New Features Guide

FortiAnalyzer 7.4.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 26, 2024
FortiAnalyzer 7.4.0 New Features Guide
05-740-898228-20240326

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-05-15	Initial release.
2023-05-16	Added: • Per-ADOM log rate on page 76 • Fabric of FAZ: Central report support and creating Fabric groups on page 143
2023-05-19	Added: • Webhook Connector to Support MS Teams on page 13 • Report guidance on page 93 • CIS Controls Security Rating report on page 100
2023-05-31	Added Operational Technology on page 156.
2023-06-16	Added: • FortiSoC GUI reorganization on page 46 • New charts in the Asset Identity Center on page 44 • Shadow IT Report on page 101 • Time zone settings per ADOMs/Reports on page 115
2023-06-21	Added Fluentd support for public cloud integration on page 89.
2023-06-30	Added Operational Technology (OT) Security Service on page 156.
2023-07-17	Updated Time zone settings per ADOMs/Reports on page 115.
2023-08-31	Initial release of FortiAnalyzer 7.4.1.
2023-09-06	Added MITRE ATT&CK matrices for Enterprise and ICS 7.4.1 on page 51.
2023-09-14	Updated Webhook Connector to Support MS Teams on page 13.
2023-09-26	Added Geo-redundant High Availability (HA) on page 121.
2023-10-04	Updated MITRE ATT&CK matrices for Enterprise and ICS 7.4.1 on page 51.
2023-10-11	Updated Shadow IT Report on page 101.
2023-10-13	Added FortiManager and FortiAnalyzer support HTTP/2 for improved security, multiplexing, and reduced network latency 7.4.1 on page 148.
2023-10-20	Added: • Licensing adjustment on page 164 • New API to restore logs on page 118 • Playbook event trigger correleation rules 7.4.1 on page 19 • SD-WAN Cloud Assisted Monitoring service widgets 7.4.1 on page 31 • Support parsing and addition of third-party application logs to the SIEM DB in JSON format 7.4.1 on page 84

Date	Change Description
2023-11-01	Added Exporting a report with settings 7.4.1 on page 108.
2023-11-24	Added: • FortiEDR Report 7.4.1 on page 105 • ISO 27001:2022 Compliance Security Rating Report 7.4.1 on page 107 • FortiAnalyzer supports packet header information for FortiWeb traffic log 7.4.1 on page 86
2023-12-21	Initial release of FortiAnalyzer 7.4.2.
2024-01-24	Added: • Data leak prevention monitor in FortiView 7.4.1 on page 35 • HIPAA report 7.4.2 on page 114 • Compromised hosts improvements 7.4.2 on page 40 • Per-ADOM admin profile 7.4.2 on page 127
2024-02-02	Added: • New predefined correlation event handlers on page 20 • FortiProxy central visibility 7.4.1 on page 38 • Replay attacks in the Threat Map 7.4.2 on page 42 • Update to the Event Handler rule configuration 7.4.2 on page 26
2024-03-07	Added • Deliver reports, event handlers, and SIEM rules as FortiGuard packages 7.4.2 on page 62 • Support additional log fields for long live session logs 7.4.2 on page 88
2024-03-26	Added: • Reference individual fabric devices 7.4.1 on page 9 • DLP report 7.4.1 on page 110 • PCI DSS security rating report update 7.4.1 on page 112 • MITRE information included in outbreak detection 7.4.2 on page 66

Overview

This guide provides details of new features introduced in FortiAnalyzer 7.4. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable.

The FortiAnalyzer new features are organized into the following categories:

- Security Fabric on page 9
- Fabric View on page 13
- Security Operations (SOC) on page 19
- Log and Report on page 69
- System on page 121
- Cloud Services on page 152
- Operational Technology on page 156
- Other on page 164

For a list of all features organized by the version number that they were introduced, see Index on page 167.

Security Fabric

This section lists the new features added to FortiAnalyzer for Security Fabric:

- Others on page 9

Others

This section lists the new features added to FortiAnalyzer for other topics relating to Security Fabric:

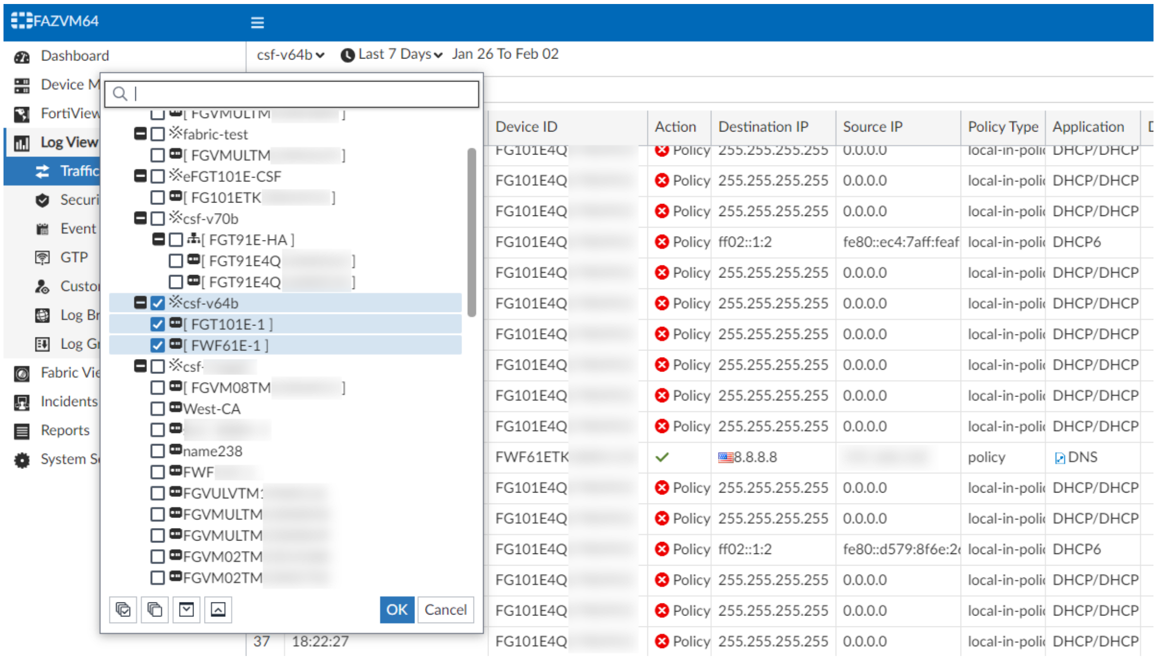
- Reference individual fabric devices 7.4.1 on page 9

Reference individual fabric devices - 7.4.1

You can now refer to individual devices or to the full fabric when filtering by device in *LogView*, *FortiView*, and *Reports*.

To select fabric devices in LogView:

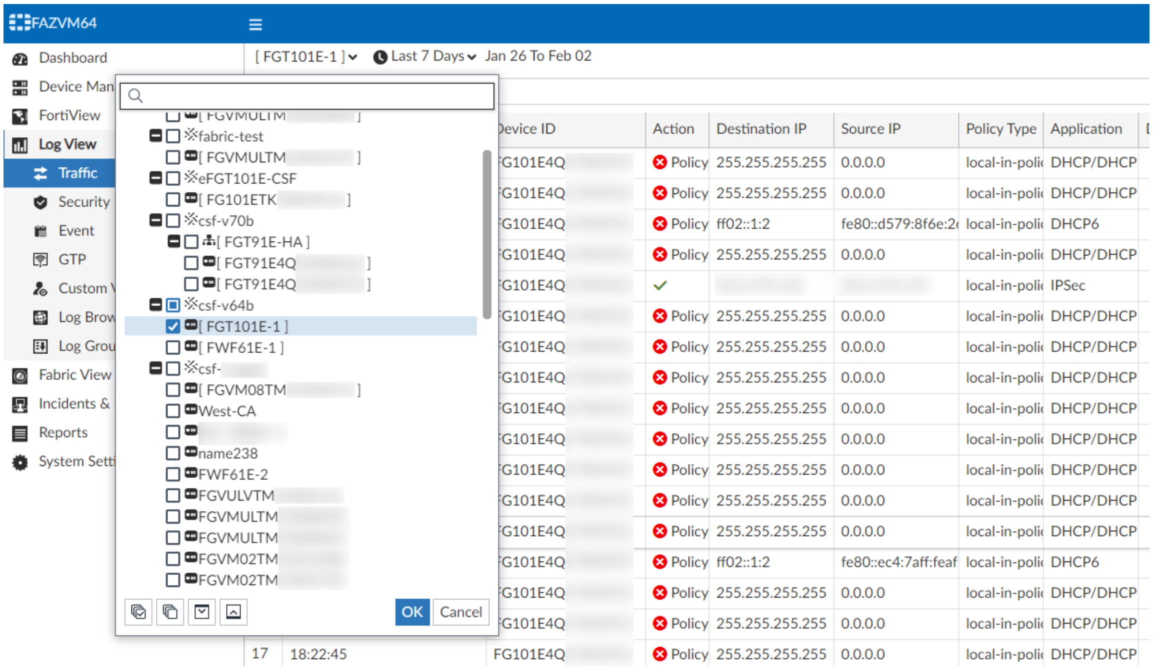
1. In *LogView*, click the device dropdown. In this example, the admin uses *LogView* > *Traffic*.
2. Select the security fabric name to select the entire fabric security. Logs are filtered accordingly.



□ [FGVMULTM [redacted]]
□ fabric-test
  □ [FGVMULTM [redacted]]
□ eFGT101E-CSF
  □ [FG101ETK [redacted]]
□ csf-v70b
  □ [FGT91E-HA]
    □ [FGT91E4Q [redacted]]
    □ [FGT91E4Q [redacted]]
☑ csf-v64b
  ☑ [FGT101E-1]
  ☑ [FWF61E-1]
□ csf-[redacted]
  □ [FGVM08TM [redacted]]
  □ West-CA
  □ [redacted]
  □ name238
  □ FWF[redacted]
  □ FGVULVTM[redacted]
  □ FGVMULTM[redacted]
  □ FGVMULTM[redacted]
  □ FGVM02TM[redacted]
  □ FGVM02TM[redacted]

Device ID	Action	Destination IP	Source IP	Policy Type	Application	D
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	ff02::1:2	fe80::ec4:7aff:feaf	local-in-poli	DHCP6	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FWF61ETK[redacted]	✓	8.8.8.8	[redacted]	policy	DNS	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	ff02::1:2	fe80::d579:8f6e:2	local-in-poli	DHCP6	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	
FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-poli	DHCP/DHCP	

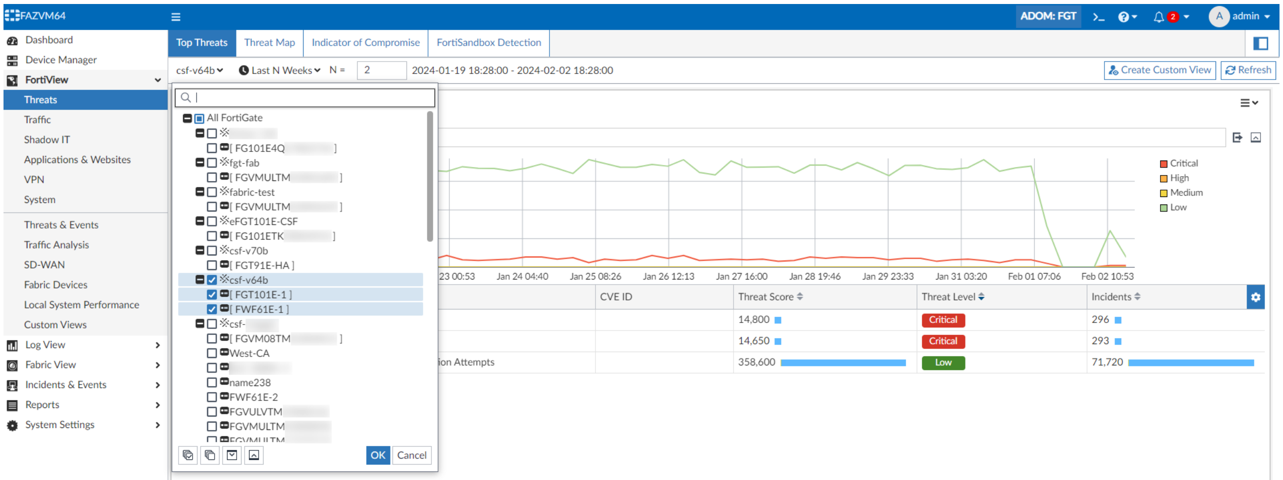
3. Alternatively, select devices within the fabric separately. Logs are filtered accordingly.



		Device ID	Action	Destination IP	Source IP	Policy Type	Application
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	ff02::1:2	fe80::d579:8f6e:2(	local-in-polic	DHCP6
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	✓	[redacted]	[redacted]	local-in-polic	IPSec
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	ff02::1:2	fe80::ec4:7aff:feaf	local-in-polic	DHCP6
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
		G101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP
17	18:22:45	FG101E4Q[redacted]	☒ Policy	255.255.255.255	0.0.0.0	local-in-polic	DHCP/DHCP

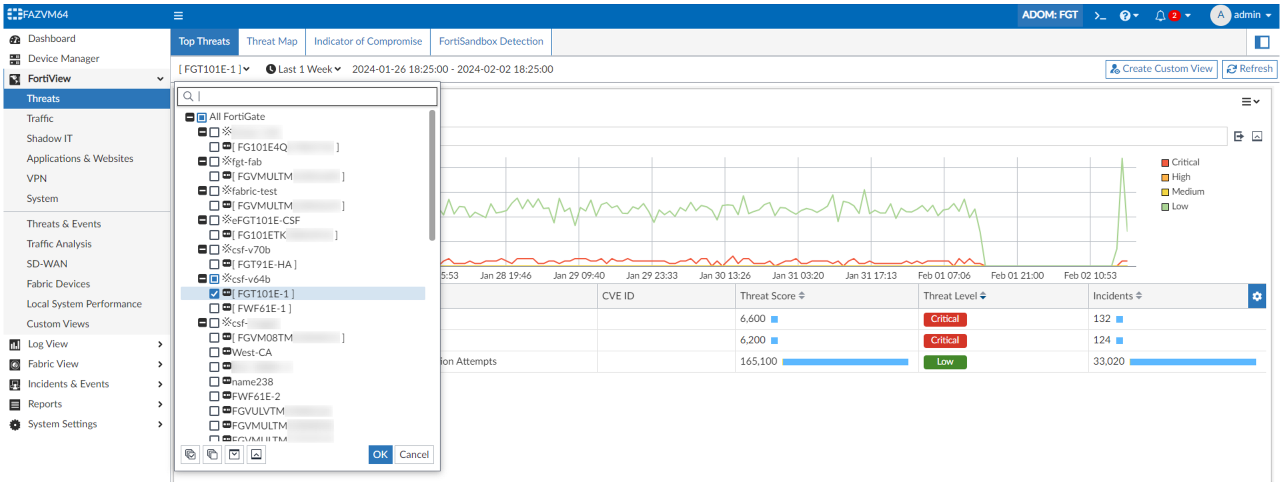
To select fabric devices in FortiView

1. In a *FortiView* dashboard, click the device dropdown. In this example, the admin uses *FortiView* > *Threats* > *Top Threats*.
2. Select the security fabric name to select the entire fabric security. Data is filtered accordingly.



	CVE ID	Threat Score	Threat Level	Incidents
		14,800	Critical	296
		14,650	Critical	293
ion Attempts		358,600	Low	71,720

3. Alternatively, select devices within the fabric separately. Data is filtered accordingly.



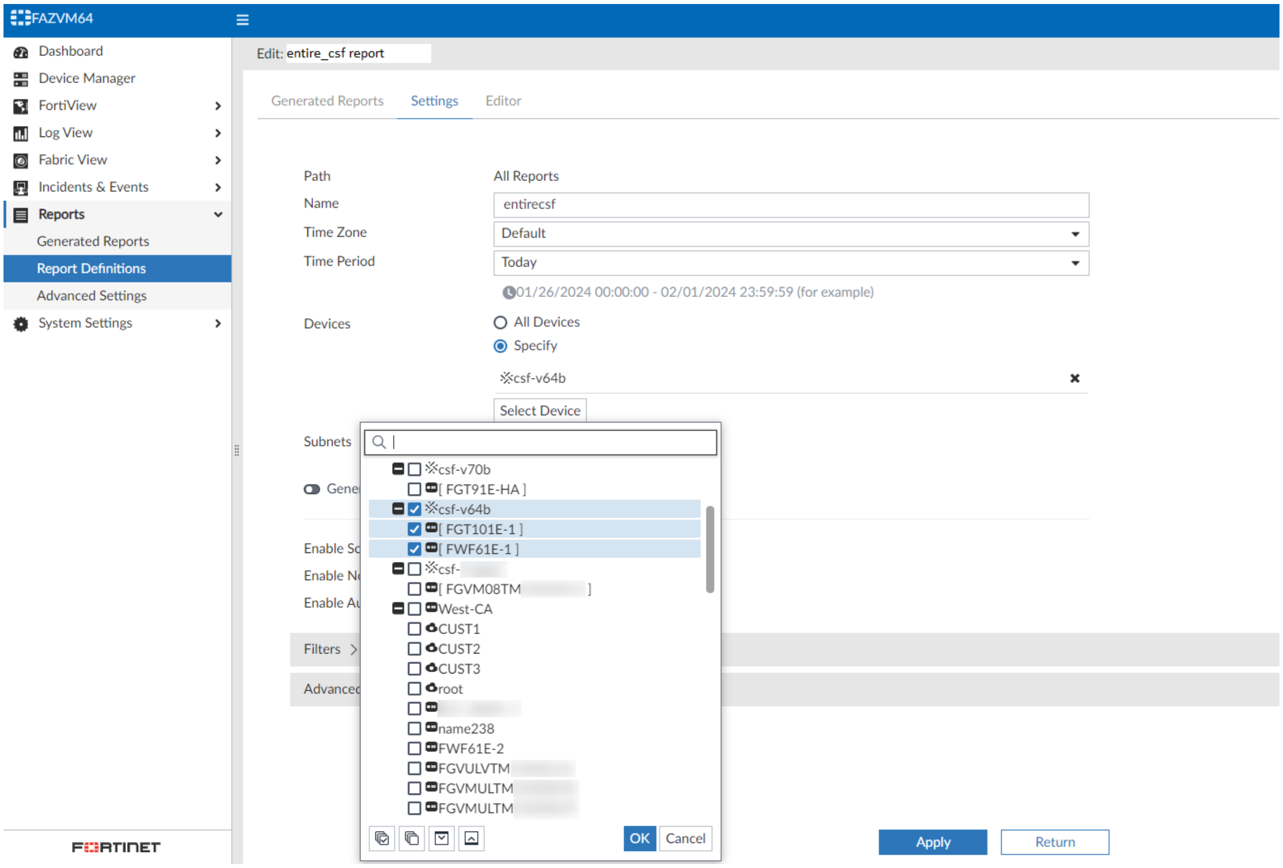
[FGT101E-1] Last 1 Week 2024-01-26 18:25:00 - 2024-02-02 18:25:00

- ▣ All FortiGate
  - □ [redacted]
    - □ [FG101E4Q [redacted]]
  - □ fgt-fab
    - □ [FGVMULTM [redacted]]
  - □ fabric-test
    - □ [FGVMULTM [redacted]]
  - □ eFGT101E-CSF
    - □ [FG101ETK [redacted]]
  - □ csf-v70b
    - □ [FGT91E-HA]
  - ▣ csf-v64b
    - ☑ [FGT101E-1]
    - □ [FWF61E-1]
  - □ csf- [redacted]
    - □ [FGVM08TM [redacted]]
    - □ West-CA
    - □ [redacted]
    - □ name238
    - □ FWF61E-2
    - □ FGVULVTM [redacted]
    - □ FGVMULTM [redacted]
    - □ FGVMULTM

	CVE ID	Threat Score	Threat Level	Incidents
		6,600	Critical	132
		6,200	Critical	124
ion Attempts		165,100	Low	33,020

To select fabric devices in Reports:

1. In *Report Definitions*, select a report and click *Edit*.
2. Go to the *Settings* tab.
3. For the *Devices* field, select *Specify* and click the device dropdown.
4. Select the security fabric name to select the entire fabric security. After the changes are applied, a report for the complete security fabric can be generated.

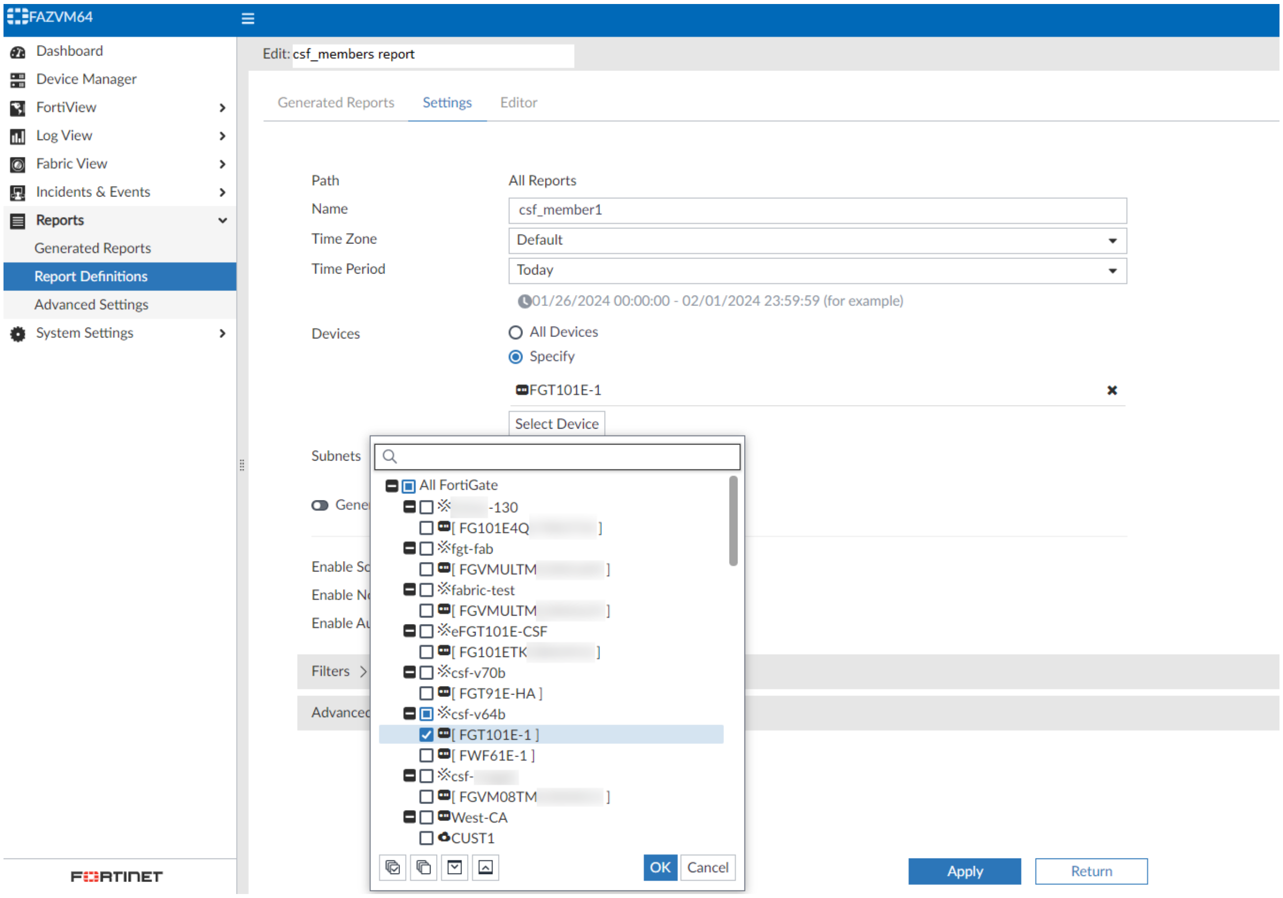


Edit: entire_csf report

Path	All Reports
Name	entirecsf
Time Zone	Default
Time Period	Today
	01/26/2024 00:00:00 - 02/01/2024 23:59:59 (for example)
Devices	○ All Devices ● Specify csf-v64b
Subnets	

- □ csf-v70b
  - □ [FGT91E-HA]
- ☑ csf-v64b
  - ☑ [FGT101E-1]
  - ☑ [FWF61E-1]
- □ csf- [redacted]
  - □ [FGVM08TM [redacted]]
- □ West-CA
  - □ CUST1
  - □ CUST2
  - □ CUST3
  - □ root
- □ [redacted]
- □ name238
- □ FWF61E-2
- □ FGVULVTM [redacted]
- □ FGVMULTM [redacted]
- □ FGVMULTM [redacted]

5. Alternatively, select devices within the fabric separately. Data is filtered accordingly. After the changes are applied, a report for the selected devices can be generated.



Edit: csf_members report

Path	All Reports
Name	csf_member1
Time Zone	Default
Time Period	Today
	01/26/2024 00:00:00 - 02/01/2024 23:59:59 (for example)
Devices	○ All Devices ● Specify FGT101E-1 ✖ Select Device

- ☐ All FortiGate
  - ☐ [redacted]-130
    - ☐ [FG101E4Q[redacted]]
  - ☐ fgt-fab
    - ☐ [FGVMULTM[redacted]]
  - ☐ fabric-test
    - ☐ [FGVMULTM[redacted]]
  - ☐ eFGT101E-CSF
    - ☐ [FG101ETK[redacted]]
  - ☐ csf-v70b
    - ☐ [FGT91E-HA]
  - ☐ csf-v64b
    - ☑ [FGT101E-1]
    - ☐ [FWF61E-1]
  - ☐ csf-[redacted]
    - ☐ [FGVM08TM[redacted]]
  - ☐ West-CA
  - ☐ CUST1

Fabric View

This section lists the new features added to FortiAnalyzer for Fabric View:

- Connectors on page 13

Connectors

This section lists the new features added to FortiAnalyzer for connectors:

- Webhook Connector to Support MS Teams on page 13

Webhook Connector to Support MS Teams

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Creating or editing ITSM connectors

A webhook connector has been added in FortiAnalyzer to support MS Teams. This connector can be used to post a message in MS Teams.

