- The reference to tactics, techniques, and procedures (TTPs), behaviors, and indicators helps narrow down to more specific questions
 - Frequently aligned with the MITRE ATT&CK or the Cyber Kill Chain frameworks
- Can also come in the form of an if-then statement, for example:
 - If you have DNS C&C in the network, then you should see abnormal DNS traffic
- A simplified example:



Threat hunting consists of proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach helps the analyst find any threats that might have eluded detection by the current security solutions or configurations.

The threat hunting process usually starts with a broad question, or hypothesis, that determines which type of threat you are trying to find. You can also start with an if-then statement. For example, if you have a DNS command and control attack in your network, then you should see abnormal DNS traffic.

The process is frequently aligned to the MITRE ATT&CK or Cyber Kill Chain frameworks. This allows you to narrow down to more specific questions. The Cyber Kill Chain framework establishes a seven-step process to understand how a cyberattack is conducted and what steps you can take to secure your network. You can find more information on the Cyber Kill Chain framework on the Lockheed Martin website.

The frameworks are not mutually exclusive: You can use both frameworks together to help analyze and protect your network.

DO NOT REPRINT

© FORTINET

Threat Hunting (Contd)

- The **Threat Hunting** window takes advantage of the security information and event management (SIEM) framework to allow advanced correlation and analysis to hunt for threats

Log View > Logs > Threat Hunting

#	Application Name	Count	Sent (bytes)	Average Sent	Max Sent (bytes)
1	[Redacted]	202,284(69%)	73.8 KB	185.0 B	517.0 B
2	DNS	87,799(30%)	7.4 MB	170.0 B	28.5 KB
3	HTTP.BROWSER	1,688(1%)	513.8 KB	548.0 B	6.7 KB
4	HTTP	937(< 1%)	1.7 MB	1.8 KB	27.8 KB
5	HTTPS	515(< 1%)	565.3 MB	1.1 MB	554.9 MB
6	HTTPS.BROWSER	390(< 1%)	301.8 KB	1.4 KB	3.3 KB
7	Dropbox_File.Download	132(< 1%)	217.8 KB	3.3 KB	3.8 KB
8	Blogger	52(< 1%)	27.7 KB	978.0 B	3.3 KB
9	udp/443	51(< 1%)	896.7 KB	17.6 KB	17.6 KB
10	Vimeo_Video.Play	44(< 1%)	31.1 KB	1.4 KB	2.3 KB
11	Dropbox_File.Upload	44(< 1%)	44.3 KB	2.0 KB	3.0 KB
12	Instazram	42(< 1%)	41.6 KB	1.7 KB	4.3 KB

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 17

FortiAnalyzer's **Threat Hunting** window offers a SOC analytics dashboard using the SIEM database.

Threat Hunting uses cached data to allow SOC analysts to quickly drill down on logs in fields of interest. To view the **Threat Hunting** dashboard, click **Threat Hunting**. This dashboard includes a **Log Count** chart and SIEM log analytics table.

To change the displayed time range, select a time from the drop-down field in the upper-left corner of the dashboard. You can configure custom time ranges by selecting either **Last N Minutes**, **Last N Hours**, or **Last N Days**. Apply filters to the dashboard using **Add Filter** or by right-clicking a value in the table and selecting the corresponding filter. The SIEM log analytics table displays only logs matching the selected time range and filter.

In the left pane, click the field for which you want to view the corresponding data. The table displays detailed statistics, including count (number of logs), percentage, sent bytes, and session duration information. Double-click an item in the table to view the detailed log information.

By examining the information on this tool, you may produce a specific hypothesis. For example, based on the image on this slide, the following questions may arise:

- Is the number of DNS logs for this time period expected?
- Is the amount of HTTPS data at this hour normal for your network?
- Should social media websites be allowed?
- Should cloud storage websites be allowed?

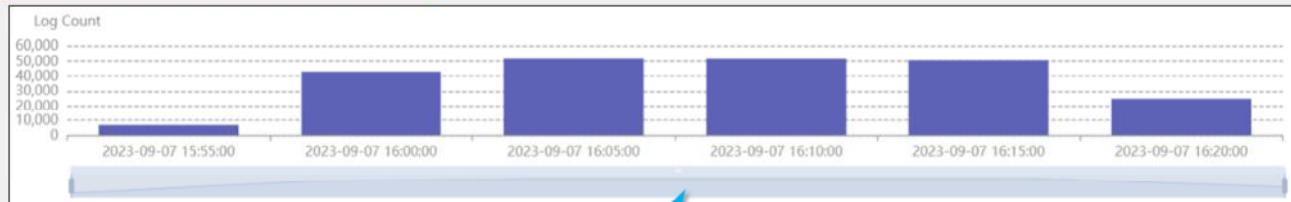
DO NOT REPRINT

© FORTINET

Log Count Chart

- The **Log Count** chart allows the administrators to narrow down which logs will be analyzed based on a time range
- The details in the SIEM log table adjust to the timeframe selected in this chart

Log View > Logs > Threat Hunting



Adjust the time bar
to include only a
specific time frame

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 18

The top of the **Threat Hunting** dashboard shows a chart displaying the total log count during the specified time range. This section is called the **Log Count** chart.

You can zoom in and out on the displayed time range by using your mouse's scroll wheel or by adjusting the time bar below the graph. You can adjust the time bar by dragging the start and stop bars on either side of the selected time range, or by clicking and dragging the entire time range to the left or right. For example, you could search for suspicious activity occurring outside business hours.

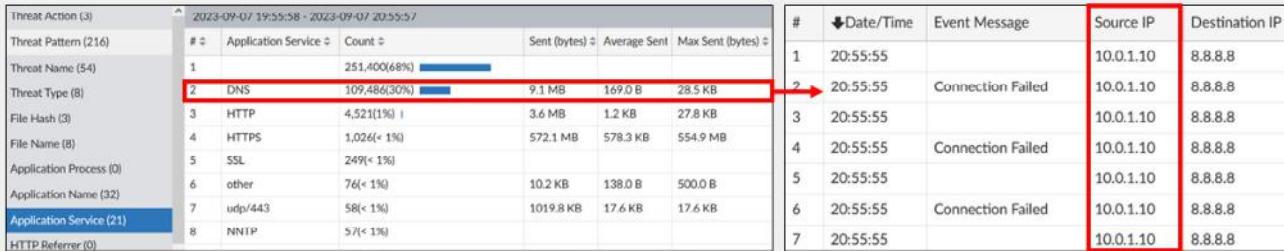
Only logs displayed within the time period visible in the chart appear in the SIEM log analytics table.

DO NOT REPRINT

© FORTINET

Threat Hunting Example With FortiAnalyzer

- Based on the MITRE ATT&CK tactic *Exfiltration*, technique *Exfiltration over alternative protocol*, establish the following hypothesis/question:
 - Has DNS tunneling been used to extract confidential data from the local network?*
- In this example, the analyst used the **Log Chart** to discover an unusual amount of DNS traffic
- Analysis shows the IP address 10.0.1.10 sending continuous queries at odd hours



The screenshot shows two tables side-by-side. The left table is a 'Threat Action' report for September 7, 2023, from 19:55:58 to 20:55:57. It lists threat patterns, names, types, file hashes, file names, application processes, application names, and service counts. The right table is a log chart showing DNS traffic from 10.0.1.10 to 8.8.8.8 at 20:55:55, with an arrow pointing from the DNS row in the first table to the second table.

Threat Action (3)	2023-09-07 19:55:58 - 2023-09-07 20:55:57					
Threat Pattern (216)	#	Application Service	Count	Sent (bytes)	Average Sent	Max Sent (bytes)
Threat Name (54)	1		251,400(6%)			
Threat Type (8)	2	DNS	109,486(30%)	9.1 MB	169.0 B	28.5 KB
File Hash (3)	3	HTTP	4,521(1%)	3.6 MB	1.2 KB	27.8 KB
File Name (8)	4	HTTPS	1,026(< 1%)	572.1 MB	578.3 KB	554.9 MB
Application Process (0)	5	SSL	249(< 1%)			
Application Name (32)	6	other	76(< 1%)	10.2 KB	138.0 B	500.0 B
Application Service (21)	7	udp/443	58(< 1%)	1019.8 KB	17.6 KB	17.6 KB
HTTP Referrer (0)	8	NNTP	57(< 1%)			

#	Date/Time	Event Message	Source IP	Destination IP
1	20:55:55		10.0.1.10	8.8.8.8
2	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
3	20:55:55		10.0.1.10	8.8.8.8
4	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
5	20:55:55		10.0.1.10	8.8.8.8
6	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
7	20:55:55		10.0.1.10	8.8.8.8

- Further investigation determined that the host had been compromised. A new incident was created, and the SOC responders started containment and eradication steps

Note: The images shown here do not represent a real attack. They are used only to illustrate the scenario described.

Training Institute

© Fortinet Inc. All Rights Reserved. 19

This slide illustrates an example of how an analyst can use FortiAnalyzer to perform a threat-hunting procedure.

Based on the MITRE ATT&CK framework, tactic *Exfiltration*, and technique *Exfiltration over alternative protocol*, the SOC team wants to answer the following question: *Has DNS tunneling been used to extract confidential data from the local network?*

Using the log chart, the analyst found that an unusual amount of DNS traffic was being generated, including outside normal business hours. By checking the details of the DNS logs, the analyst found that the host with IP address 10.0.1.10 was the main source for this abnormal traffic.

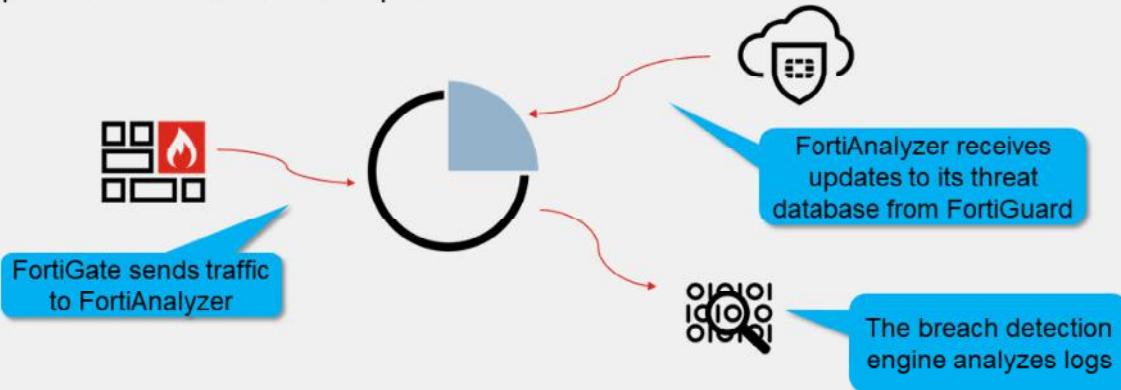
This triggered the creation of a new incident. The SOC team determined that the host had been compromised and proceeded to follow the steps in the company's security plan to contain and eradicate this breach.

DO NOT REPRINT

© FORTINET

IOCs (Compromised Hosts)

- The IOC engine detects end users with suspicious web usage compromises by checking new and historical logs against IOC signatures
- Uses FortiGuard threat intelligence to provide information about current threats
- Requires a FortiGuard subscription



The IOC engine detects end users with suspicious web usage compromises by checking new and historical logs against the IOC signatures, which are based on a FortiGuard subscription.

The IOC service on FortiAnalyzer uses the FortiGuard database to analyze web filtering, DNS, and traffic logs on FortiGate for breach detection. It is updated daily to reflect the real-world threat landscape. Note that antivirus logs, IPS logs, and similar logs aren't used because these threats have already been detected or prevented by these services on FortiGate. When FortiAnalyzer identifies a threat match, it assigns a threat score to the end user based on the overall ranking score. After the check is completed, FortiAnalyzer aggregates all the threat scores of an end user and provides its verdict on the overall IOC of the end user. The verdict can be one of the following:

- Infected:** Indicates a real breach. FortiAnalyzer found matches of the blacklisted IPs or domain generation algorithms (DGAs) in the web logs.
- Suspicious:** Indicates a possible breach with varying degrees of confidence.

DO NOT REPRINT**© FORTINET**

IOC Log Type and Data

- Depending on the log type, FortiAnalyzer identifies possible compromised hosts by checking the threat database against the log's IP address, domain, and URL
- This table shows which data in the logs FortiAnalyzer checks against the threat database:

Log type	Data
Attack logs	URLs, domains, and IP addresses
DNS	IP addresses
Email filter logs	URLs, domains, and IP addresses
Event logs	Threat type
Traffic logs	IP addresses
Web filter	URLs, domains, and IP addresses

Depending on the log type, FortiAnalyzer identifies possible compromised hosts by checking the threat database against the log's IP address, domain, and URL. The table on this slide displays which data in the logs FortiAnalyzer checks against the threat database.

The results for each affected end user are displayed in an IOC. You can drill down from the table to review the details of the affected host, including the detection pattern and detection method for each IOC. You can also drill down further from these detections to examine the logs where the matches were initially found in FortiAnalyzer.

DO NOT REPRINT

© FORTINET

IOC/Compromised Host Example

The screenshot shows the FortiView interface with the following details:

FortiView > Threats > Indicators of Compromise

Compromised Hosts

#	Source (User/IP)	Last Detected	Host Name	OS	Verdict	# of Threats	Acknowledge	Device Name	Device ID
1	10.0.3.20(10.0.3.20)	2023-08-18 13:19	10.0.3.20		Infected	3	Ack	ISFW	FGVM010000077646

Compromised Hosts > Blocklist

srclip = 10.0.3.20 | Add Filter

Summary

- Source (User/IP): 10.0.3.20(10.0.3.20)
- Last Detected: 2023-08-18 13:19
- Host Name: 10.0.3.20
- OS:
- Verdict: Infected
- Acknowledge:
- Device Name: ISFW
- Device ID: FGVM010000077646
- # of Threats: 3

Threat Details

#	Detect Pattern	Threat Type	Threat Name	Category	Detect Method	# of Events	Log Type	Security Actions	Scan Time
16	xn--13cgcicdbwb6ctd.com	Malware	CnC	Spyware and Malware infected-domain	infected-domain	1	webfilter	Details	2023-08-18 12:54:33
17	zinomp3.com	Malware	CnC	Pornography	infected-domain	1	webfilter	Details	2023-08-18 12:53:53
18	208.100.26.245	Malware	CnC	Spyware and Malware infected-ip	infected-ip	1	webfilter	Details	2023-08-18 13:09:43
19	52.86.6.113:80	Malware	CnC	Spyware and Malware infected-ip	infected-ip	1	webfilter	Details	2023-08-18 13:22:53
20	galvoice.net	Malware	CnC	Spyware and Malware infected-domain	infected-domain	1	webfilter	Details	2023-08-18 13:09:43
21	208.91.196.145	PUP	SpywareCnC		infected-ip	1	traffic	Details	2023-08-18 13:14:33
22	5.79.71.205	Malware	CnC	Spyware and Malware infected-ip	infected-ip	1	traffic	Details	2023-08-18 13:18:43
23	85.17.31.122	Malware	CnC	Spyware and Malware infected-ip	infected-ip	1	traffic	Details	2023-08-18 12:53:53
24	91.195.240.123:80	Malware	CnC	Spyware and Malware infected-ip	infected-ip	1	traffic	Details	2023-08-18 13:23:53
25	56834764387462384.org	Malware	Sinkhole	Not Rated	infected-domain	1	webfilter	Details	2023-08-18 13:08:03

Annotations:

- A red box highlights the "Verdict" column for the first row, which is "Infected". A blue callout bubble says: "A real breach was detected, with three different threats. This entry has not yet been acknowledged".
- A red arrow points from the "Blocklist" link in the navigation bar to the "Blocklist" section below.
- A blue callout bubble says: "Displays blocklist detection method used by the IOC".

FOURINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

This slide presents an example of an IOC hit in FortiView. The IOC engine has confirmed a genuine breach, as indicated by the **Infected** verdict. The **# of Threats** column shows that three distinct threats are associated with this hit.

On the IOC FortiView, you can also:

- Filter the entries by specifying devices or a time period.
- Acknowledge the IOC by clicking **Ack** in the **Acknowledge** column. By default, you can view acknowledged IOCs, unless you configure the system not to show them. You can add a short comment when acknowledging an entry.
- Double-click an entry to drill down and view threat details.

When you double-click an entry, more details are displayed, and you can filter the view based on two categories:

- Blocklist, which indicates items marked as infected after checking the blocklist included in the IOC database downloaded from FortiGuard. You can verify that this traffic was blocked by clicking **Details** under the **Security Actions** column. If you believe that the IP address or domain listed under the **Detect Pattern** column is valid, you can report it as misrated by clicking on that entry.
- Suspicious (not shown on this slide), which indicates a match was found in the suspicious list included in the IOC database downloaded from FortiGuard. In this case, FortiAnalyzer flags the endpoint for further analysis, compares the flagged log entries with the endpoint's previous statistics for the same day, and then updates the score. If the score exceeds the threshold, that endpoint is listed or updated in **Compromised Hosts**.

DO NOT REPRINT

© FORTINET

MITRE ATT&CK Framework Matrices

- Consist of cybersecurity tactics and techniques organized into matrices

Incidents & Events > Incidents > MITRE ATT&CK® > Attack

Reconnaissance	Resource Development	Initial Access
10 techniques	8 techniques	9 techniques
Active Scanning Covered	Acquire Access	Drive-by Compromise
Gather Victim Host Information Covered	Acquire Infrastructure Covered	Exploit Public-Facing Application Covered
Gather Victim Identity Information	Compromise Accounts	External Remote Services
Gather Victim Network Information	Compromise Infrastructure 9	Hardware Additions

The column headers are the tactics

The tiles under the columns are the techniques

Click a tile to see associated incidents and events

Incidents & Events > Incidents > MITRE ATT&CK® > Coverage

110 Event Handlers - 41% Coverage		
Reconnaissance	Resource Development	Initial Access
10 techniques	8 techniques	9 techniques
Active Scanning 3	Acquire Access	Drive-by Compromise
Gather Victim Host Information 1	Acquire Infrastructure 1	Exploit Public-Facing Application 3
Gather Victim Identity Information	Compromise Accounts	External Remote Services
Gather Victim Network Information	Compromise Infrastructure 8	Develop

Click a tile to see which event handlers have coverage against the technique

Note: Not all tactics and techniques are shown

© Fortinet Inc. All Rights Reserved. 23

The **MITRE ATT&CK®** and **MITRE ATT&CK® ICS** panes are based on the MITRE ATT&CK framework matrices. The MITRE ATT&CK framework provides a vast knowledge base of information about cybersecurity threats, including classifications, descriptions of attack vectors, real-life examples, mitigation steps, detection methodology, and so on. You can find more information about the framework on the MITRE website.

The column headers are the tactics in the matrices. They describe the adversary's objective for using techniques on your network, such as performing reconnaissance.

The tiles under the columns are the techniques in the matrices. They describe how an adversary can achieve their objective on your network, such as using active scanning to perform reconnaissance.

You can review the incidents and events associated with a technique, including their severity, information on the technique and subtechnique, affected endpoints, and the total number of incidents and events. For example, the **Compromise Infrastructure** tile has nine associated events.