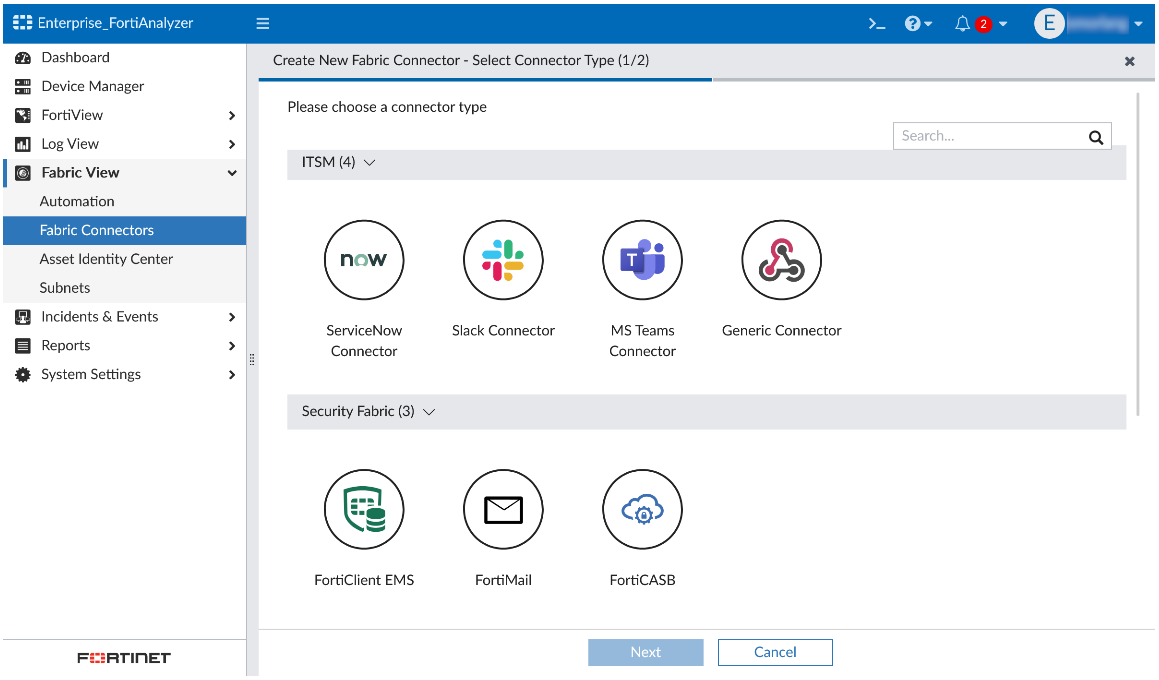
After an MS Teams connector is created, it can be added in the incident settings, notification profiles for event handlers, or as part of a playbook.

This topic contains the following instructions:

- To create a MS Teams connector:
- To use the MS Teams connector in a playbook:
- To use the MS Teams connector in incident settings:
- To use the MS Teams connector in a notification profile:

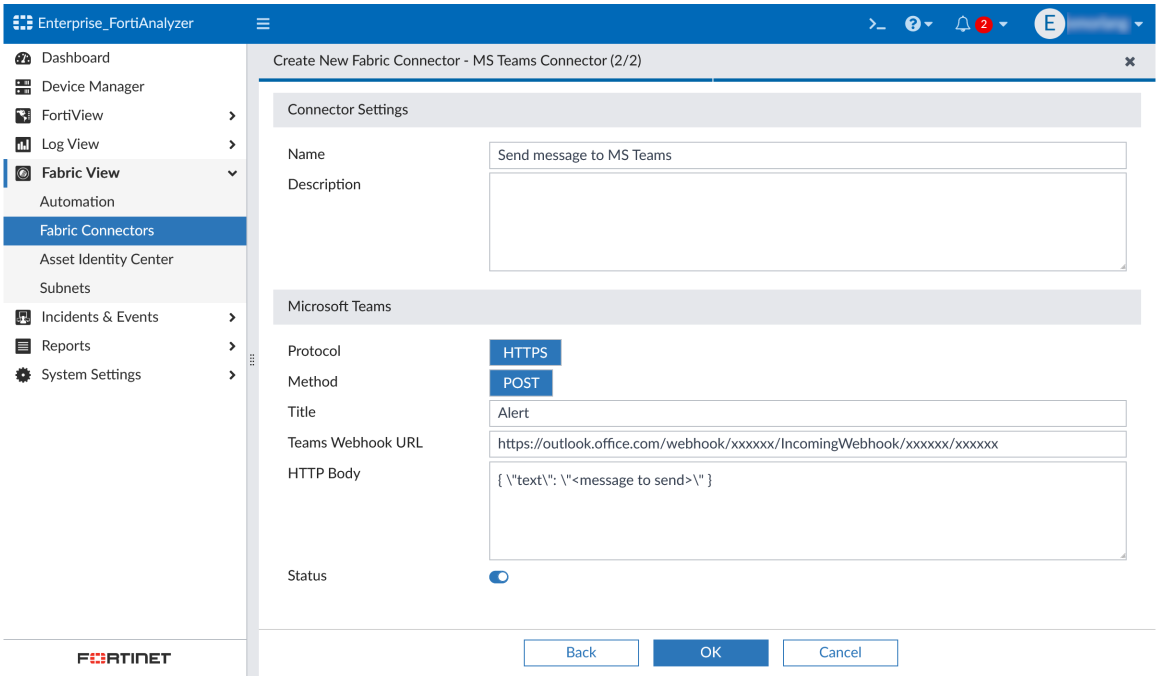
To create a MS Teams connector:

1. Go to *Fabric View* > *Fabric Connectors*.
2. Click *Create New*.
   The *Create New Fabric Connector* pane displays.



3. In the *ITSM* section, double-click *MS Teams Connector*.
4. Configure the following options:

Name	Type a name for the fabric connector.
Description	(Optional) Type a description for the fabric connector.
Protocol	Select HTTPS.
Method	Select POST.
Title	Type a title for the fabric connector.
Teams Webhook URL	Enter the incoming webhook URL created in MS Teams.
HTTP Body	Enter the HTTP body of the message that should be sent by the connector. For example, `{ \"text\": \"<message to send>\" }`.
Status	Enabled by default. The connector can be disabled, as needed.



Create New Fabric Connector - MS Teams Connector (2/2)

Connector Settings

Name	Send message to MS Teams
Description	

Microsoft Teams

Protocol	HTTPS
Method	POST
Title	Alert
Teams Webhook URL	https://outlook.office.com/webhook/xxxxxx/IncomingWebhook/xxxxxx/xxxxxx
HTTP Body	{ \"text\": \"<message to send>\" }
Status	●

5. Click *OK*.

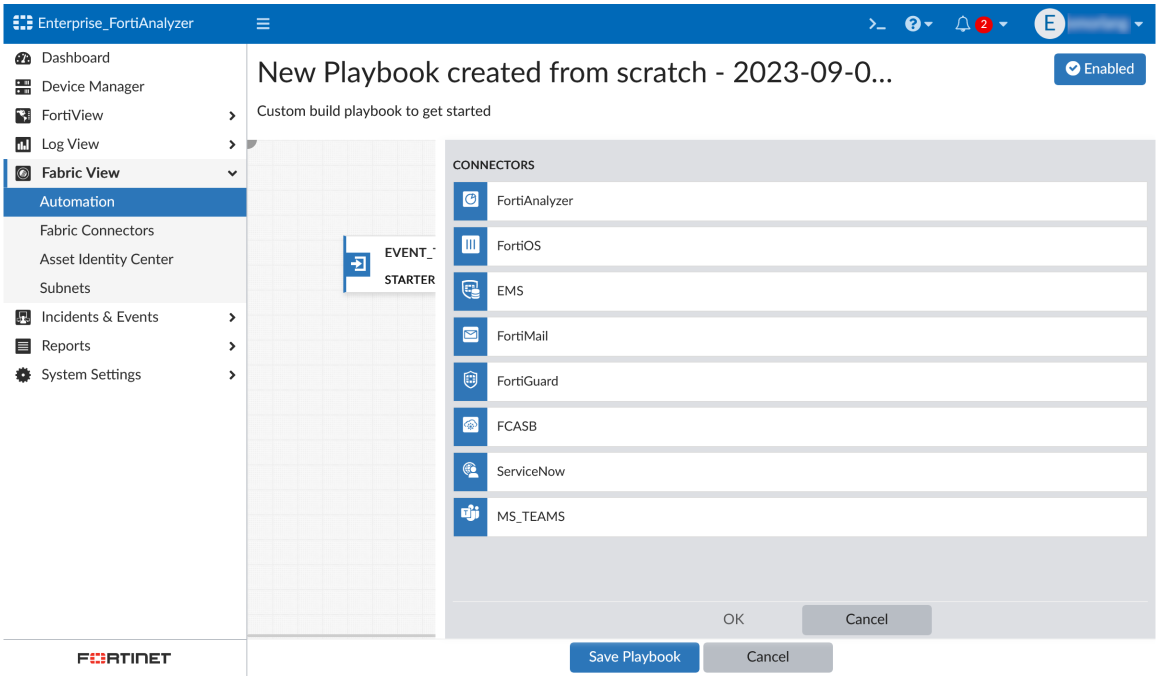
Use `${}` for macros in the *HTTP Body* field. The following macros and variables are supported:

Category	Variable	Macro	Description
Global	type	${type}	Notification type
Global	adom	${adom}	Adom name
Global	from	${from}	FAZ SN
Global	timestamp	${timestamp}	Notification timestamp
Event	event	${event}	All event fields
Event	eventid	${event.eventid}	Event id
Event	alertid	${event.alertid}	Alert id (same with eventid, but name consistent with previous notification format)
Event	logtype	${event.logtype}	Log type
Event	devtype	${event.devtype}	Device type
Event	eventtime	${event.eventtime}	Event time
Event	alerttime	${event.alerttime}	Alert time (same with eventtime, but name consistent with previous notification format)
Event	firstlogtime	${event.firstlogtime}	First log time
Event	lastlogtime	${event.lastlogtime}	Last log time
Event	devid	${event.devid}	Device id

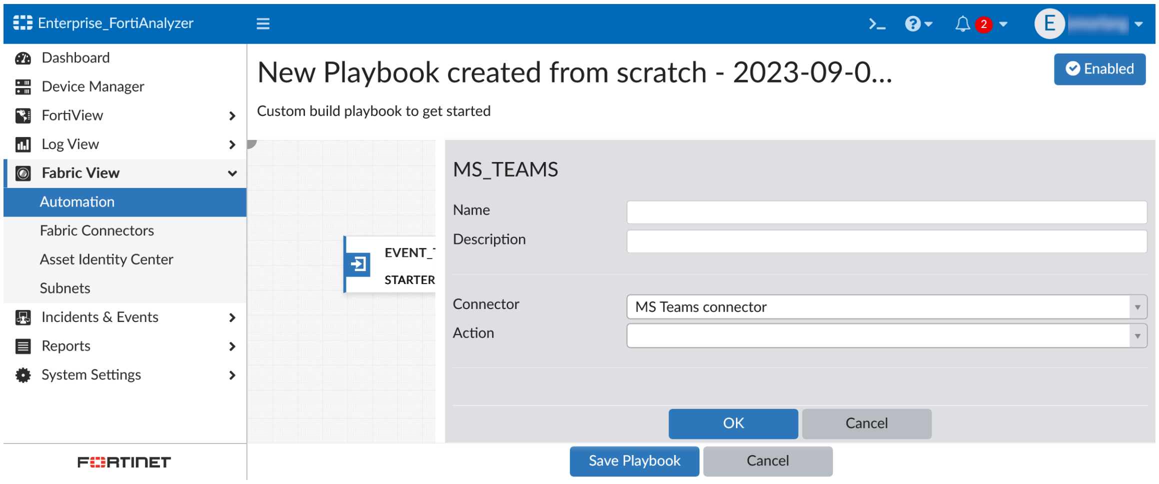
Category	Variable	Macro	Description
Event	devname	${event.devname}	Device name
Event	eventtype	${event.eventtype}	Event type
Event	groupby1	${event.groupby1}	groupby1
Event	groupby2	${event.groupby2}	grouby2
Event	groupby3	${event.groupby3}	grouby3
Event	indicator	${event.indicator}	indicator
Event	severity	${event.severity}	severity
Event	subject	${even.subject}	subject
Event	tag	${event.tag}	tag
Event	triggername	${event.triggername}	Trigger name
Event	vdom	${event.vdom}	vdom
Event	epid	${event.epid}	epid
Event	euid	${event.euid}	euid
Event	epip	${event.epip}	epip
Event	epname	${event.epname}	epname
Event	euname	${event.euname}	euname
Event	extrainfo	${event.extrainfo}	Additional info
Event	log-length	${event.log-length}	Log length
Event	log-detail	${event.log-detail}	Log detail
Incident	incident	${incident}	All incident fields
Incident	incid	${incident.incid}	Incident ID
Incident	type	${incident.type}	Notification type
Incident	revision	${incident.revision}	revision
Incident	attach_revision	${incident.attach_revision}	attach revision

To use the MS Teams connector in a playbook:

1. When adding a connector in a playbook, select *MS_TEAMS*.



2. From the *Connector* dropdown, select the MS Teams connector that you created.



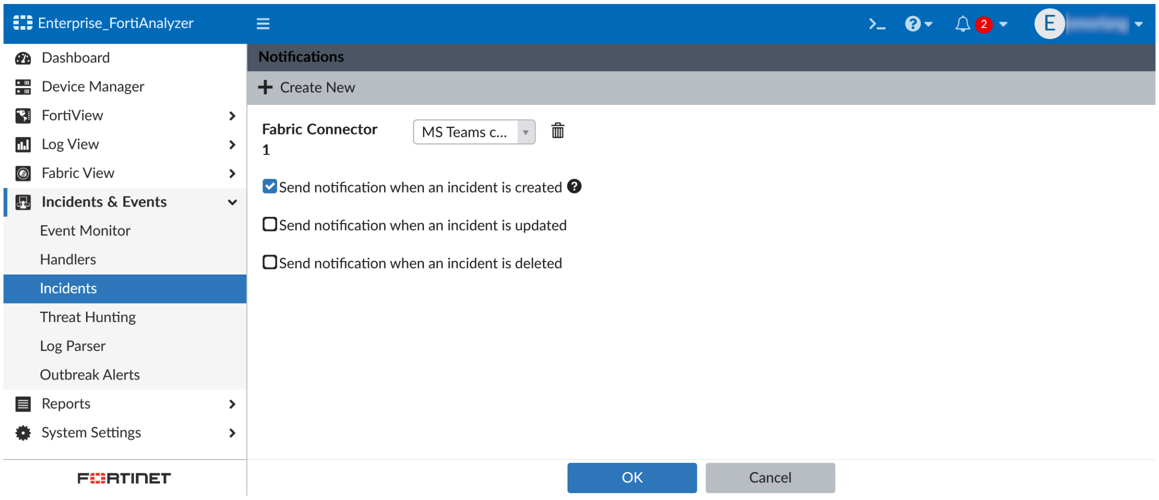
Name	
Description	
Connector	MS Teams connector
Action	

3. Configure the other options for the playbook as needed.

   For more information, see the FortiAnalyzer Administration Guide.

To use the MS Teams connector in incident settings:

1. Go to *Incidents & Events* > *Incidents*.
2. In the toolbar, click *Settings*.
3. From the *Fabric Connector* dropdown, select the MS Teams connector that you created.



Fabric Connector 1: MS Teams c...

☑ Send notification when an incident is created

☐ Send notification when an incident is updated

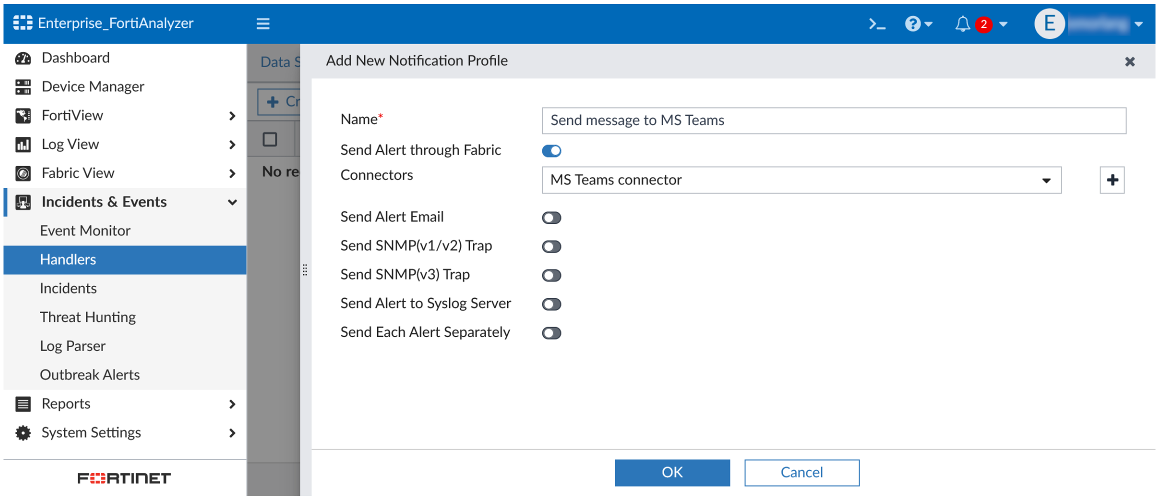
☐ Send notification when an incident is deleted

4. Configure the other options for the incident settings as needed.

   For more information, see the FortiAnalyzer Administration Guide.

To use the MS Teams connector in a notification profile:

1. When selecting the *Connectors* for a notification profile, select the MS Teams connector that you created.



Add New Notification Profile

Name*: Send message to MS Teams

Send Alert through Fabric Connectors: ● On

MS Teams connector

Send Alert Email: ○ Off

Send SNMP(v1/v2) Trap: ○ Off

Send SNMP(v3) Trap: ○ Off

Send Alert to Syslog Server: ○ Off

Send Each Alert Separately: ○ Off

2. Configure the other options for the notification profile as needed.

   For more information, see the FortiAnalyzer Administration Guide.

Security Operations (SOC)

This section lists the new features added to FortiAnalyzer for security operations (SOC):

- SOC automation on page 19
- Incident and Event Management on page 20
- Dashboards on page 31
- Asset and Identity on page 44
- Others on page 46

SOC automation

This section lists the new features added to FortiAnalyzer for SOC automation:

- Playbook event trigger correleation rules 7.4.1 on page 19

Playbook event trigger correleation rules - 7.4.1

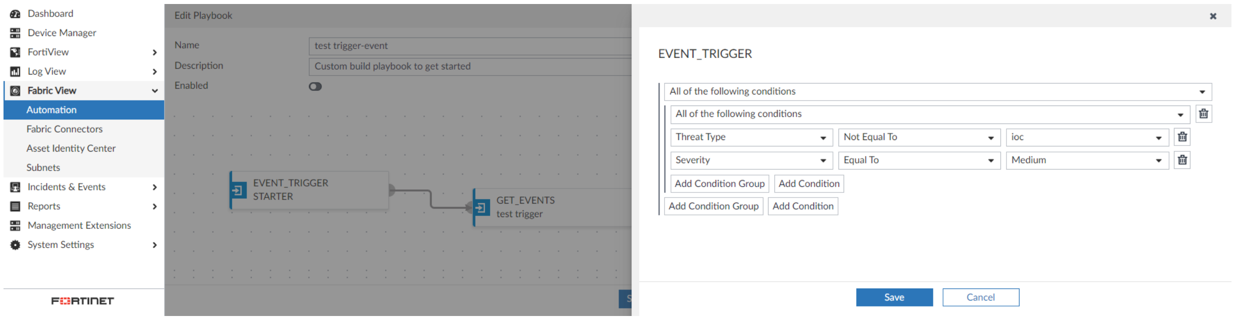
This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Playbook triggers and tasks

FortiAnalyzer v7.4.1 introduces extra flexibility on playbooks by implementing:

- Option to select *Any of the following conditions* (OR): The event is triggered if any of the defined conditions are met.
- Nested groups: Conditions can be grouped together and linked by either AND or OR.

When creating a playbook in *Fabric View > Automation > Playbook*, the *EVENT_TRIGGER* configuration includes options to *Add Condition* and *Add Condition Group*.



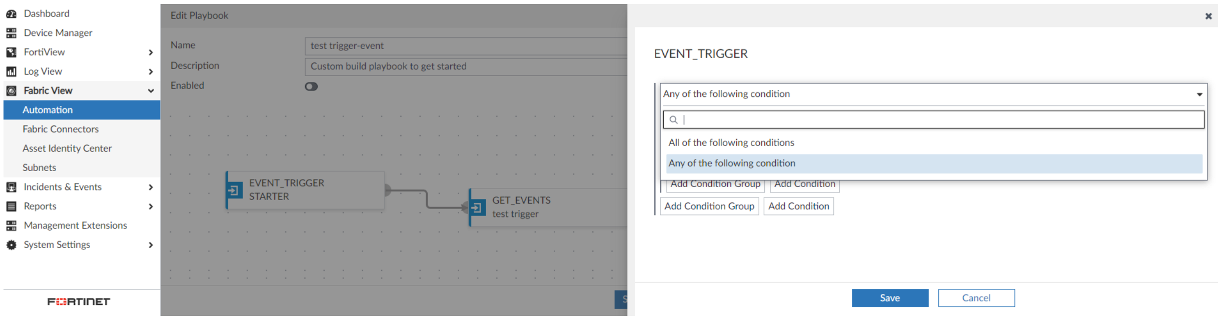
Name: test trigger-event
Description: Custom build playbook to get started
Enabled

EVENT_TRIGGER

All of the following conditions
All of the following conditions
Threat Type | Not Equal To | ioc
Severity | Equal To | Medium

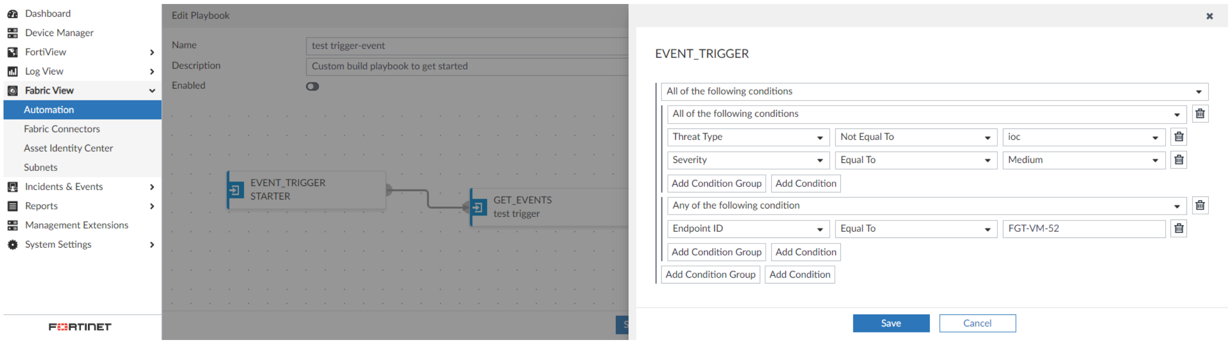
When adding a condition, you can select one of the following:

- *All of the following conditions* (AND)
- *Any of the following conditions* (OR)



Name: test trigger-event
Description: Custom build playbook to get started
Enabled
Any of the following condition

The conditions can be nested in groups. For example, "(group1 AND group2) OR (group3)". See below.



Name: test trigger-event
Description: Custom build playbook to get started
Enabled

All of the following conditions
- All of the following conditions
  - Threat Type | Not Equal To | ioc
  - Severity | Equal To | Medium
- Any of the following condition
  - Endpoint ID | Equal To | FGT-VM-52

Incident and Event Management

This section lists the new features added to FortiAnalyzer for incident and event management:

- New predefined correlation event handlers on page 20
- Update to the Event Handler rule configuration 7.4.2 on page 26

New predefined correlation event handlers

In 7.4.0, 33 predefined correlation event handlers have been added for nine use cases. The nine use cases include:

Use case	Description
Command & Control (CnC)	To identify suspicious traffic between internal systems and external destinations.
Credential Access	To identify when credentials are compromised, indicating that an attacker may have gained access.
Defense Evasion	To identify if an endpoint is compromised.
Execution	To identify if any malware is downloaded and executed.
Exfiltration	To identify any data leaks in the network.
Initial Access	To identify any suspicious activities after a new user gained access.

Use case	Description
Lateral Movement	To identify if there is any advancement from the attacker on a already compromised network.
Persistence	To identify when an attacker maintains unauthorized access and performs malicious activities.
Privilege Escalation	To identify if an attacker tries to get access over sensitive information.

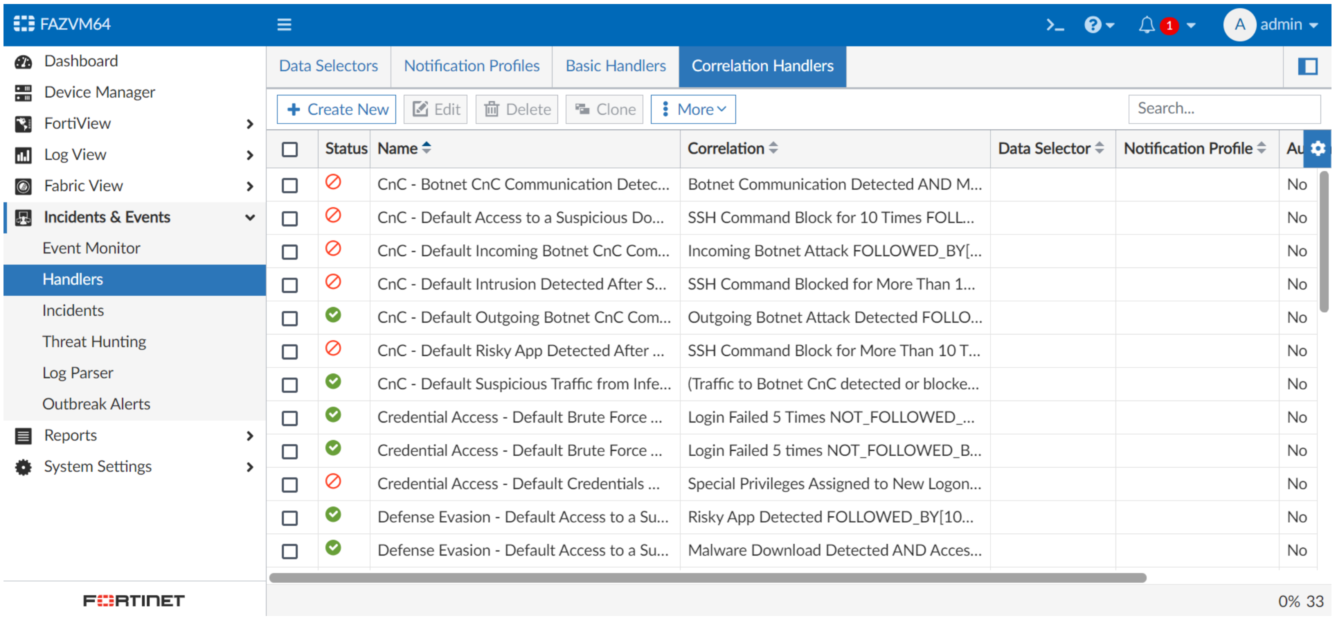
To view the predefined correlation event handlers, go to *Incidents & Events* > *Handlers* > *Correlation Handlers*. From the *More* dropdown, select *Show Predefined* and deselect *Show Custom*. The related use case is included in the name of the predefined correlation event handler.

Correlation event handler	Description
CnC - Botnet CnC Communication Detected	Botnet communication detected and multiple TXT type DNS request detected which is a way of hiding the communication to botnet and carry commands from the botnet. This is strong indication there is a botnet attack event.
CnC - Default Access To A Suspicious Domain After SSH Command Block For Many Times	A user tries to SSH from FortiGate to an endpoint get blocked for many times shortly followed by access to a suspicious domain from that endpoint may indicate the endpoint is compromised.
CnC - Default Incoming Botnet CnC Communication Callback Detected	Incoming Botnet communication detected followed by multiple TXT type DNS request which is a way to hide the Command and Control communication to the botnet. This may indicate the endpoint is trying to send the message to the botnet to confirm the endpoint is being controlled, and carry commands from the botnet.
CnC - Default Intrusion Detected After SSH Command Block For Many Times	A user try to SSH from FortiGate to another device but failed for many times followed by intrusion detected from the endpoint the user tries to access to. This may indicate the user has gained access to the endpoint and trigger the intrusion.
CnC - Default Outgoing Botnet CnC Communication Callback Detected	Outgoing Botnet communication detected followed by multiple TXT type DNS request which is a way to hide the Command and Control communication to the botnet. This may indicate the endpoint is trying to send the message to the botnet to confirm the endpoint is being controlled, and carry commands from the botnet.
CnC - Default Risky App Detected After SSH Command Block For Many Times	A user tries to SSH from FortiGate to an endpoint gets blocked many times shortly followed by risky app detected from that endpoint, which may indicate the endpoint is compromised.
CnC - Default Suspicious Traffic from Infected Endpoint	This handler is to detect if an endpoint is infected and there is a large traffic from the same endpoint.
Credential Access - Default Brute Force Account Login Attack FAZ	This handler is to detect if an account login failed many times not followed by a login success for FortiAnalyzer.
Credential Access - Default Brute Force Account Login Attack FGT	This handler is to detect if an account login failed many times not followed by a login success for FortiGate.