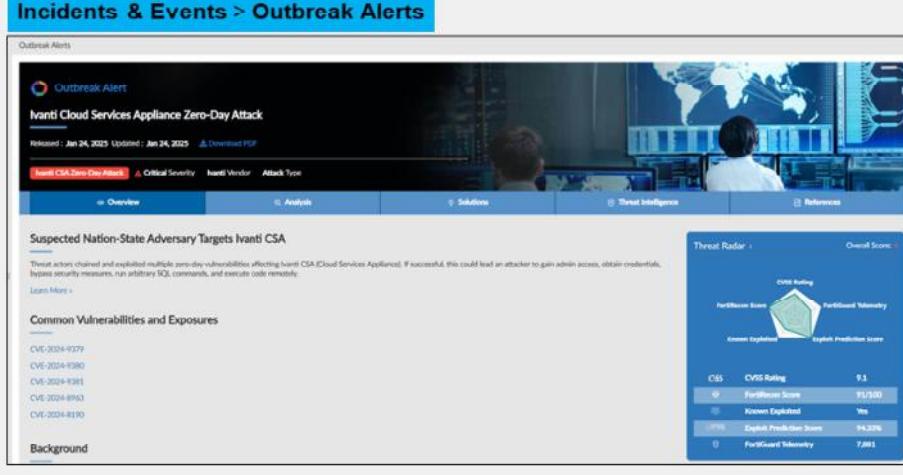
You can review event handler coverage in the **Coverage** window. It displays the number of event handlers and the percentage of coverage the FortiAnalyzer device has against attacks in the matrices. The number on each tile shows how many event handlers are associated with the technique. For example, the **Compromise Infrastructure** tile has eight associated event handlers. You can click a tile to view a list of event handlers related to the specific technique.

To leverage the **MITRE ATT&CK® ICS** matrix, which is not depicted on this slide, the OT Security Service license is required on FortiAnalyzer.

DO NOT REPRINT
© FORTINET

Outbreak Detection Service Overview

- Licensed feature
- Allows customers to receive information about malware outbreaks
- Automatically downloads new event handlers and reports related to the outbreaks



The screenshot shows the FortiAnalyzer interface with the title "Incidents & Events > Outbreak Alerts". A specific alert is highlighted: "Ianti Cloud Services Appliance Zero-Day Attack" (Revised: Jan 24, 2025, Updated: Jan 24, 2025). The alert details include "Critical Severity", "Ianti Vendor", and "Attack Type". Below the alert, there's a "Suspected Nation-State Adversary Targets Ianti CSA" section with a note about exploiting multiple zero-day vulnerabilities. A "Threat Radar" chart displays scores for CVSS Rating, FortiAnalyzer Score, and FortGuard Velocity. A table provides detailed threat metrics:

CID	CVSS Rating	Overall Score
1	FortiAnalyzer Score	91/100
2	Known Exploited	Yes
3	Exploit Prediction Score	94.22%
4	FortGuard Velocity	7.001

At the bottom left is the "FORTINET Training Institute" logo, and at the bottom right is the copyright notice "© Fortinet Inc. All Rights Reserved. 24".

The FortiAnalyzer Outbreak Detection Service is a licensed feature that allows FortiAnalyzer administrators to receive and view outbreak alerts and automatically download related event handlers and reports from FortiGuard. Outbreak event handlers and reports are created in real time by Fortinet to detect and respond to emerging outbreaks.

The **Outbreak Alerts** pane displays alerts from Fortinet, which are available on all ADOMs.

DO NOT REPRINT
© FORTINET

Outbreak Alert Handlers and Reports

	Status	Name
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Outbreak Alert - Microsoft Outlook Elevator
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Outbreak Alert - MSDT DogWalk Vulnerability
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Outbreak Alert - Log4j2 Vulnerability Event

- New event handlers are added to the list of available handlers, and you can use them in the same way as the others

Event handlers
downloaded
through the
outbreak alerts
service

	Title
<input type="checkbox"/>	Outbreak Alert - Atlassian Information Disclosure Report
<input type="checkbox"/>	Outbreak Alert - BURNTCIGAR Malware Report
<input type="checkbox"/>	Outbreak Alert - Cacti Command Injection Report
<input type="checkbox"/>	Outbreak Alert - CISAtop20_PRC2022 Report
<input type="checkbox"/>	Outbreak Alert - CosmicEnergy Malware Report
<input type="checkbox"/>	Outbreak Alert - CWP OS Command Injection Report

- The same is true for the newly downloaded reports

Reports
downloaded
through the
outbreak alerts
service

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved. 25

Once downloaded, the new handlers are available in the **Event Handler** list, and you can use them in the same ways described in an earlier section. That is, you can clone, export, import them, and so on.

The same is true for the new reports.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which feature allows the automatic download of new event handlers?
 A. Threat-hunting SIEM table
 B. Outbreak detection service

DO NOT REPRINT

© FORTINET

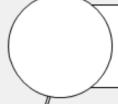
Lesson Progress



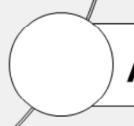
FortiAI



Threat Hunting



Troubleshooting



Automation Stitches

Good job! You now understand threat hunting.

Now, you will learn how to troubleshoot logging issues on FortiAnalyzer.

DO NOT REPRINT**© FORTINET**

Troubleshooting and Managing Logs

Objectives

- Collect log volume statistics



© Fortinet Inc. All Rights Reserved. 28

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

By demonstrating competence in collecting log statistics, you will be able to identify issues that may affect the performance of FortiAnalyzer.

DO NOT REPRINT
© FORTINET

Gathering Log Rate and Device Usage Statistics

- Use the following FortiAnalyzer CLI commands to troubleshoot logging issues

What to investigate	CLI command to use
What is the log receive rate for each second?	# diagnose fortilogd lograte
What are the log receive rate totals?	# diagnose fortilogd lograte-total
What is the device log rate?	# diagnose fortilogd lograte-device
What is the log rate for each log type?	# diagnose fortilogd lograte-type
What is the message receive rate for each second?	# diagnose fortilogd msgrate
What is the SQL insertion status?	# diagnose sql status sqlplugind
What is the device log usage for all logging devices?	# diagnose log device

- Example

```
FAZVM64-KVM # diagnose fortilogd lograte
last 5 seconds: 0.6, last 30 seconds: 2.2, last 60 seconds: 1.7
FAZVM64-KVM # diagnose fortilogd msgrate
last 5 seconds: 0.2, last 30 seconds: 0.4, last 60 seconds: 0.4
```

Difference between log rate and message rate: one log message can consist of multiple logs in LZ4 format

© Fortinet Inc. All Rights Reserved.

29

FORTINET
 Training Institute

To understand the log volume and whether your disk quota is configured appropriately, you can use the CLI commands shown on this slide to gather log rate and device usage statistics.

For example, if your log volume is too high, you won't be able to retain your analytics logs or archive logs for the amount of time configured in the ADOM.

DO NOT REPRINT

© FORTINET

Gathering Log Rate and Log Volume per ADOM

- Use the following FortiAnalyzer CLI commands to calculate log rate and log volume per ADOM

What to investigate	CLI command to use
Log receive rate for all ADOMs or a specific ADOM?	# diagnose fortilogd lograte-adom {all adom-name}
Log volume for all ADOMs or a specific ADOM?	# diagnose fortilogd logvol-adom {all adom-name}

- Example

```
FAZVM64-KVM # diagnose fortilogd logvol-adom root
2025-04-22 2025-04-21 2025-04-20 2025-04-19 2025-04-18 2025-04-17 2025-04-16 average
adom 'root':
8.77 MB   10.15 MB   15.65 MB   17.68 MB   22.89 MB   22.64 MB   22.71 MB   17.21 MB
```

Volume of the last seven days and the average volume for the root ADOM

To understand the log rate and log volume per ADOM, you can use the CLI commands shown on this slide to gather log rate and volume statistics. This is very useful in environments where the FortiAnalyzer administrator is using multiple ADOMs to manage multiple FortiGate devices, like managed security service providers (MSSPs).

DO NOT REPRINT

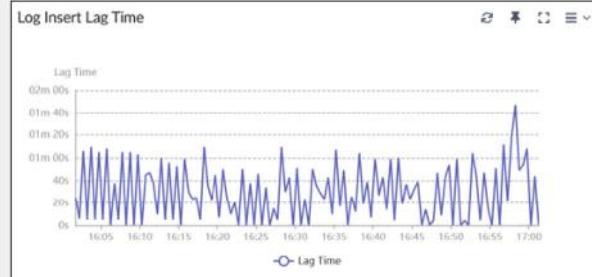
© FORTINET

Insert Rate vs. Receive Rate and Log Insert Lag

- **Insert Rate vs. Receive rate**

- Insert rate = SQL insertion rate
 - Handled by sqlplugind
- Receive rate = Raw receiving rate
 - Handled by fortilogd

Dashboard > Widgets



You can view log insert rate, receive rate, and log insert lag time using the respective dashboard widgets. If these widgets are not already on the dashboard, you can add them by clicking **Toggle Widgets** in the upper-left corner and selecting the widgets from the list.

Insert Rate vs Receive Rate is a graph that shows the rate at which raw logs reach FortiAnalyzer (receive rate) and the rate at which they are indexed (insert rate) by the SQL database and the sqlplugind daemon (insert rate). The difference between these parameters should usually be consistent. Ideally, it should be as small as possible, but variations during the day can be expected. Create a baseline during normal operation and compare it to verify performance.

Log Insert Lag Time shows the amount of time between when a log was received and when it was indexed. Ideally, this parameter should be as small as possible, with only occasional spikes, according to the network activity being logged. You should create a good baseline to help with the identification of possible performance issues. Similarly, the lag time should be as small as possible, and variations during the day can be expected.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which data does the CLI command # diagnose fortilogd lograte provide?
 A. The log receive rate per second
 B. The message receive rate per second

2. Which FortiAnalyzer process handles the insert rate?
 A. fortilogd
 B. sqlplugind

DO NOT REPRINT

© FORTINET

Lesson Progress



FortiAI



Threat Hunting



Troubleshooting



Automation Stitches

Good job! You now know how to troubleshoot logging issues on FortiAnalyzer.

Now, you will learn about automation stitches on FortiAnalyzer.

DO NOT REPRINT**© FORTINET**

Automation Stitches

Objectives

- Describe FortiAnalyzer and FortiGate automation stitches
- Configure an automation stitch
- Configure an event handler with an automation stitch enabled

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

By demonstrating competence in understanding the purpose of playbooks and their components, you will be able to configure automation stitches between FortiAnalyzer and FortiGate.

DO NOT REPRINT
© FORTINET

FortiAnalyzer and FortiGate Automation Stitch

- FortiAnalyzer can activate an automation stitch on authorized FortiGate devices
- An event handler must have the automation stitch option enabled
 - This allows FortiGate to detect the event handler from a list of potential triggers

The image shows two screenshots illustrating the integration between FortiAnalyzer and FortiGate.

FortiAnalyzer Event Handler: A configuration screen for an event handler named "Default-Botnet-Communication-Detection". It includes fields for Name, Description, MITRE Tech ID (T1584.005 Botnet), Data Selector, and Automation Stitch (which is checked). The Automation Stitch field is highlighted with a red box.

FortiGate Automation Trigger: A screenshot showing the "FortiAnalyzer Event Handler" trigger in the FortiGate interface. It lists the triggered event ("A specified FortiAnalyzer event handler was triggered") and its details. The event handler name is "Default-Botnet-Communication-Detection". Under "Event tag", it shows "FortiAnalyzer (2)" and lists two automation stitches: "Default-Botnet-Communication-Detection" and "Default-FFW-Botnet-Communication-Detect", both of which are highlighted with red boxes.

FORTINET Training Institute is visible at the bottom left, and the copyright notice "© Fortinet Inc. All Rights Reserved. 35" is at the bottom right.

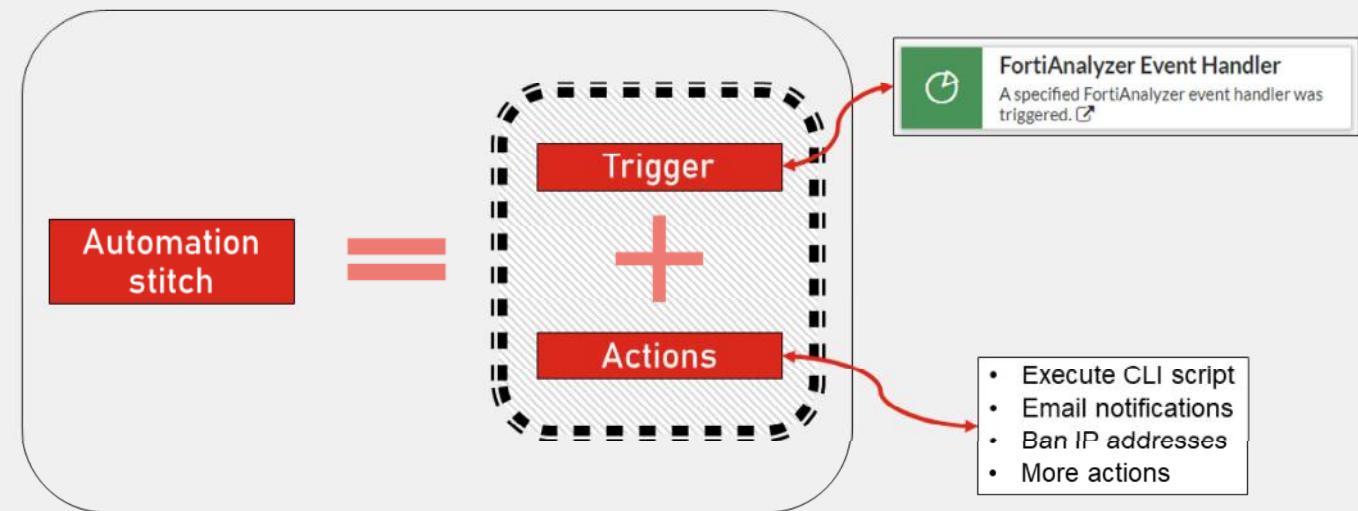
When a handler with automation stitch enabled generates an event, FortiAnalyzer sends a notification to the FortiGate automation framework. If an automation stitch is configured on FortiGate, the notification triggers the related automation stitch and activates an action in response. For example, FortiGate could send a custom email notification, execute a CLI script, and perform a system action in response to the trigger.

By default, two basic event handlers, Default-Botnet-Communication-Detection and Default-FFW-Botnet-Communication-Detection, have an automation stitch enabled.

You can also enable automation stitches for any custom event handler.

DO NOT REPRINT
© FORTINET

FortiAnalyzer and FortiGate Automation Stitch (Contd)



An automation stitch consists of two parts: the trigger and the action. The trigger is the condition or event that activates the action, such as a FortiAnalyzer event handler that generates an event. The action is what FortiGate does in response to the trigger. Automation stitches are configured on the Security Fabric root FortiGate.

While FortiGate can run automation stitches without having FortiAnalyzer in the topology, the advantages of having FortiAnalyzer in the workflow include:

- Scalability: The configured event handlers can apply to all authorized FortiGate devices, or you can use data selectors to narrow the selection.
- Granularity: You have finer control over which logs generate an event.
- Centralized SOC view: You can create events and incidents on FortiAnalyzer in addition to using its event correlation and reporting capabilities.
- Playbooks: You can perform more actions on FortiAnalyzer, such as automatically creating an incident if an event matches your conditions.

Many other types of triggers are available on FortiGate. However, this course focuses only on FortiAnalyzer event handlers as the automation trigger.

DO NOT REPRINT

© FORTINET

FortiAnalyzer and FortiGate Automation Stitch (Contd)

- This example automation stitch bans an IP address on FortiGate if the web filter violation category description matches social networking
- These images show the FortiAnalyzer configuration

The screenshot shows two side-by-side configurations. On the left is the 'Event Handler' configuration for FortiAnalyzer, and on the right is the 'Event Handler Rule' configuration for FortiGate.

Event Handler (Left):

- Status: Enabled (green)
- Name: Web Filter IP Ban (highlighted with a red box)
- Description: (empty)
- MITRE Tech ID: (empty)
- Data Selector: (empty)
- Automation Stitch: Enabled (green)

Event Handler Rule (Right):

- Log Device Type: FortiGate
- Log Type: Web Filter (webfilter)
- Description: The system will categorize logs into smaller groups based on the chosen log fields.
- Log Field: Destination IP (dstip) (highlighted with a red box)
- Refine Your Logs: Not in use
- Description: Once logs are grouped, you can refine the data within each group by applying filter with retained within each group.
- Log Filters: All Filters (highlighted with a red box), Any One of the Filters (selected)
 - Log Field: Match Criteria
 - Log Filter by Text: catdesc='Social Networking' (highlighted with a red box)

FOURINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

The example on this slide illustrates the configuration of an automation stitch integration with FortiGate. This automation stitch triggers an IP address ban for the source computer on the FortiGate device where the security event occurs. If the FortiGate is part of a Security Fabric, you can select which devices within the Security Fabric will activate the stitch.

First, you must create an event handler and enable the automation stitch option. You must then define a rule for that event handler that specifies which logs generate an event. In this case, the generic text filter specifies the category description as social networking. If you are unsure about the log field, you can generate a log event and then view the raw logs under **Log View** to see the names of the field and the associated properties.

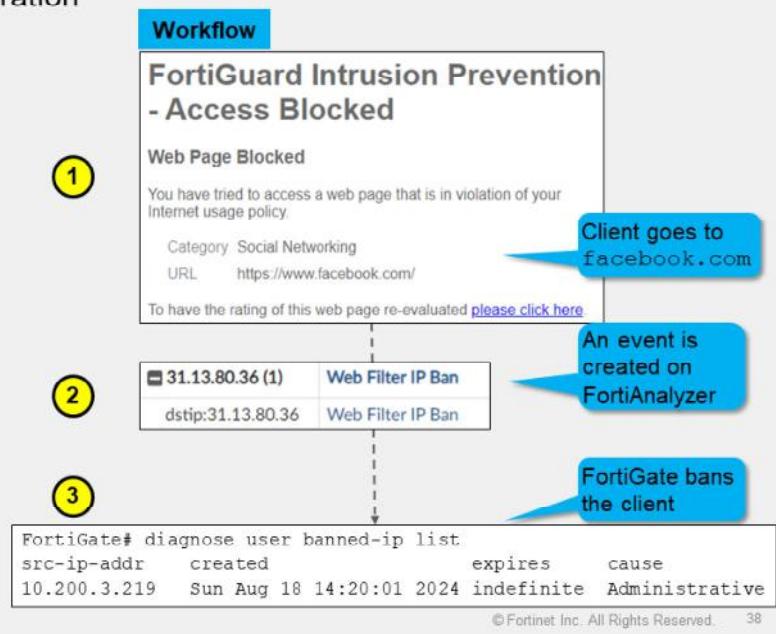
DO NOT REPRINT

© FORTINET

FortiAnalyzer and FortiGate Automation Stitch (Contd)

- This slide shows the FortiGate configuration

The screenshot shows the 'Automation Stitch' configuration on FortiGate. It includes fields for Name (Web Filter Social Networking Block), Status (Enable), FortiGate(s) (All FortiGates), Action execution (Sequential), and Description (0/255). The 'Stitch' section shows a flow from a 'Trigger' (Web Filter IP Ban Trigger) to an 'Action' (IP Ban). A red box highlights the 'Trigger' and 'Action' components.