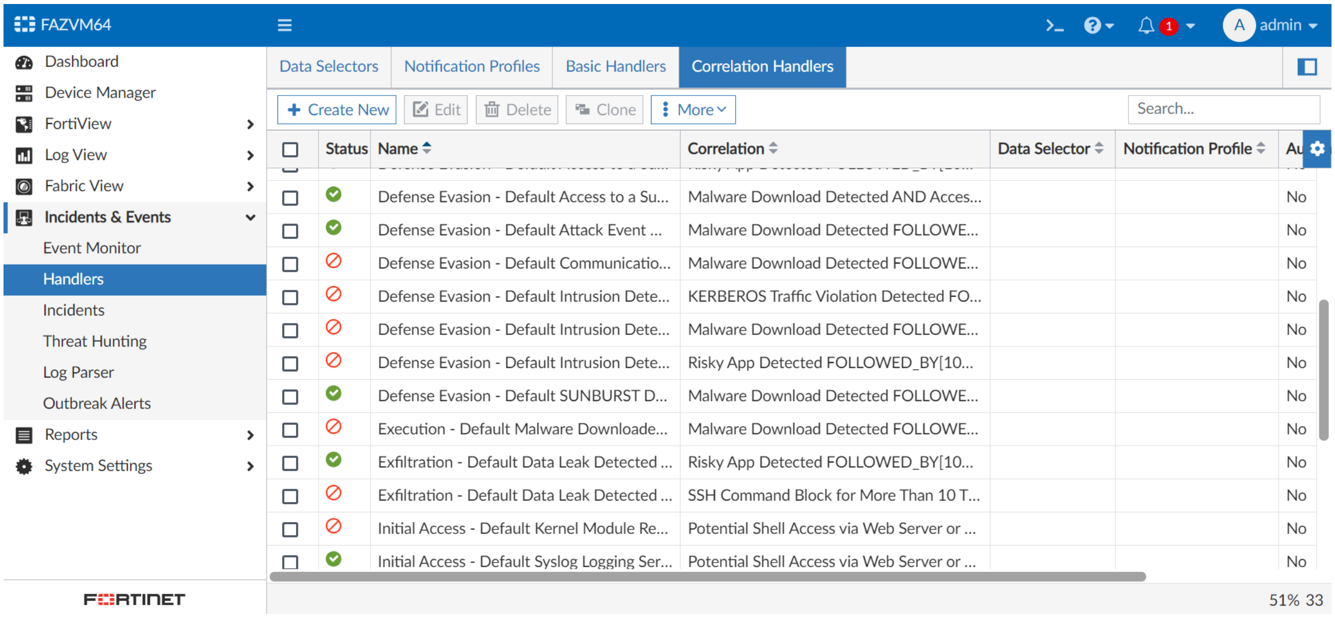
Correlation event handler	Description
Credential Access - Default Credentials Were Read After Special Privileges Assigned	Privileges assigned to a user shortly followed by credentials were read may indicate the user is suspicious.
Defense Evasion - Default Access To A Suspicious Domain After Malware Downloaded	Access to a suspicious domain after attempted to download malware but blocked for many times which may indicated the malware is penetrated the defense and the device is compromised.
Defense Evasion - Default Access To A Suspicious Domain After Risky App Detected	High/Critical risk App detected followed by connection to a new registered domain may indicate the risky app is trying to talk to a botnet server which require attention.
Defense Evasion - Default Attack Event Detected After Malware Downloaded	Malware download detected followed by an attack event may indicate the endpoint is compromised by the malware.
Defense Evasion - Default Communication To Botnet Detected After Malware Detected	Malware download detected followed by multiple TXT type DNS request which is a way of hiding the communication to botnet and carry commands from the botnet. This may indicate the endpoint is being controlled.
Defense Evasion - Default Intrusion Detected After KERBEROS Traffic Violation	KERBEROS traffic violation followed by intrusion detected may indicated the unwanted user gain access to the endpoint by KERBEROS.
Defense Evasion - Default Intrusion Detected After Malware Detected	Malware download blocked for many times followed by intrusion detected. This may indicate the malware is penetrated the defense and the endpoint is compromised.
Defense Evasion - Default Intrusion Detected After Risky App Detected	High/Critical risk App detected followed by intrusion detected may indicate the risky app triggered the intrusion.
Defense Evasion - Default SUNBURST Domain Traffic Detected After Malware Downloaded	SUNBURST Domain Traffic Detected after malware download attempt blocked multiple times. This event may indicate the malware escaped and executed to communicate with SUNBURST Command and Control servers.
Execution - Default Malware Downloaded And Execution Detected	User attempted to download malware on their endpoint for many times followed by detecting high or critical risk app on FortiGate application control log may indicate the user bypassed the security and downloaded the malware, and then executed the malware or infected software.
Exfiltration - Default Data Leak Detected After Risky App Detected	High/Critical risk App detected followed by data leak detected may indicate the endpoint is compromised.
Exfiltration - Default Data Leak Detected After SSH Command Block For Many Times	A user tries to SSH from FortiGate to an endpoint get blocked for many times shortly followed by data leak from that endpoint may indicate the endpoint is compromised.

Correlation event handler	Description
Initial Access - Default Kernel Module Removed After A New User Access to The Linux via Shell	A new user access to the Linux via shell followed by the kernel module is removed may indicate the new user is suspicious.
Initial Access - Default Syslog Logging Service Deactivated After A New User Access To The Linux via Shell	Potential shell access via web server or new user access to the Ubuntu shell followed by syslog logging service disabled may indicate the unwanted user has gained the access to the endpoint and disabled the syslog logging service.
Lateral Movement - Default Access To A Suspicious Domain On A Device with Vulnerability	Access to a suspicious domain on a device with vulnerability, which may indicate the device is compromised.
Lateral Movement - Default Data Leak Found On A Device with Vulnerability	Data Leak Found On a Device with Vulnerability may indicate the device is compromised.
Lateral Movement - Default Virus Detected On A Device with Vulnerability	Virus detected on a device with vulnerability may indicate it is compromised; need not only remove the virus, but also fix the vulnerability.
Lateral Movement - Default Vulnerability And Intrusion Detected	Vulnerability detected by FCT and intrusion detected. Both event happened on an endpoint may indicate the endpoint is compromised.
Persistence - Default Firewall Service Deactivated After Authentication Failed For Many Times	Authentication failed for many times followed by firewall service deactivated may indicate the unwanted user has gained the access to the endpoint and disabled the firewall service.
Persistence - Default Kernel Module Removed After Authentication Failed For Many Times	Authentication failed for many times followed by kernel module removed may indicate the unwanted user has gained the access to the endpoint and removed the kernel module.
Persistence - Default Syslog Logging Service Deactivated After Authentication Failed For Many Times	Authentication failed for many times followed by syslog logging service deactivated may indicate the unwanted user has gained the access to the endpoint and disabled the logging service.
Privilege Escalation - Default Firewall Disabled After Special Privileges Assigned to New Logon	Firewall disabled after special privileges assigned to new logon may indicate this new logon user is suspicious.
Privilege Escalation - Default Windows Event Logging Service Is Down Or Log Is Cleared After Privileges Assigned	Privileges assigned to a user shortly followed by event logging server is down or log is cleared may indicate the user is suspicious.

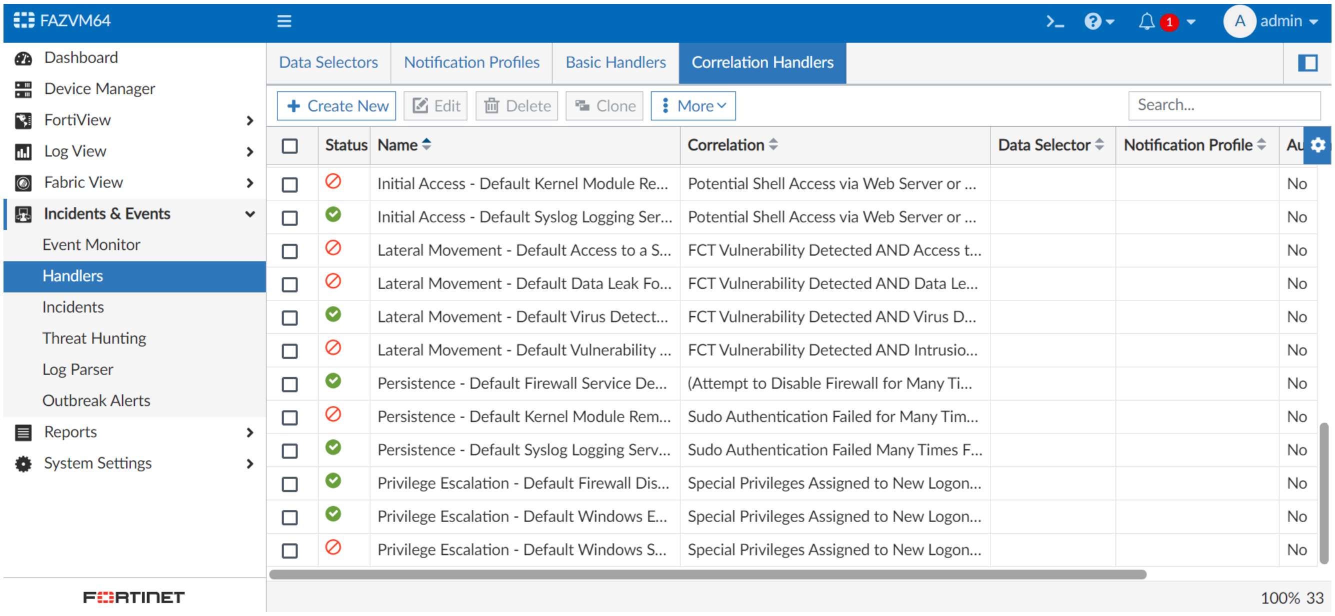
Correlation event handler	Description
Privilege Escalation - Default Windows System Time Was Changed After Privileges Assigned To A New Logon	Privileges assigned to a new logon followed by windows system time was changed may indicate this is a time travel attack. For example, setting the clock back on a client to a previous point in time could cause the system to accept rogue Transport Layer Security (TLS) certificates that may have been already revoked, thereby giving attackers a way to decrypt encrypted communications.



□	Status	Name	Correlation	Data Selector	Notification Profile	Au
□	⊘	CnC - Botnet CnC Communication Detec...	Botnet Communication Detected AND M...			No
□	⊘	CnC - Default Access to a Suspicious Do...	SSH Command Block for 10 Times FOLL...			No
□	⊘	CnC - Default Incoming Botnet CnC Com...	Incoming Botnet Attack FOLLOWED_BY[...			No
□	⊘	CnC - Default Intrusion Detected After S...	SSH Command Blocked for More Than 1...			No
□	✓	CnC - Default Outgoing Botnet CnC Com...	Outgoing Botnet Attack Detected FOLLO...			No
□	⊘	CnC - Default Risky App Detected After ...	SSH Command Block for More Than 10 T...			No
□	✓	CnC - Default Suspicious Traffic from Infe...	(Traffic to Botnet CnC detected or blocke...			No
□	✓	Credential Access - Default Brute Force ...	Login Failed 5 Times NOT_FOLLOWED_...			No
□	✓	Credential Access - Default Brute Force ...	Login Failed 5 times NOT_FOLLOWED_B...			No
□	⊘	Credential Access - Default Credentials ...	Special Privileges Assigned to New Logon...			No
□	✓	Defense Evasion - Default Access to a Su...	Risky App Detected FOLLOWED_BY[10...			No
□	✓	Defense Evasion - Default Access to a Su...	Malware Download Detected AND Acces...			No



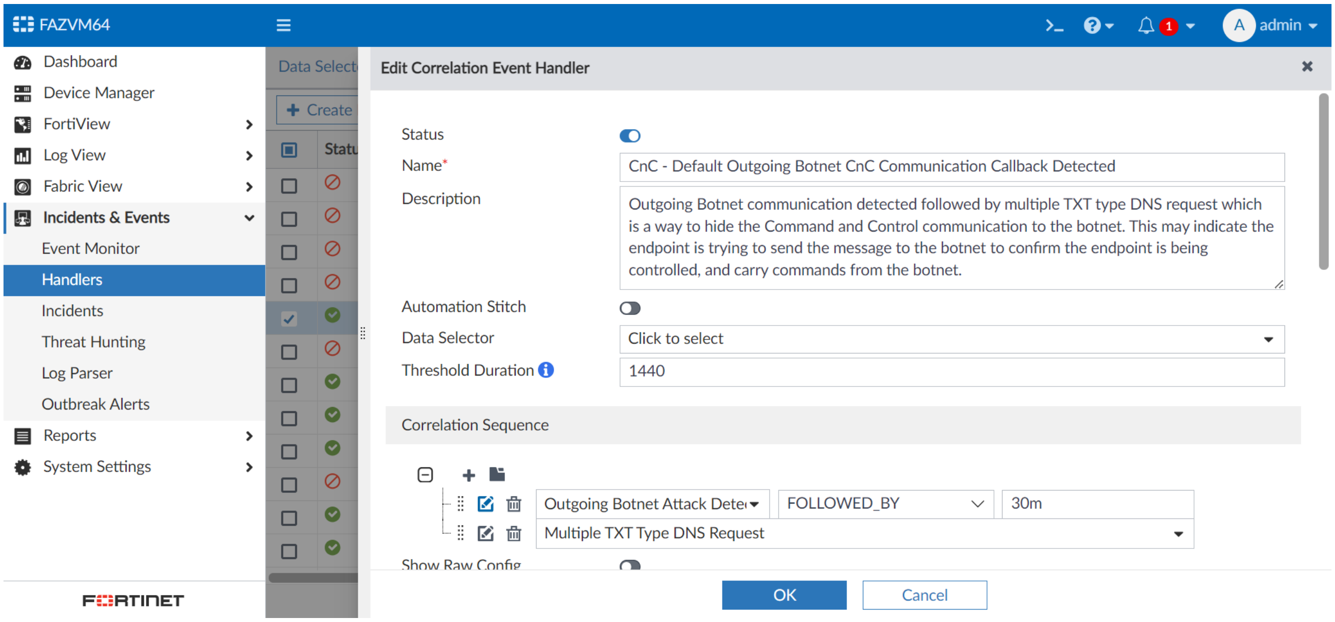
□	Status	Name	Correlation	Data Selector	Notification Profile	Au
□	✓	Defense Evasion - Default Access to a Su...	Malware Download Detected AND Acces...			No
□	✓	Defense Evasion - Default Attack Event ...	Malware Download Detected FOLLOWE...			No
□	⊘	Defense Evasion - Default Communicatio...	Malware Download Detected FOLLOWE...			No
□	⊘	Defense Evasion - Default Intrusion Dete...	KERBEROS Traffic Violation Detected FO...			No
□	⊘	Defense Evasion - Default Intrusion Dete...	Malware Download Detected FOLLOWE...			No
□	⊘	Defense Evasion - Default Intrusion Dete...	Risky App Detected FOLLOWED_BY[10...			No
□	✓	Defense Evasion - Default SUNBURST D...	Malware Download Detected FOLLOWE...			No
□	⊘	Execution - Default Malware Downloade...	Malware Download Detected FOLLOWE...			No
□	✓	Exfiltration - Default Data Leak Detected ...	Risky App Detected FOLLOWED_BY[10...			No
□	⊘	Exfiltration - Default Data Leak Detected ...	SSH Command Block for More Than 10 T...			No
□	⊘	Initial Access - Default Kernel Module Re...	Potential Shell Access via Web Server or ...			No
□	✓	Initial Access - Default Syslog Logging Ser...	Potential Shell Access via Web Server or ...			No



☐	Status	Name	Correlation	Data Selector	Notification Profile	Au
☐	⊘	Initial Access - Default Kernel Module Re...	Potential Shell Access via Web Server or ...			No
☐	✓	Initial Access - Default Syslog Logging Ser...	Potential Shell Access via Web Server or ...			No
☐	⊘	Lateral Movement - Default Access to a S...	FCT Vulnerability Detected AND Access t...			No
☐	⊘	Lateral Movement - Default Data Leak Fo...	FCT Vulnerability Detected AND Data Le...			No
☐	✓	Lateral Movement - Default Virus Detect...	FCT Vulnerability Detected AND Virus D...			No
☐	⊘	Lateral Movement - Default Vulnerability ...	FCT Vulnerability Detected AND Intrusio...			No
☐	✓	Persistence - Default Firewall Service De...	(Attempt to Disable Firewall for Many Ti...			No
☐	⊘	Persistence - Default Kernel Module Rem...	Sudo Authentication Failed for Many Tim...			No
☐	✓	Persistence - Default Syslog Logging Serv...	Sudo Authentication Failed Many Times F...			No
☐	✓	Privilege Escalation - Default Firewall Dis...	Special Privileges Assigned to New Logon...			No
☐	✓	Privilege Escalation - Default Windows E...	Special Privileges Assigned to New Logon...			No
☐	⊘	Privilege Escalation - Default Windows S...	Special Privileges Assigned to New Logon...			No

To edit a predefined correlation event handler, select it and click *Edit*. You can enable or disable these handlers according to your needs. You can also include a data selector or notification profile where appropriate. For more information about editing a correlation event handler, see Creating a custom correlation handler in the FortiAnalyzer Administration Guide.

In the *Edit Correlation Event Handler* pane, you can review the description of the handler as well as the correlation sequence and criteria.



Edit Correlation Event Handler

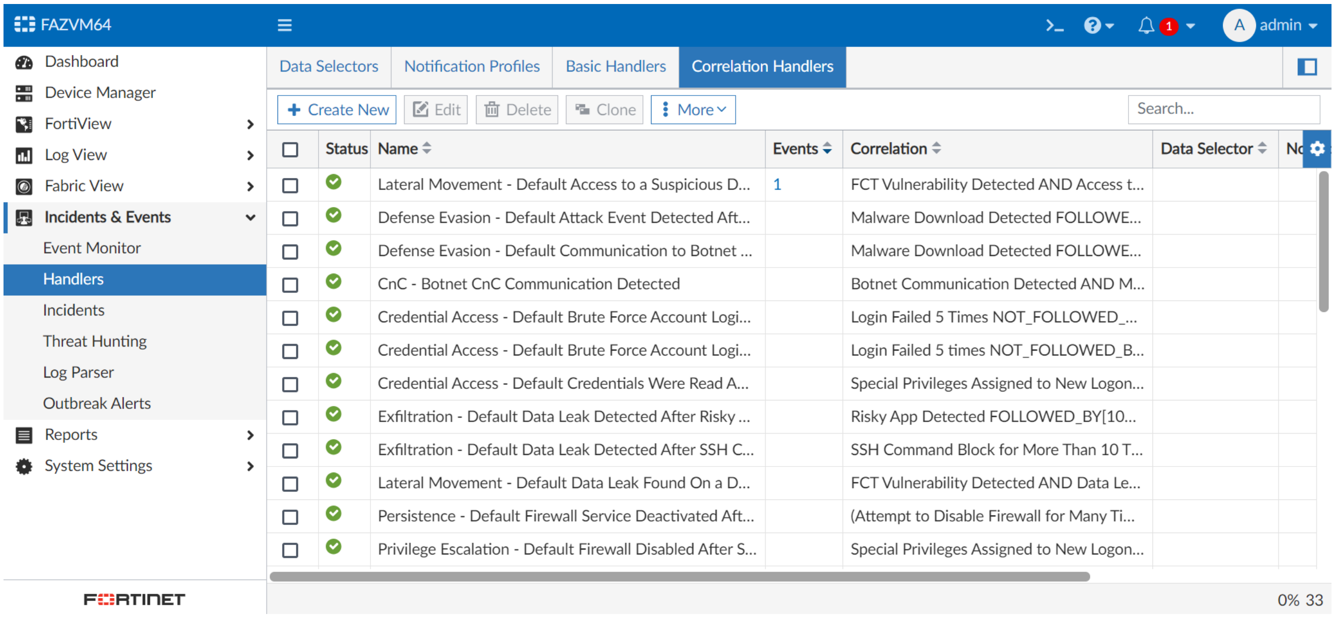
Status	●
Name*	CnC - Default Outgoing Botnet CnC Communication Callback Detected
Description	Outgoing Botnet communication detected followed by multiple TXT type DNS request which is a way to hide the Command and Control communication to the botnet. This may indicate the endpoint is trying to send the message to the botnet to confirm the endpoint is being controlled, and carry commands from the botnet.
Automation Stitch	○
Data Selector	Click to select
Threshold Duration	1440

Correlation Sequence

Outgoing Botnet Attack Dete	FOLLOWED_BY	30m
Multiple TXT Type DNS Request		

Show Raw Config ○

When these predefined correlation event handlers are enabled, incoming logs that satisfy the correlation sequence will trigger events. To view the triggered events, click the event count in the *Events* column.



☐	Status	Name	Events	Correlation	Data Selector	No
☐	✓	Lateral Movement - Default Access to a Suspicious D...	1	FCT Vulnerability Detected AND Access t...		
☐	✓	Defense Evasion - Default Attack Event Detected Aft...		Malware Download Detected FOLLOWE...		
☐	✓	Defense Evasion - Default Communication to Botnet ...		Malware Download Detected FOLLOWE...		
☐	✓	CnC - Botnet CnC Communication Detected		Botnet Communication Detected AND M...		
☐	✓	Credential Access - Default Brute Force Account Logi...		Login Failed 5 Times NOT_FOLLOWED_...		
☐	✓	Credential Access - Default Brute Force Account Logi...		Login Failed 5 times NOT_FOLLOWED_B...		
☐	✓	Credential Access - Default Credentials Were Read A...		Special Privileges Assigned to New Logon...		
☐	✓	Exfiltration - Default Data Leak Detected After Risky ...		Risky App Detected FOLLOWED_BY[10...		
☐	✓	Exfiltration - Default Data Leak Detected After SSH C...		SSH Command Block for More Than 10 T...		
☐	✓	Lateral Movement - Default Data Leak Found On a D...		FCT Vulnerability Detected AND Data Le...		
☐	✓	Persistence - Default Firewall Service Deactivated Aft...		(Attempt to Disable Firewall for Many Ti...		
☐	✓	Privilege Escalation - Default Firewall Disabled After S...		Special Privileges Assigned to New Logon...		

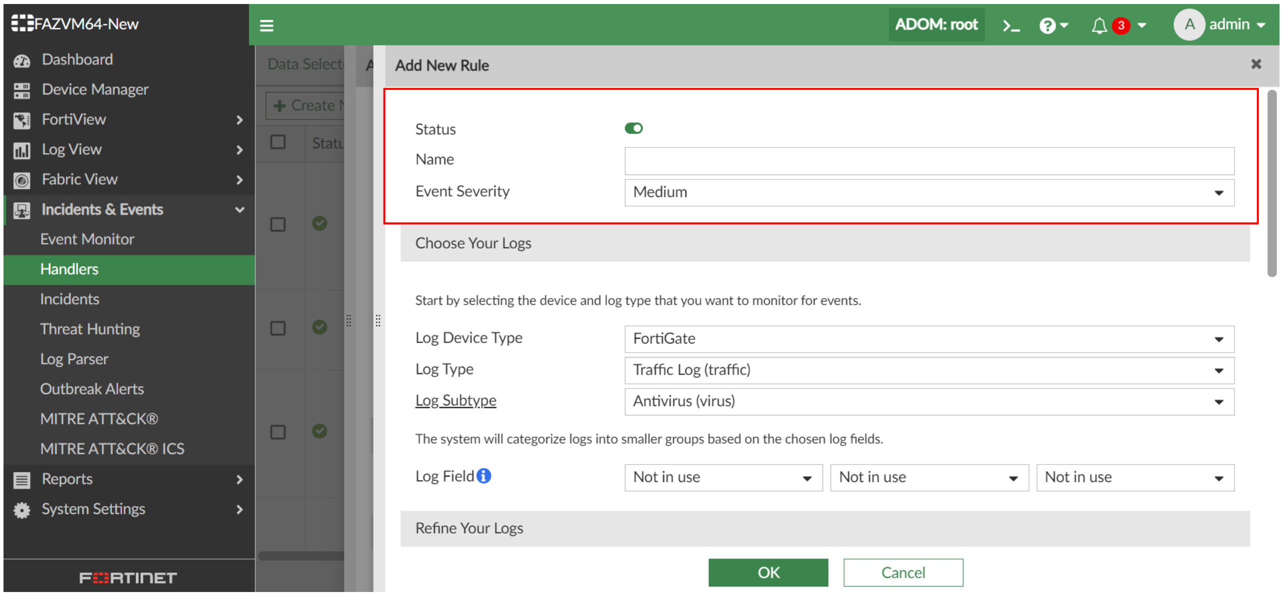
Update to the Event Handler rule configuration - 7.4.2

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Creating a custom event handler

When configuring rules for a basic event handler in the GUI, the configuration is now organized into four sections:

1. General: Set the rule status, name, and severity of the triggered event.



Add New Rule

Status	●
Name	
Event Severity	Medium

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	Antivirus (virus)

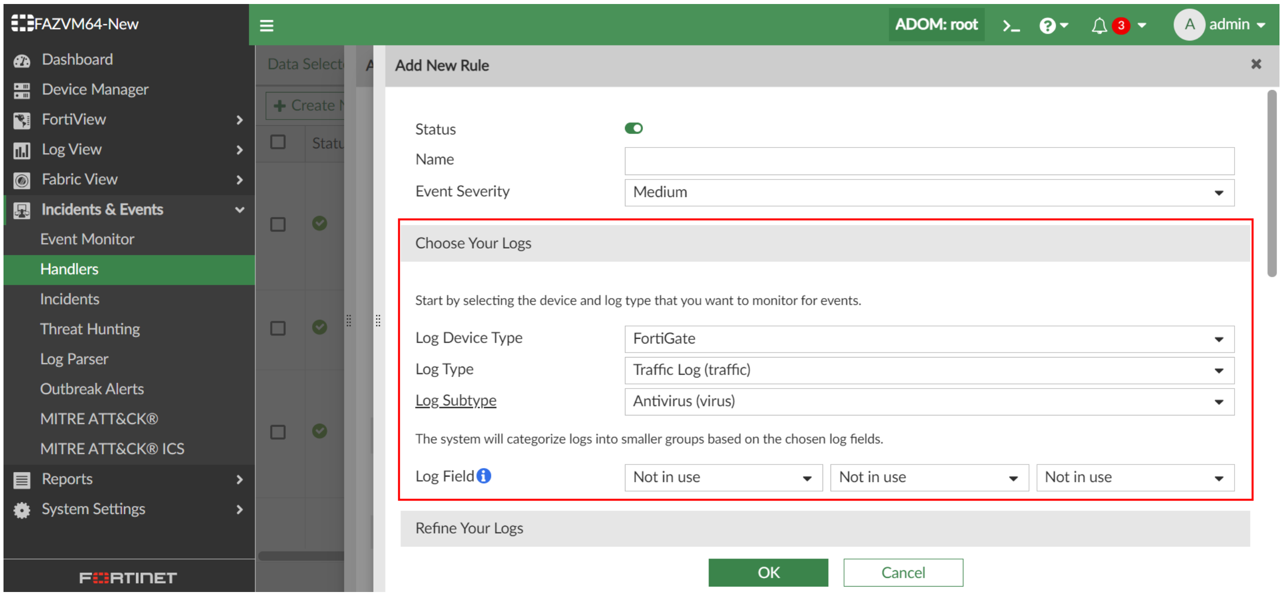
The system will categorize logs into smaller groups based on the chosen log fields.

Log Field	Not in use	Not in use	Not in use

Refine Your Logs

OK Cancel

2. *Choose Your Logs*: Select the device and log type that you want to monitor for events. Choose up to three log fields to categorize logs into smaller groups.



Add New Rule

Status: ●
Name:
Event Severity: Medium

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: Antivirus (virus)

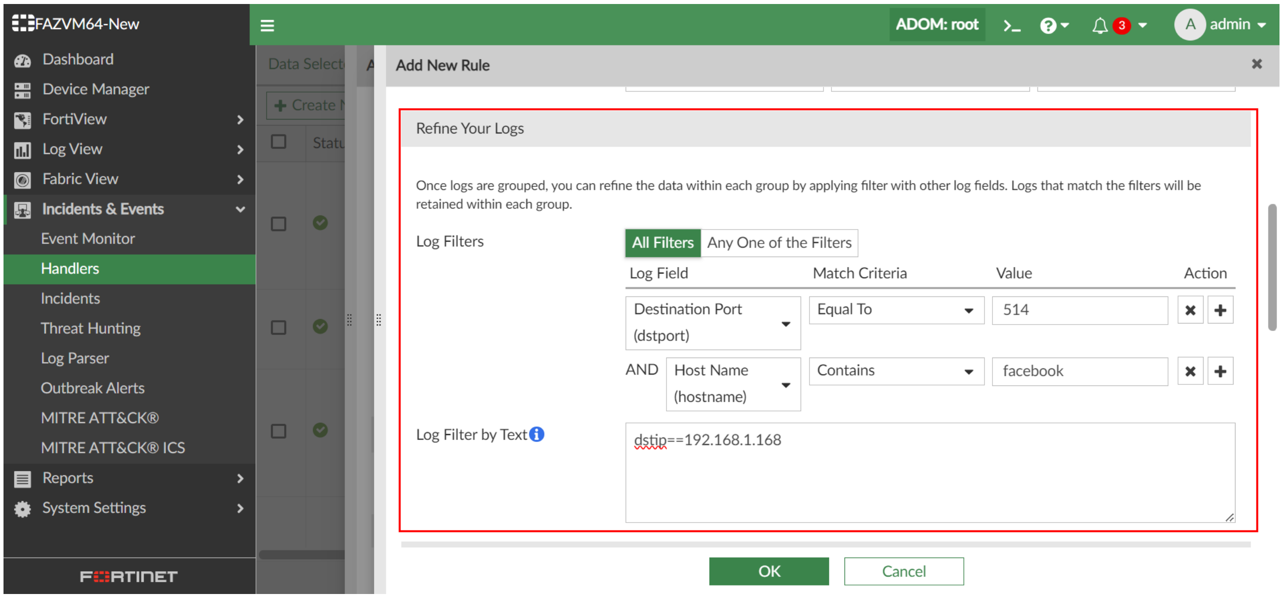
The system will categorize logs into smaller groups based on the chosen log fields.

Log Field: Not in use | Not in use | Not in use

Refine Your Logs

OK | Cancel

3. *Refine Your Logs*: Once logs are grouped, you can further refine the data within each group by applying filters with other log fields. Logs that match the filters will be retained within each group.



Add New Rule

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.

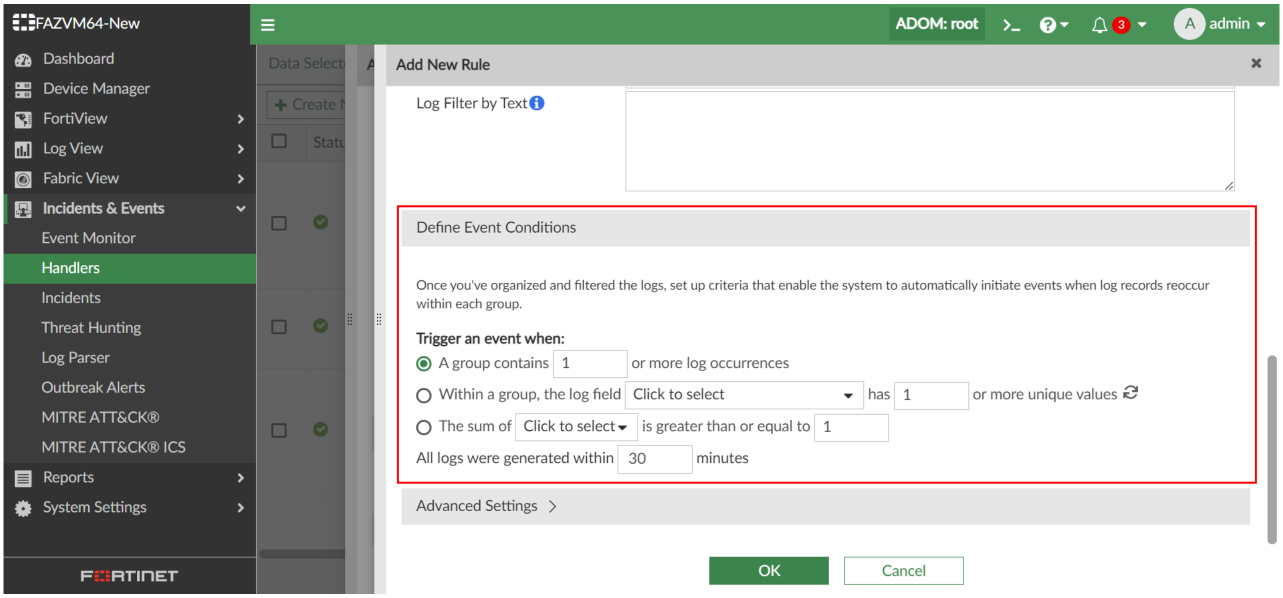
Log Filters: All Filters | Any One of the Filters

	Log Field	Match Criteria	Value	Action
	Destination Port (dstport)	Equal To	514	✖ ✚
AND	Host Name (hostname)	Contains	facebook	✖ ✚

Log Filter by Text: dstip==192.168.1.168

OK | Cancel

4. *Define Event Conditions*: Once you've organized and filtered the logs, set up criteria that enables the system to automatically initiate events when log records reoccur within each group.



Add New Rule

Log Filter by Text

Define Event Conditions

Once you've 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 1 or more log occurrences

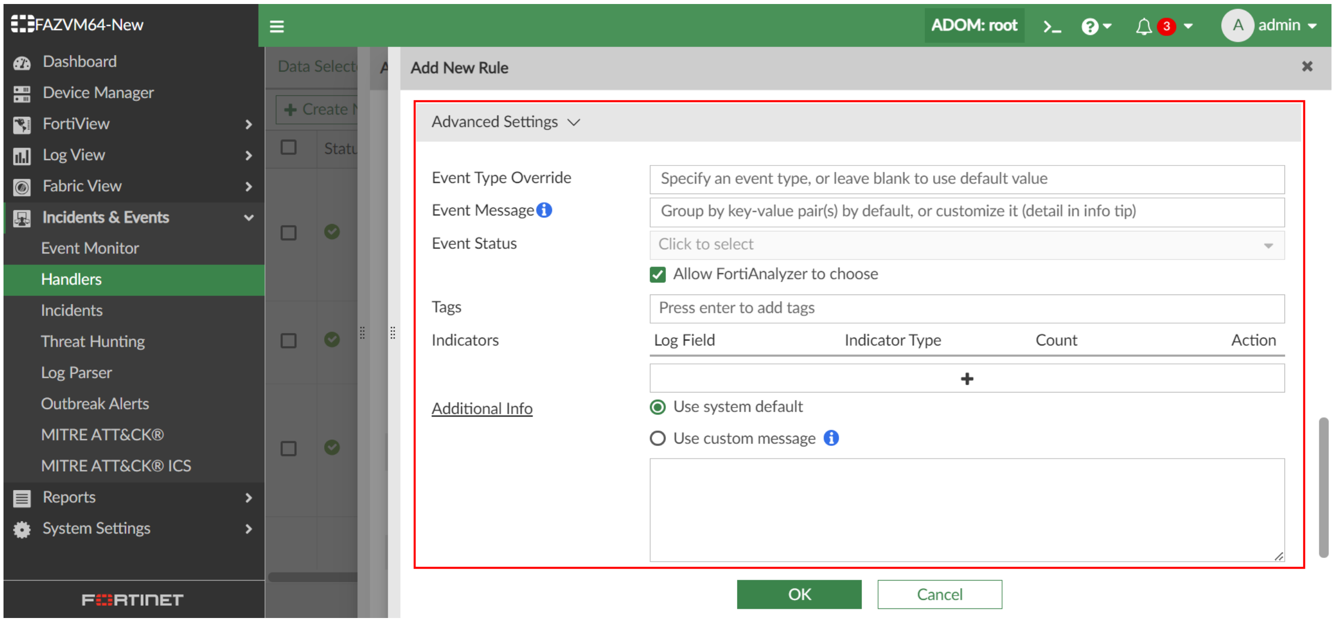
○ Within a group, the log field Click to select has 1 or more unique values

○ The sum of Click to select is greater than or equal to 1

All logs were generated within 30 minutes

Advanced Settings

There is also a section for *Advanced Settings*, which is useful to specify the details for the triggered events. This includes the event message, event status, tags, and indicators.



Add New Rule

Advanced Settings

Event Type Override: Specify an event type, or leave blank to use default value

Event Message: Group by key-value pair(s) by default, or customize it (detail in info tip)

Event Status: Click to select

☑ Allow FortiAnalyzer to choose

Tags: Press enter to add tags

Indicators:

Log Field	Indicator Type	Count	Action

Additional Info

● Use system default

○ Use custom message

Some option names and descriptions have also been updated from previous versions to provide more clarity.

To configure a rule for a basic event handler:

The following instructions are based on FortiAnalyzer version 7.4.2. For the latest version, see the option descriptions in the following topic from the FortiAnalyzer Administration Guide:

- Creating a custom event handler

1. Go to *Incidents & Events* > *Handlers* > *Basic Handlers*.
2. Click *Create New*.

   The *Add New Basic Event Handler* pane displays.
3. In the *Rules* section for the event handler, click *Add New Rule*.

   The *Add New Rule* pane displays.
4. Configure the following options:

Option	Description
Status	Enable or disable the rule. If the rule is disabled, it will not be used to generate events.
Name	Enter a name for the rule.
Event Severity	Select the severity from the dropdown list: *Critical*, *High*, *Medium*, or *Low*.
Choose Your Logs Start by selecting the device and log type that you want to monitor for events.	
Log Device Type	If you are in a Security Fabric ADOM, select the log device type from the dropdown list. If you are not in a Security Fabric ADOM, you cannot change the *Log Device Type*. The *Fabric* log device type can be used to generate alerts from SIEM logs when SIEM logs are available.
Log Type	Select the log type from the dropdown list. When *Devices* is set to *Local Device*, you cannot change the *Log Type* or *Log Subtype*.
Log Subtype	Select the category of event that this event handler monitors. The available options depend on the platform type. This option is only available when the *Log Type* has a subtype. For example, *Event Log* and *Traffic Log* have log subtypes which can be selected from the dropdown.
Log Field	Select the log fields for the system to categorize logs into smaller groups. For example, consider the scenario where the *Log Field* is set using `Source IP (srcip)`. When log entries are recorded with source IPs such as 192.168.1.1, 192.168.1.2, and 192.168.1.3, the system will categorize these logs into distinct groups: • Group 1: Logs with the source IP 192.168.1.1 • Group 2: Logs with the source IP 192.168.1.2 • Group 3: Logs with the source IP 192.168.1.3 This grouping mechanism allows analysis of log data based on the specified source IP addresses.
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	Select *All Filters* or *Any One of the Filters*.

Option	Description
	Configure the filter(s): • **Log Field**: Select a log field from the dropdown. After the log device and log type are selected, the *Log Field* dropdown list will only include log fields that belong to the specified log type. For example, the *Botnet IP* log field is available when the *Log Type* is *DNS*, but not available when the *Log Type* is *Event Log*. • **Match Criteria**: Select an operator from the dropdown. The available options depends on the selected log field. Some log fields, such as *Source Port*, will provide a variety of operators in the dropdown list, such as *Equal To*, *Not Equal To*, *Greater Than or Equal To*, *Less Than or Equal To*, *Greater Than*, and *Less Than*. Other log fields, such as *Log Description*, will be limited to *Equal To* and *Not Equal To*. • **Value**: Select a value from the dropdown list or enter a value in the text box. The available options depends on the selected log field. If there is no dropdown list provided by FortiAnalyzer, you must manually enter a value to find in the raw log. If a dropdown list is provided, you can select a value from the list. For some log fields, such as *Level*, the dropdown list also allows you to enter a custom value. If there is no textbox to enter a custom value in the dropdown list, you must use the *Generic Text Filter* instead. In the **Action** column, click plus (**+**) to insert a new filter below. You can insert multiple filters. To delete a filter, click the **x** next to the filter.
Log Filter by Text	Enter a generic text filter. See the FortiAnalyzer Administration Guide. For information on text format, hover the cursor over the help icon. The operator `~` means contains and `!~` means does not contain.
Define Event Conditions Once you've 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:	Select the radio button for one of the following options and configure the criteria: • A group contains `<integer>` or more log occurences • Within a group, the log field `<log field>` has `<integer>` or more unique values ◦ Click the toggle icon to change to "[...] has fewer than `<integer>` unique values" • The sum of `<measure>` is greater than or equal to `<integer>` Additionally, configure the following in relation to your selection: • All logs were generated within `<integer>` minutes

5. Configure the Advanced Settings for the rule, if needed, and click *OK* to save the rule.
6. You can add more rules to the event handler, as needed. All rules for the basic event handler will have an OR relationship. To configure rules with different correlation criteria, configure a correlation event handler. For more information, see the FortiAnalyzer Administration Guide.

7. Configure the options for the event handler, and click *OK*.

Dashboards

This section lists the new features added to FortiAnalyzer for dashboards:

- SD-WAN Cloud Assisted Monitoring service widgets 7.4.1 on page 31
- Data leak prevention monitor in FortiView 7.4.1 on page 35
- FortiProxy central visibility 7.4.1 on page 38
- Compromised hosts improvements 7.4.2 on page 40
- Replay attacks in the Threat Map 7.4.2 on page 42

SD-WAN Cloud Assisted Monitoring service widgets - 7.4.1

New widgets are introduced in FortiAnalyzer 7.4.1 for the SD-WAN Cloud Assisted Monitoring service on FortiOS.

Topology

This feature requires an SD-WAN connected to the internet to run speed tests on SD-WAN member interfaces. The FortiGate must use version 7.4.0 or higher, so SD-WAN Bandwidth Monitoring Result event logs can be sent from FortiGate.

To run speed tests from the FortiGate devices:

Enter the following command to download the speed test server list from FortiGate Cloud:

```
exec speed-test-server download
```

Enter the following command to list all available servers:

```
exec speed-test-server list
```

Enter the following command to measure bandwidth on an interface to a test server:

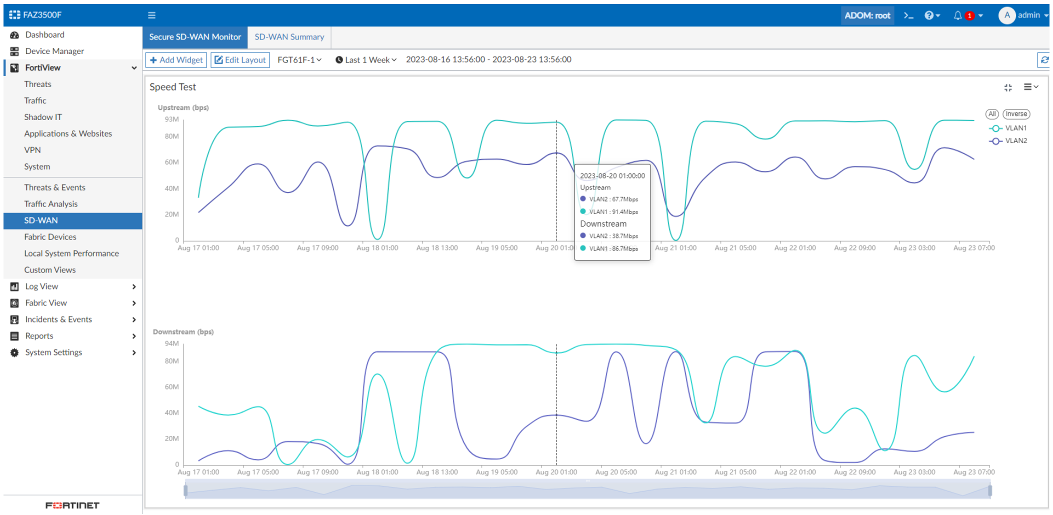
```
exec speed-test {auto | <outgoing interface name>} <server>
```

For more information, see the FortiGate / FortiOS Administration Guide.

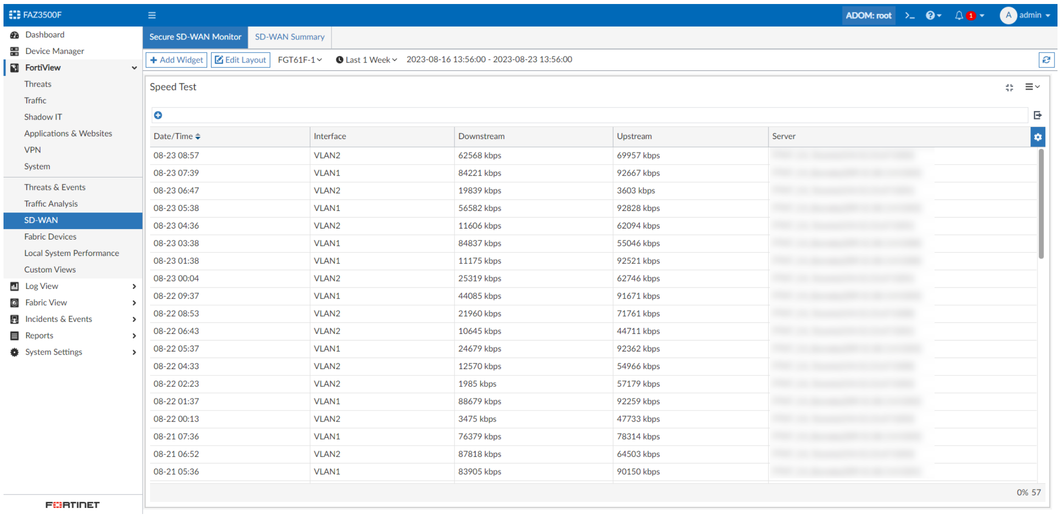
New SD-WAN Cloud Assisted Monitoring widgets and charts in FortiAnalyzer:

Speed Test is a new widget added to the *Secure SD-WAN Monitor* dashboard. This widget displays the download and upload speeds for all tests run on SD-WAN interfaces through the specified time period. You can select to display as a combined line chart or as a table chart.

The following is an example of the line chart for *Speed Test*:



The following is an example of the table for *Speed Test*:

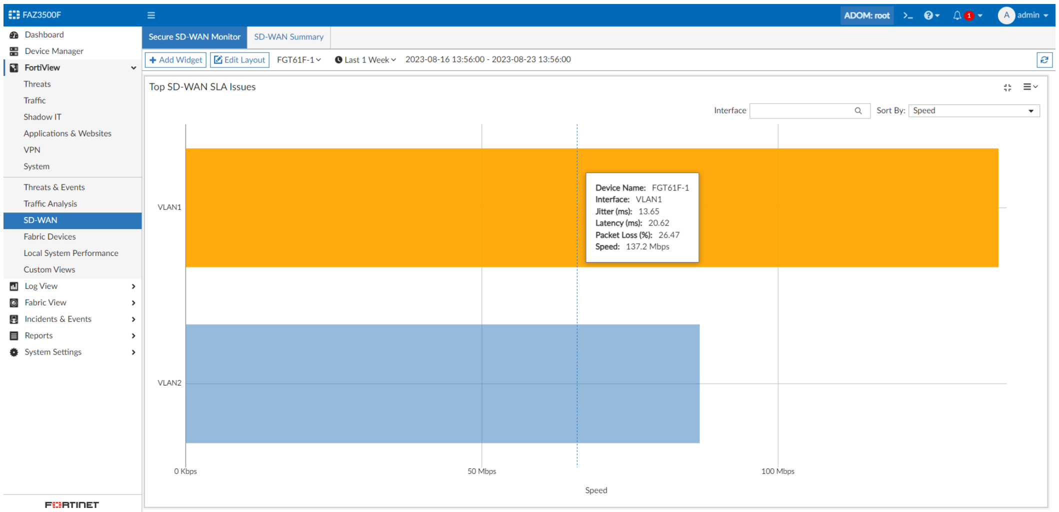


Speed Test

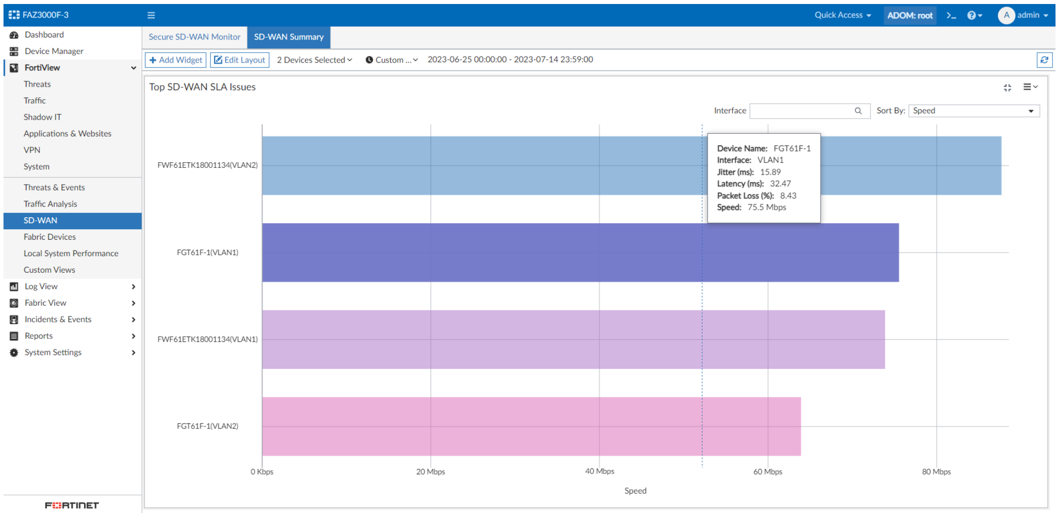
Date/Time	Interface	Downstream	Upstream	Server
08-23 08:57	VLAN2	62568 kbps	69957 kbps	[redacted]
08-23 07:39	VLAN1	84221 kbps	92667 kbps	[redacted]
08-23 06:47	VLAN2	19839 kbps	3603 kbps	[redacted]
08-23 05:38	VLAN1	56582 kbps	92828 kbps	[redacted]
08-23 04:36	VLAN2	11606 kbps	62094 kbps	[redacted]
08-23 03:38	VLAN1	84837 kbps	55046 kbps	[redacted]
08-23 01:38	VLAN1	11175 kbps	92521 kbps	[redacted]
08-23 00:04	VLAN2	25319 kbps	62746 kbps	[redacted]
08-22 09:37	VLAN1	44085 kbps	91671 kbps	[redacted]
08-22 08:53	VLAN2	21960 kbps	71761 kbps	[redacted]
08-22 06:43	VLAN2	10645 kbps	44711 kbps	[redacted]
08-22 05:37	VLAN1	24679 kbps	92362 kbps	[redacted]
08-22 04:33	VLAN2	12570 kbps	54966 kbps	[redacted]
08-22 02:23	VLAN2	1985 kbps	57179 kbps	[redacted]
08-22 01:37	VLAN1	88679 kbps	92259 kbps	[redacted]
08-22 00:13	VLAN2	3475 kbps	47733 kbps	[redacted]
08-21 07:36	VLAN1	76379 kbps	78314 kbps	[redacted]
08-21 06:52	VLAN2	87818 kbps	64503 kbps	[redacted]
08-21 05:36	VLAN1	83905 kbps	90150 kbps	[redacted]

0% 57

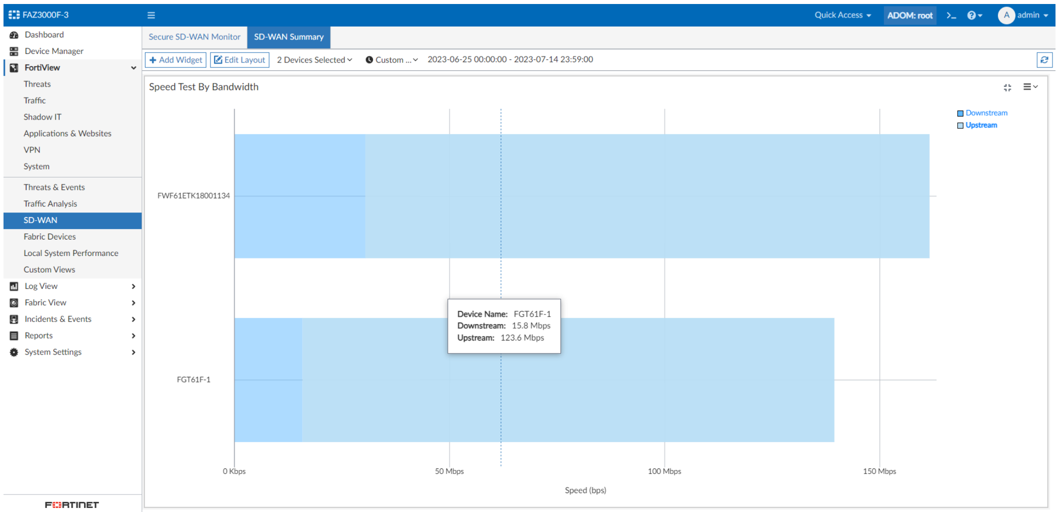
Sort By Speed is a new option added to the *Top SD-WAN SLA Issues* widget in the *Secure SD-WAN Monitor* dashboard. This option displays the peak speed run on SD-WAN interfaces through specified time period.