On FortiGate, you must create a trigger that references the created event handler. Next, you must specify the action or actions that you want to occur when the trigger happens. Finally, you must create the automation stitch by combining the trigger and action. In the example shown on this slide, the IP Ban action is a default action in FortiOS.

If an automation stitch contains more than one action, FortiGate can perform them in sequence or in parallel. In sequential execution, actions execute one after another, with an optional delay between each action. However, if any action in the chain fails, the entire chain stops. In parallel execution, all actions execute simultaneously when the automation stitch is triggered. Note that in parallel execution, log action parameters (such as %%log%% or %%results%%) cannot be used because there is no subsequent action to pass this information to. In the example shown on this slide, since there is only one action, the sequential or parallel setting has the same effect.

In the example shown on this slide, the following workflow occurs:

- The client with the IP address of 10.200.3.219 tries to access facebook.com, and FortiGate blocks it because of a web filter violation.
- On FortiAnalyzer, the **Web Filter IP Ban** event handler is triggered. This event handler has the automation stitch option enabled.
- On FortiGate, an automation stitch has that event handler configured as a trigger, and one configured action to ban the offending client. As a result, you can see that the device is banned indefinitely.

Note that, unlike the FortiClient EMS quarantine depicted earlier, which is a host-level block, this configuration is blocking at a network level. This means that the host is banned only for traffic traversing FortiGate. In contrast, the host-level block restricts all network activity on the compromised host.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. How many triggers and actions can each automation stitch support?
 - A. One trigger and one action
 - B. One trigger and multiple actions

DO NOT REPRINT

© FORTINET

Lesson Progress



FortiAI



Threat Hunting



Troubleshooting



Automation Stitches

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe FortiAI operations and use cases
- ✓ Describe threat hunting
- ✓ Use the log count chart
- ✓ Use the SIEM log analytics table
- ✓ Describe outbreak alerts
- ✓ Collect log volume statistics
- ✓ Configure an automation stitch
- ✓ Configure an event handler with an automation stitch enabled

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

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiAnalyzer Analyst

Reports

 FortiAnalyzer 7.6

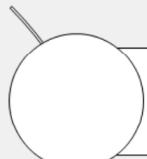
Last Modified: 16 July 2025

In this lesson, you will learn how to extract useful information from your logs for analysis purposes. You will also learn how data is formatted, stored, and organized in the database, and how to use the FortiAnalyzer reporting feature to view captured data for forensics and compliance.

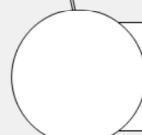
DO NOT REPRINT

© FORTINET

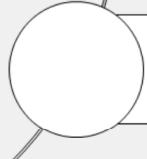
Lesson Progress



Report Concepts



Reports, Charts, and Datasets



Managing and Troubleshooting Reports

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

DO NOT REPRINT

© FORTINET

Report Concepts

Objectives

- Describe the elements that constitute a report
- Describe how charts extract data from the database
- Describe how reports function within ADOMs

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

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

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 Definitions > All Reports

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

Default reports categories

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

Note that reports generally do not provide 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

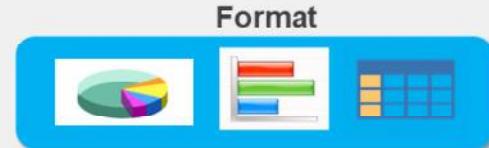


Charts define:

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



Datasets are specific SQL SELECT queries



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

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

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

DO NOT REPRINT

© FORTINET

How Do Charts Extract Data From the Database?

- Data populates a chart
- Datasets are SQL SELECT queries used to extract data from the database
- SELECT statements are read-only

The screenshot shows two windows side-by-side. The left window is titled 'Chart' and contains fields for 'Name' (Top 5 Attacks by Severity), 'Description' (Top 5 attacks by severity), and 'Dataset' (set to 'threat-Attacks-By-Severity'). A red box highlights the 'Dataset' field. The right window is titled 'Reports > Report Definitions > Dataset' and shows a dataset named 'threat-Attacks-By-Severity' with 'Intrusion Prevention' as the log type. A red box highlights the 'Query' field. Below it, the actual SQL query is displayed:

```

1 select (case when severity='critical' then
'Critical' when severity='high' then 'High' when
severity='medium' then 'Medium' when severity='low'
then 'Low' when severity='info' then 'Info' end) as
severity, count(*) as totalnum from $log where
$filter group by severity order by totalnum desc

```

To populate a chart with specific log data that has been collected, stored, and sorted in the SQL database, reports rely on a dataset query to extract that log data. A dataset is a specific SQL SELECT query—a read-only statement that retrieves data from the database.

The SELECT statement is the first word used in a query—it is the declarative verb describing what you want done—and is followed by the column(s) from which you want to extract information. You can extract all entries, or you can use clauses to make the query more specific.

In the example on this slide, the **Top 5 Attacks by Severity** chart contains a dataset named **threat-Attacks-By-Severity**.

The dataset uses a SQL SELECT query to:

- Find intrusion prevention logs.
- Group logs with the same severity levels.
- Tally the total number of logs for each level.
- Sort each level in descending order.

DO NOT REPRINT**© FORTINET**

SELECT Statement

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

Clause	Definition
FROM	From which table(s) or view(s) the data is extracted
WHERE	Sets the conditions (rows that do not satisfy the condition are not shown in the output)
GROUP BY	Collects data across multiple records, and groups the results by one or more columns
ORDER BY	Orders the results by specific column(s): ascending or descending
LIMIT	Limits the number of records returned based on a limit value
OFFSET	Often used with the LIMIT clause to offset the results by a set value

Note: Clauses must be coded in a specific sequence

- For more information, see the supplementary *FortiAnalyzer SQL and Datasets* lesson

To extract the desired data, you must specify the criteria to be used. To put this criteria into a language that SQL understands, you must use one or more clauses recognized by the `SELECT` statement.

The main clauses FortiAnalyzer reports use are as follows:

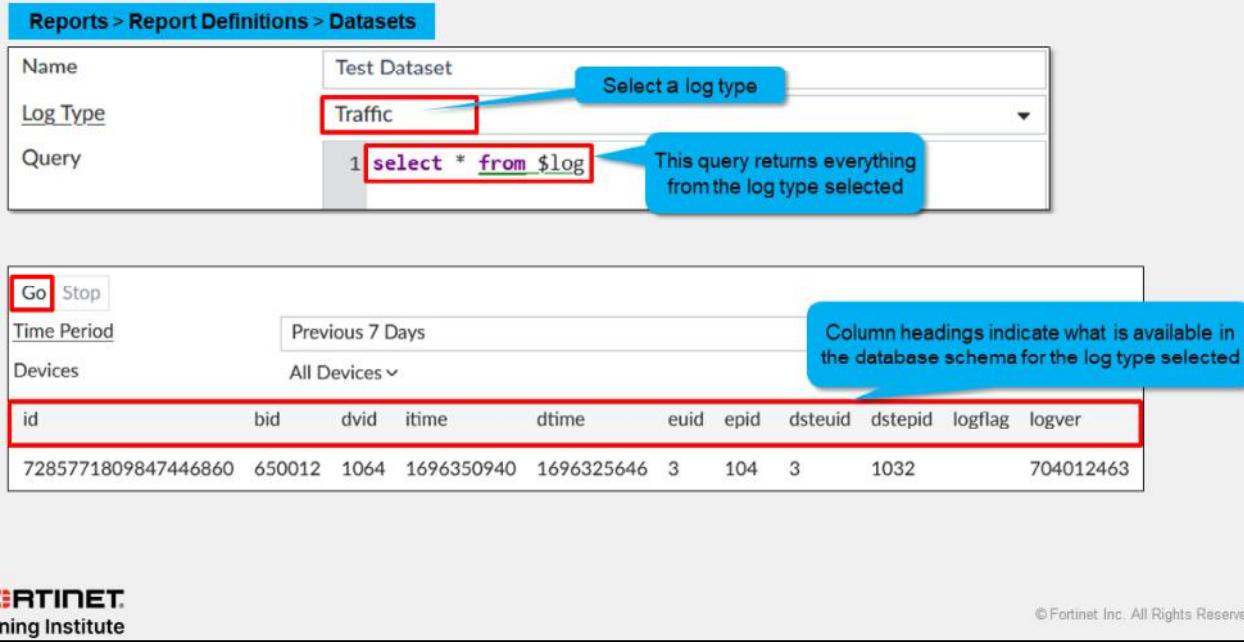
- `FROM`, which specifies from which table(s) or view(s) the data is extracted.
- `WHERE`, which specifies the conditions. All rows that don't satisfy the condition are not shown in the output.
- `GROUP BY`, which collects data across multiple records and groups the results by one or more columns.
- `ORDER BY`, which orders the results by specific column(s). If `ORDER BY` is not given, the records are returned in whatever order the system finds the fastest to produce.
- `LIMIT`, which limits the number of records returned based on a specified value.
- `OFFSET`, which is a clause often used along with `LIMIT`, to offset 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. Accordingly, following the `SELECT` keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide. For example, you can't use the `WHERE` clause before the `FROM` clause. You don't have to use all optional clauses, but whichever ones you do use must be in the correct sequence.

For more information about SQL and datasets for use with FortiAnalyzer reports, see the supplementary *FortiAnalyzer SQL and Datasets* lesson.

DO NOT REPRINT
© FORTINET

Accessing the SQL Schema



The screenshot shows the FortiAnalyzer interface for creating a dataset. In the 'Name' field, 'Test Dataset' is entered. In the 'Log Type' dropdown, 'Traffic' is selected. Below, in the 'Query' field, the SQL command `1 select * from $log` is typed. A blue callout box points to this query with the text: 'This query returns everything from the log type selected'. At the bottom, there's a table of log schema information with columns: id, bid, dvid, itime, dtime, euid, epid, dsteuid, dstepid, logflag, and logver. The first row of data is shown: 7285771809847446860, 650012, 1064, 1696350940, 1696325646, 3, 104, 3, 1032, 704012463. Above the table, 'Go' and 'Stop' buttons are visible, along with 'Time Period' set to 'Previous 7 Days' and 'Devices' set to 'All Devices'. A blue callout box points to the column headings with the text: 'Column headings indicate what is available in the database schema for the log type selected'.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 8

To create a query, you first need to know what is included in the database schema. The schema is the different fields or columns that are available from which you can extract information for reports. On FortiAnalyzer, you can obtain the schema for a specific log type by creating and testing the following dataset query:

```
SELECT * FROM $log
```

This query can be read as: "Select everything from the logs table."

For traffic logs, for example, associate the **Traffic** log type with this dataset in the **Log Type** field. This query returns everything from the **Traffic** log type. The column heading names indicate what is available in the database schema for the log type selected. The * symbol returns all data. Note that not all column headings are shown in the example on this slide.

After you type the query in the **Query** field, click **Go** to run the query.

DO NOT REPRINT
© FORTINET

Accessing the SQL Schema (Contd)

Name	Test Dataset
Log Type	Traffic
Query	<code>1 select * from \$log</code>

Hover your mouse over
the hyperlink to display the
schema

These are all the
available fields you can
use for queries

Table "Logs" has the following fields:

```

id, bid, dvid, itime, dtime, euid, epid, dsteuid, dstepid, logflag, logver,
sfsid, type, subtype, level, action, utmaction, policyid, sessionid, srchip,
dstip, transip, transip, srccport, dstport, transport, transport, transdisp,
duration, proto, vrf, slot, sentbyte, rcvdbyte, sentdelta, rcvddelta,
sentpkt, rcvdpkt, logid, user, unauthuser, dstunauthuser, srccname, dstname,
group, service, app, appcat, fctuid, srcintfrole, dstintfrole, srccserver,
dstserver, appid, appact, apprisk, wanoptapptype, polictype, centralnatid,
channel, wuplanid, shapingpolicyid, avantime, valid, shaperdropsanhyte,
shaperdroprcvdbyte, shaperperipdropbyte, wanin, wanout, lanin, lanout,
crscore, craction, clevel, countapp, countav, countdp, countemail,
countips, countweb, countwaf, countssl, countssh, countdns, srccuid, dstuid,
poluid, srccmac, masterdstmac, dstmac, masterdstvendor, srchinvendor,
srchinversion, srccfamily, srccversion, dsthwvendor, dsthvversion, dstfamily,
dstswversion, devtype, devcategory, dstdevtype, dstdevcategory, osname,
osversion, datosname, datosversion, srccountry, srccssid, dstssid,
srcintf, dstintf, srccintf, dstintfsv, unauthusersource,
dstunauthusersource, authserver, applist, vpn, vpntype, radioband,
policyname, policymode, ssaction, url, agent, comment, ap, apsn, vulservice,
vulquality, collectedemail, dstcollectedemail, shapersentname,
shaperrcvdname, shaperperipname, msg, custom_field1, utmevent, utmsubtype,
sender, recipient, virus, attack, hostname, catdesc, dipsensor, utmref,
tdinfoid, dstowner, tdtype, tdscantime, tdtreattype, tdtreatname, tdmfcate,
threatugts, threatcnts, threatlvs, saasinfo, ebtime, clouduser, threats,
threattyps, apps, countff, identifier, securityid, securityact, tz,
srccdomain, counticap, dtregion, srcregion, dstcity, srccity, signal, snr,
dstauthserver, dstgroup, dstuser, tunneld, vulname, srcthreatfeed,
dstthreatfeed, psrccport, pdstport, countcptf, srcreputation, dstreputation,
vip, accessproxy, gatewayid, clientdeviceid, clientdeviceowner,
clientdevicetags, httpmethod, referralurl, saasname, srccmacvendor,
shapingpolicyname, accessctrl, countcifs, proxyapptype,
clientdevice manageable, emsconnection, realserverid, fudsrv, replydstintf,
repliesrcintf, countvpatch, countcasb, devid, vd, devname, csf, devgrps

```

© Fortinet Inc. All Rights Reserved.

9

FORTINET
Training Institute

You can hover your mouse over the hyperlink in the query to open a window that displays all the available fields for that table.

As this slide shows, the number of fields can be very large. For this reason, cloning and editing one of the predefined datasets may be the best approach, if none of them meet your requirements.

DO NOT REPRINT

© FORTINET

Accessing the SQL Schema (Contd)

- srcip and srcport chosen from the schema

Table "Logs" has the following fields:
sfsid, type, subtype, level, action, utmaction, policyid, sessionid, srcip,
dstip, tranip, transip, srcport, dstport, tranport, transport, trandisp,

- Sample query using srcip and srcport

```
1 select srcip as "Source IP", srcport as "Source Port"  
2 from $log  
3 where $filter and srcip = '10.0.1.10'  
4 group by srcip, srcport  
5 order by srcport desc
```

- Results

Source IP	Source Port
10.0.1.10	60999
10.0.1.10	60998
10.0.1.10	60993

© Fortinet Inc. All Rights Reserved. 10

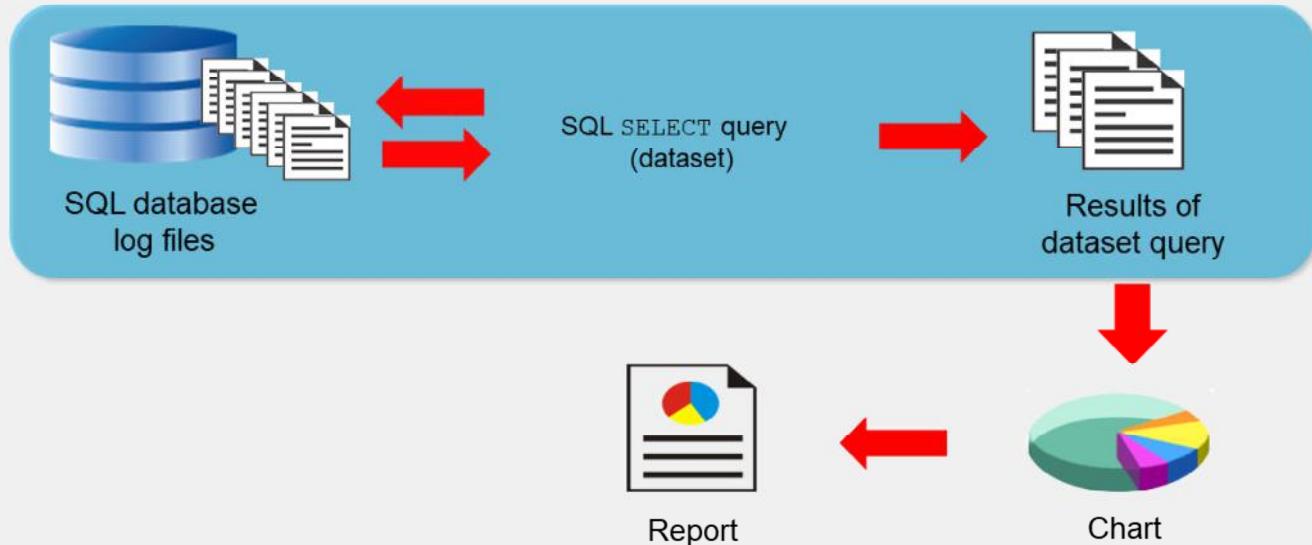
You can use the fields you identify in the schema to build your queries. For example, you can select srcip and srcport from the traffic log type and then create a query.

In the example shown on this slide, the results return the same IP address, 10.0.1.10, but there are three different source ports, sorted by descending order.

After validating that your query is returning the desired results, you can add the dataset to a chart and then use the chart in a report.

DO NOT REPRINT**© FORTINET**

Report Workflow



As this slide shows, the SQL database contains all logs. A SQL `SELECT` query polls the database for specific information. Based on the query, a subset of information stored in the logs is extracted. This subset of data populates a chart, and one or more charts exist within a report.

DO NOT REPRINT**© FORTINET**

Reports and ADOMs

- Each administrative domain (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

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

Reports > Report Definitions > 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

© Fortinet Inc. All Rights Reserved. 12

FORTINET
Training Institute

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

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

DO NOT REPRINT**© FORTINET**

Report Considerations

- Audience
 - Level and type of information may vary depending on the intended reader
- Purpose
 - What information do you want?
 - Align with the dataset query
- Level of detail
 - Too much detail can overwhelm the reader
 - Best practice → Keep reports short and concise
 - Too many charts in a report tie up the CPU for a long time
- Format
 - What is the best way to display the information?
 - Select the *best* chart format for your purpose

Before you configure or create a report, there are certain factors you need to consider to ensure the report is as effective as possible.

The first consideration is your audience. Who's going to be reading this report? Depending on their role, knowledge base, and skill level, you may need to add, remove, or modify charts in order to convey the information appropriately.

The second consideration is your purpose. If you look at the predefined reports, each one focuses on a specific piece of information. They are based on specific datasets and contain charts that format the query. So, reports must be focused to be effective and easily digestible, and this is achieved by having a strong purpose.

The next consideration is the level of detail. A best practice is to keep reports short and concise. Not only do they focus your view of your network and users, but shorter reports have fewer charts and fewer queries to run. This helps with performance because large reports affect CPU and memory.

The final consideration is format. You need to know how you want to format the data so that it displays in the most digestible and informative way possible. A table chart, bar chart, and pie chart don't necessarily represent the same data with the same effectiveness. Based on your query, you may only be able to use one type of chart, but if options are available, you need to select the best chart. Think about how the data would best be represented visually, and about the audience consuming the data.