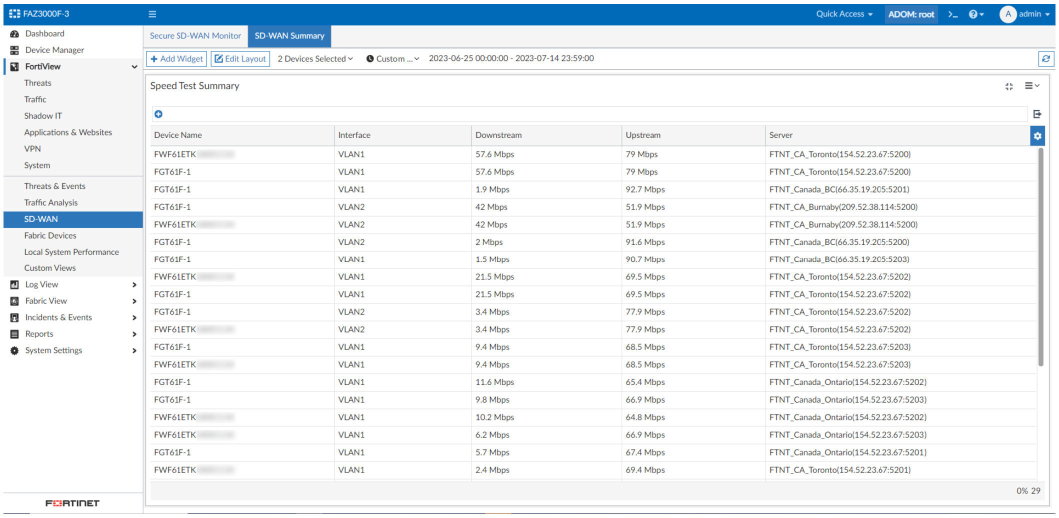
The new *Sort By Speed* option is also added to the *Top SD-WAN SLA Issues* widget in the *SD-WAN Summary* dashboard. This option displays the peak speed run on SD-WAN interfaces through specified time period for selected devices.



Speed Test By Bandwidth is a new widget added to the *SD-WAN Summary* dashboard. This widget displays a bar chart of the combined download and upload speeds for all SD-WAN interfaces on each device.



Speed Test Summary is a new widget added to the *SD-WAN Summary* dashboard. This widget displays a table of the download and upload speeds for all tests run on SD-WAN interfaces through specified time period on selected devices.



2023-06-25 00:00:00 - 2023-07-14 23:59:00

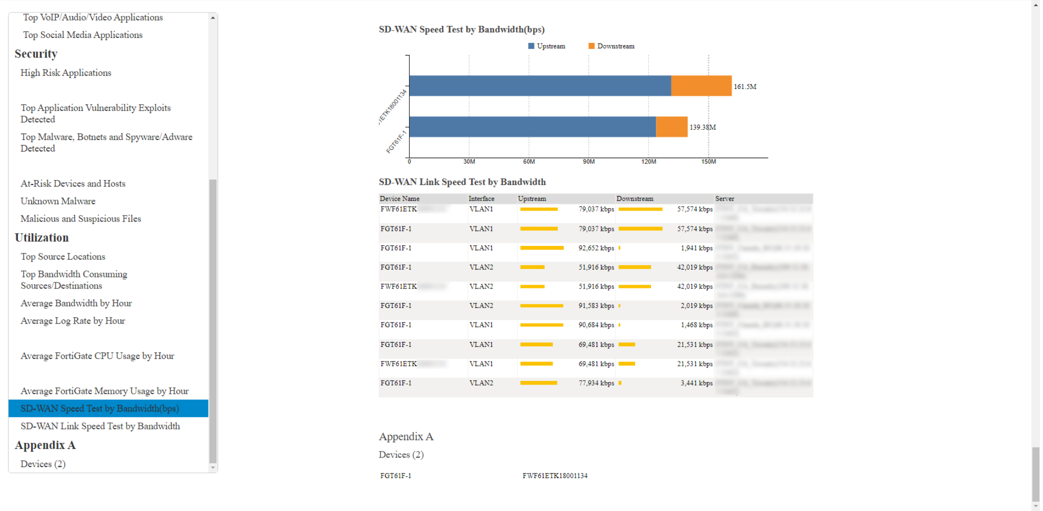
Speed Test Summary

Device Name	Interface	Downstream	Upstream	Server
FWF61ETK[redacted]	VLAN1	57.6 Mbps	79 Mbps	FTNT_CA_Toronto(154.52.23.67:5200)
FGT61F-1	VLAN1	57.6 Mbps	79 Mbps	FTNT_CA_Toronto(154.52.23.67:5200)
FGT61F-1	VLAN1	1.9 Mbps	92.7 Mbps	FTNT_Canada_BC(66.35.19.205:5201)
FGT61F-1	VLAN2	42 Mbps	51.9 Mbps	FTNT_CA_Burnaby(209.52.38.114:5200)
FWF61ETK[redacted]	VLAN2	42 Mbps	51.9 Mbps	FTNT_CA_Burnaby(209.52.38.114:5200)
FGT61F-1	VLAN2	2 Mbps	91.6 Mbps	FTNT_Canada_BC(66.35.19.205:5200)
FGT61F-1	VLAN1	1.5 Mbps	90.7 Mbps	FTNT_Canada_BC(66.35.19.205:5203)
FWF61ETK[redacted]	VLAN1	21.5 Mbps	69.5 Mbps	FTNT_CA_Toronto(154.52.23.67:5202)
FGT61F-1	VLAN1	21.5 Mbps	69.5 Mbps	FTNT_CA_Toronto(154.52.23.67:5202)
FGT61F-1	VLAN2	3.4 Mbps	77.9 Mbps	FTNT_CA_Toronto(154.52.23.67:5202)
FWF61ETK[redacted]	VLAN2	3.4 Mbps	77.9 Mbps	FTNT_CA_Toronto(154.52.23.67:5202)
FGT61F-1	VLAN1	9.4 Mbps	68.5 Mbps	FTNT_CA_Toronto(154.52.23.67:5203)
FWF61ETK[redacted]	VLAN1	9.4 Mbps	68.5 Mbps	FTNT_CA_Toronto(154.52.23.67:5203)
FGT61F-1	VLAN1	11.6 Mbps	65.4 Mbps	FTNT_Canada_Ontario(154.52.23.67:5202)
FGT61F-1	VLAN1	9.8 Mbps	66.9 Mbps	FTNT_Canada_Ontario(154.52.23.67:5203)
FWF61ETK[redacted]	VLAN1	10.2 Mbps	64.8 Mbps	FTNT_Canada_Ontario(154.52.23.67:5202)
FWF61ETK[redacted]	VLAN1	6.2 Mbps	66.9 Mbps	FTNT_Canada_Ontario(154.52.23.67:5203)
FGT61F-1	VLAN1	5.7 Mbps	67.4 Mbps	FTNT_Canada_Ontario(154.52.23.67:5201)
FWF61ETK[redacted]	VLAN1	2.4 Mbps	69.4 Mbps	FTNT_CA_Toronto(154.52.23.67:5201)

0% 29

An *SD-WAN Speed Test By Bandwidth(bps)* bar chart is added to the *Secure SD-WAN Assessment Report*. This chart displays the combined download and upload speeds for all SD-WAN interfaces on each device.

A *SD-WAN Link Speed Test by Bandwidth* table is also added to the *Secure SD-WAN Assessment Report*. This table displays the download and upload speeds for all tests run on SD-WAN interfaces through the specified time period on selected devices


Top VoIP/Audio/Video Applications
Top Social Media Applications
Security
High Risk Applications
Top Application Vulnerability Exploits Detected
Top Malware, Botnets and Spyware/Adware Detected
At-Risk Devices and Hosts
Unknown Malware
Malicious and Suspicious Files
Utilization
Top Source Locations
Top Bandwidth Consuming Sources/Destinations
Average Bandwidth by Hour
Average Log Rate by Hour
Average FortiGate CPU Usage by Hour
Average FortiGate Memory Usage by Hour
SD-WAN Speed Test by Bandwidth(bps)
SD-WAN Link Speed Test by Bandwidth
Appendix A
Devices (2)
SD-WAN Speed Test by Bandwidth(bps)
Upstream
Downstream
FWF61ETK18001134
FGT61F-1
161.5M
139.38M
0
30M
60M
90M
120M
150M

SD-WAN Link Speed Test by Bandwidth

Device Name	Interface	Upstream	Downstream	Server
FWF61ETK[redacted]	VLAN1	79,037 kbps	57,574 kbps	[redacted]
FGT61F-1	VLAN1	79,037 kbps	57,574 kbps	[redacted]
FGT61F-1	VLAN1	92,652 kbps	1,941 kbps	[redacted]
FGT61F-1	VLAN2	51,916 kbps	42,019 kbps	[redacted]
FWF61ETK[redacted]	VLAN2	51,916 kbps	42,019 kbps	[redacted]
FGT61F-1	VLAN2	91,583 kbps	2,019 kbps	[redacted]
FGT61F-1	VLAN1	90,684 kbps	1,468 kbps	[redacted]
FGT61F-1	VLAN1	69,481 kbps	21,531 kbps	[redacted]
FWF61ETK[redacted]	VLAN1	69,481 kbps	21,531 kbps	[redacted]
FGT61F-1	VLAN2	77,934 kbps	3,441 kbps	[redacted]

Appendix A

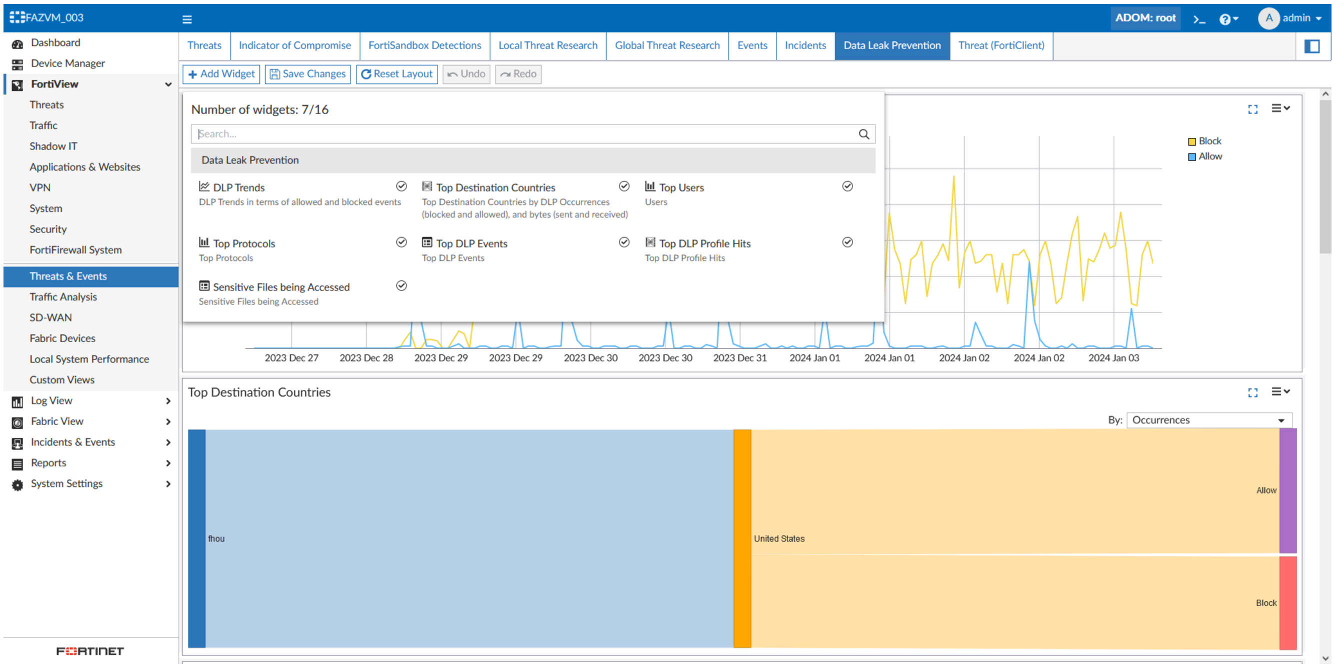
Devices (2)

FGT61F-1 FWF61ETK18001134

Data leak prevention monitor in FortiView - 7.4.1

A data leak prevention (DLP) monitor with seven new widgets has been added to FortiView in FortiAnalyzer.

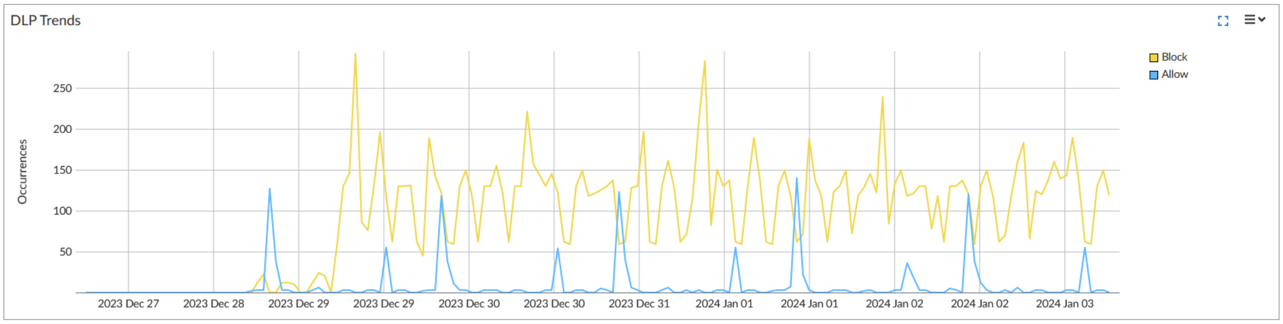
To access this monitor in the GUI, go to *FortiView* > *Threats & Events* > *Data Leak Prevention*. Widgets can be added, removed, or re-sized according to your needs.



The following widgets are available:

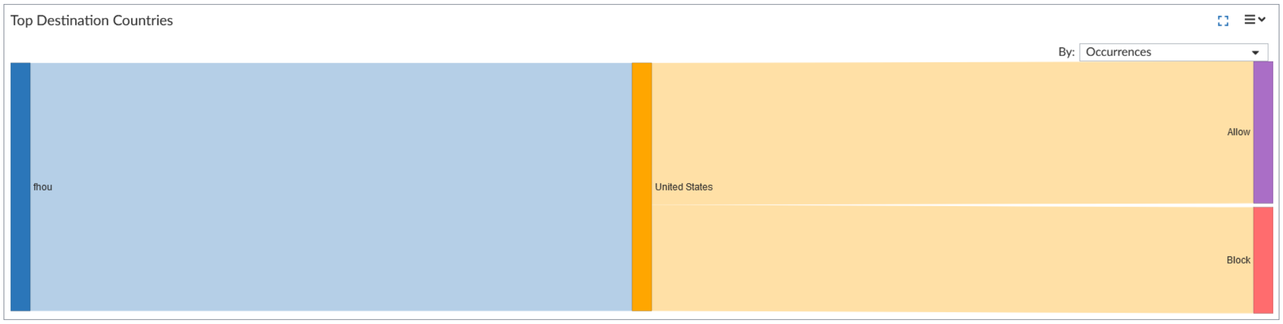
- *DLP Trends*: Line chart displaying the number of DLP occurrences over a period of time by *Allow* or *Block* security actions.

  Mouse over an area of the chart to display values at that time in a tooltip.



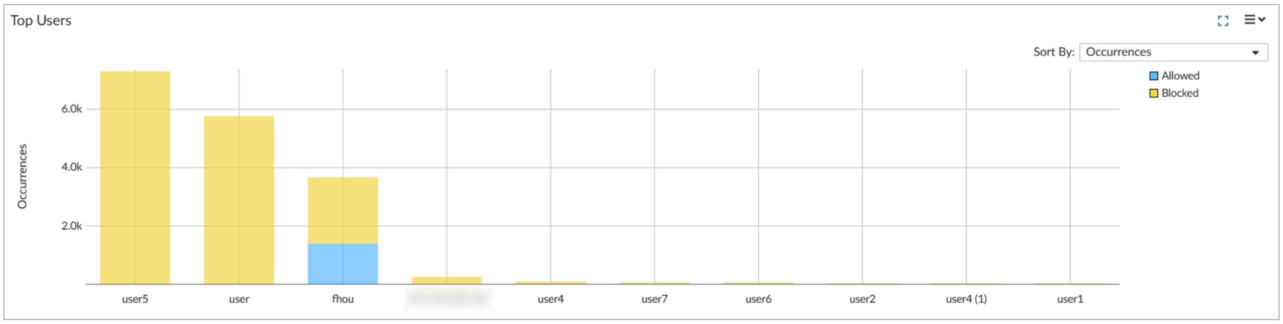
- *Top Destination Countries*: Sankey graph displaying user, destination country, and security action.

  You can change the graph to display the information by *Occurrence* or *Bytes*. Mouse over a section of the graph to display the *From*, *To*, *Session*, or *Bytes* values in a tooltip. Click a destination country to drill down to the corresponding *Log View*.



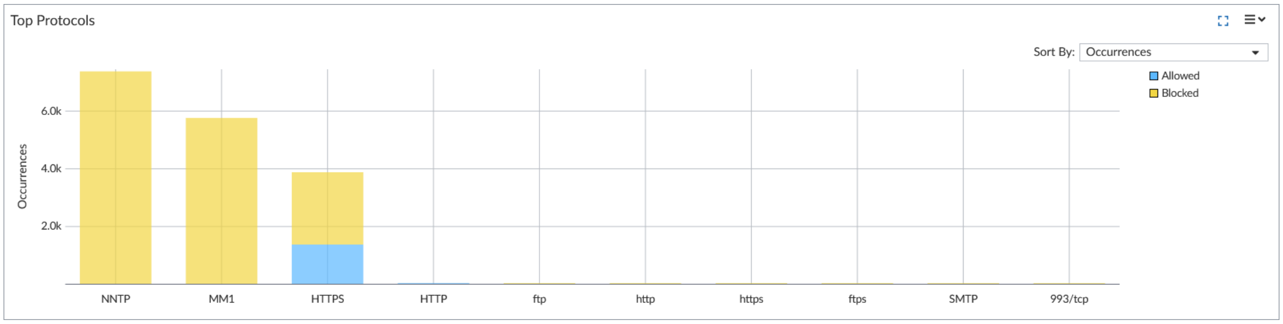
- *Top Users*: Bar graph displaying the top users for DLP.

  The graph can be sorted by *Occurrences* or *Bytes*. Mouse over a user to show the *User (Source/IP)*, *Occurrence*, and *Bytes* in a tooltip. The number of top users can be set in the widget's settings menu. Click a user to drill down to the corresponding *Log View*.



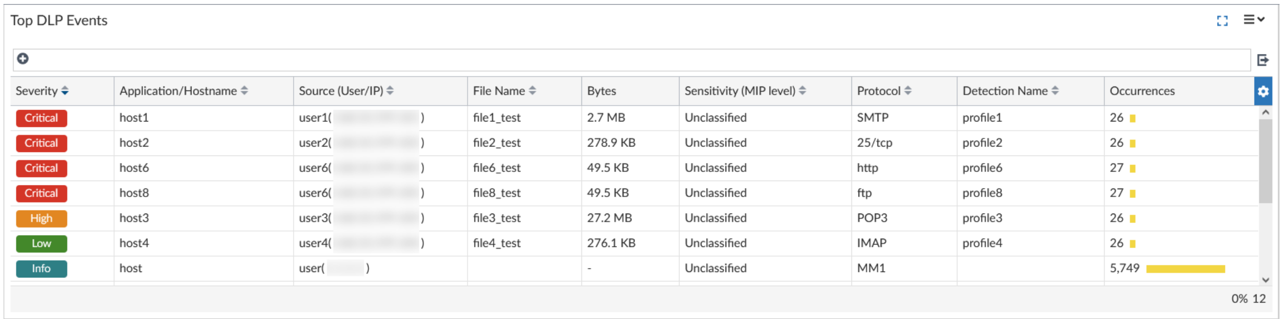
- *Top Protocols*: Bar graph displaying the top protocols for DLP.

  The view can be sorted by *Occurrences* or *Bytes*. Mouse over a protocol to display *Protocol Name*, *Occurrence*, and *Bytes* in a tooltip. The number of top protocols can be set in widget's settings menu. Click a protocol to drill down to the corresponding *Log View*.



- *Top DLP Events*: Table displaying DLP events sorted by *Severity* by default.

  The table can be sorted by other available columns: *Application/Hostname*, *Source (User/IP)*, *File Name*, *Sensitivity (MIP level)*, *Protocol*, or *Detection Name*. Click a row to drill down to the corresponding *Log View*. Any of the columns can be set as a filter for the table. Number of top DLP events can be set in widget's settings menu. The results can also be exported to PDF file or Report Chart.



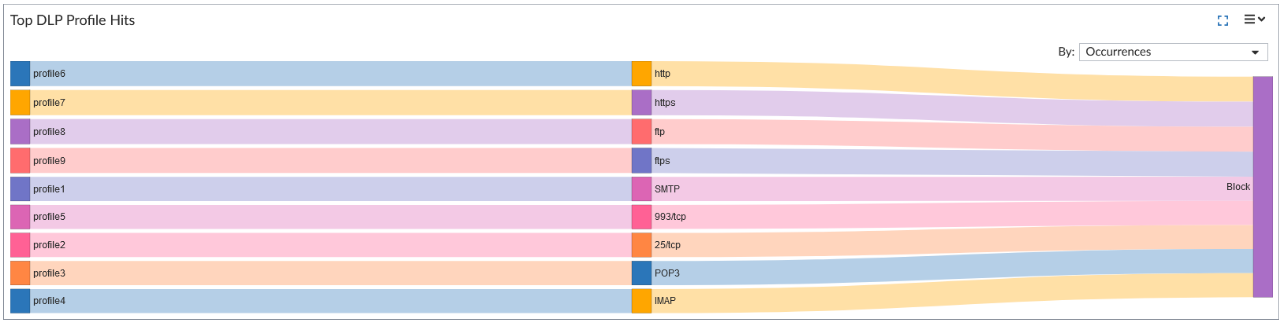
Top DLP Events

Severity	Application/Hostname	Source (User/IP)	File Name	Bytes	Sensitivity (MIP level)	Protocol	Detection Name	Occurrences
Critical	host1	user1([redacted])	file1_test	2.7 MB	Unclassified	SMTP	profile1	26
Critical	host2	user2([redacted])	file2_test	278.9 KB	Unclassified	25/tcp	profile2	26
Critical	host6	user6([redacted])	file6_test	49.5 KB	Unclassified	http	profile6	27
Critical	host8	user6([redacted])	file8_test	49.5 KB	Unclassified	ftp	profile8	27
High	host3	user3([redacted])	file3_test	27.2 MB	Unclassified	POP3	profile3	26
Low	host4	user4([redacted])	file4_test	276.1 KB	Unclassified	IMAP	profile4	26
Info	host	user([redacted])		-	Unclassified	MM1		5,749

0% 12

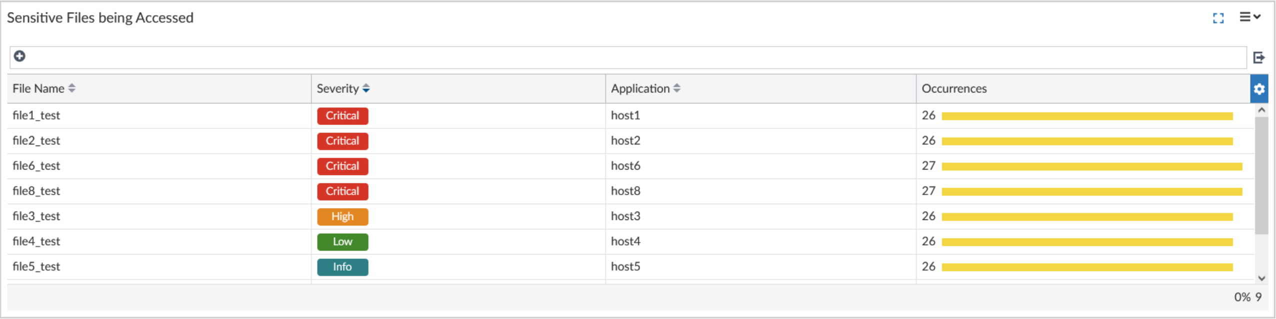
- *Top DLP Profile Hits*: Sankey graph displaying the FortiOS DLP profile name or FortiCASB filter name that triggered the DLP event, the protocols, and the security action taken.

  The graph can be sorted by *Occurrences* or *Bytes*. Mouse over a section to display the *Name*, *From*, *To*, *Session*, or *Bytes* in a tooltip according to the graph location. Click a profile to drill down to the corresponding *Log View*.



- *Sensitive Files being Accessed*: Table displaying file names and attributes set in DLP profiles.

  The table is sorted by *Severity* by default, but can also be sorted by *File Name* or *Application*. Click a row to drill down to the corresponding *Log View*. Any of the columns can be set as a filter for the table. The number of results can be set in widget's settings menu. The results can also be exported to PDF file or Report Chart.



Sensitive Files being Accessed

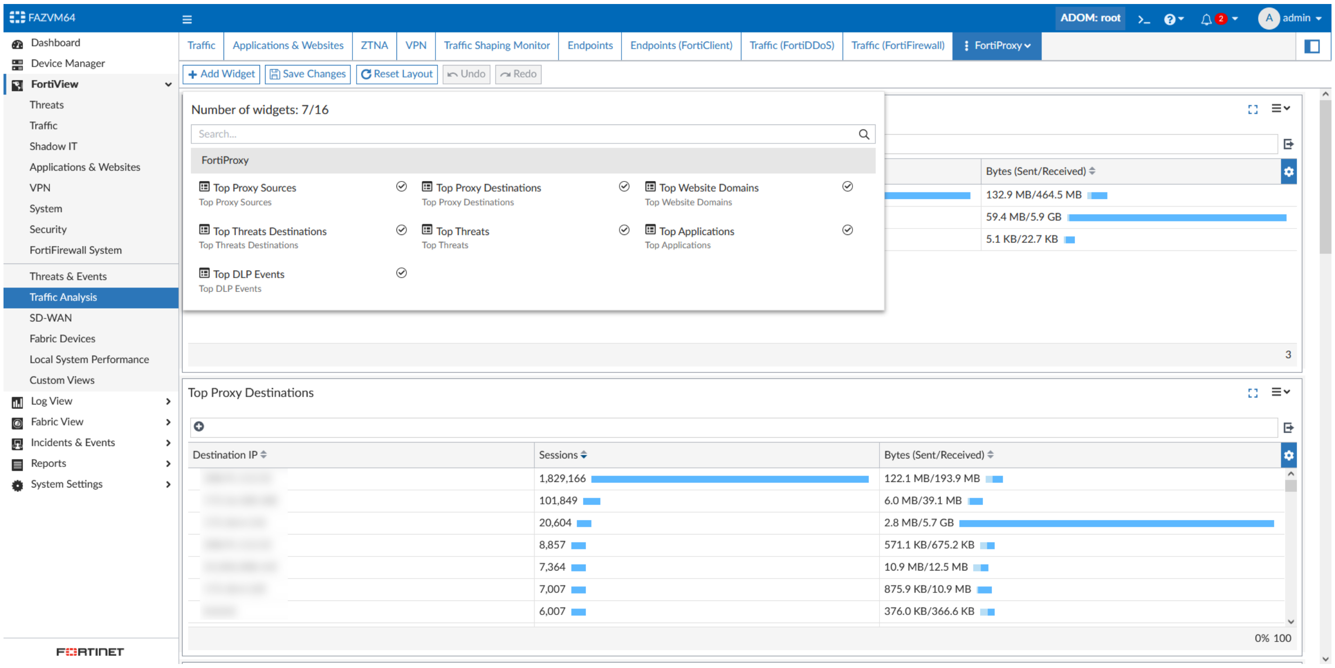
File Name	Severity	Application	Occurrences
file1_test	Critical	host1	26
file2_test	Critical	host2	26
file6_test	Critical	host6	27
file8_test	Critical	host8	27
file3_test	High	host3	26
file4_test	Low	host4	26
file5_test	Info	host5	26

0% 9

FortiProxy central visibility - 7.4.1

FortiView provides central visibility for FortiProxy deployments with the addition of the following widgets under *FortiView > Traffic Analysis > FortiProxy*.

Widgets can be added, removed, or re-sized according to your needs. You can also select the FortiProxy devices and time range to filter all widgets in the monitor.



Number of widgets: 7/16

FortiProxy

- Top Proxy Sources — Top Proxy Sources
- Top Proxy Destinations — Top Proxy Destinations
- Top Website Domains — Top Website Domains
- Top Threats Destinations — Top Threats Destinations
- Top Threats — Top Threats
- Top Applications — Top Applications
- Top DLP Events — Top DLP Events

Bytes (Sent/Received)
132.9 MB/464.5 MB
59.4 MB/5.9 GB
5.1 KB/22.7 KB

3

Top Proxy Destinations

Destination IP	Sessions	Bytes (Sent/Received)
[redacted]	1,829,166	122.1 MB/193.9 MB
[redacted]	101,849	6.0 MB/39.1 MB
[redacted]	20,604	2.8 MB/5.7 GB
[redacted]	8,857	571.1 KB/675.2 KB
[redacted]	7,364	10.9 MB/12.5 MB
[redacted]	7,007	875.9 KB/10.9 MB
[redacted]	6,007	376.0 KB/366.6 KB

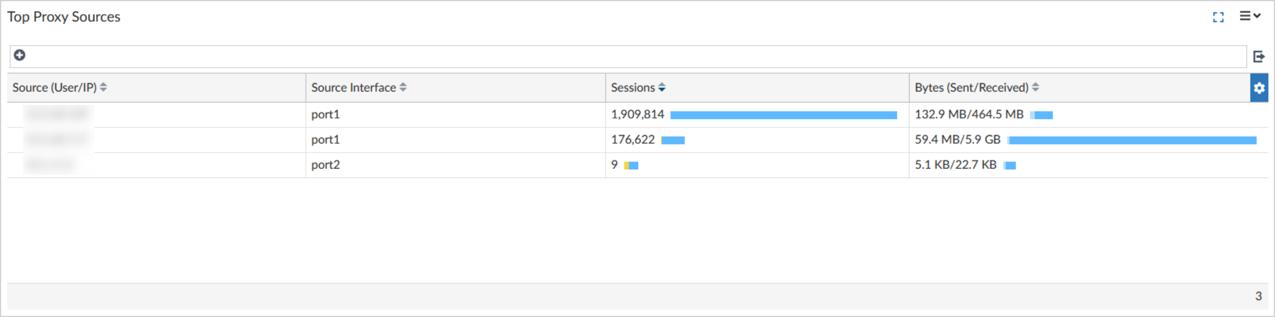
0% 100

Within each widget, you can set filters according to the available columns. You can also sort tables by any available column. From the widget's settings menu, you can set the refresh interval and, where appropriate, set the number of top results to show in the table. Click a row within a table to drill down to the corresponding *Log View*.

The following widgets are available:

- *Top Proxy Sources*: Table displaying a list of FortiProxy Sources, grouped by User/IP and sorted by number of Sessions.

  The following columns are available: Source, Source Interface, number of Sessions, and Bytes.



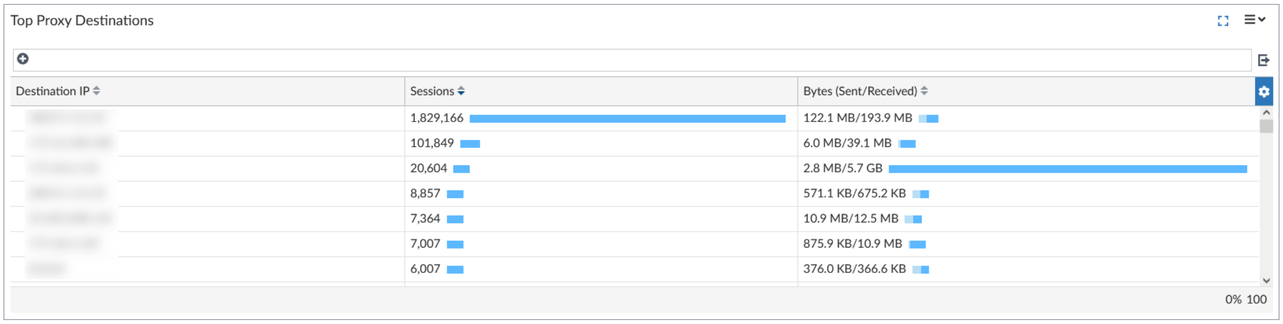
Top Proxy Sources

Source (User/IP)	Source Interface	Sessions	Bytes (Sent/Received)
[redacted]	port1	1,909,814	132.9 MB/464.5 MB
[redacted]	port1	176,622	59.4 MB/5.9 GB
[redacted]	port2	9	5.1 KB/22.7 KB

3

- *Top Proxy Destinations*: Table displaying a list of FortiProxy Destinations, grouped by Destination IP and sorted by number of Sessions.

  The following columns are available: Destination IP, number of Sessions, and Bytes.



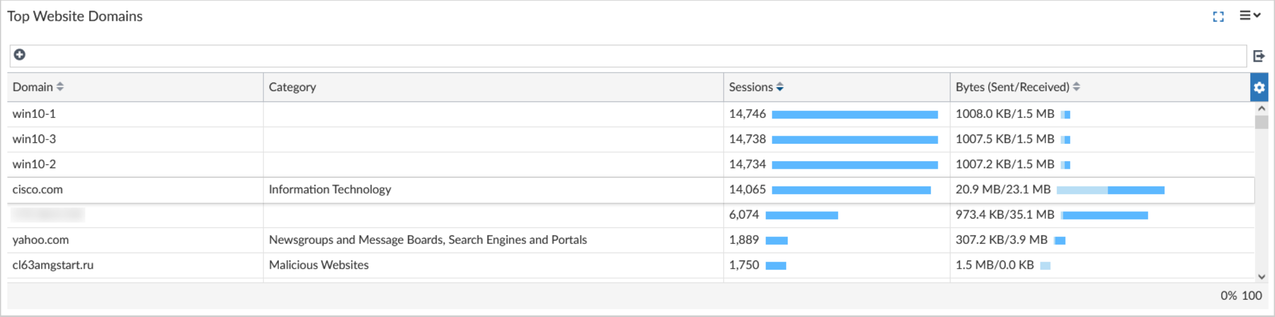
Top Proxy Destinations

Destination IP	Sessions	Bytes (Sent/Received)
[redacted]	1,829,166	122.1 MB/193.9 MB
[redacted]	101,849	6.0 MB/39.1 MB
[redacted]	20,604	2.8 MB/5.7 GB
[redacted]	8,857	571.1 KB/675.2 KB
[redacted]	7,364	10.9 MB/12.5 MB
[redacted]	7,007	875.9 KB/10.9 MB
[redacted]	6,007	376.0 KB/366.6 KB

0% 100

- *Top Website Domains*: Table displaying a list of Website Domains accessed by FortiProxy devices, grouped by Domains and sorted by number of Sessions.

  The following columns are available: Domain, Category, number of Sessions, and Bytes.



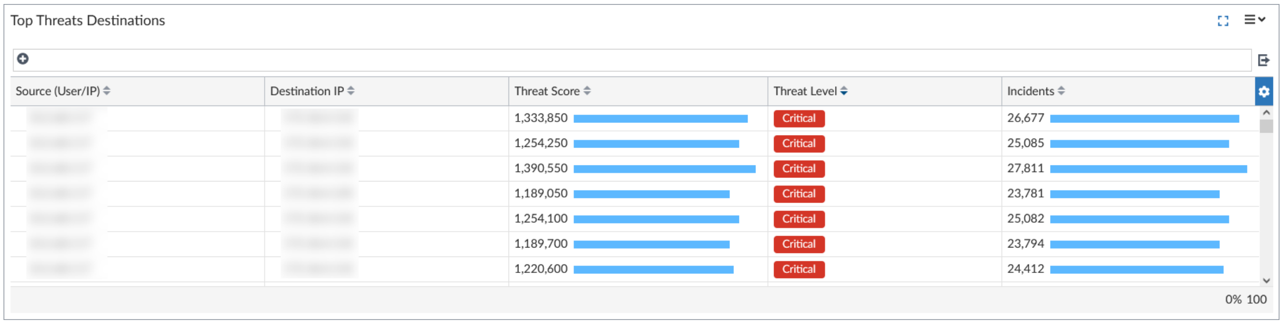
Top Website Domains

Domain	Category	Sessions	Bytes (Sent/Received)
win10-1		14,746	1008.0 KB/1.5 MB
win10-3		14,738	1007.5 KB/1.5 MB
win10-2		14,734	1007.2 KB/1.5 MB
cisco.com	Information Technology	14,065	20.9 MB/23.1 MB
[redacted]		6,074	973.4 KB/35.1 MB
yahoo.com	Newsgroups and Message Boards, Search Engines and Portals	1,889	307.2 KB/3.9 MB
cl63amgstart.ru	Malicious Websites	1,750	1.5 MB/0.0 KB

0% 100

- *Top Threats Destinations*: Table displaying a list of threat Sources and Destinations logged by FortiProxy devices sorted by Threat Level.

  The following columns are available: Source, Destination IP, Threat Score, Threat Level, and number of Incidents.



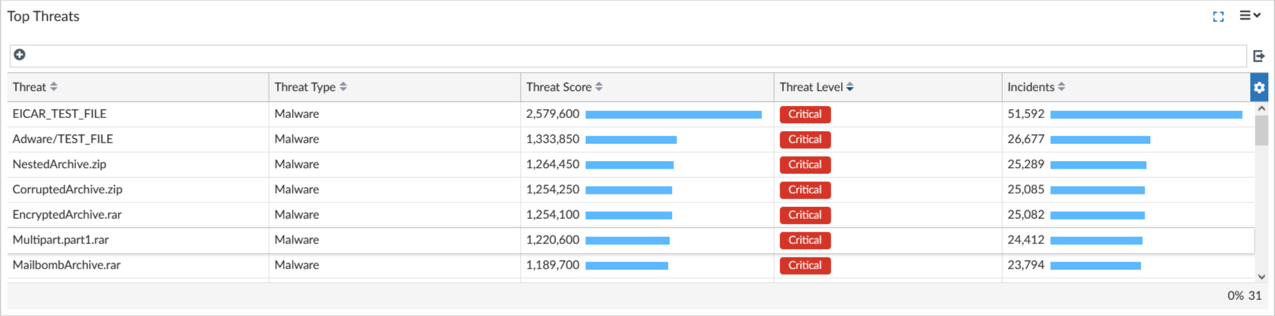
Top Threats Destinations

Source (User/IP)	Destination IP	Threat Score	Threat Level	Incidents
[redacted]	[redacted]	1,333,850	Critical	26,677
[redacted]	[redacted]	1,254,250	Critical	25,085
[redacted]	[redacted]	1,390,550	Critical	27,811
[redacted]	[redacted]	1,189,050	Critical	23,781
[redacted]	[redacted]	1,254,100	Critical	25,082
[redacted]	[redacted]	1,189,700	Critical	23,794
[redacted]	[redacted]	1,220,600	Critical	24,412

0% 100

- *Top Threats*: Table displaying a list of Threats logged by FortiProxy devices sorted by Threat Level.

The following columns are available: Threat name, Threat Type, Threat Score, Threat Level, and number of Incidents.



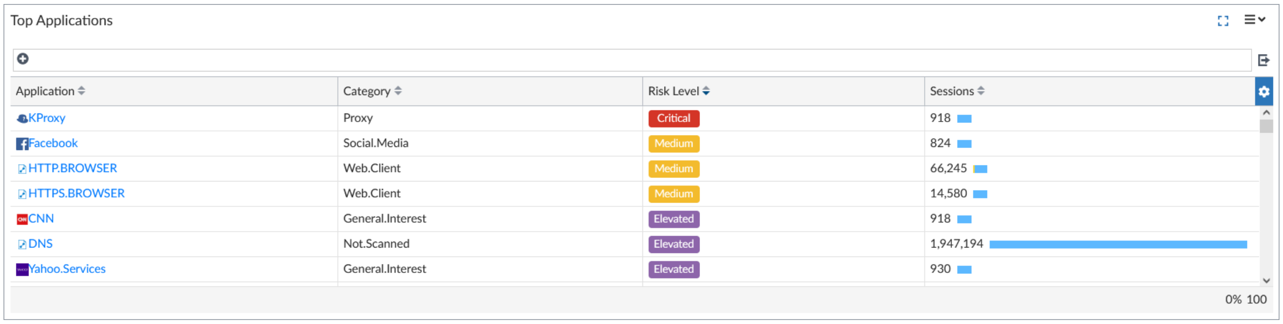
Top Threats

Threat	Threat Type	Threat Score	Threat Level	Incidents
EICAR_TEST_FILE	Malware	2,579,600	Critical	51,592
Adware/TEST_FILE	Malware	1,333,850	Critical	26,677
NestedArchive.zip	Malware	1,264,450	Critical	25,289
CorruptedArchive.zip	Malware	1,254,250	Critical	25,085
EncryptedArchive.rar	Malware	1,254,100	Critical	25,082
Multipart.part1.rar	Malware	1,220,600	Critical	24,412
MailbombArchive.rar	Malware	1,189,700	Critical	23,794

0% 31

- *Top Applications*: Table displaying a list of Applications used and logged by FortiProxy devices sorted by Risk Level.

  The following columns are available: Application name, Category, Risk Level, and number of Sessions.



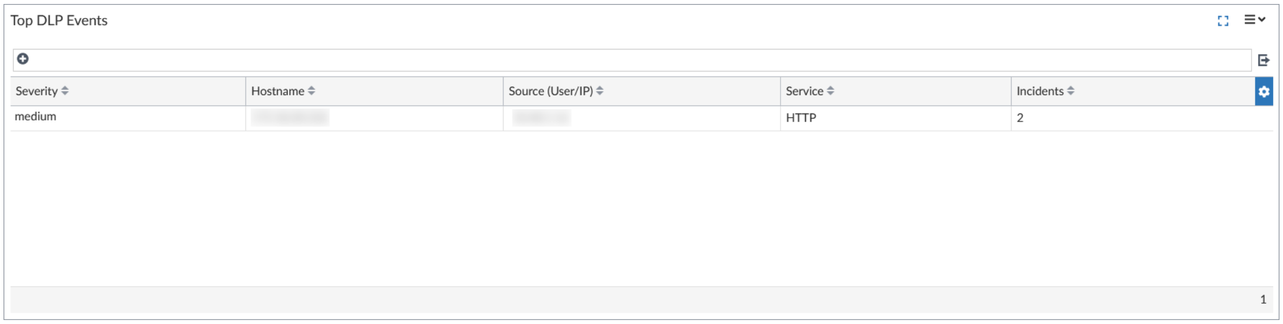
Top Applications

Application	Category	Risk Level	Sessions
KProxy	Proxy	Critical	918
Facebook	Social.Media	Medium	824
HTTP.BROWSER	Web.Client	Medium	66,245
HTTPS.BROWSER	Web.Client	Medium	14,580
CNN	General.Interest	Elevated	918
DNS	Not.Scanned	Elevated	1,947,194
Yahoo.Services	General.Interest	Elevated	930

0% 100

- *Top DLP Events*: Table displaying a list of Data Loss Prevention (DLP) events logged by FortiProxy devices sorted by Severity.

  The following columns are available: Severity, Hostname, Source, Service, number of Incidents.



Top DLP Events

Severity	Hostname	Source (User/IP)	Service	Incidents
medium	[redacted]	[redacted]	HTTP	2

1

Compromised hosts improvements - 7.4.2

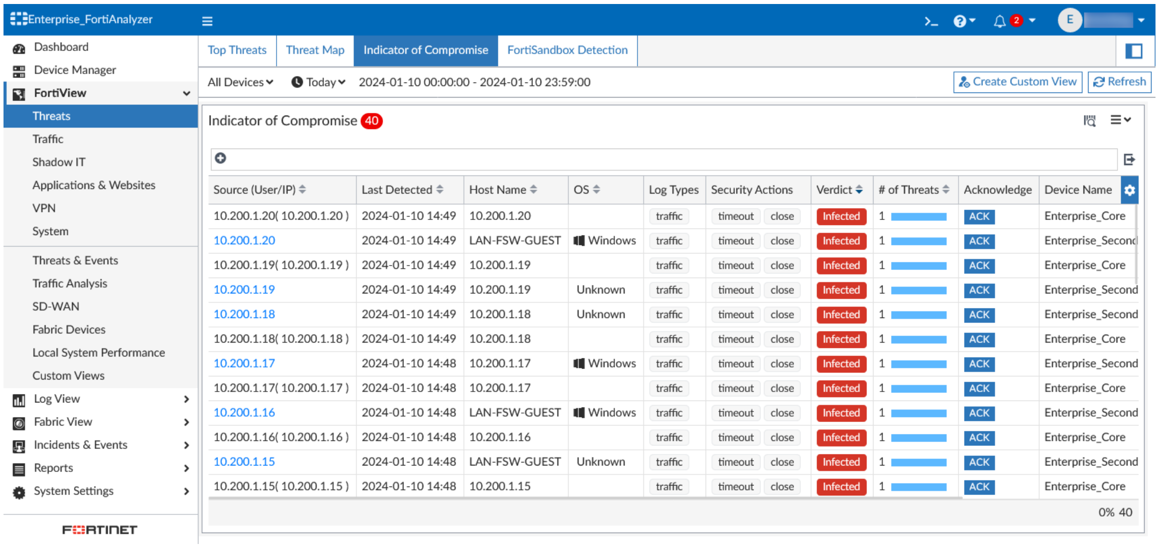
This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Working with IOC information

The FortiAnalyzer *Compromised Hosts* dashboard has been renamed to *Indicator of Compromise*. To access the dashboard, go to *FortiView* > *Threats* > *Indicator of Compromise*.

The table view in *Indicator of Compromise* includes two new columns:

- *Log Types*
- *Security Actions*



2024-01-10 00:00:00 - 2024-01-10 23:59:00

Indicator of Compromise 40

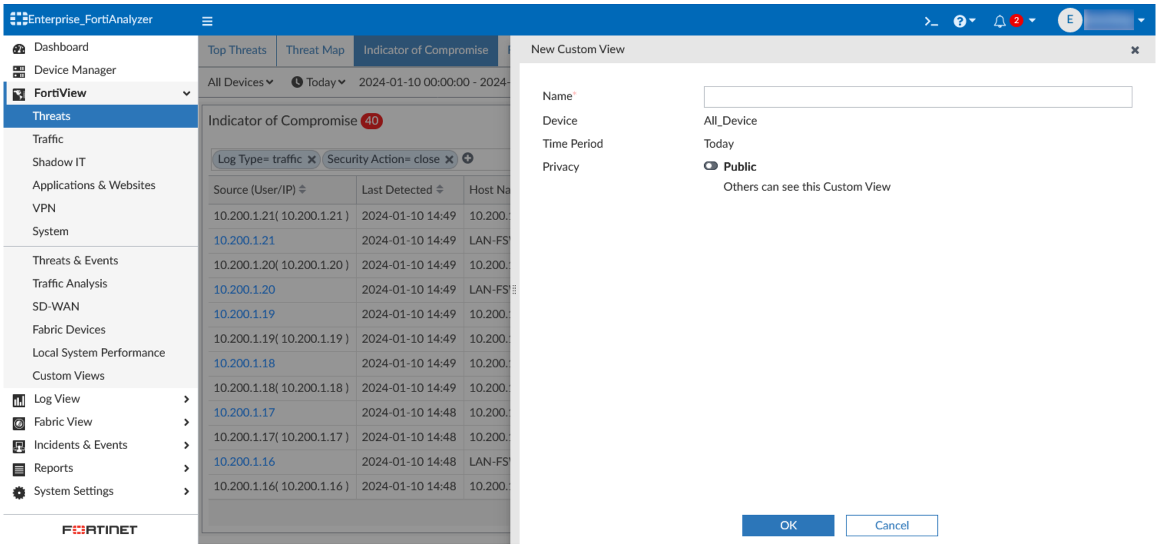
Source (User/IP)	Last Detected	Host Name	OS	Log Types	Security Actions	Verdict	# of Threats	Acknowledge	Device Name
10.200.1.20(10.200.1.20)	2024-01-10 14:49	10.200.1.20		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.20	2024-01-10 14:49	LAN-FSW-GUEST	Windows	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.19(10.200.1.19)	2024-01-10 14:49	10.200.1.19		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.19	2024-01-10 14:49	10.200.1.19	Unknown	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.18	2024-01-10 14:49	10.200.1.18	Unknown	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.18(10.200.1.18)	2024-01-10 14:49	10.200.1.18		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.17	2024-01-10 14:48	10.200.1.17	Windows	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.17(10.200.1.17)	2024-01-10 14:48	10.200.1.17		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.16	2024-01-10 14:48	LAN-FSW-GUEST	Windows	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.16(10.200.1.16)	2024-01-10 14:48	10.200.1.16		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.15	2024-01-10 14:48	LAN-FSW-GUEST	Unknown	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.15(10.200.1.15)	2024-01-10 14:48	10.200.1.15		traffic	timeout close	Infected	1	ACK	Enterprise_Core

0% 40

You can now filter the table by log types and firewall security actions.

You can also create a custom view for the *Indicator of Compromise* table directly from the dashboard. After setting your filters in *FortiView* > *Threats* > *Indicator of Compromise*, click *Create Custom View*. In the *New Custom View* pane, configure the following options and click *OK*.

Name	Enter a name for the custom view.
Device	Displays the devices to be used for the custom view.
Time Period	Displays the time period to be used for the custom view.
Privacy	Toggle to *Public* or *Private*.



Indicator of Compromise 40

Log Type= traffic × Security Action= close ×

New Custom View

Name*

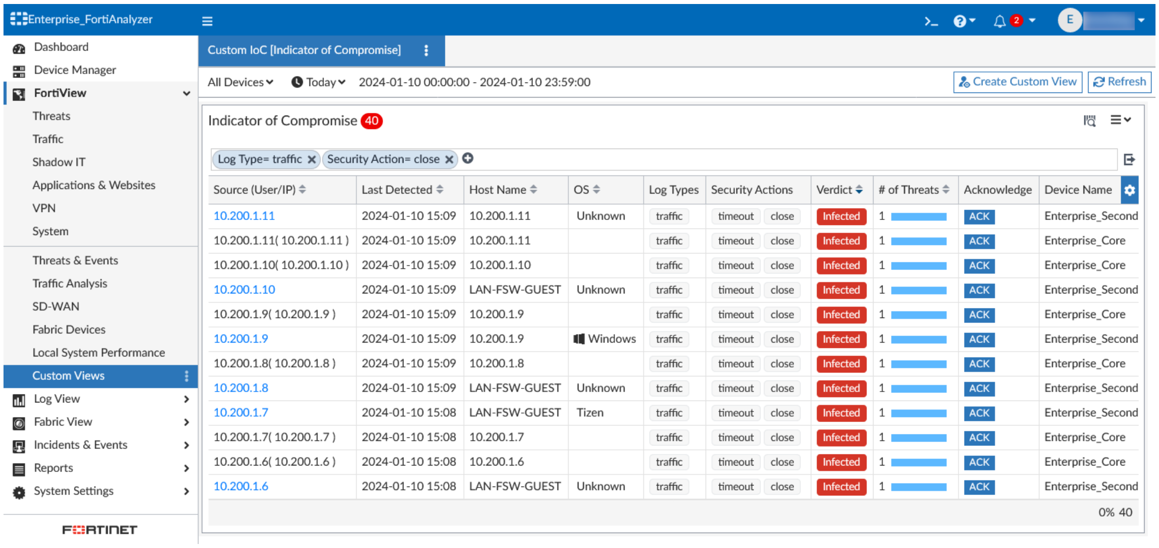
Device All_Device

Time Period Today

Privacy Public

Others can see this Custom View

To open your custom view, go to *FortiView* > *Custom View* > *[Name of the Indicator of Compromise custom view]*. The dashboard displays the filters you had set prior to creating the custom view.



All Devices Today 2024-01-10 00:00:00 - 2024-01-10 23:59:00

Indicator of Compromise 40

Log Type= traffic ✕ Security Action= close ✕

Source (User/IP)	Last Detected	Host Name	OS	Log Types	Security Actions	Verdict	# of Threats	Acknowledge	Device Name
10.200.1.11	2024-01-10 15:09	10.200.1.11	Unknown	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.11(10.200.1.11)	2024-01-10 15:09	10.200.1.11		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.10(10.200.1.10)	2024-01-10 15:09	10.200.1.10		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.10	2024-01-10 15:09	LAN-FSW-GUEST	Unknown	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.9(10.200.1.9)	2024-01-10 15:09	10.200.1.9		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.9	2024-01-10 15:09	10.200.1.9	Windows	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.8(10.200.1.8)	2024-01-10 15:09	10.200.1.8		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.8	2024-01-10 15:09	LAN-FSW-GUEST	Unknown	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.7	2024-01-10 15:08	LAN-FSW-GUEST	Tizen	traffic	timeout close	Infected	1	ACK	Enterprise_Second
10.200.1.7(10.200.1.7)	2024-01-10 15:08	10.200.1.7		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.6(10.200.1.6)	2024-01-10 15:08	10.200.1.6		traffic	timeout close	Infected	1	ACK	Enterprise_Core
10.200.1.6	2024-01-10 15:08	LAN-FSW-GUEST	Unknown	traffic	timeout close	Infected	1	ACK	Enterprise_Second

0% 40

Replay attacks in the Threat Map - 7.4.2

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Viewing FortiView dashboards

In *FortiView* > *Threats* > *Threat Map*, you can now replay threats from historical UTM logs.

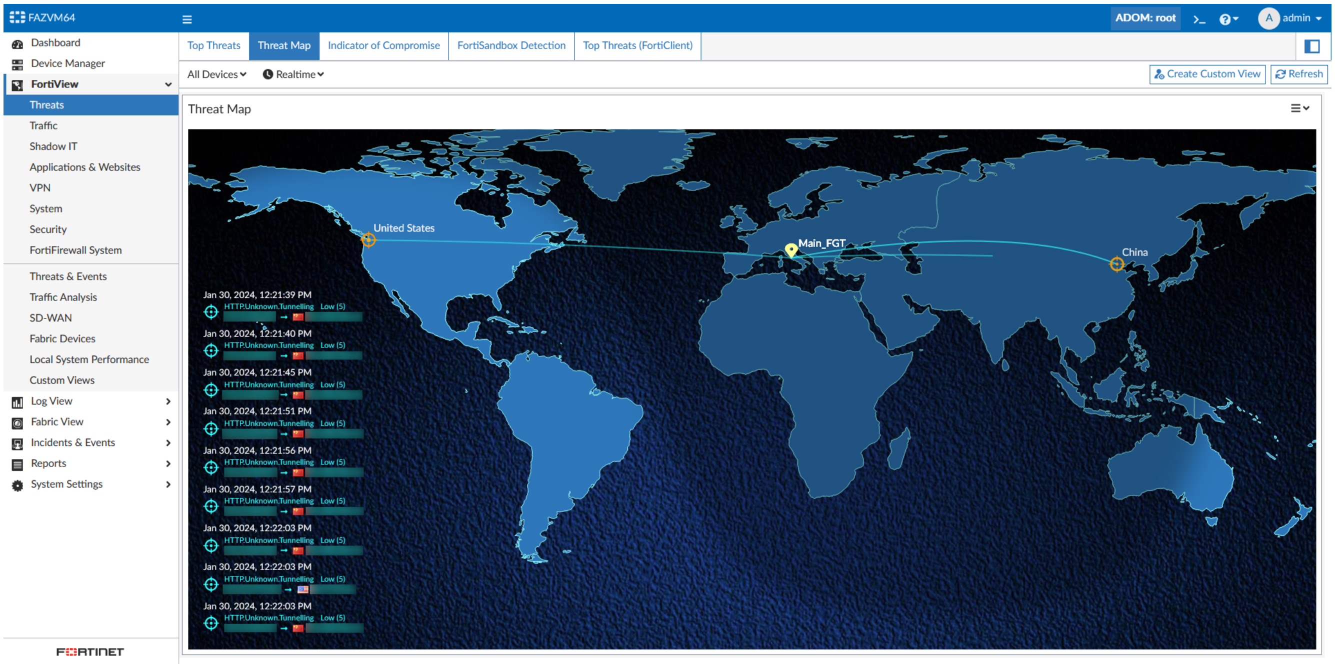
The following options are available in the toolbar and map view for the *Threat Map*:

Option	Description
Timeframe	Select *Realtime* to display threats in the map as soon as they are received by FortiAnalyzer. Alternatively, select a timeframe to display historical UTM logs fetched from the database and replay them in order of occurrence.
Devices	Select devices to filter the threats, if needed.
Pause/Play	This option only available when the timeframe is not *Realtime*. Click to pause or play the threats replay in the map. The ring around the play/pause button indicates the progress of the replay.
Replay rate	This option only available when the timeframe is not *Realtime*. Use the plus (+) and minus (-) buttons to increase or decrease the replay speed. The fastest replay speed is 7 and the slowest is 1. The default is 3.