In addition to the chart format, you can change the report's design by adding separators, inserting page breaks, using images, and renaming charts.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. On FortiAnalyzer, what is a dataset?
 - A. The database schema with all available fields in the table
 - B. A specific SQL SELECT query that retrieves data from the database

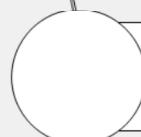
DO NOT REPRINT

© FORTINET

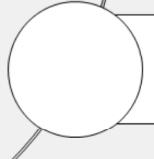
Lesson Progress



Report Concepts



Reports, Charts, and Datasets



Managing and Troubleshooting Reports

Good job! You now understand report concepts.

Now, you will learn how to generate and customize reports in FortiAnalyzer.

DO NOT REPRINT

© FORTINET

Reports, Charts, and Datasets

Objectives

- Describe templates
- Run predefined reports
- Fine-tune reports
- Apply report customization options
- Use macros in reports
- Customize and create charts
- Customize and create datasets



© Fortinet Inc. All Rights Reserved.

16

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

By demonstrating competence in report generation and customization, you will be able to generate reports specific to your requirements.

DO NOT REPRINT

© FORTINET

Templates

- A template specifies the layout—text, charts, and macros—to include in the report that uses it
- FortiAnalyzer provides predefined templates (which match the predefined reports)
 - Can clone predefined templates or create custom templates
 - Can't edit or delete predefined templates

All Reports	Templates	Chart Library	Macro Library
<input type="button"/> Create New	<input type="button"/> Edit	<input type="button"/> Delete	<input type="button"/> More
<input type="checkbox"/> Title			
<input type="checkbox"/> Template - 360 Protection Report			
<input type="checkbox"/> Template - 360 Security Report			
<input type="checkbox"/> Template - 360-Degree Security Review			

All Reports	Templates	Chart Library	Macro Library
<input type="button"/> Run Report	<input type="button"/> Report	<input type="button"/> Folder	<input type="button"/> More
<input type="checkbox"/> Title			
<input type="checkbox"/> 360 Protection Report			
<input type="checkbox"/> 360 Security Report			
<input type="checkbox"/> 360-Degree Security Review			

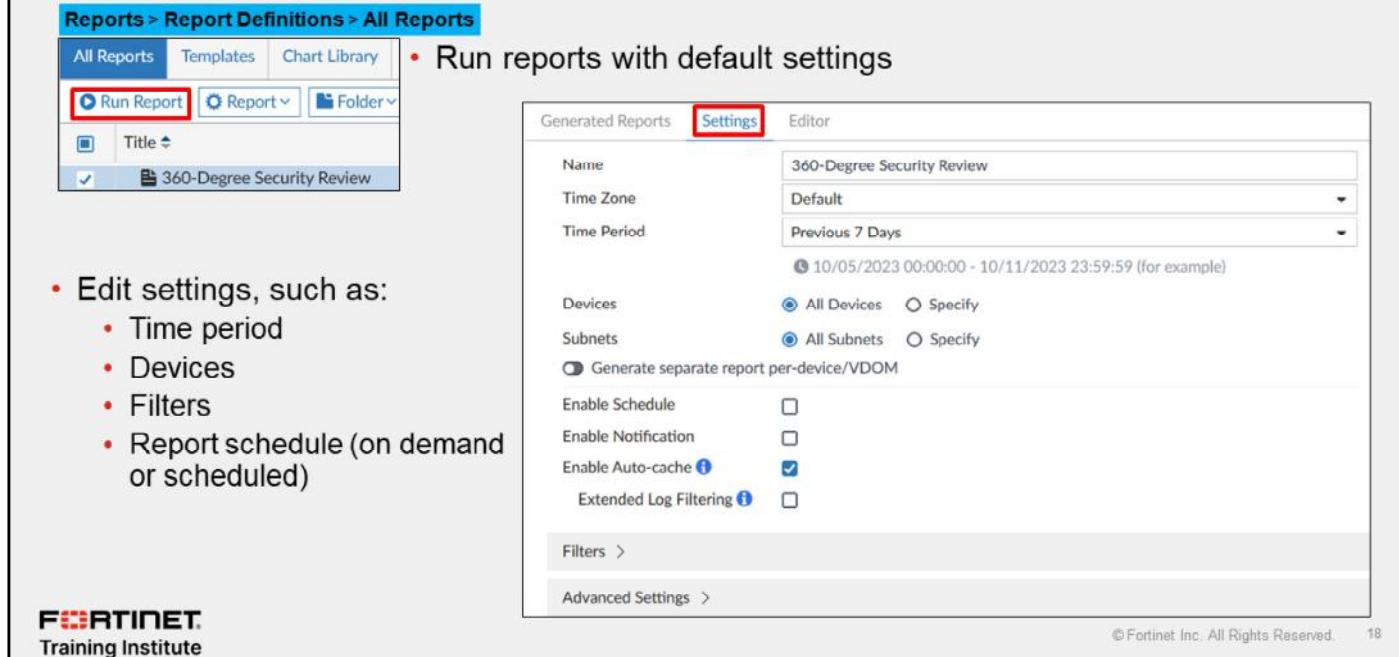
FortiAnalyzer provides predefined templates for reports. A template specifies the layout—text, charts, and macros—to include in the report that uses it. By default, these predefined templates are associated with their respective predefined reports. For example, the Template – 360-Degree Security Review template is the template used by the predefined 360-degree Security Review report.

Templates don't contain any data. Data is added to the report when you generate it.

You can't edit a predefined template, but you can clone it and edit the clone to fit your requirements. You can also create your own template from scratch.

DO NOT REPRINT
© FORTINET

Running Predefined Reports



The screenshot shows the 'Report Definitions > All Reports' section of the FortiAnalyzer interface. On the left, there's a toolbar with 'All Reports' selected, followed by 'Templates' and 'Chart Library'. Below the toolbar are buttons for 'Run Report' (highlighted with a red box), 'Report', and 'Folder'. A list of reports is shown, with '360-Degree Security Review' selected (indicated by a checkmark). On the right, a detailed configuration window for the '360-Degree Security Review' report is open. The 'Settings' tab is selected (highlighted with a red box). The configuration includes:

- Name:** 360-Degree Security Review
- Time Zone:** Default
- Time Period:** Previous 7 Days (with a note: 10/05/2023 00:00:00 - 10/11/2023 23:59:59 (for example))
- Devices:** All Devices (radio button selected)
- Subnets:** All Subnets (radio button selected)
- Generate separate report per-device/VDOM:** Off (checkbox unselected)
- Enable Schedule:** Off (checkbox unselected)
- Enable Notification:** Off (checkbox unselected)
- Enable Auto-cache:** On (checkbox selected)
- Extended Log Filtering:** Off (checkbox unselected)

Below the main configuration area are 'Filters >' and 'Advanced Settings >' buttons.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

18

FortiAnalyzer also provides predefined reports, each associated with a predefined template (the layout). Predefined reports come with basic, default settings already configured. These basic settings define the time period in which the report runs, which device, or devices, to run the report on, and whether the report generates as a single report or separate reports per device or VDOM.

You can run the predefined reports *as is*, but at minimum, you should examine and adjust, if necessary, the basic default settings. You can right-click any predefined report and select **Edit** to change its settings. For example, if today is the first day FortiAnalyzer has been collecting logs, your report contains no data if the time period is set to **Previous 7 Days**. Previous <n> days is handled differently in FortiView than in reports. In reports, the current day is not included. You can specify a custom time period instead or use a previous <n> minutes or previous <n> hours setting.

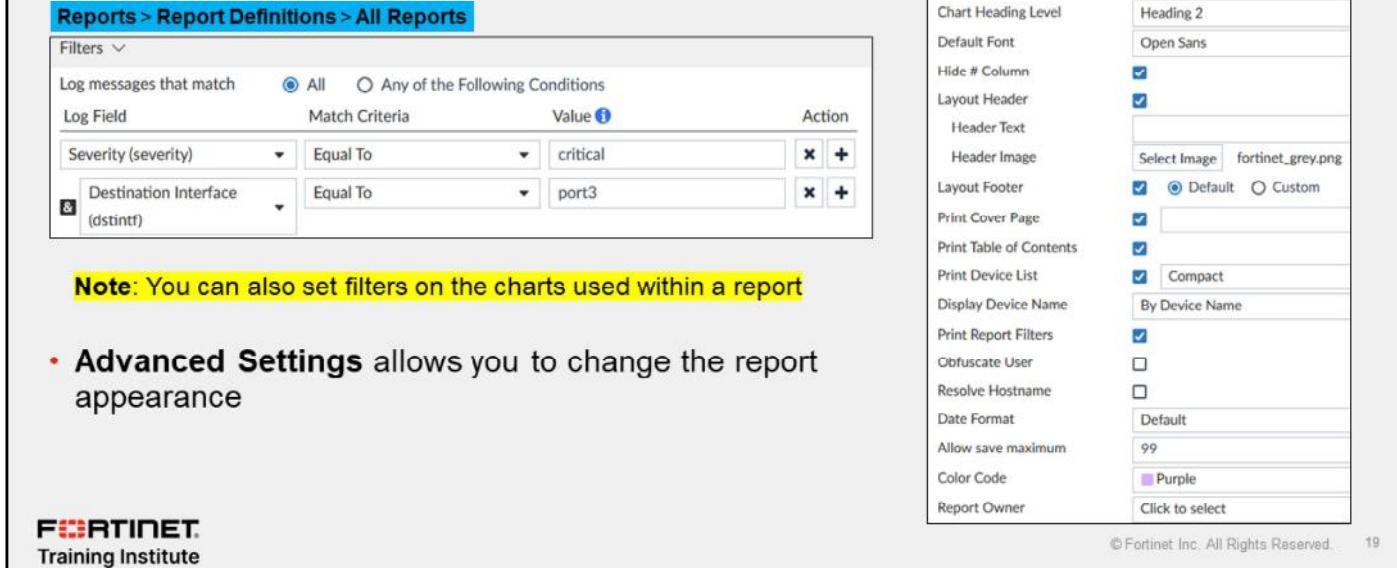
You can run reports on demand, or schedule them for a specific time by enabling scheduling.

After it is generated, you can view a report in multiple formats, including HTML, PDF, XML, CSV, and JSON.

DO NOT REPRINT
© FORTINET

Running Predefined Reports (Contd)

- You can filter which logs are included in a report



The screenshot shows the 'Reports > Report Definitions > All Reports' section. On the left, there are filters for log messages. The 'Log messages that match' dropdown is set to 'All'. There are two filter rows: one for 'Severity (severity)' set to 'critical' and another for 'Destination Interface (dstintf)' set to 'port3'. On the right, the 'Advanced Settings' panel is open, showing various options like Language (English), Print Orientation (Portrait), Font (Open Sans), and Layout (Header, Footer, Cover Page, Table of Contents, Device List, etc.). A note in the center states: 'Note: You can also set filters on the charts used within a report'.

- Advanced Settings** allows you to change the report appearance

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

19

If a predefined report comes extremely close to meeting all your requirements, you may be able to fine-tune its settings to fit your needs.

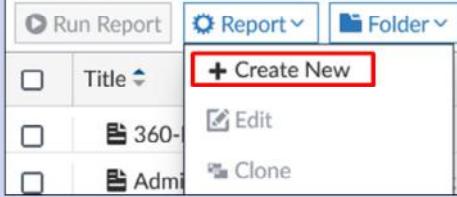
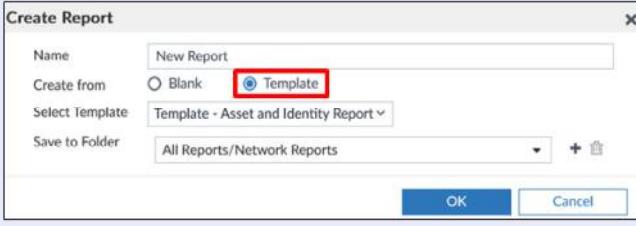
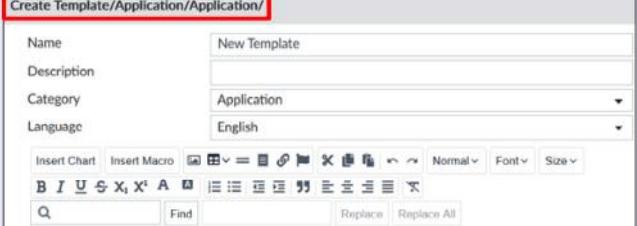
Fine-tuning encompasses minimal modifications, such as:

- Adding log message filters to further refine the log data that is included in the report
- Enabling queries on a pre-existing LDAP server to add an LDAP query to the report
- Configuring report language, print settings, and other settings. For example, you can print and customize the cover page, print the table of contents, print a device list, obfuscate users, and set the color code for the report to appear under **Report Calendar**.

DO NOT REPRINT

© FORTINET

Customization Options

Minor / Moderate Customizations	Major Customizations
<p>Clone a report or template, then edit the clone</p> 	<p>Create a new report from scratch (blank)</p> 
<p>Create a new report from an existing template, then edit</p> 	<p>Create a new template (which you can use in a report)</p> 

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 20

Predefined reports may not meet all your organization's requirements, even after you fine-tune the report settings. FortiAnalyzer provides you with the option to create new templates and reports from scratch, or you can customize existing templates and reports.

To make minor or moderate changes to existing templates or reports, you can use cloning. To use cloning, you clone a report or template and then edit the clone to suit your requirements.

For reports only, you can create a new report but base it on an existing template. Then, you can edit that new report to suit your requirements.

While you can edit the layout of predefined reports (but not templates) directly, it is a best practice to clone and edit predefined reports instead. This preserves the default reports if your direct edits are not successful.

If you need to make major changes to existing templates or reports (if no report comes close to meeting your needs), you can create a new report or template from scratch.

DO NOT REPRINT
© FORTINET

Customization—Template vs. Report

- Which customization approach do you take: template or report?
- Most important difference: templates only include the layout of the report—they don't include report settings (either basic configurations or advanced settings)
- A best practice is to approach it from an efficiency and needs standpoint
- Think about:
 - The amount of customization you need
 - Whether you want to preserve report settings
 - Whether you want to use the layout for one report or many reports

The image contains two side-by-side screenshots of a software interface for managing report definitions. The top screenshot shows the 'Report Definitions > Templates' section. It has fields for Name (Template - IPS Report), Description (Intrusions detected by type, severity, victims, sources, blocked, monitored, attacks over http-https.), Category (Security), and Language (English). Below these are buttons for 'Insert Chart', 'Insert Macro', and a toolbar with font and size options. A search bar and a 'Summary' section with a pie chart titled 'Intrusions By Severity' are also present. The bottom screenshot shows the 'Report Definitions > All Reports' section. It includes tabs for 'Generated Reports', 'Settings', and 'Editor' (which is highlighted with a red box). It has the same toolbar and summary section with the same pie chart.

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved. 21

Templates and reports are closely related. As discussed earlier, you can clone and edit both reports and templates, and you can create both new reports and new templates. So, how do you know which customization approach to take? Do you approach the customization from the template side or the report side?

One of the most vital differences between templates and reports is that templates include only the details you can find under the **Editor** tab of the report—they don't include report settings (neither the basic configuration nor advanced settings). So, when deciding whether to perform customizations on the template side or the report side, the choice depends on what you want to preserve and what you want to modify.

In the end, there is no *correct* approach. Multiple methods can achieve the same results. A best practice is to approach the decision from an efficiency and needs standpoint.

DO NOT REPRINT
© FORTINET

Inserting Macros as Abbreviated Dataset Queries

- Macros specify which data to extract from the logs
 - Macros represent a sequence of instructions (dataset queries) in abbreviated form

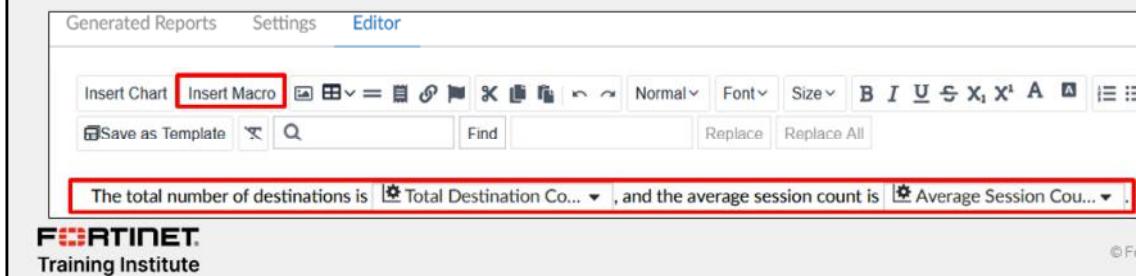
Reports > Report Definitions > Macro Library

Name	Total Destination Count
Description	Total Destination Count
Dataset	bandwidth-app-Detailed-Traffic-Statistics
Query	select count(distinct app) as total_app, count(total_endpoint, count(distinct distip) as total)
Data Binding	total_dest
Display	Counter (K/M/G)

Example report with macros

The total number of destinations is 68 , and the average session count is 46.09 K.

- Insert macros as data into templates and reports



The screenshot shows the FortiAnalyzer Editor interface. At the top, there are tabs for Generated Reports, Settings, and Editor, with the Editor tab selected. Below the tabs is a toolbar with various icons for chart creation, macro insertion, and text editing. The 'Insert Macro' button is highlighted with a red box. To the right of the toolbar is a preview area containing the following text:

The total number of destinations is **[macro]** Total Destination Co... ▾ , and the average session count is **[macro]** Average Session Cou... ▾ .

At the bottom left of the editor is the Fortinet Training Institute logo, and at the bottom right are copyright and page number information: © Fortinet Inc. All Rights Reserved. 22

On FortiAnalyzer, macros specify which data to extract from the logs—they represent dataset queries in abbreviated form. You can insert macros as data in your reports, without having to use a chart to display the data. FortiAnalyzer provides predefined macros, or you can create your own custom macros.

Note that macros are ADOM-specific.

DO NOT REPRINT**© FORTINET**

If Predefined Charts or Datasets Do Not Meet Requirements

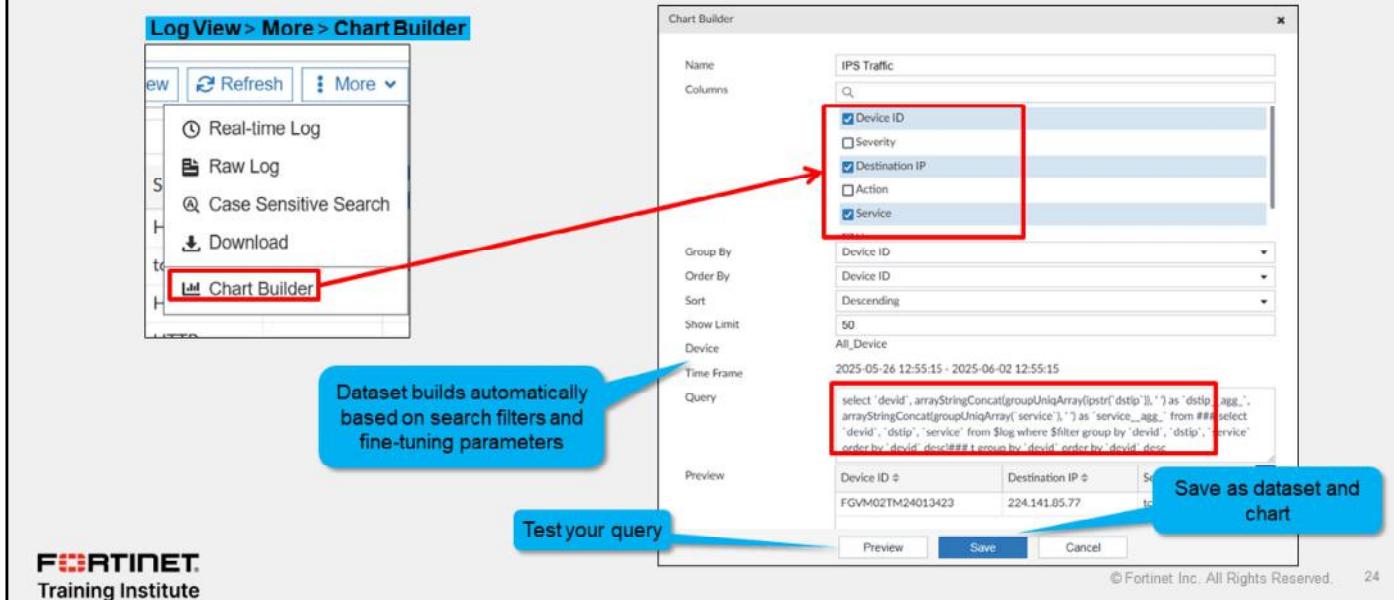
- By default, the chart library contains hundreds of charts
 - Can't edit default charts
- By default, the datasets library contains hundreds of datasets
 - Can't edit default datasets
- Just like templates and reports, you can clone and edit both charts and datasets, and create new ones
- Gives you the flexibility to pull a unique combination of data from the database that doesn't exist in any default chart or dataset

In some cases, simply adding or removing default charts from a report or template may not meet your requirements: You might need to pull a unique combination of data from the database when no predefined chart or dataset for that unique combination exists. In cases like these, you can either clone and edit charts and datasets or create new charts and datasets from scratch.

DO NOT REPRINT
© FORTINET

Building Datasets and Charts From Search Results

- In **Log View**, set filters to search for logs and then use the chart builder



A quick way to build a custom dataset and chart is to use the chart builder tool. This tool allows you to build a dataset and chart automatically, based on your filtered search results. In **Log View**, set filters to return the logs you want. Then, in the **Tools** menu, select **Chart Builder** to automatically build the search into a dataset and chart. You can also fine-tune the dataset further by:

- Adding more columns
- Setting group by, order by, and sort filters
- Setting a limit on results
- Setting the device and time frame

DO NOT REPRINT
© FORTINET

Export From FortiView to a Chart

- You can export a chart from FortiView

Chart export will include any filters you set

The screenshot shows the 'Top Threats' section of FortiView. A line chart displays Threat Score (Y-axis, 0 to 250.0k) against time (X-axis, Apr 21 14:13 to Apr 22 12:26). A red box highlights the 'Export to Report Chart' button. A blue callout bubble states: 'Chart export will include any filters you set'. Below the chart is a table with columns: Threat, Threat Type, Threat Score, Threat Level, and Incidents. The table shows one entry: 'tcp_syn_flood' under Threat, 'IPS' under Threat Type, '10,150' under Threat Score (with a yellow bar), 'Critical' under Threat Level, and '203' under Incidents. A red box highlights the 'Filter' field in the 'Export to Report Chart' dialog, which contains: Name: 'IPS Traffic', Time: 'From 2025-4-21 11:32 To 2025-4-22 12:32', Device: 'All_Device', Filter: 'threattype=ips', and Top: '0'. The Fortinet Training Institute logo is at the bottom left, and copyright information is at the bottom right.

You can export a chart from FortiView. The chart export includes any filters you set on FortiView.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What is not found in templates?
 A. Report schedule
 B. Charts

2. Which statement about macros is true?
 A. Macros are abbreviated dataset queries.
 B. Macros cannot be customized.

DO NOT REPRINT

© FORTINET

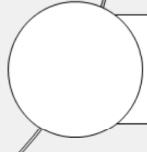
Lesson Progress



Report Concepts



Reports, Charts, and Datasets



Managing and Troubleshooting Reports

Good job! You now understand how to generate and customize reports, charts, and datasets.

Now, you will learn how to manage and troubleshoot reports.

DO NOT REPRINT**© FORTINET**

Managing and Troubleshooting Reports

Objectives

- Configure external storage for reports
- Enable auto-cache
- Group reports
- Import and export reports and charts
- Attach reports to incidents
- Manage scheduled reports
- Troubleshoot reports



© Fortinet Inc. All Rights Reserved. 28

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

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

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
- 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)	

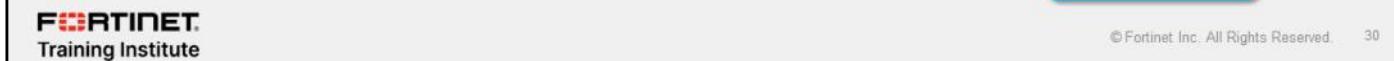
You can configure FortiAnalyzer to email generated reports to specific administrators, or to upload generated reports to an external server.

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

DO NOT REPRINT
© FORTINET

Configure External Storage for Reports (Contd)

- Configure output profiles per 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 > 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
<input checked="" type="checkbox"/> Email Generated Reports	
Subject	Generated Reports
Body	Please review these reports 27/1023
Recipients	Email Server Mail_Server: 10.200.1.254
<input checked="" type="checkbox"/> Upload Report to Server	
Server Type	FTP
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 Inc. All Rights Reserved. 30

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

An output profile specifies the following:

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

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

DO NOT REPRINT

© FORTINET

SQL Hard Cache (hcache)

- The hcache must build before FortiAnalyzer can build 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 the hcache for most reports to ensure they are efficiently generated
 - 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) x

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. 31

When a report is generated, the system builds the charts from precompiled SQL hard-cache data, known as the hcache. hcache is a proprietary FortiAnalyzer caching system that stays on the disk in the form of a database table. Unlike other caches, hcache tables are persistent and are not removed based on a set period of time.

If the hcache is not built when you run the report, the system must create the hcache first and then build the report, which adds time to the report generation. However, if FortiAnalyzer does not receive any new logs for the reporting period, when you run the report a second time, it is much faster because the hcache data is already precompiled.

To boost the report performance and reduce report generation time, you can enable auto-cache in the settings of the report. When you do this, the hcache is automatically updated when new logs come in and new log tables are generated.

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

Additionally, you can enable extended log filtering to cache specific log fields for faster filtering.

DO NOT REPRINT

© FORTINET

Grouping Reports to Improve Report Generation Time

- Benefits:
 - Reduces the number of hcache tables
 - Improves auto-cache completion time

```
# configure system report group
edit 0
  set adom <ADOM-name>
  config group-by
    edit <SQL-column>
    next
    edit vd
    next
  end
  set report-like <report name string>
end
```

```
# execute sql-report list-schedule <ADOM-name>
```

```
# execute sql-report hcache-build <ADOM-name>
<schedule-name> "<start-time>" "<end-time>"
```

View report grouping information

Must rebuild hcache tables

SQL column is added to the hcache creation queries with any related report

Group report function is applied to any report that contains this case-sensitive string

If the same (or similar) reports are run against many different FortiGate devices, you can significantly improve report generation time by grouping the reports. Report grouping can reduce the number of hcache tables and improve auto-cache completion time and report completion time.

After you configure report grouping using the `configure system report group` CLI command, you must rebuild the report hcache tables. You can rebuild the hcache tables for those reports.

DO NOT REPRINT**© FORTINET**

Moving Reports Between ADOMs

- Each ADOM has its own reports, libraries, and advanced settings
- Export reports and charts (default and custom) and import them into a different ADOM based on the same type (that is, FortiGate ADOM to FortiGate ADOM)
 - Charts import datasets associated with charts
 - Can save layout of imported report as a template

The screenshot shows the FortiAnalyzer interface. On the left, there is a list of reports under 'Report' tab. One report, '360 Protection Report version 2.0', is selected and highlighted with a blue background. To the right of the report list is a toolbar with buttons for 'Run Report', 'Report', 'Folder', and 'More'. The 'More' button is expanded, showing 'Import' and 'Export' options, which are both enclosed in a red box. To the right of the toolbar is a modal window titled 'Import Report'. The modal has a 'File' section with a 'Drag & Drop your files or Browse' button. Below it is a 'Save to Folder' dropdown set to 'All Reports'. At the bottom of the modal are three buttons: 'Keep Current Settings' (highlighted in blue), 'Reject with Error', and 'Overwrite'. At the bottom of the main interface, there is a 'FORTINET Training Institute' logo and copyright information: '© Fortinet Inc. All Rights Reserved. 33'.

Remember, each ADOM has its own reports, libraries, and advanced settings. You can, however, import and export reports and charts (whether default or custom) into different ADOMs within the same FortiAnalyzer device or a different FortiAnalyzer device. Both ADOMs must be of the same type.

You can't export templates and datasets. However, when you import an exported report, you can save the layout of the report as a template. When you export a chart, the associated dataset is exported with it, so when you import an exported chart, the associated dataset is imported as well.

You can export and import reports through the right-click menu on the **Reports** page.

The chart library includes export and import functions in the toolbar.

DO NOT REPRINT

© FORTINET

Attach Reports to Incidents

- Attach a report to add historical data to an incident
- There are three ways to attach a report:
 - Manually, from an existing report
 - Manually, from an existing incident
 - Automatically, through playbook automation

The screenshot shows the FortiAnalyzer interface. At the top, there's a navigation bar with 'Edit' and 'Refresh' buttons. Below it is a detailed view of an incident: IN00001463, a DDoS attempt on a firewall, assigned to admin, with analysis in progress. The main area displays reports for 'Today (2)' and 'Earlier This Week (28)'. A context menu is open over a report from 'Earlier This Week', with options like 'Delete', 'Retrieve Diagnostic', 'Create New Incident', and 'Add to Existing Incident'. The 'Add to Existing Incident' option is highlighted with a red box. Another red box highlights the 'Reports' tab in the navigation bar at the bottom. A blue callout points to the 'Add to Existing Incident' option with the text 'Right-click on a generated report'. Another blue callout points to the 'Reports' tab with the text 'Add a report to an existing incident'.

You can attach reports to incidents to add historical data in addition to real-time events.

These are the three ways that you can attach a report:

- Manually, from an existing report
- Manually, from an existing incident
- Automatically, through automation playbooks

This slide shows how to manually attach reports from an existing report and from an existing incident.

DO NOT REPRINT

© FORTINET

Viewing Scheduled Reports Through Calendar

- Graphic view of scheduled (generated and pending) reports

Reports > Advanced Settings > Report Calendar



Note: The report color is configured on the **Settings > Advanced Settings** page

The report calendar provides an overview of all your scheduled reports. A check mark means the report was generated, and a clock icon means it is pending. When you hover your mouse over a scheduled report, a notification opens displaying the report name, status, device type, and start time. You can edit and disable upcoming, scheduled reports, as well as delete or download completed reports, by right-clicking the name of the report in the calendar. Note that you do not configure scheduling on this page. You configure scheduling in the specific report configuration. You can also configure reports to display in a specific color in the report calendar in the **Advanced Settings** window associated with the report.

DO NOT REPRINT
© FORTINET

Troubleshooting Report Generation Run Time

- Retrieve report diagnostics
 - Check the **Report Summary** for details, including hcache building time
 - If hcache is not precompiled, the report generation time increases
- Check log rates
- Check insert rate and receive rate
- Check log insert lag
- Enable auto-cache on report settings →

Enable Schedule	<input type="checkbox"/>
Enable Notification	<input type="checkbox"/>
Enable Auto-cache	<input checked="" type="checkbox"/>

Reports > Generated Reports

The screenshot shows the 'Generated Reports' section of the FortiAnalyzer interface. It lists reports for 'Today' (1) and 'Earlier This Week' (1). For the 'Today' report, a context menu is open with the following options: Delete, Retrieve Diagnostic (highlighted with a red box), Create New Incident, and Add to Existing Incident. A red arrow points from the 'Retrieve Diagnostic' option to the 'Report Summary' window on the right. The 'Report Summary' window displays the following details:

```

Report Summary
Tue May 20 07:19:43 2025
-----
Number of charts: 32
Number of tables: 41
Number of hcaches requested: 168
-----
HCACHE building time: 19.69s
Rendering time: 6.87s
Total time: 26.56s
  
```

If your network has a high volume of devices sending logs to FortiAnalyzer as well as high log volume, reports can take some time to generate. If you find reports are taking too long to generate, there are a few steps you can take to troubleshoot:

- Run diagnostics on your report and view the report summary at the end of the report. Look at the hcache time to see how long it took to build.
- Check your log rates to get an idea of log volumes.
- Check the insert rate, receive rate, and log insert lag. They can tell you the rate at which raw logs are reaching FortiAnalyzer (receive rate) and the rate at which they are indexed by the SQL database (insert rate) by the sqlplugin daemon. The log insert lag time tells you how many seconds the database is behind in processing the logs.
- Enable auto-cache in the report settings to boost the reporting performance and reduce report generation time. Scheduled reports have auto-cache enabled already.

DO NOT REPRINT**© FORTINET**

Report Troubleshooting CLI Commands

- Use the following FortiAnalyzer CLI commands to troubleshoot report generation time issues

What to Investigate	CLI Command to Use
What is the SQL insertion status? What are the SQL query connections and hcache status?	# diagnose sql status sqlplugind # diagnose sql status sqlreportd
What are the log file-related activities (file rolled/deleted/uploaded)? Can indicate if the hcache creation is able to catch up?	# diagnose test application logfiled 2
What are the current SQL processes running (any log queries)?	# diagnose sql process list
What is the configuration status of all configured reports?	# execute sql-report list-schedule <ADOM>
Is the hcache creation able to catch up?	# diagnose test application sqlrptcached 2
What is the state of the hcache?	# diagnose sql hcache status
What is the hcache size on the file system?	# diagnose sql show hcache-size

This slide shows some CLI commands you can use to troubleshoot issues related to report generation time.

DO NOT REPRINT

© FORTINET

Empty Reports

- Check the time frame covered by the report
- Verify that you have logs from the time frame the report was run and from the device that the report was run for
- Test the datasets to ensure that the expected data is retrieved
 - If not, check the SQL query associated with the dataset

The image shows two screenshots of a FortiAnalyzer interface. On the left, a configuration window titled 'App-Risk-High-Risk-Application' shows a SQL query for selecting risk, behavior, and session details. On the right, a results table displays three rows of data: BitTorrent (P2P), Dropbox_File.Download (Storage.Backup), and Vimeo_Video.Play (Video/Audio), all categorized as Excessive-Bandwidth.

d_risk	d_behavior	id	name	app_cat
4	Evasive,Excessive-Bandwidth	6	BitTorrent	P2P
3	Excessive-Bandwidth,Cloud	35421	Dropbox_File.Download	Storage.Backup
3	Excessive-Bandwidth,Cloud	38473	Vimeo_Video.Play	Video/Audio

- Check the report advanced settings (such as **user obfuscate**)
 - Verify that the logs match any filter that you have set for the report

What happens if you run a report and it is empty or doesn't contain the desired information? Here are some troubleshooting tips:

- Check the time frame covered by the report, which is listed within the report.
- Verify that you have logs from the time frame the report was run and from the device that the report was run for. A common cause of empty reports is logs being overwritten too quickly. In this case, the solution is to increase the disk quota and retention policy to ensure that logs are retained longer.
- Test the dataset in question and verify that it is retrieving the correct information. If it isn't, troubleshoot the SQL query because the dataset probably contains the error.
- Check your advanced settings for the report. A setting such as **user obfuscate** can result in abnormal usernames appearing in the report. Also, verify the filters attached to a report. It is possible that your filter is filtering out the desired logs.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which data does the CLI command # diagnose sql show hcache-size provide?
 A. Hcache size on the file system
 B. State of the hcache

DO NOT REPRINT

© FORTINET

Lesson Progress



Report Concepts



Reports, Charts, and Reports



Managing and Troubleshooting Reports

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Run and fine-tune predefined reports
- ✓ Customize reports with macros, custom charts, and datasets
- ✓ Configure external storage for reports
- ✓ Group reports
- ✓ Import and export reports and charts
- ✓ Attach reports to incidents
- ✓ Manage and troubleshoot reports



© Fortinet Inc. All Rights Reserved. 41

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

By mastering the objectives covered in this lesson, you learned how data is formatted, stored, and organized in the database, and how to use the FortiAnalyzer reporting feature to view and extract useful information from logs.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiAnalyzer Analyst

Playbooks

 FortiAnalyzer 7.6

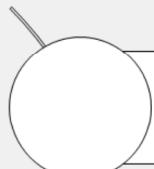
Last Modified: 16 July 2025

In this lesson, you will learn how to use the automation capabilities included in FortiAnalyzer.

DO NOT REPRINT

© FORTINET

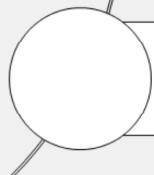
Lesson Overview



Playbook Components



Creating Playbooks



Managing Playbooks

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

DO NOT REPRINT

© FORTINET

Playbook Components

Objectives

- Describe FortiAnalyzer automation capabilities
- Describe playbook concepts
- Describe trigger types and characteristics
- Describe connector types
- Describe playbook tasks



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

3

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

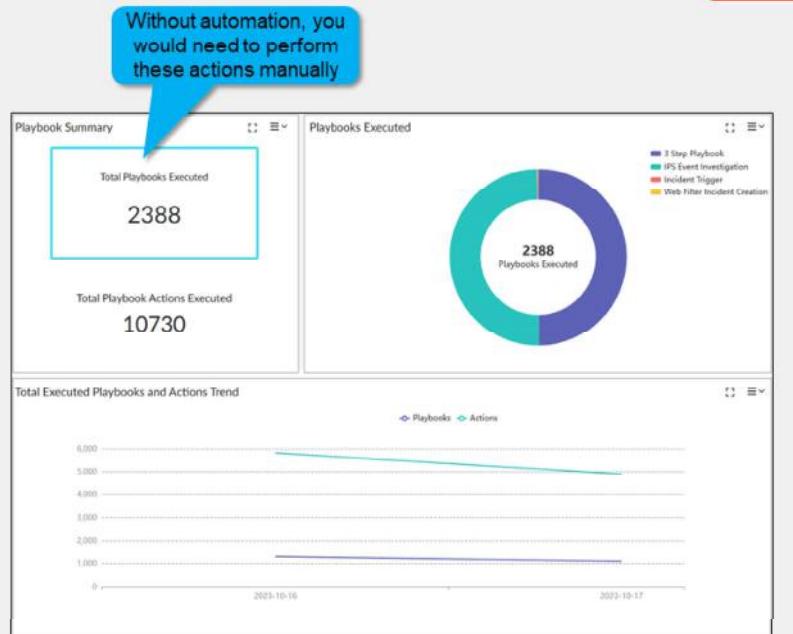
By demonstrating competence in understanding the purpose of playbooks and their components, you will be able to use playbooks effectively.

DO NOT REPRINT

© FORTINET

Why Automation?