The list of threats that overlays the map view displays the following data:

- Date and time of threat
- Threat name
- Threat level
- Threat Source and Destination IPs, threat direction, and country flag if it is available

Below is an example of the *Threat Map* displaying threats in *Realtime*:



Jan 30, 2024, 12:21:39 PM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 12:21:40 PM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 12:21:45 PM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 12:21:51 PM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 12:21:56 PM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

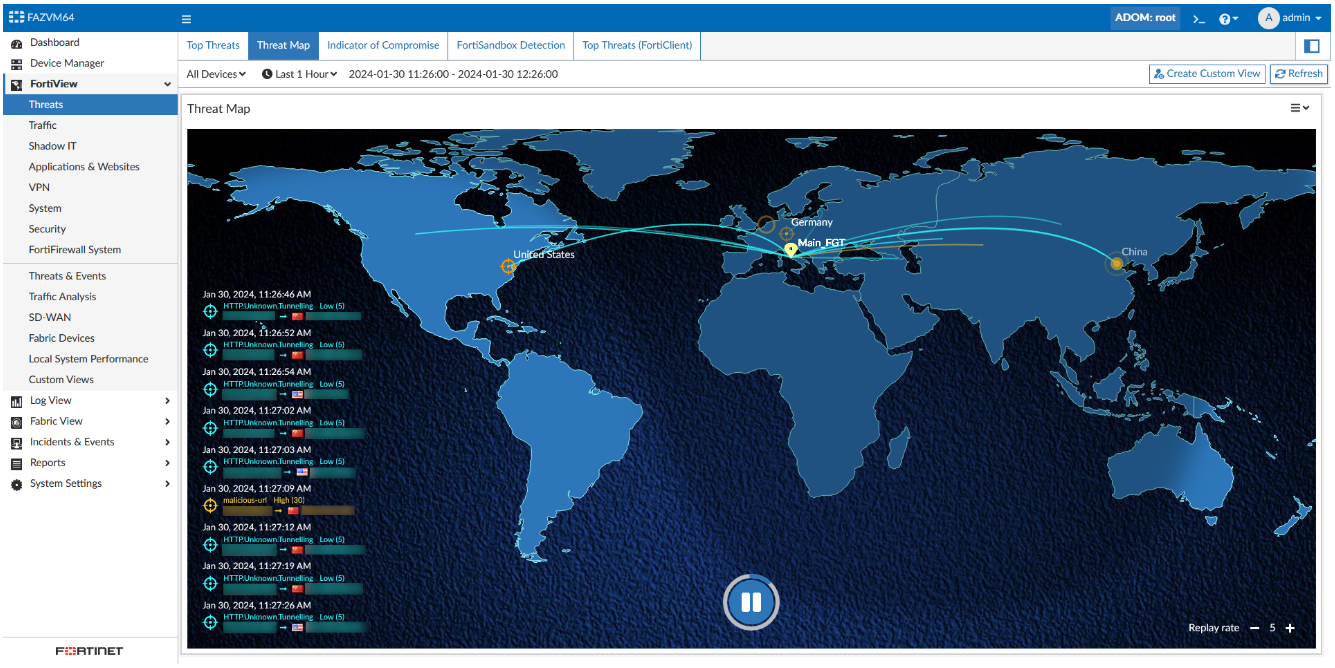
Jan 30, 2024, 12:21:57 PM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 12:22:03 PM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 12:22:03 PM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇺🇸 [redacted]

Jan 30, 2024, 12:22:03 PM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Below is an example of the *Threat Map* displaying a replay of threats from the last hour:



2024-01-30 11:26:00 - 2024-01-30 12:26:00

Jan 30, 2024, 11:26:46 AM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 11:26:52 AM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 11:26:54 AM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇺🇸 [redacted]

Jan 30, 2024, 11:27:02 AM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 11:27:03 AM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇺🇸 [redacted]

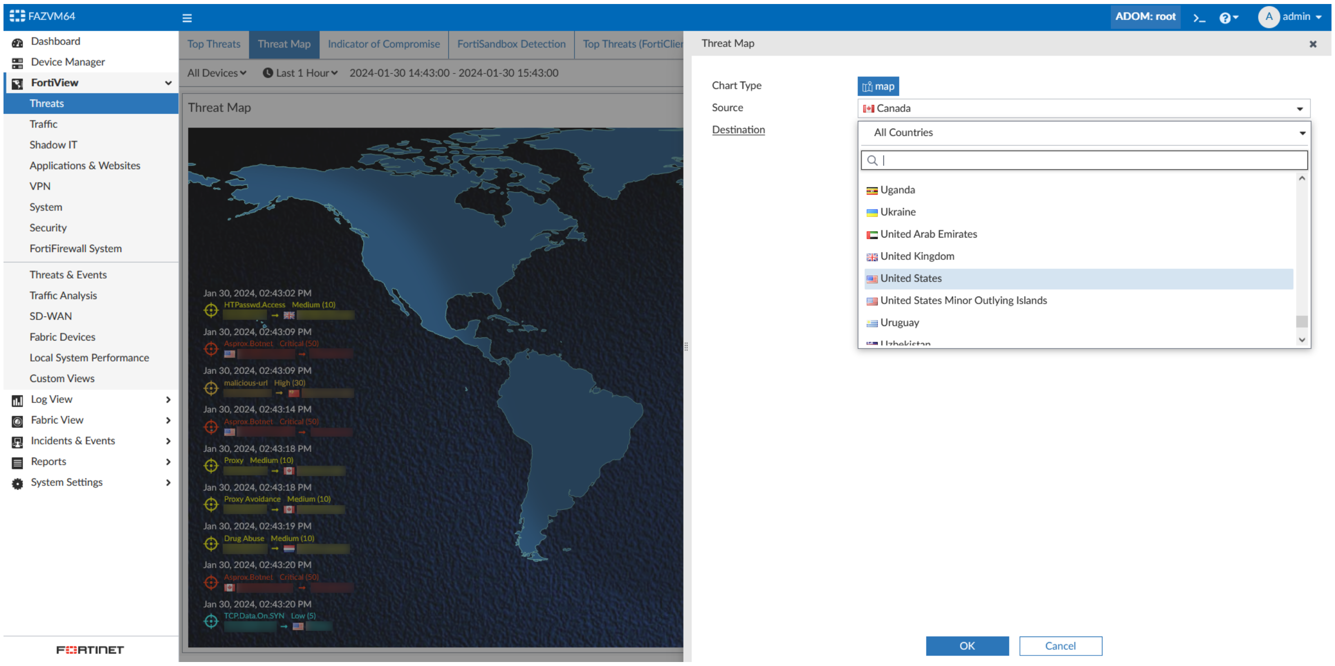
Jan 30, 2024, 11:27:09 AM
malicious-url High (30)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 11:27:12 AM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 11:27:19 AM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇨🇳 [redacted]

Jan 30, 2024, 11:27:26 AM
HTTP.Unknown.Tunnelling Low (5)
[redacted] → 🇺🇸 [redacted]

From the settings menu for the *Threat Map*, you can select the Source and/or Destination country of the threat. For example, see below.



2024-01-30 14:43:00 - 2024-01-30 15:43:00

Jan 30, 2024, 02:43:02 PM
HTPasswd.Access Medium (10)

Jan 30, 2024, 02:43:09 PM
Asprox.Botnet Critical (50)

Jan 30, 2024, 02:43:09 PM
malicious-url High (30)

Jan 30, 2024, 02:43:14 PM
Asprox.Botnet Critical (50)

Jan 30, 2024, 02:43:18 PM
Proxy Medium (10)

Jan 30, 2024, 02:43:18 PM
Proxy Avoidance Medium (10)

Jan 30, 2024, 02:43:19 PM
Drug Abuse Medium (10)

Jan 30, 2024, 02:43:20 PM
Asprox.Botnet Critical (50)

Jan 30, 2024, 02:43:20 PM
TCP.Data.On.SYN Low (5)

Threat Map

Chart Type: map
Source: Canada
Destination: All Countries

- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay
- Uzbekistan

Asset and Identity

This section lists the new features added to FortiAnalyzer for asset and identity:

- New charts in the Asset Identity Center on page 44

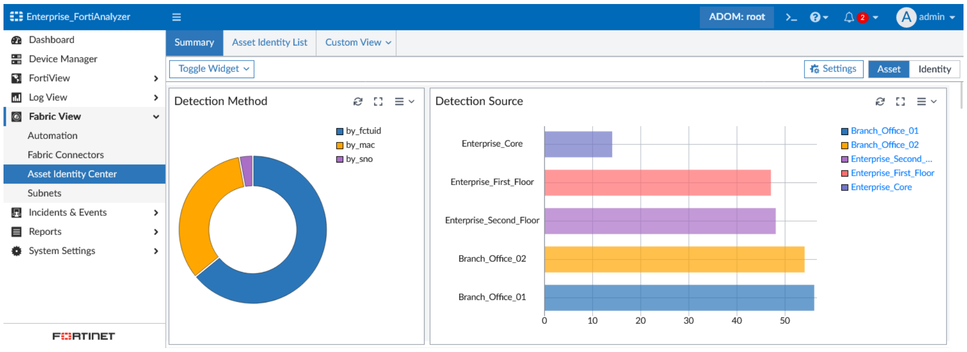
New charts in the Asset Identity Center

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Asset Summary
- Identity Summary

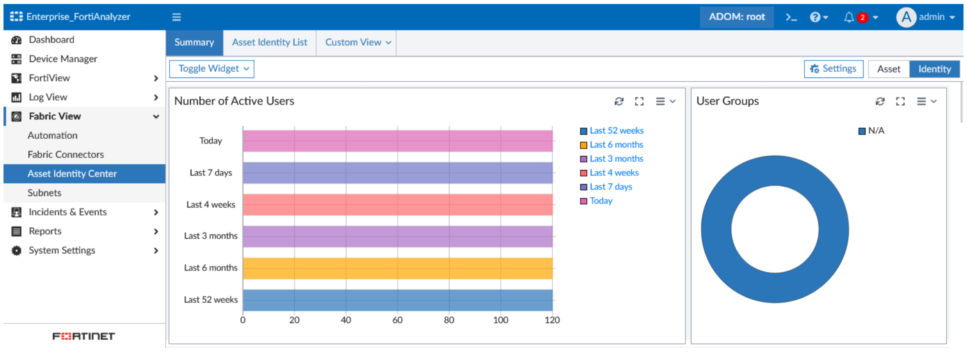
The new *Asset Identity Center* pane combines the previous *Asset Center* and *Identity Center* panes. There are new and updated widgets in the *Asset Identity Center*, which can be used for analysis of endpoints and end users.

Go to *Fabric View* > *Asset Identity Center* > *Summary*. By default, the pane displays the *Asset* dashboard. You can click *Identity* to display the *Identity* dashboard. From the *Toggle Widgets* dropdown, select which widgets should display on the dashboard. You can filter all widgets on the dashboard from *Settings*.



The *Asset* dashboard includes the following widgets:

Detection Method	Displays endpoint detections by method.
Detection Source	Displays a breakdown of the asset center data sources.
Identification/Unidentified Asset	Displays the number of detected endpoint assets that are identified and unidentified.
Hardware/OS Distribution	Displays endpoint hardware operating system distribution.
Discovery Timeline	Displays an asset discovery timeline.
Identified Active Asset	Displays identified asset visibility over the past 24 hours to 52 weeks.
Assets By Location	Displays identified assets by location.
Identified Activity Timeline	Displays a first seen, last update, and last seen identified asset activity timeline.
Changes Timeline	Displays an asset changes timeline.
Unidentifed Active Asset	Displays unidentified asset visibility over the past 24 hours to 52 weeks.
Unidentifed Activity Timeline	Displays a first seen, last update, and last seen unidentified asset activity timeline.



The *Identity* dashboard includes the following widgets:

Top Users	Displays asset user data.
Number of Active Users	Displays user visibility data over the past 24 hours to 52 weeks.
User Groups	Displays user groups.

User's Location	Displays user numbers by location.
User's Manager	Displays user numbers by manager.
Discovery Timeline	Displays the user discovery timeline.
Activity Timeline	Displays the user activity timeline.
Endpoint Tag Distribution	Displays the distribution of endpoint tags.

Others

This section lists the new features added to FortiAnalyzer for other topics related to security operations:

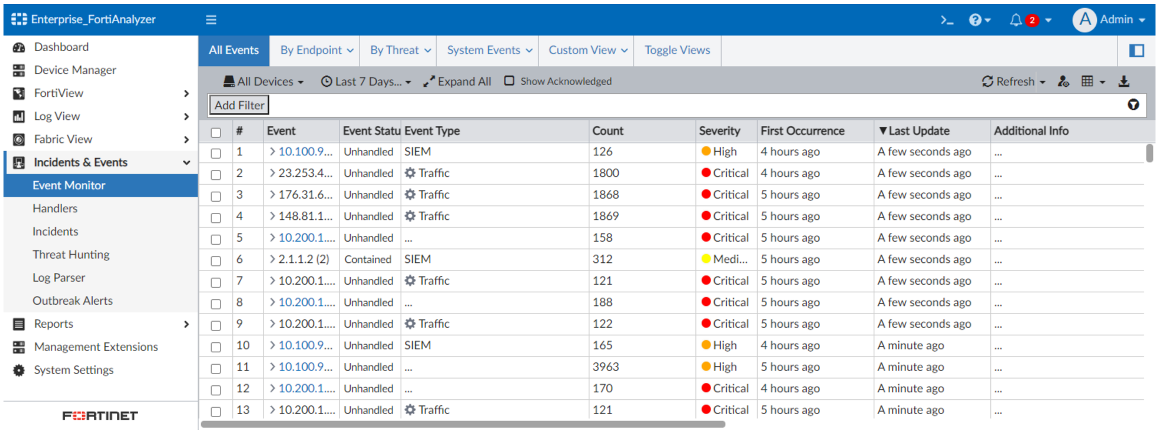
- FortiSoC GUI reorganization on page 46
- Notifications for new Outbreak Alerts 7.4.1 on page 49
- MITRE ATT&CK matrices for Enterprise and ICS 7.4.1 on page 51
- Deliver reports, event handlers, and SIEM rules as FortiGuard packages 7.4.2 on page 62
- MITRE information included in outbreak detection 7.4.2 on page 66

FortiSoC GUI reorganization

The *FortiSoC* features have been organized in the following areas of the GUI:

- *Incidents & Events*
- *FortiView*
- *Fabric View*

To create and manage events, go to *Incidents & Events*.



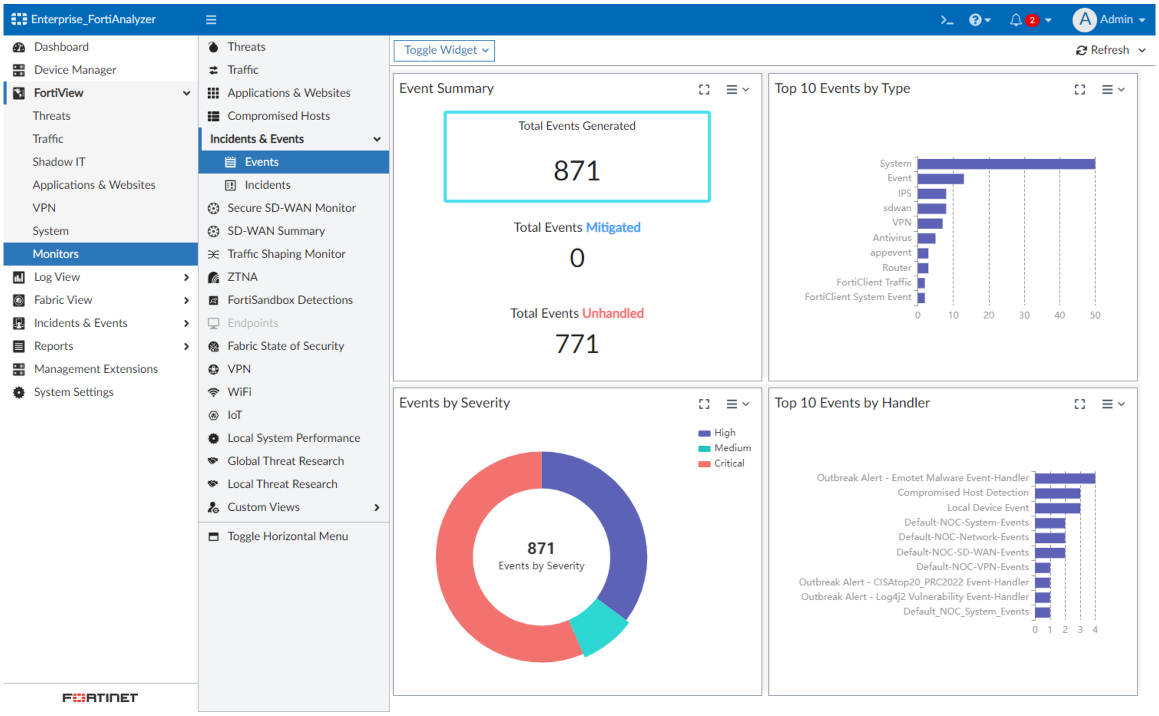
□	#	Event	Event Statu	Event Type	Count	Severity	First Occurrence	▼Last Update	Additional Info
□	1	> 10.100.9...	Unhandled	SIEM	126	● High	4 hours ago	A few seconds ago	...
□	2	> 23.253.4...	Unhandled	Traffic	1800	● Critical	4 hours ago	A few seconds ago	...
□	3	> 176.31.6...	Unhandled	Traffic	1868	● Critical	5 hours ago	A few seconds ago	...
□	4	> 148.81.1...	Unhandled	Traffic	1869	● Critical	5 hours ago	A few seconds ago	...
□	5	> 10.200.1....	Unhandled	...	158	● Critical	5 hours ago	A few seconds ago	...
□	6	> 2.1.1.2 (2)	Contained	SIEM	312	● Medi...	5 hours ago	A few seconds ago	...
□	7	> 10.200.1....	Unhandled	Traffic	121	● Critical	5 hours ago	A few seconds ago	...
□	8	> 10.200.1....	Unhandled	...	188	● Critical	5 hours ago	A few seconds ago	...
□	9	> 10.200.1....	Unhandled	Traffic	122	● Critical	5 hours ago	A few seconds ago	...
□	10	> 10.100.9...	Unhandled	SIEM	165	● High	4 hours ago	A minute ago	...
□	11	> 10.100.9...	Unhandled	...	3963	● High	5 hours ago	A minute ago	...
□	12	> 10.200.1....	Unhandled	...	170	● Critical	4 hours ago	A minute ago	...
□	13	> 10.200.1....	Unhandled	Traffic	121	● Critical	5 hours ago	A minute ago	...

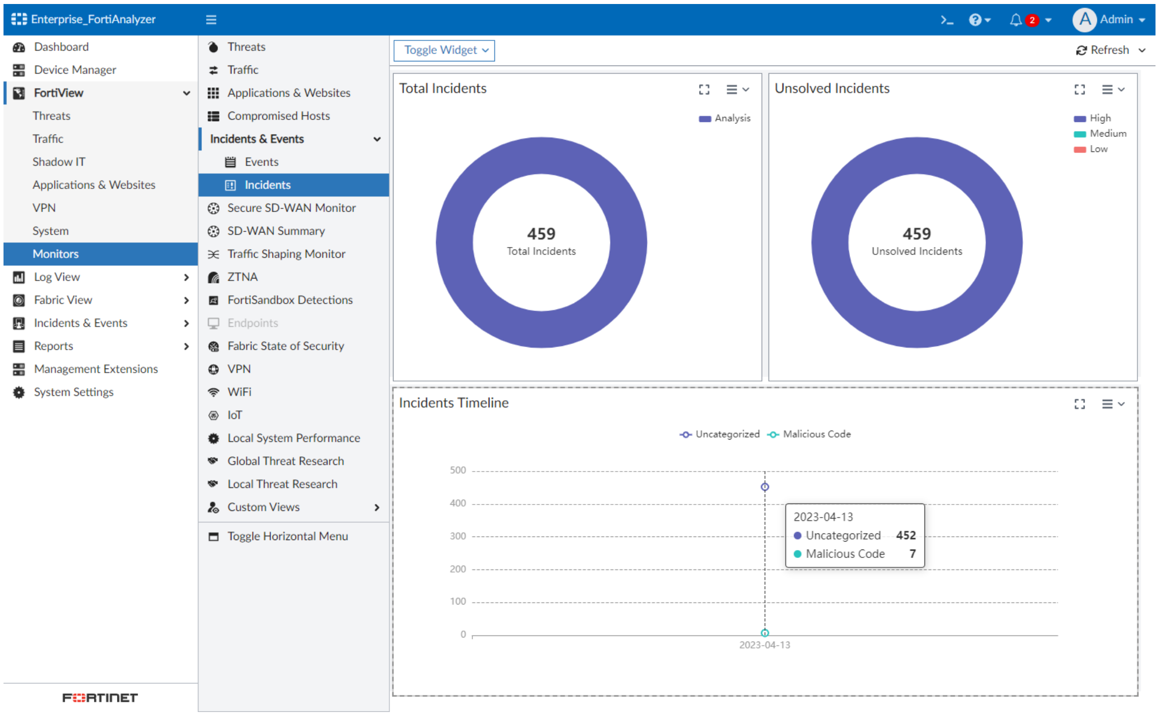
Incidents & Events includes the following:

Event Monitor	View events generated by event handlers. For more information, see the FortiAnalyzer Administration Guide.

Handlers	Configure data selectors, notification profiles, basic event handlers, and correlation event handlers. For more information, see the FortiAnalyzer Administration Guide.
Incidents	Create and update incidents to track and analyze events. For more information, see the FortiAnalyzer Administration Guide.
Threat Hunting	View a log count chart and SIEM log analytics table. The *Threat Hunting* dashboard is only available in Fabric ADOMs when ADOMs are enabled. For more information, see the FortiAnalyzer Administration Guide.
Log Parser	View and manage SIEM log parsers. For more information, see the FortiAnalyzer Administration Guide.
Outbreak Alerts	View outbreak alerts and automatically download related event handlers and reports from FortiGuard. The FortiAnalyzer Outbreak Detection Service is a licensed feature. For more information, see the FortiAnalyzer Administration Guide.

To review incidents and events in dashboards, go to *FortiView* > *Monitors* > *Incidents & Events*.

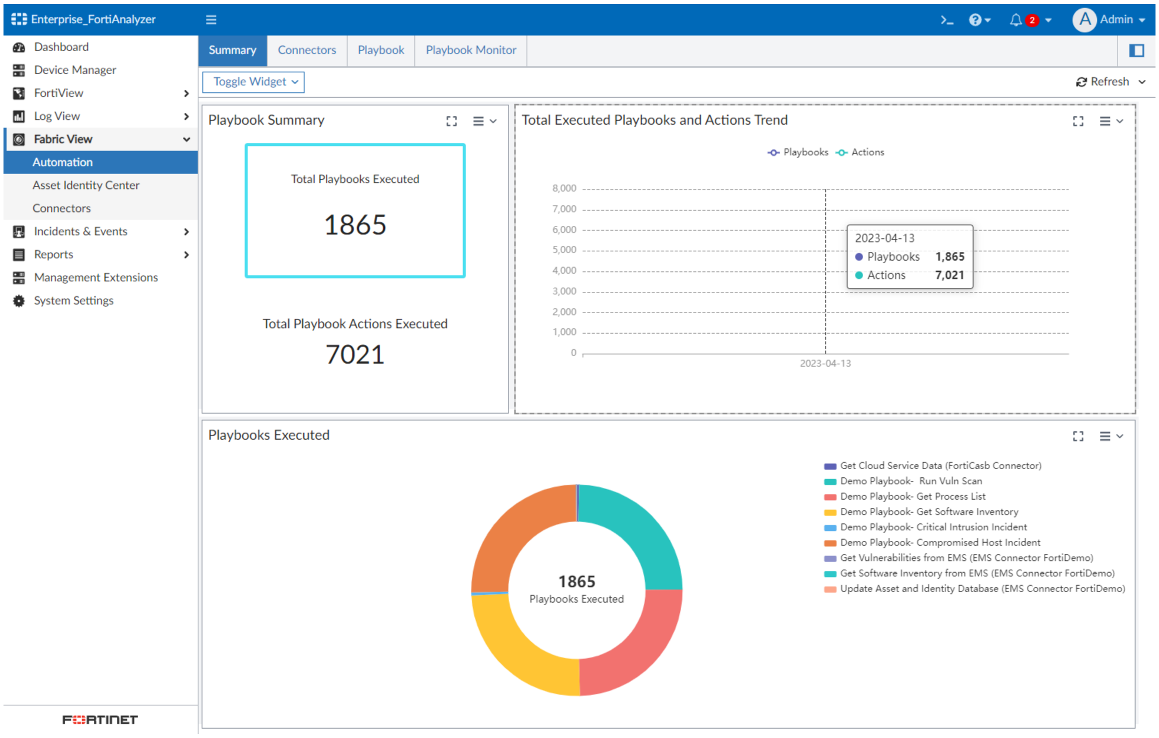




FortiView > *Monitors* > *Incidents & Events* includes the following dashboards:

Events	This dashboard includes the following widgets: • *Event Summary* • *Top 10 Events by Type* • *Events by Severity* • *Top 10 Events by Handler*
Incidents	This dashboard includes the following widgets: • *Total Incidents* • *Unsolved Incidents* • *Incidents Timeline*

To configure FortiSoC playbooks, go to *Fabric View* > *Automation*.