- The benefits of using automation include:
 - Improved productivity
 - Increased efficiency
 - Reduced costs
 - Fewer human errors
- In a SOC environment, using playbooks results in:
 - Faster incident response time
 - Faster data analysis
 - Better use of analysts' time
 - Better compliance management
 - Consistent security posture



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

4

Automation is critical for security teams who are facing the ever-changing threat landscape. Generally speaking, automation improves productivity, reduces cost, increases efficiency, and minimizes human errors.

In a SOC environment, automation provides, among other results, faster response times, faster data analysis, better use of analyst time, better compliance management, and a more consistent security posture.

FortiAnalyzer allows SOC analysts to automate common and repetitive tasks with the use of playbooks.

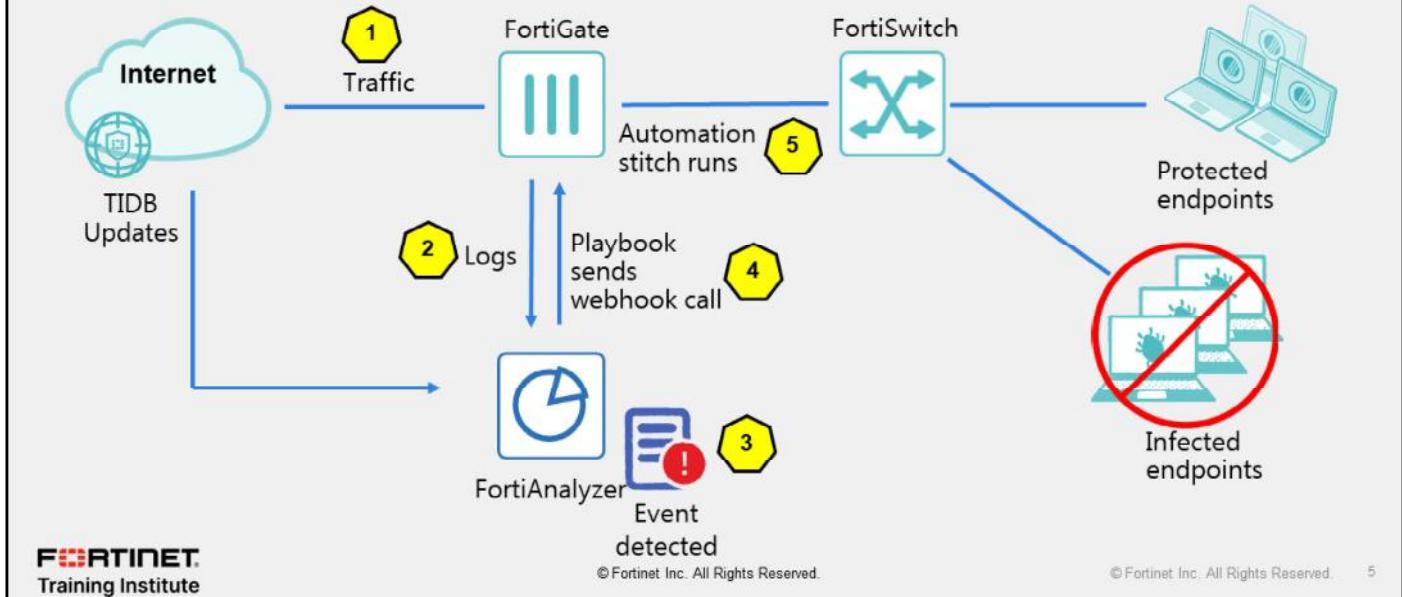
FortiAnalyzer works with standalone devices but is also integrated with the Security Fabric. This integration allows FortiAnalyzer to communicate with other devices in the Security Fabric to detect security events and trigger corrective or preventive actions automatically by running automated playbooks.

For example, you can create playbooks that automatically generate a report, or instruct FortiGate to quarantine a compromised host, just to mention two use cases. The available actions depend on the device type. Using devices that are compatible with the Security Fabric allows you to exploit their capabilities to their full extent.

In this lesson, you will learn more about these capabilities.

DO NOT REPRINT
© FORTINET

An Example of Automation With a Playbook



This slide shows an example of a playbook being used to automate tasks.

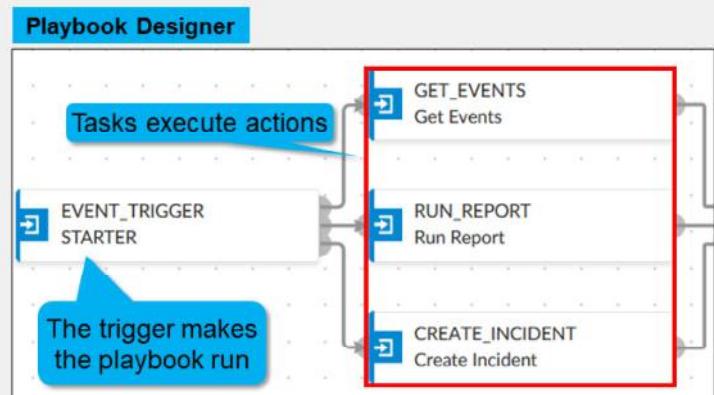
1. Traffic flows through FortiGate.
2. FortiGate sends logs to FortiAnalyzer.
3. FortiAnalyzer detects some suspicious traffic and generates an event.
4. The event triggers the execution of a playbook on FortiAnalyzer, which sends a webhook call to FortiGate.
5. FortiGate runs the automation stitch with the corrective or preventive actions.

DO NOT REPRINT

© FORTINET

Playbook Concepts

- Playbooks allow you to automate common SOC tasks
 - They are created per ADOM
- Each playbook has only one trigger
 - It determines when a playbook executes
- Playbooks have one or more tasks
 - They are the actions that will take place
- The actions that can be performed by a task depend on the connector used
 - Different devices allow different actions
- Playbooks can be created from built-in templates or from scratch



- Playbooks are created using an intuitive playbook designer
 - Flow diagrams help you visualize the workflow

Playbooks include a starter event (trigger) that determines when a playbook runs, and one or more tasks that are executed.

After a playbook is triggered, it flows through the existing tasks defined within the playbook designer.

Each task includes the automated action that needs to take place. The available actions depend on the connector used. Connectors allow tasks to be performed on supported devices.

You can create playbooks from scratch or using predefined templates. Playbooks are available only in the ADOM where they were created, unless they are exported to a different ADOM.

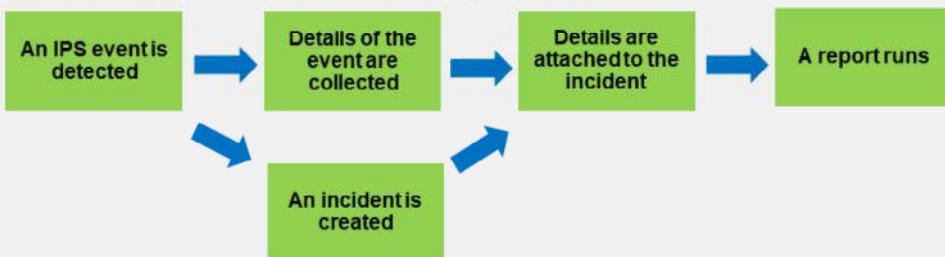
DO NOT REPRINT
© FORTINET

Playbook Concepts (Contd)

- A simple playbook execution sequence
 - Tasks run one after another



- Multiple tasks can be triggered
- Tasks can be sequential or run in parallel
 - The second step has two tasks that run at the same time



In the simplest case, a playbook consists of a trigger and a series of tasks that are executed one after the other. However, playbooks also allow for more complex designs that involve multiple tasks running simultaneously. Additionally, if needed, the output of one task can be used by the tasks that follow it.

For example, one task can collect specific events, and the next task can add those events to an incident.

DO NOT REPRINT

© FORTINET

Triggers

Trigger Type	Description
EVENT_TRIGGER	The playbook is run when an event is created that matches the configured filters When no filters are set, all events will trigger the playbook
INCIDENT_TRIGGER	The playbook is run when an incident is created that matches the configured filters When no filters are set, all incidents will trigger the playbook
ON_SCHEDULE	The playbook is run during the configured schedule You can define the start time, end time, interval type, and interval frequency for the schedule
ON_DEMAND	The playbook is run when it is manually started by an administrator



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

8

Every playbook starts with a trigger that determines when the playbook is executed. Each playbook can include only one trigger.

After a playbook is triggered, it flows through the configured tasks, as defined in the playbook designer.

The following four triggers are available:

- EVENT_TRIGGER: The playbook runs when an event is created that matches the configured filters. When no filters are set, all events will trigger the playbook.
- INCIDENT_TRIGGER: The playbook runs when an incident is created that matches the configured filters. When no filters are set, all incidents will trigger the playbook.
- ON_SCHEDULE: The playbook runs during the configured schedule. You can define the start time, the end time, the interval, and the interval frequency for the schedule.
- ON_DEMAND: The playbook runs when it is manually started by an administrator.

To run a playbook manually, go to **Playbook**, select the desired playbook, and click **Run**. Additionally, if present, you can run playbooks from the incident **Analysis** page.

Note that playbooks with the ON_SCHEDULE trigger can also be executed manually. This allows you to test them outside of their configured time frame.

DO NOT REPRINT

© FORTINET

Triggers (Contd)

- A wide variety of categories can be used as filters for the event and incident triggers
 - You can use more than one condition to narrow down when the playbook will run
 - AND (all conditions must match) and OR logic (any condition must match) are supported
- ON_SCHEDULE** trigger parameters are all based on timeframes
- ON_DEMAND** triggers have no extra configurable parameters

The screenshot shows the 'Incidents & Events > Automation > Playbooks' interface. It displays three main trigger configuration sections:

- EVENT_TRIGGER**: Filters include Basic Handler Name, Event Time, Threat Type, Device ID, Severity, Endpoint ID, Endpoint Name, Endpoint MAC, and Endpoint IP.
- INCIDENT_TRIGGER**: Filters include Change Types (e.g., MITRE Tech ID), Reporter, Endpoint ID, End User ID, Endpoint, and Category.
- ON_SCHEDULE**: Parameters include The start time of the schedule (2025-06-03), The end time of the schedule (2025-08-03), The interval of the schedule (N-MINUTES), and The frequency of the interval (60).

A blue callout bubble points to the EVENT_TRIGGER section with the text: "Available filters depend on the chosen trigger type".

Example

EVENT_TRIGGER

All of the following conditions

Severity	Equal To	Critical	<input type="button" value="Delete"/>
Device ID	Equal To	FGVM0123456789	<input type="button" value="Delete"/>

© Fortinet Inc. All Rights Reserved. © Fortinet Inc. All Rights Reserved. 9

The trigger type you select determines the options you can use to specify exactly when you want the playbook to run.

For example, you can configure an event trigger to run only when FortiAnalyzer detects an event with critical severity on a specific device.

If you set more than one condition for a trigger, you can choose to either require all conditions to match, or any one condition to match.

DO NOT REPRINT

© FORTINET

Connectors

- Allow playbooks to interact with devices in the Security Fabric and standalone devices
 - Determine which actions can be performed by playbook tasks
- Many connector types are available:
 - EMS
 - FortiOS
 - FortiGuard
 - FortiMail
 - VirusTotal
 - Local (FortiAnalyzer)
 - And more
- Only the local connector is ready to be used by default
- The status of each connector is shown:
 - Green: connection successful
 - Orange: connection unknown
 - Red: connection down



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 10

Connectors determine which automated actions can be performed in playbooks. The available actions vary depending on the connector type used. Each type allows for different actions.

To view fabric connectors, click **Active Connectors**.

The status of connectors is indicated by a colored icon:

- Green: The API connection successful.
- Orange: The API connection is unknown.
- Red: The API connection is down.

You can see when the status was last updated by hovering your mouse over the status icon. Click the refresh icon to get an updated status.

By default, the local connector, which is for the local FortiAnalyzer, is ready to be used. Other connector types require extra configuration.

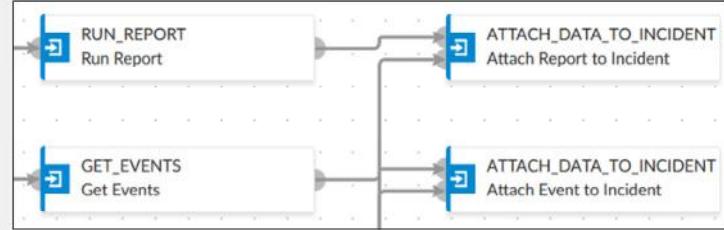
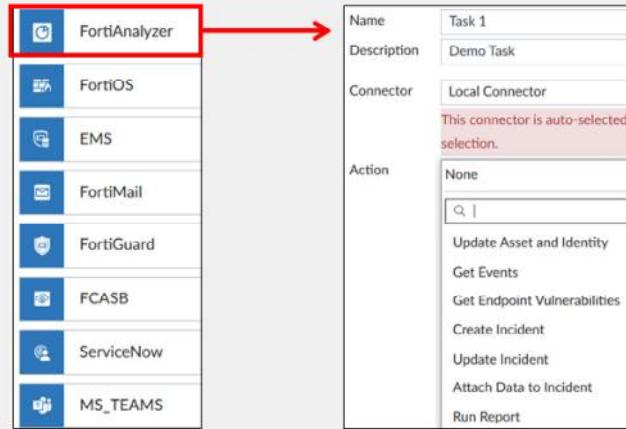
For example, the FortiOS connector will be listed as soon as the first FortiGate device is added to FortiAnalyzer. However, to see the actions related to that FortiOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on FortiGate.

DO NOT REPRINT

© FORTINET

Tasks

- Tasks are the actions that execute when a playbook runs
- The available actions depend on the connector you choose
- You can chain one task to another task to execute a sequence of actions
- You can use the output of one task as the input of the next task in the sequence



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

11

Tasks are the actions that take place after a playbook starts running. Each starter can trigger the execution of one or more tasks, and each task can perform one action.

Tasks can also be chained so that the output of one task becomes the input of the next task. For example, a task can be created to collect some data, and then provide that data to the next task, where it can then be added to a report.

When adding a new task, you must choose a relevant connector before you can select the desired action. On this slide, the actions associated with the local connector are shown. The available actions vary depending on the connector type that you select.

You can configure tasks that use default input values or that take inputs from the trigger or from the preceding tasks.

You must configure automation rules on FortiGate before you can see the list of available actions on FortiOS connectors.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What determines which actions are available in a playbook task?

- A. The type of connector used
- B. The type of trigger used

2. Which type of connector is enabled by default?

- A. Local host
- B. FortiOS



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 12

DO NOT REPRINT

© FORTINET

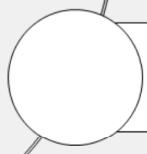
Lesson Progress



Playbook Components



Creating Playbooks



Managing Playbooks

Good job! You now understand playbook components.

Now, you will learn how to create playbooks and use them to automate tasks.

DO NOT REPRINT**© FORTINET**

Creating Playbooks

Objectives

- Create new playbooks from a template
- Customize playbook settings
- Create new playbooks from scratch
- Use variables in tasks



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

14

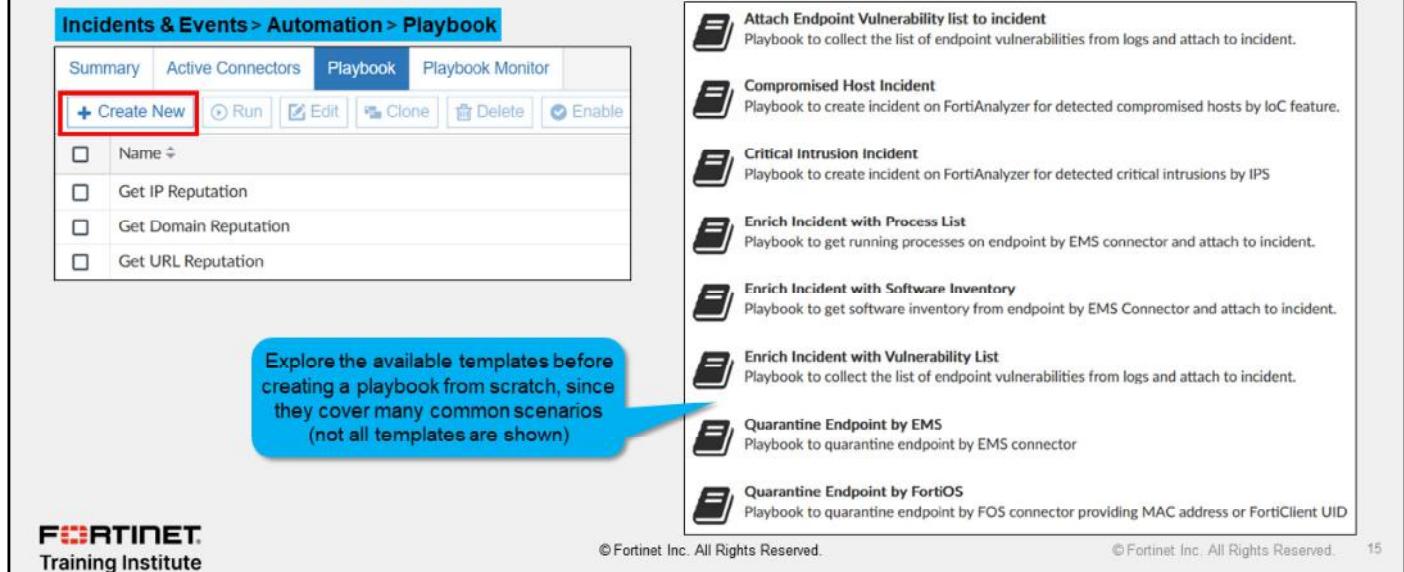
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in automating tasks with playbooks, you will be able to increase the efficiency of SOC operations in your organization.

DO NOT REPRINT
© FORTINET

Creating Playbooks From a Template

- FortiAnalyzer includes several playbook templates
- You can customize playbooks created from these templates to fit your needs



Incidents & Events > Automation > Playbook

Summary		Active Connectors		Playbook	Playbook Monitor
				+ Create New	<input type="button" value="Run"/> <input type="button" value="Edit"/> <input type="button" value="Clone"/> <input type="button" value="Delete"/> <input type="button" value="Enable"/>
<input type="checkbox"/>	Name <input type="text" value=" "/>				
<input type="checkbox"/>	Get IP Reputation				
<input type="checkbox"/>	Get Domain Reputation				
<input type="checkbox"/>	Get URL Reputation				

Explore the available templates before creating a playbook from scratch, since they cover many common scenarios (not all templates are shown)

- Attach Endpoint Vulnerability list to incident**
Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.
- Compromised Host Incident**
Playbook to create incident on FortiAnalyzer for detected compromised hosts by IoC feature.
- Critical Intrusion Incident**
Playbook to create incident on FortiAnalyzer for detected critical intrusions by IPS
- Enrich Incident with Process List**
Playbook to get running processes on endpoint by EMS connector and attach to incident.
- Enrich Incident with Software Inventory**
Playbook to get software inventory from endpoint by EMS Connector and attach to incident.
- Enrich Incident with Vulnerability List**
Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.
- Quarantine Endpoint by EMS**
Playbook to quarantine endpoint by EMS connector
- Quarantine Endpoint by FortiOS**
Playbook to quarantine endpoint by FOS connector providing MAC address or FortiClient UID

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. © Fortinet Inc. All Rights Reserved. 15

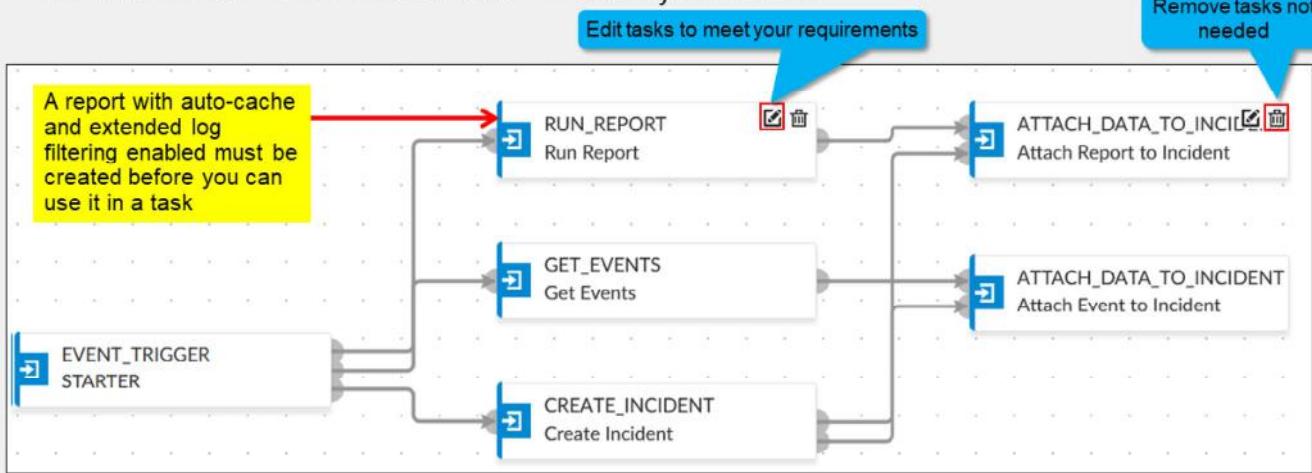
FortiAnalyzer includes several playbook templates that SOC analysts can customize. The templates included allow you to perform tasks such as:

- Investigate compromised host incidents and critical intrusion incidents.
- Enrich data for assets and identity, and for hosts under investigation.
- Block command-and-control (C&C) server IP addresses.
- Quarantine and run antivirus scans on endpoints.

DO NOT REPRINT
© FORTINET

Customizing Playbook Settings

- A new playbook created from a template comes with all required components
- You can remove or customize tasks to meet your needs



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

16

When you select a playbook template, the playbook designer is displayed and automatically populated with a trigger and one or more tasks. The trigger type and the tasks included depend on the template you select.

You can configure, add, or remove tasks to customize the playbook.

This slide shows an example of a playbook that will:

- Run when the specified event or events are generated.
- Create a new incident.
- Get the list of events specified in the task filter and add them to the incident.
- Run a report and attach it to the incident.

Running the playbook will result in the incident including relevant information that the analyst in charge can use during an incident investigation.

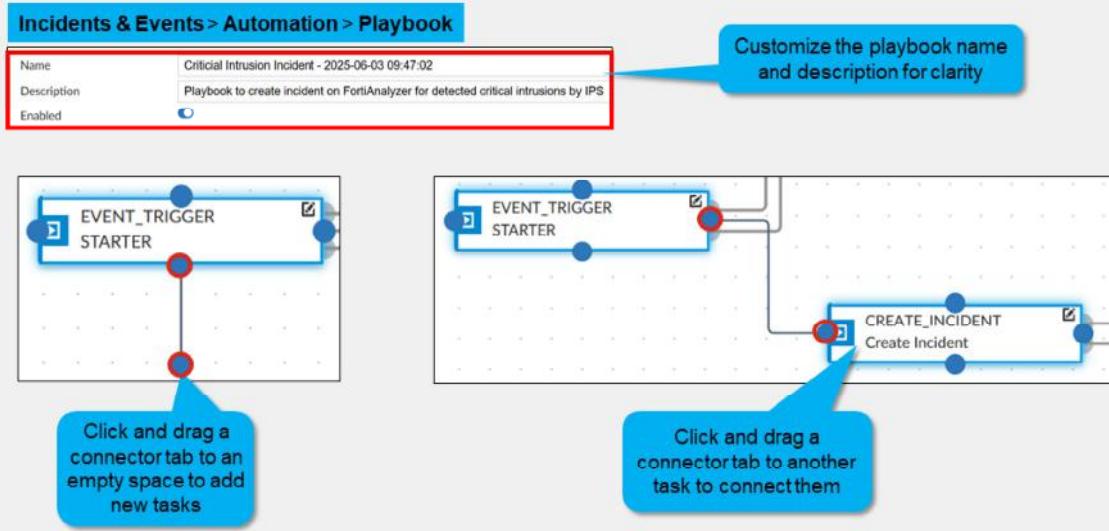
Note that to run a report as a task, it must already exist and have both auto-cache and extended log filtering enabled.

To edit any of the tasks, click the pencil icon in the upper-right corner. Remember to save the changes.

To remove a task, click the trash can icon in the upper-right corner.

DO NOT REPRINT
© FORTINET

Customizing Playbook Settings (Contd)



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 17

By default, every new playbook created from a template comes with the same generic name, plus the date it was created, appended to the end. This can make them difficult to distinguish, so Fortinet recommends that you edit the names and descriptions of new playbooks to something easily recognizable.

To add new tasks, click and drag the connector tabs attached to the current tasks or the trigger. An empty task will be displayed, and you will need to edit its settings.

To connect tasks to each other or to the trigger, click and drag a connector tab onto another connector tab.

DO NOT REPRINT
© FORTINET

Creating a New Playbook From Scratch

The screenshot shows the FortiAnalyzer interface for creating a new playbook. In the top navigation bar, the 'Playbook' tab is selected. Below it, a 'Choose from Playbook Templates' section is shown, with the first template, 'New Playbook created from scratch', highlighted with a red box. A callout bubble points to this template with the text: 'FortiAnalyzer needs a few minutes to parse a newly created playbook'. In the main 'Edit Playbook' area, the 'Name' field is populated with 'New Playbook created from scratch -'. The 'Description' field contains 'Custom build playbook to get started'. The 'Enabled' checkbox is checked. Under the 'ON_DEMAND' connector tab, there is a placeholder text 'Select a Step'. On the right side, a sidebar lists four trigger types: 'EVENT_TRIGGER', 'INCIDENT_TRIGGER', 'ON_SCHEDULE', and 'ON_DEMAND'. A red callout bubble points to the 'ON_DEMAND' trigger with the text: 'Add a Trigger to start the playbook'. At the bottom of the screen, a red banner displays the error message: 'Server error: FAZ is parsing the recent created playbook: 301f8fc9-7831. Please wait for about 5 minutes.'

If none of the templates meets your needs, you can always create a playbook from scratch. To do so, click **Playbook > Create New**, and then select the first option in the list. The playbook designer will open.

First, you must select a trigger. Remember that, depending on the trigger type you choose, you have the option to add filters to make the playbook run only if the specified criteria is matched.

Then, you must add the task or tasks that you want to be executed by dragging and dropping the connector tabs.

When editing tasks, keep in mind that the actions can also include filters that will reduce the processing of unneeded data. For example, a task set to **Get Events** can use a filter to include only events generated by a specific event handler, or only events with a specific severity.

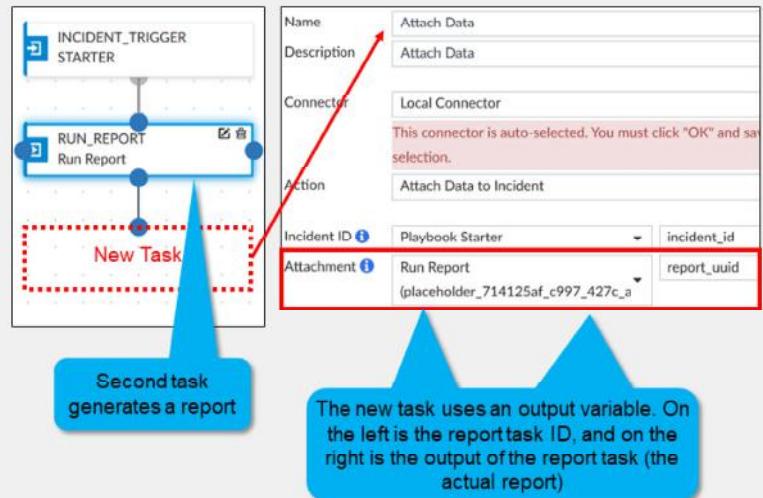
Also, keep in mind that after you create a new playbook, FortiAnalyzer will need a few minutes to parse it. For example, if you try to run a newly created playbook configured with an ON_DEMAND trigger before it is parsed, you will see an error, like the one shown on the slide, telling you why the playbook failed to run.

DO NOT REPRINT

© FORTINET

Using Variables in Tasks

- You can use output variables and trigger variables in playbook tasks
- Output variables: Use the output of the previous task as the input of the current task
 - Format \${task_id.output}
 - Previous task ID is needed
- Trigger variables: Use some of the information from the trigger to filter the action in the task
 - Format \${trigger.variable}



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

19

You can use variables when configuring tasks. There are two types of playbook variables: output variables and trigger variables.

Output variables allow you to use the output from a preceding task as input to the current task.

An output variable consists of the task ID, followed by the task output, as shown on this slide.

On the slide, the new task being created will use the report generated by the previous task to add it to an incident.

Trigger variables allow you to use information from the trigger of a playbook when it has been configured with an incident or event trigger. For example, a single playbook can be triggered by more than one device. A **Run Report** action can include a filter for the endpoint IP address from the event that triggered the playbook.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What is the purpose of an output variable?
 - A. To use the input of one task as the output of another task
 - B. To use the output of one task as the input of another task

2. What is the first thing that you need to configure when creating a playbook from scratch?
 - A. The connector type that will be used
 - B. The trigger type that will be used



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 20

DO NOT REPRINT

© FORTINET

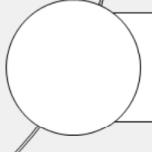
Lesson Progress



Playbook Components



Creating Playbooks



Managing Playbooks

Good job! You now know how to create playbooks and use them to automate tasks.

Now, you will learn how to manage playbooks.

DO NOT REPRINT

© FORTINET

Managing Playbooks

Objectives

- Monitor playbooks
- Export and import playbooks



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

22

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

By demonstrating competence in monitoring playbooks, you will be able to identify whether all automated tasks ran successfully. You will also be able to export playbooks to another ADOM or device.

DO NOT REPRINT

© FORTINET

Running Playbooks

Incidents & Events > Automation > Playbook

After a playbook runs, the **Playbook Tasks** page shows the playbook details, timeline, and raw logs.

Playbook Tasks

Playbook ▾

Job ID	2025-05-21 14:20:16.339791-07
Playbook	Lab6_On_Demand_Playbook
Trigger	user(admin)
Start Time	2025-05-21 14:20:23-0700
End Time	2025-05-21 14:20:28-0700
Status	Failed

Timeline ▾

```

graph TD
    A[On_Demand Starter] --> B[Lab6_Create_Incident]
    B --> C[Lab6_Create_Incident]
    
```

Raw Log - Lab6_Create_Incident ▾

```

[2025-05-21T14:20:24.384-0700] {task_command.py:426} INFO - Running <TaskInstance: 198_940a5571-6f39-4
[2025-05-21T14:20:24.514-0700] {taskinstance.py:2905} ERROR - Task failed with exception
ValueError: invalid literal for int() with base 10: 'abc'
[2025-05-21T14:20:24.582-0700] {standard_task_runner.py:110} ERROR - Failed to execute job 10036 for t
    
```

Playbook Tasks

Playbook ▾

Job ID	2025-06-03 07:23:38.325098-07
Playbook	Indicator Enrichment
Trigger	user(admin)
Start Time	2025-06-03 07:23:41-0700
End Time	2025-06-03 07:23:51-0700
Status	Success

Timeline ▾

```

graph TD
    A[On_Demand Starter] --> B[Enrichment start]
    B --> C[VirusTotal enrichment]
    C --> D[FortGuard enrichment]
    
```

Raw Log - Enrichment start ▾

```

[2025-06-03T07:23:41-0700] [task_command.py:426] INFO - Running <TaskInstance: 199_855de9b3-c407-404c-8d60-1f7
[2025-06-03T07:23:41-0700] [base.py:84] INFO - Using connection ID 'redis' for task execution.
[2025-06-03T07:23:41-0700] [base.py:84] INFO - Using connection ID 'redis' for task execution.
[2025-06-03T07:23:41-0700] [base.py:84] INFO - Using connection ID 'redis' for task execution.
[2025-06-03T07:23:41-0700] [base.py:84] INFO - Using connection ID 'redis' for task execution.
[2025-06-03T07:23:41-0700] [base.py:84] INFO - Using connection ID 'redis' for task execution.
    
```

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 23

After you run a playbook, the **Playbook Tasks** page opens showing details such as the job ID, the playbook start and end times, and the status of the playbook.

You also see the playbook timeline and the raw logs of the playbook as it was running.

This slide shows two examples of a playbook after it was run: once when it failed and once when it was successful.

DO NOT REPRINT

© FORTINET

Monitoring Playbooks

- To see the details of a playbook job, click **Details** and then **View Log**

Incidents & Events > Automation > Playback Monitor

Playbook	Trigger	Start Time	Status	Details
Create 2 Incidents	user(admin)	2023-10-17 15:07	failed(Scheduled:0/Running:0/Success:1/Failed:1)	

Task ID	Task	Start Time	End Time	Status
placeholder_7a3688b5_fca3_4bad	Create Incident 1	2023-10-17 15:07:14-0700	2023-10-17 15:07:15-0700	failed
placeholder_9ad9c67b_7957_48a	Create Incident 2	2023-10-17 15:07:14-0700	2023-10-17 15:07:15-0700	success


```
[2023-10-17T15:07:15.076-0700] {taskinstance.py:1824} ERROR - Task failed with exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 223, in execute
    self.euid = int(FAZUtilsOperator.parse_input(context, self.euid, context_dict))
TypeError: int() argument must be a string, a bytes-like object or a number, not 'NoneType'
[2023-10-17T15:07:15.158-0700] {standard_task_runner.py:104} ERROR - Failed to execute job 16119 for task placeholder_7a3688b5_fca3_4bad_88cf_b448da08cde2 (int()) argument must be a string, a bytes-like object or a number, not 'NoneType'; 21500
```

This playbook has two tasks: one task ran successfully, but the other one failed

This playbook failed because one task was expecting a value for the euid field, but it received nothing

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 24

When troubleshooting playbooks, it is very useful to review their logs. Details about the execution of a playbook job are available in the associated log.

The status of a playbook can be one of the following:

- Running
- Success
- Failed

To see detailed logs, go to **Playback Monitor**, select the desired entry, click the **Details** icon, and then click **View Log**.

Playbook jobs that include one or more failed tasks are labeled as **Failed** in **Playback Monitor**. However, a failed status does not mean that all tasks failed. Some individual actions may have completed successfully.

In the example shown on the slide, the playbook has two tasks configured and only the task, named `Create Incident 1`, failed to run. Therefore, the playbook job is considered to have failed. The specific reason for the failure in the example is that the end user ID field expects a value; however, none was provided.

DO NOT REPRINT
© FORTINET

Exporting Playbooks

- Playbooks are defined per ADOM
- Export the playbooks that are to be used in a different ADOM or device
- The connectors can be included in the exported file
- The resulting file uses a JSON format
 - You can choose to compress the file



Playbooks are defined per ADOM. If you want to use an existing playbook on a different ADOM or a different FortiAnalyzer device, you can export the playbook.

To export a playbook, right-click the playbook, and then click **Export**. You can export more than one playbook at the same time by selecting multiple playbooks. The **Export Playbook** window opens.

Configure the settings to export the selected playbook:

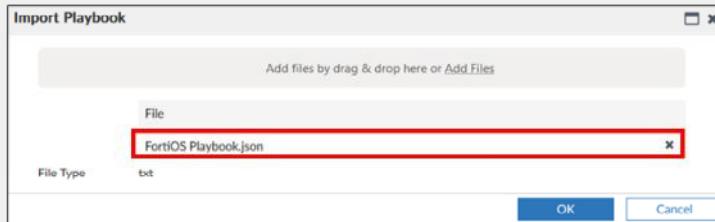
- **Do you want to include Connector:** When this setting is enabled, connectors required to run this playbook will be included in the exported file. This is recommended, for example, if a non-default connector like the EMS connector is configured, so that all required components are included in the resulting file.
- **Select Export Data Type:** Select the export file type as either plain text JSON or zipped/base 64 encoded JSON.

If you must be able to read the contents of the JSON file in plain text, you must choose the text version during the export process.

DO NOT REPRINT**© FORTINET**

Importing Playbooks

- Import a previously exported playbook on the destination ADOM or device



To import a playbook, right-click anywhere on the playbook dashboard, and then click **Import**.

The **Import Playbook** window opens. Browse to select the playbook file that you want to import.

If the imported playbook has the same name as an existing playbook, to avoid conflicts, FortiAnalyzer will create a new name that includes a timestamp.

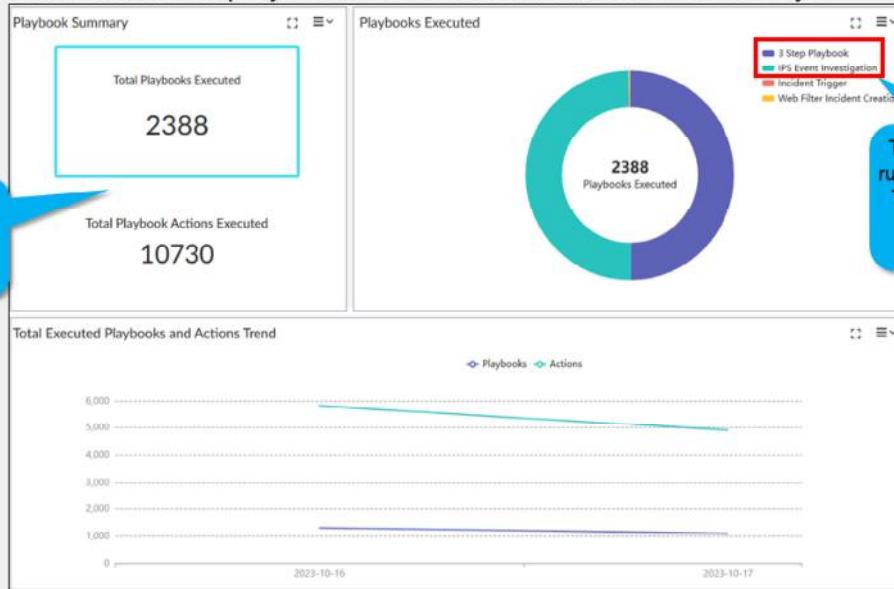
Playbooks are imported with the same status they had (enabled or disabled) when they were exported. Playbooks set to run automatically should be exported while they are disabled, to prevent the playbook from unintentionally running on the destination.

DO NOT REPRINT

© FORTINET

Playbooks Dashboard

- This dashboard tracks all playbooks executed in the last seven days



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 27

These two playbooks have run more times than the rest. This could be normal, or it could be due to a misconfiguration

The **Playbooks** dashboard includes information organized and presented in these categories: **Total Playbooks Executed**, **Total Playbook Actions Executed**, **Playbooks Executed**, and **Total Executed Playbooks and Actions Trend**.

This dashboard shows all the playbooks that have been executed in the last seven days, including their names and the total number of actions performed. This information gives you an idea of how much time has been saved by automating tasks.

In the example shown on this slide, 2388 playbooks have been executed; however, 10,730 actions have been taken. This shows that one or more of the playbooks listed have more than one action configured. The image also shows the names of the most executed playbooks. It is the responsibility of the SOC analyst to ensure playbooks are correctly configured so they run only when required.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. When is the execution of a playbook with three tasks considered to have failed?
 - A. When all three tasks fail
 - B. When any of the three tasks fail

2. At what level are playbooks created?
 - A. Per ADOM
 - B. Per device



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 28

DO NOT REPRINT

© FORTINET

Lesson Progress



Playbook Components



Creating Playbooks



Managing Playbooks

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe FortiAnalyzer automation capabilities
- ✓ Describe playbook concepts
- ✓ Describe trigger types and characteristics
- ✓ Describe connector types
- ✓ Create new playbooks
- ✓ Use variables in tasks
- ✓ Monitor playbooks
- ✓ Export and import playbooks



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 30

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

By mastering the objectives covered in this lesson, you learned what playbooks are and how you to create them to automate tasks in FortiAnalyzer. You also learned how to monitor and manage playbooks.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiAnalyzer Analyst

FortiOS Logging

 FortiAnalyzer 7.6

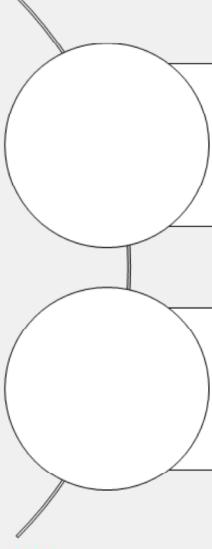
Last Modified: 16 July 2025

This supplemental material provides an overview of the log workflow and how logging works on FortiGate.

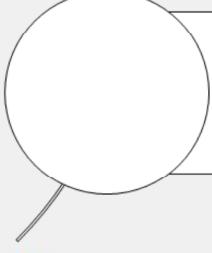
DO NOT REPRINT

© FORTINET

Lesson Overview



Log Basics



Storage Options

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT

© FORTINET

Log Basics

Objectives

- Describe the log workflow
- Identify log types and subtypes
- Describe log severity levels
- Describe the layout of a log message



© Fortinet Inc. All Rights Reserved.

3

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

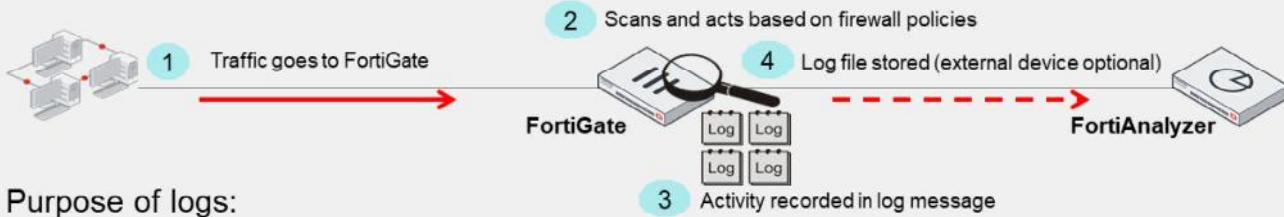
By demonstrating competence in FortiAnalyzer logs and their structure, you will be able to use logs properly to obtain information about your FortiAnalyzer device.

DO NOT REPRINT

© FORTINET

Logging Workflow

1. Traffic passes through FortiGate
2. FortiGate scans the traffic and acts based on configured firewall policies
3. FortiGate records the activity and stores the information in a log message
4. FortiGate adds the log message to a log file on a device capable of storing logs (local FortiGate device or an external device, such as FortiAnalyzer)



- Purpose of logs:
 - Monitor network and internet traffic volume
 - Diagnose problems
 - Establish normal baselines to recognize anomalies and trends

When traffic passes through FortiGate, FortiGate scans the traffic and then acts based on the firewall policies in place. FortiGate records this activity and stores the information in a log message. The log message is stored in a log file, which is then stored on a device capable of storing logs. FortiGate can store logs locally or send them to an external storage device, such as FortiAnalyzer.

Logs help you monitor your network traffic, locate problems, establish baselines, and more. Logs give you valuable insight into your network, enabling you to adjust your network security as needed.

Some organizations have legal requirements regarding logging, so it is important to be aware of your organization's policies during configuration.

For effective logging, your FortiGate system date and time should be accurate. You can either manually set the system date and time or configure FortiGate to keep its time correct automatically by synchronizing with a Network Time Protocol (NTP) server. Fortinet recommends the use of an NTP server.

DO NOT REPRINT

© FORTINET

Log Types and Subtypes

- *Traffic* logs record traffic flow information, such as an HTTP/HTTPS request and its response (if any)
- *Event* logs record system and administrative events, such as adding or modifying a setting, or daemon activities
- *Security* logs record security events, such as virus attacks and intrusion attempts, based on the security profile type (log type = utm)
 - If no security logs exist, the menu item does not appear in the GUI

Traffic	Event	Security
Forward	Endpoint control	Application control
Local	High availability	Antivirus
Sniffer	System	Data loss prevention (DLP)
	User	Antispam
	Router	Web filter
	VPN	Intrusion prevention system (IPS)
	WAD	Anomaly (DoS policy)
	Wireless	Web application firewall (WAF)

WAN optimization logs are found within traffic logs

GPRS Tunneling Protocol (GTP) logs are handled separately from default event logs

FortiGate has three types of logs: traffic, event, and security. Each type is divided into subtypes.

Traffic logs record traffic flow information, such as an HTTP/HTTPS request and its response. It contains the subtypes forward, local, and sniffer:

- Forward traffic logs contain information about traffic that FortiGate either accepted or rejected according to a firewall policy.
- Local traffic logs contain information about traffic sent directly to and from the FortiGate management IP addresses. They also include connections to the GUI and FortiGuard queries.
- Sniffer logs contain information related to traffic seen by the one-arm sniffer.

Event logs record system and administrative events, such as adding or modifying a setting, or daemon activities. Event logs contain subtypes named endpoint control, high availability, system, user, router, VPN, WAD, and wireless:

- System event logs contain information related to operations, such as automatic FortiGuard updates and GUI logins.
- User logs contain logon and logoff events for firewall policies with user authentication.
- Router, VPN, WAD, and wireless subtypes include logs for those features. For example, VPN contains IPsec and SSL VPN log entries.

Security logs record security events, such as virus attacks and intrusion attempts. They contain log entries based on the security profile type (log type = utm), including application control, antivirus, DLP, anti-spam (email filter), web filter, intrusion protection, anomaly (DoS-policy), and WAF. Security logs and subtypes are visible in the GUI only if logs are created within it—if no security logs exist, the menu item does not appear.

DO NOT REPRINT**© FORTINET**

Log Severity Levels

- Each log entry includes a log level (also known as priority level) that ranges in order of importance
 - 0 = high importance / 6 = low importance

Levels	Description
0 – Emergency	System unstable
1 – Alert	Immediate action required
2 – Critical	Functionality effected
3 – Error	Error exists that can affect functionality
4 – Warning	Functionality could be affected
5 – Notification	Information about normal events
6 – Information	General system information
7 – Debug	Diagnostic information for investigating issues

Rarely used, unless actively investigating an issue with Fortinet Support

Each log entry includes a log level (or priority level) that ranges in order of importance from Emergency to Information.

The Debug level adds diagnostic information to an event log. It is rarely used unless you are actively investigating an issue with Fortinet Support.

Generally, the lowest log level you should use is Information, but even this level generates many logs and can cause premature hard disk failure. Depending on the type of log and your organization's needs, you may want to use only Notification logs or higher.

DO NOT REPRINT**© FORTINET**

Log Message Layout

- Log header (similar in all logs)

- Type and subtype = Name of log file

- Level = Severity level

```
date=2016-06-14 time=12:05:28 logid=0316013056 type=utm subtype=webfilter
eventtype=ftgd_blk level=warning vd=root
```

- Log body (varies by log type)

- policyid = Firewall policy applied to session
- hostname = URL or IP of host

- srcip and dstip = Source and destination IP address
- action = Action taken by FortiGate
- msg = Reason for the action

```
policvid=1 sessionid=10879 user="" srcip=10.0.1.10 srcport=60952 srcintf="port3"
dstip=52.84.14.233 dstport=80 dstintf="port1" proto=6 service="HTTP"
hostname="miniclip.com" profile="default" action=blocked reqtype=direct
url="/favicon.ico" sentbyte=297 rcvdbyte=0 direction=outgoing
msg="URL belongs to a denied category in policy" method=domain cat=20 catdesc="Games"
crscore=30 crlevel=high
```

Every log message has a standard layout comprising two sections: a header and a body.

The header contains fields that are common to all log types, such as originating date and time, log identifier, log category, severity level, and VDOM. The value of each field is specific to the log message. In the raw log entry example shown on this slide, the log type is UTM, the subtype is webfilter, and the level is warning. The type and subtype of logs determine which fields appear in the log body.

The body, therefore, describes the reason the log was created and the actions that FortiGate took. These fields vary by log type. In the example shown on this slide, the fields are as follows:

- The **policyid** field indicates which firewall rule matched the traffic.
- The **srcip** field indicates the source IP address.
- The **dstip** field indicates the destination IP address.
- The **hostname** field indicates the URL or IP of the host.
- The **action** field indicates what FortiGate did when it found a policy that matched the traffic.
- The **msg** field indicates the reason for the action taken. In this example, the action is **blocked**, which means that FortiGate prevented this IP packet from passing, and the reason is that it belongs to a denied category in the firewall policy.

If you log onto a third-party device, such as a syslog server, knowing the log structure is crucial to integration. For information on log structures and associated meanings, visit <http://docs.fortinet.com>.

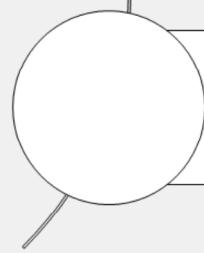
DO NOT REPRINT

© FORTINET

Lesson Progress



Log Basics



Storage Options

Good job! You now understand the basics of logging on FortiGate devices.

Now, you will learn about log storage options.

DO NOT REPRINT

© FORTINET

Storage options

Objectives

- Configure external log storage options
- Describe how remote logging works with VDOMs
- Describe log transmission

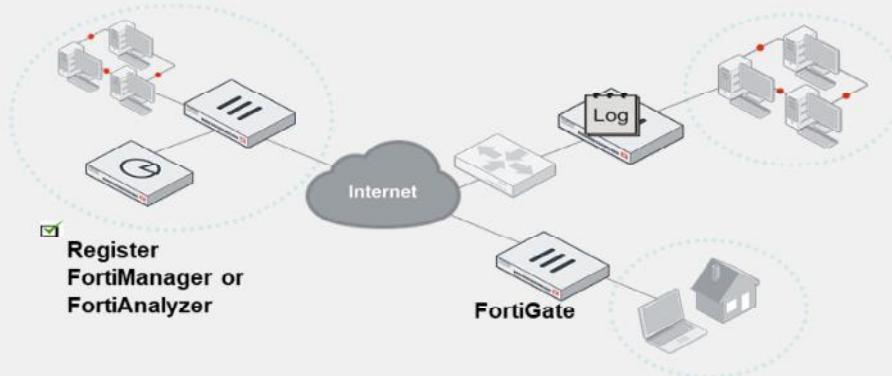
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the most common functions and operators used in FortiAnalyzer datasets, you will be able to configure appropriate storage options.

DO NOT REPRINT**© FORTINET**

Log Storage—Remote

- FortiGate can send logs to both FortiAnalyzer and FortiManager (FortiGate must be a registered device)



- Configure up to three separate FortiAnalyzer and FortiManager devices using the CLI
 - Multiple devices may be needed for redundancy
 - Generating and sending logs requires resources—be aware!

Configuring FortiGate to send logs to either FortiAnalyzer or FortiManager (with FortiAnalyzer features enabled) is the same. To enable FortiGate to send logs to these devices, you must register FortiGate with FortiAnalyzer or FortiManager. Once registered, FortiAnalyzer or FortiManager can begin accepting incoming logs from FortiGate.

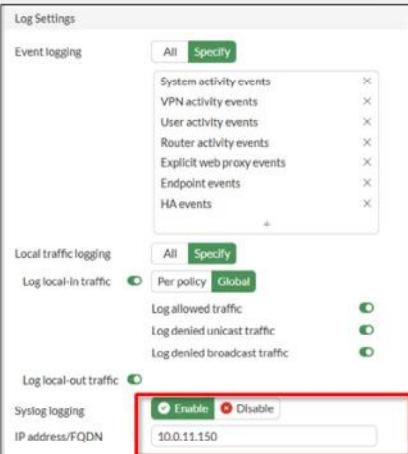
Note that the **Test Connectivity** function on the GUI will indicate a failure until FortiGate is registered on FortiAnalyzer or FortiManager, because it has not yet been authorized to send logs.

DO NOT REPRINT
© FORTINET

Configure FortiAnalyzer Logging

- GUI:

Log & Report > Log Settings



- CLI:

```
# config log [fortianalyzer|fortianalyzer2|fortianalyzer3] setting
set status enable
set server <server_IP>
end
```

Commands are not cumulative

You can configure remote logging to FortiAnalyzer or FortiManager using either the GUI or the CLI.

- GUI: On the **Log Settings** page, enable **Syslog logging**, and then type the IP address of the remote logging device.
- CLI: For both FortiAnalyzer and FortiManager, use the `config log fortianalyzer setting` command. Even though FortiManager isn't explicitly mentioned in the command, it is used for FortiManager as well. Using the CLI, you can add up to three separate devices to increase redundancy for the protection of log data. The commands for the three devices are not cumulative. Generating logs uses system resources, so if FortiGate frequently creates and sends logs to multiple locations, CPU and RAM usage increase.

DO NOT REPRINT

© FORTINET

Upload Option

- Near real-time uploading and consistent high-speed compression and analysis
- Configure logging options:
 - store-and-upload (CLI configuration only)
 - **Real Time**
 - **Every Minute**
 - **Every 5 Minutes** (default)

```
# configure log fortianalyzer setting  
set upload-option [store-and-upload |realtime/1-minute/5-minute]
```

store-and-upload
available only on
FortiGate devices that
have an internal hard
drive

- By default, if the FortiAnalyzer disk is full, the oldest logs are overwritten; however, you can configure FortiAnalyzer to stop logging

FortiGate allows near real-time uploading and consistent high-speed compression and analysis to FortiAnalyzer and FortiManager.

If your FortiGate model includes an internal hard drive, the `store-and-upload` option is available. This allows you to store logs on the disk and then upload them to FortiAnalyzer or FortiManager at a scheduled time (usually a low-bandwidth time). You can configure the `store-and-upload` option and a schedule on the CLI only.

DO NOT REPRINT
© FORTINET

VDOMs and Remote Logging

- On a FortiGate with VDOMs configured, you can globally add multiple FortiAnalyzer devices and syslog servers
 - Up to three FortiAnalyzer devices
 - Up to four syslog servers



```
config global
  config log fortianalyzer
    setting
      set status enable
      set server 10.0.1.1
    end
  config log fortianalyzer2
    setting
      set status enable
      set server 10.0.2.1
    end
```

If override of FortiAnalyzer
or syslog is needed,
enable it at the vdom level

```
# config vdom
  edit Training
    config log setting
      set faz-override enable
      set syslog-override enable
    end
```

A FortiGate with VDOMs configured can support multiple FortiAnalyzer devices and syslog servers. In the global settings, you can configure up to three FortiAnalyzer devices and up to four syslog servers.

DO NOT REPRINT
© FORTINET

VDOMs and Remote Logging (Contd)

- In each VDOM, you can override the global settings to configure up to 3 override FortiAnalyzer devices and up to 4 override syslog servers for that VDOM
- After you enable override, you can use the CLI to configure multiple FortiAnalyzer devices or syslog servers for the VDOM
 - The management VDOM sends logs to FortiAnalyzer
- If you use the override setting in a VDOM, then that VDOM sends logs to the new FortiAnalyzer or syslog server

Training VDOM

```
# config log
fortianalyzer/fortianalyzer2/fortianalyzer3
override-setting
```

```
# config log syslogd/syslogd2/syslogd3/syslogd4
override-setting
```

Three FortiAnalyzer
devices and four syslog
servers under VDOM

Training VDOM

```
(Training) # show log fortianalyzer override-setting
config log fortianalyzer override-setting
  set status enable
  set server "10.0.3.1"
end
```

For each VDOM, you can override the global settings to configure up to three override FortiAnalyzer devices and up to four override syslog servers.

The management VDOM is responsible for sending logs to FortiAnalyzer devices and syslog servers. Therefore, if you use the override setting in a VDOM, that VDOM is responsible for sending logs to the new FortiAnalyzer or syslog server you configured for it.

DO NOT REPRINT**© FORTINET**

Reliable Logging

- Changes the log transport delivery method from UDP to TCP
- TCP provides reliable data transfer
 - Acknowledgement segments to ensure the packet is received
 - Connection-oriented protocol (SYN, SYN-ACK, ACK handshake)
- If you enable logging to FortiAnalyzer using the GUI, reliable logging is auto-enabled
 - If you enable logging to FortiAnalyzer using the CLI, reliable logging is not auto-enabled. You must manually enable using the CLI command:

```
# config log fortianalyzer setting  
    set reliable [enable/disable]
```

```
# config log syslogd setting  
    set mode udp | reliable | legacy-reliable
```

- FortiCloud uses TCP, and you can set the encryption algorithm using the CLI (default setting is high)



© Fortinet Inc. All Rights Reserved. 15

When you enable reliable logging on FortiGate, the log transport delivery method changes from UDP to TCP. TCP provides reliable data transfer, guaranteeing that the data transferred remains intact and arrives in the same order in which it was sent.

If you enable logging to FortiAnalyzer or FortiManager using the GUI, reliable logging is automatically enabled. If you enable logging using the CLI, you must enable reliable logging using the CLI command shown on this slide.

Logging to FortiCloud uses TCP, and you can set the encryption algorithm using the CLI (the default setting is high).

DO NOT REPRINT**© FORTINET**

OFTPS

- Encrypt communications using SSL-secured Optimized Fabric Transfer Protocol (OFTP/OFTPS)

```
# config log fortianalyzer setting
  set status enable
  set enc-algorithm [high-medium | high | low]
  set reliable enable
end
```

Reliable logging
must be enabled to
use OFTPS

Optionally, if you use reliable logging, you can encrypt communications with SSL-encrypted OFTP traffic, ensuring that when a log message is generated, it is transmitted securely across an unsecured network. You can encrypt communications with SSL-secured OFTP by configuring the enc-algorithm setting on the CLI.

DO NOT REPRINT

© FORTINET

Lesson Progress



Log Basics



Storage Options

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 17

Congratulations! You completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe the log workflow
- ✓ Identify log types and subtypes
- ✓ Describe log severity levels
- ✓ Describe the layout of a log message
- ✓ Configure external log storage options
- ✓ Describe how remote logging works with VDOMs
- ✓ Describe log transmission

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

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.