Enterprise_FortiAnalyzer
Admin
Dashboard
Device Manager
FortiView
Log View
Fabric View
Automation
Asset Identity Center
Connectors
Incidents & Events
Reports
Management Extensions
System Settings
FORTINET
Summary
Connectors
Playbook
Playbook Monitor
Toggle Widget
Refresh
Playbook Summary
Total Playbooks Executed
1865
Total Playbook Actions Executed
7021
Total Executed Playbooks and Actions Trend
Playbooks
Actions
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
2023-04-13
2023-04-13
Playbooks 1,865
Actions 7,021
Playbooks Executed
1865
Playbooks Executed
Get Cloud Service Data (FortiCasb Connector)
Demo Playbook- Run Vuln Scan
Demo Playbook- Get Process List
Demo Playbook- Get Software Inventory
Demo Playbook- Critical Intrusion Incident
Demo Playbook- Compromised Host Incident
Get Vulnerabilities from EMS (EMS Connector FortiDemo)
Get Software Inventory from EMS (EMS Connector FortiDemo)
Update Asset and Identity Database (EMS Connector FortiDemo)

Fabric View > *Automation* includes the following:

Summary	View playbook performance in a dashboard. This includes widgets for total playbooks, playbooks executed, and an actions trend. For more information, see the FortiAnalyzer Administration Guide.
Connectors	View the status of available connectors supported for playbook automation. For more information, see the FortiAnalyzer Administration Guide.
Playbook	Configure and manage playbooks. For more information, see the FortiAnalyzer Administration Guide.
Playbook Monitor	View playbook jobs in a table view. For more information, see the FortiAnalyzer Administration Guide.

Notifications for new Outbreak Alerts - 7.4.1

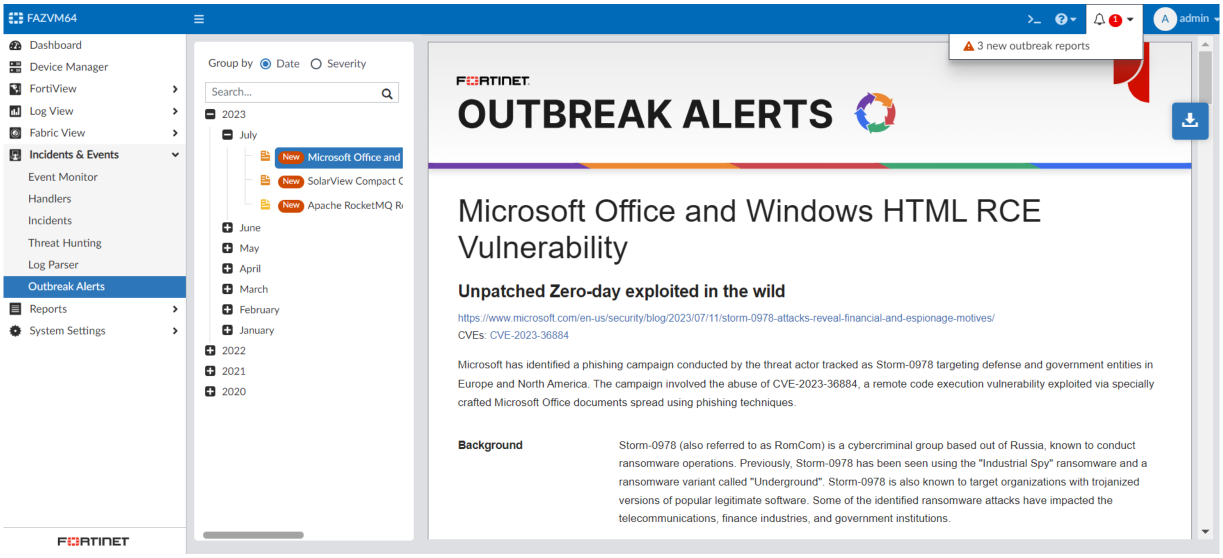
This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Outbreak Alerts

When new Outbreak Alerts are received, GUI notifications are added in the banner, ensuring timely notification for administrators.

In the *Outbreak Alerts* pane, the Outbreak Alerts can now be sorted by *Date* or *Severity*, allowing for easy browsing and retrieval based on these criteria. A "*New*" tag is also added to alerts received in the current month to distinguish them from previous alerts.

For example, see the image below.



Microsoft Office and Windows HTML RCE Vulnerability

Unpatched Zero-day exploited in the wild

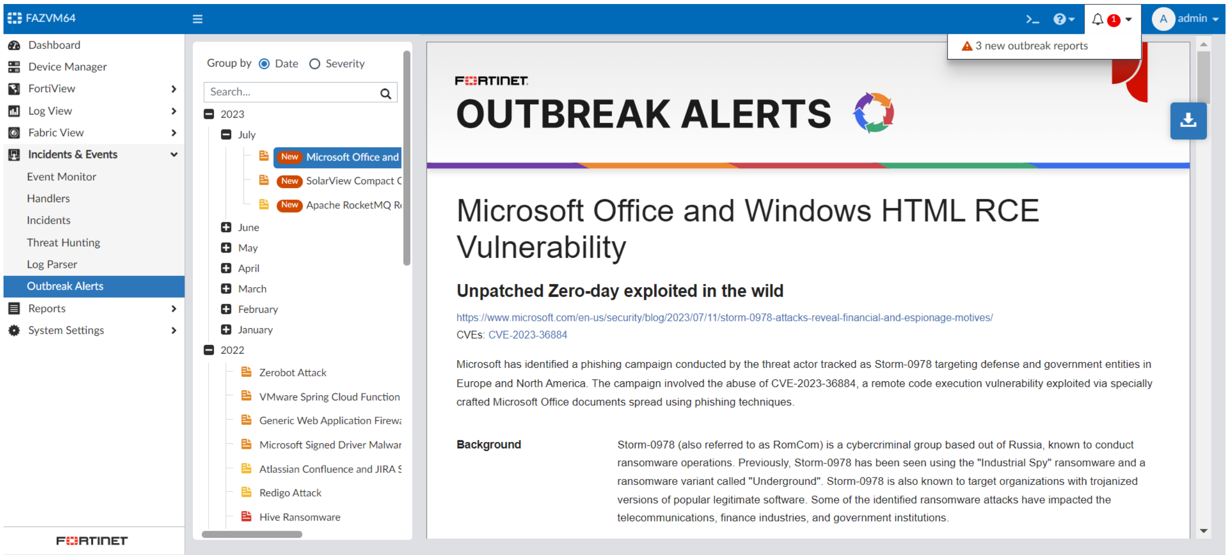
https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

CVEs: CVE-2023-36884

Microsoft has identified a phishing campaign conducted by the threat actor tracked as Storm-0978 targeting defense and government entities in Europe and North America. The campaign involved the abuse of CVE-2023-36884, a remote code execution vulnerability exploited via specially crafted Microsoft Office documents spread using phishing techniques.

Background Storm-0978 (also referred to as RomCom) is a cybercriminal group based out of Russia, known to conduct ransomware operations. Previously, Storm-0978 has been seen using the "Industrial Spy" ransomware and a ransomware variant called "Underground". Storm-0978 is also known to target organizations with trojanized versions of popular legitimate software. Some of the identified ransomware attacks have impacted the telecommunications, finance industries, and government institutions.

Use the tree menu in the sidebar to expand and browse the list of alerts.



Microsoft Office and Windows HTML RCE Vulnerability

Unpatched Zero-day exploited in the wild

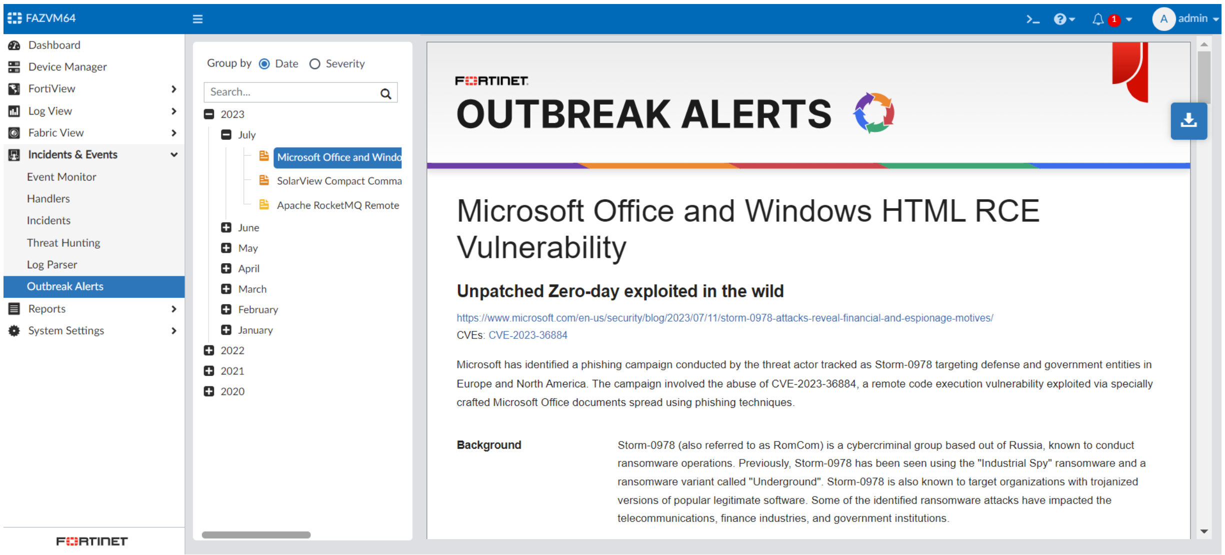
https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

CVEs: CVE-2023-36884

Microsoft has identified a phishing campaign conducted by the threat actor tracked as Storm-0978 targeting defense and government entities in Europe and North America. The campaign involved the abuse of CVE-2023-36884, a remote code execution vulnerability exploited via specially crafted Microsoft Office documents spread using phishing techniques.

Background Storm-0978 (also referred to as RomCom) is a cybercriminal group based out of Russia, known to conduct ransomware operations. Previously, Storm-0978 has been seen using the "Industrial Spy" ransomware and a ransomware variant called "Underground". Storm-0978 is also known to target organizations with trojanized versions of popular legitimate software. Some of the identified ransomware attacks have impacted the telecommunications, finance industries, and government institutions.

After refreshing the pane, you will no longer see the *New* tag.



Microsoft Office and Windows HTML RCE Vulnerability

Unpatched Zero-day exploited in the wild

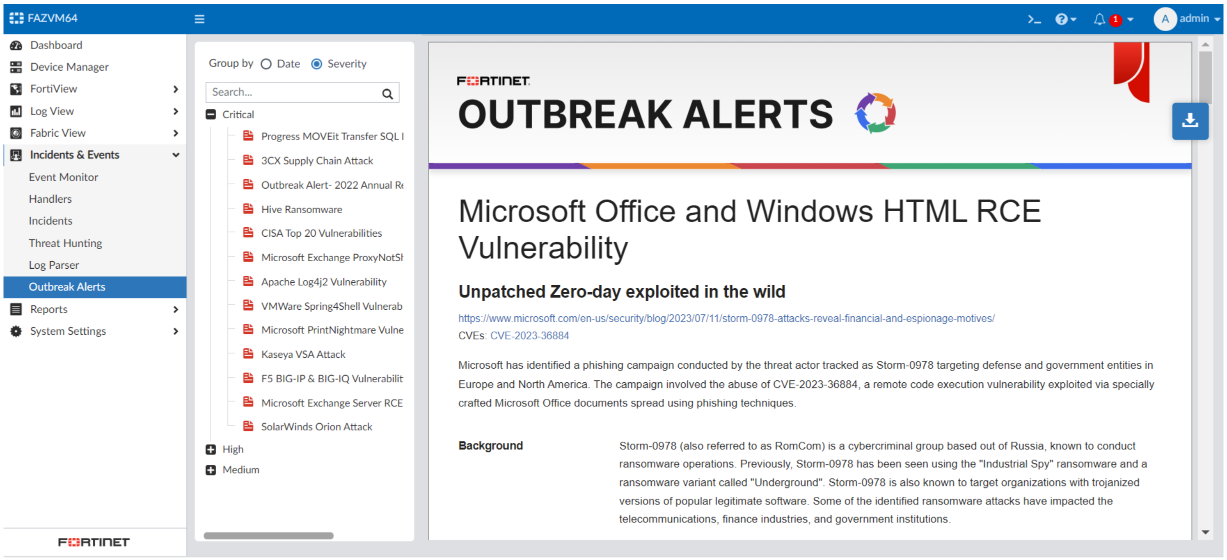
https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

CVEs: CVE-2023-36884

Microsoft has identified a phishing campaign conducted by the threat actor tracked as Storm-0978 targeting defense and government entities in Europe and North America. The campaign involved the abuse of CVE-2023-36884, a remote code execution vulnerability exploited via specially crafted Microsoft Office documents spread using phishing techniques.

Background: Storm-0978 (also referred to as RomCom) is a cybercriminal group based out of Russia, known to conduct ransomware operations. Previously, Storm-0978 has been seen using the "Industrial Spy" ransomware and a ransomware variant called "Underground". Storm-0978 is also known to target organizations with trojanized versions of popular legitimate software. Some of the identified ransomware attacks have impacted the telecommunications, finance industries, and government institutions.

To group alerts in the sidebar by severity instead of *Date*, select the *Severity* radio button.



Microsoft Office and Windows HTML RCE Vulnerability

Unpatched Zero-day exploited in the wild

https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

CVEs: CVE-2023-36884

Microsoft has identified a phishing campaign conducted by the threat actor tracked as Storm-0978 targeting defense and government entities in Europe and North America. The campaign involved the abuse of CVE-2023-36884, a remote code execution vulnerability exploited via specially crafted Microsoft Office documents spread using phishing techniques.

Background: Storm-0978 (also referred to as RomCom) is a cybercriminal group based out of Russia, known to conduct ransomware operations. Previously, Storm-0978 has been seen using the "Industrial Spy" ransomware and a ransomware variant called "Underground". Storm-0978 is also known to target organizations with trojanized versions of popular legitimate software. Some of the identified ransomware attacks have impacted the telecommunications, finance industries, and government institutions.

MITRE ATT&CK matrices for Enterprise and ICS - 7.4.1

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- MITRE ATT&CK®

The *MITRE ATT&CK®* and *MITRE ATT&CK® ICS* panes have been added in FortiAnalyzer 7.4.1.

MITRE (MIT Research Establishment) ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a matrix that helps to identify the objective of cyber attacks and the techniques that they may use. The matrix uses tactics as column headers, and there are several techniques under each tactic. The Enterprise matrix consists of 16 tactics, and the ICS matrix consists of 12 tactics.

In FortiAnalyzer, the MITRE ATT&CK matrices provide information related to the attacks identified by the associated events and incidents. These panes also provide the coverage information of event handlers defined to identify the attacks.

The OT Security Service is required for FortiAnalyzer to use all functionality in the *MITRE ATT&CK® ICS* pane. For more information about this service, see the FortiAnalyzer Datasheet.

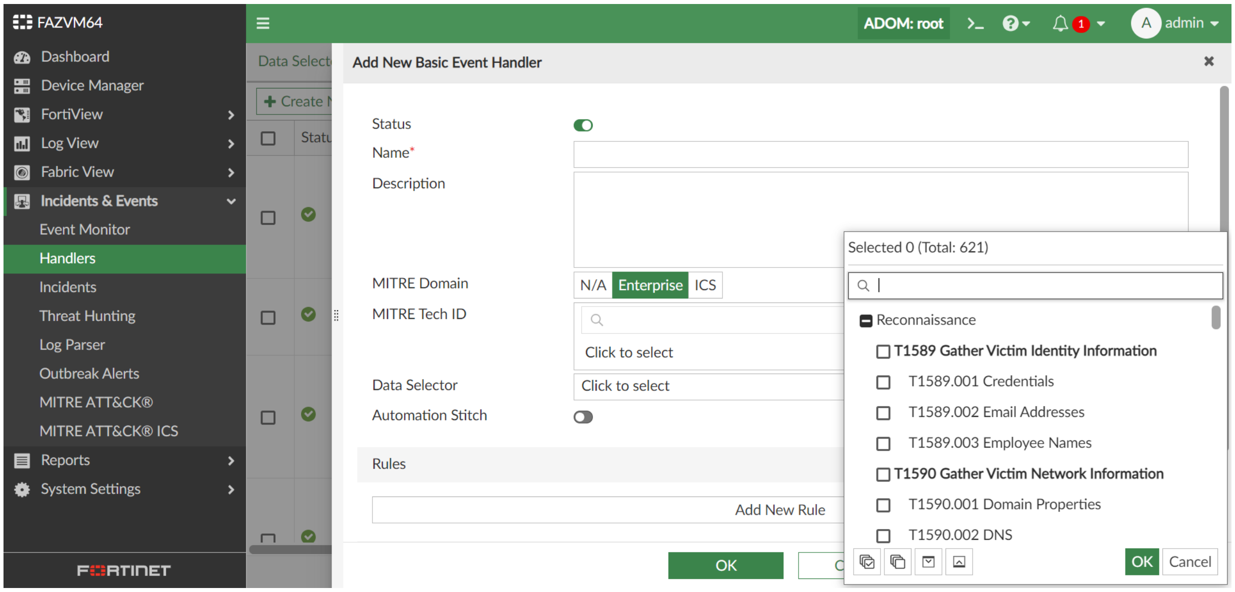
This topic includes the following information:

- To configure MITRE ATT&CK information in event handlers:
- To include MITRE ATT&CK information in an incident:
- To use the MITRE Domain or MITRE Tech ID as part of a playbook trigger:
- To use the Attack tab for a MITRE ATT&CK matrix in FortiAnalyzer:
- To use the Coverage tab for a MITRE ATT&CK matrix in FortiAnalyzer:
- MITRE ATT&CK® ICS without an OT Security Service license:

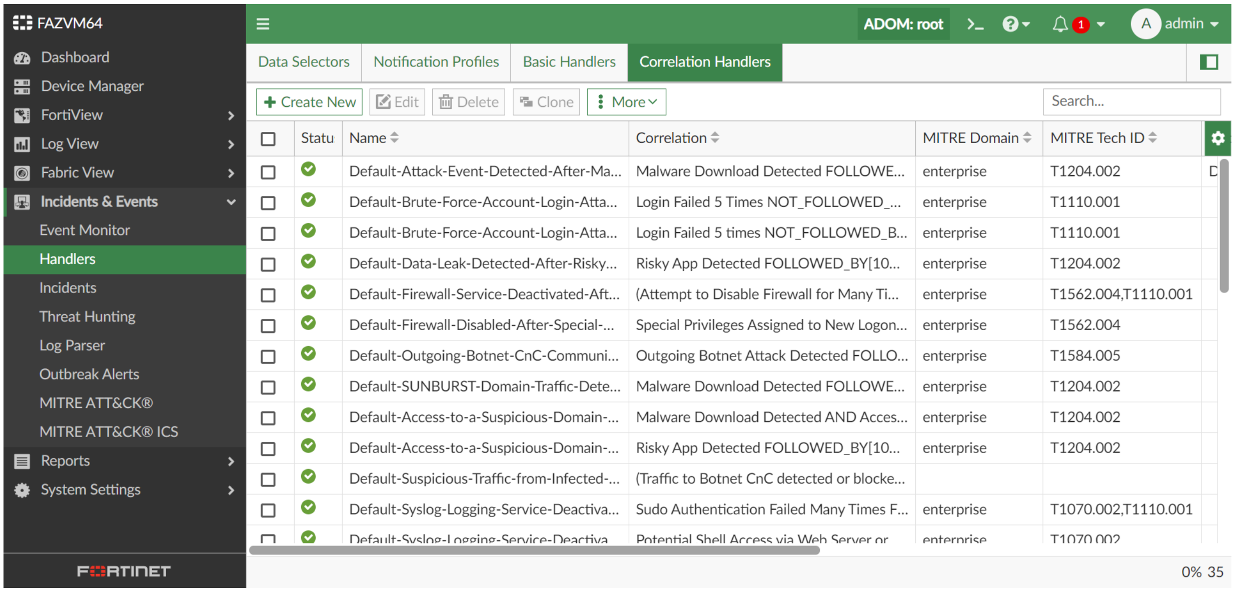
To configure MITRE ATT&CK information in event handlers:

1. When creating a basic or correlation event handler, select the *MITRE Domain*:
   - *N/A* (default)
   - *Enterprise*
   - *ICS*
2. If *Enterprise* or *ICS* is selected for the *MITRE Domain*, you can then select the *MITRE Tech ID*(s) from the dropdown.

   This dropdown is an organized list of all the tactics and techniques in the matrix. You can select any number of techniques or sub-techniques based on the rules that will be defined for the event handler.



The *MITRE Domain* and *MITRE Tech ID* columns have been added to the table views in *Incidents & Events* > *Handlers* > *Basic Handlers* and *Incidents & Events* > *Handlers* > *Correlation Handlers*. Existing default event handlers have also been updated with a *MITRE Domain* and *MITRE Tech ID* where appropriate.

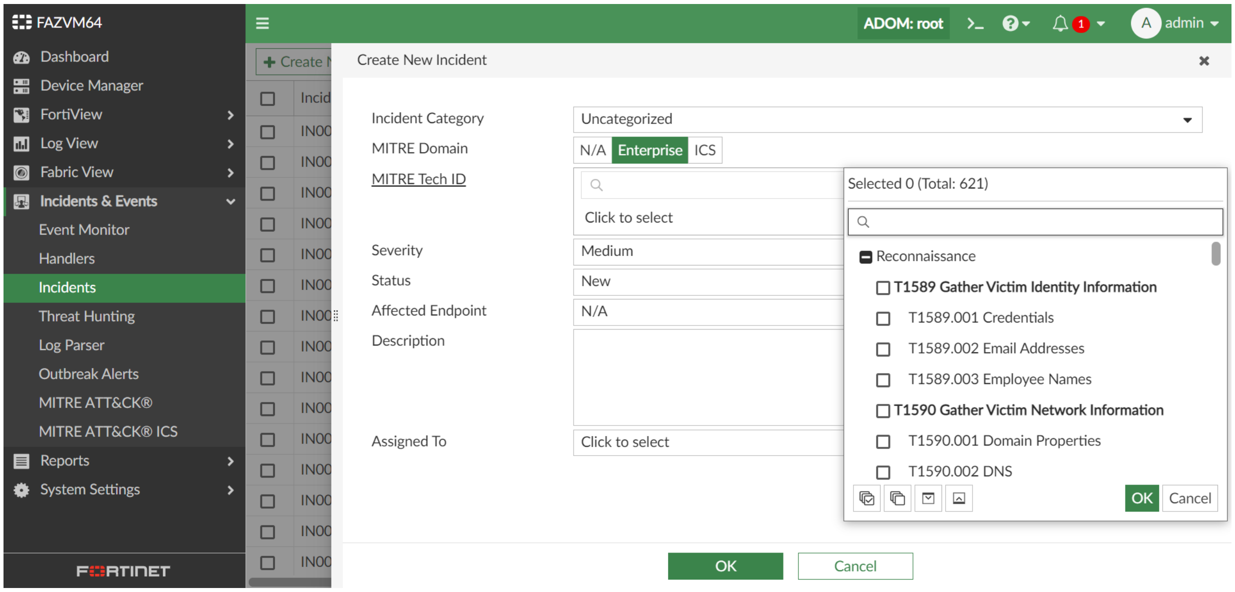


☐	Statu	Name	Correlation	MITRE Domain	MITRE Tech ID
☐	✓	Default-Attack-Event-Detected-After-Ma...	Malware Download Detected FOLLOWE...	enterprise	T1204.002
☐	✓	Default-Brute-Force-Account-Login-Atta...	Login Failed 5 Times NOT_FOLLOWED_...	enterprise	T1110.001
☐	✓	Default-Brute-Force-Account-Login-Atta...	Login Failed 5 times NOT_FOLLOWED_B...	enterprise	T1110.001
☐	✓	Default-Data-Leak-Detected-After-Risky...	Risky App Detected FOLLOWED_BY[10...	enterprise	T1204.002
☐	✓	Default-Firewall-Service-Deactivated-Aft...	(Attempt to Disable Firewall for Many Ti...	enterprise	T1562.004,T1110.001
☐	✓	Default-Firewall-Disabled-After-Special-...	Special Privileges Assigned to New Logon...	enterprise	T1562.004
☐	✓	Default-Outgoing-Botnet-CnC-Communi...	Outgoing Botnet Attack Detected FOLLO...	enterprise	T1584.005
☐	✓	Default-SUNBURST-Domain-Traffic-Dete...	Malware Download Detected FOLLOWE...	enterprise	T1204.002
☐	✓	Default-Access-to-a-Suspicious-Domain-...	Malware Download Detected AND Acces...	enterprise	T1204.002
☐	✓	Default-Access-to-a-Suspicious-Domain-...	Risky App Detected FOLLOWED_BY[10...	enterprise	T1204.002
☐	✓	Default-Suspicious-Traffic-from-Infected-...	(Traffic to Botnet CnC detected or blocke...		
☐	✓	Default-Syslog-Logging-Service-Deactiva...	Sudo Authentication Failed Many Times F...	enterprise	T1070.002,T1110.001
☐	✓	Default-Syslog-Logging-Service-Deactiva	Potential Shell Access via Web Server or	enterprise	T1070.002

To include MITRE ATT&CK information in an incident:

1. When creating an incident, select the *MITRE Domain*:
   - *N/A* (default)
   - *Enterprise*
   - *ICS*
2. If *Enterprise* or *ICS* is selected for the *MITRE Domain*, you can then select the *MITRE Tech ID*(s) from the dropdown.

   This dropdown is an organized list of all the tactics and techniques in the matrix. You can select any number of techniques or sub-techniques based on the incident details.



Create New Incident

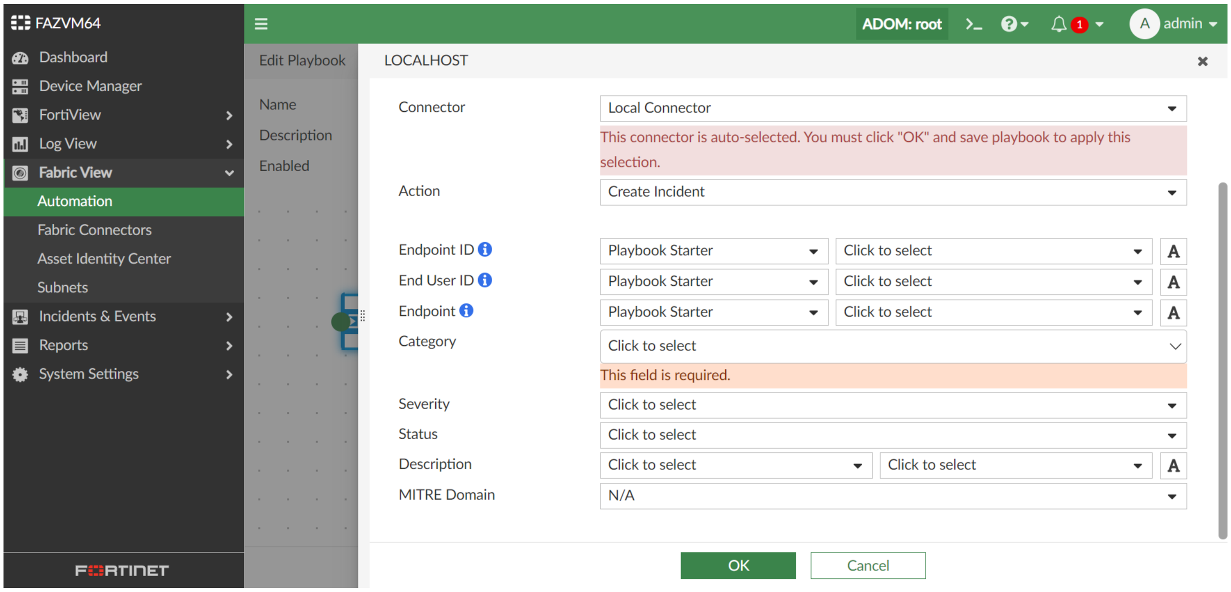
Incident Category	Uncategorized
MITRE Domain	N/A [✓ Enterprise] ICS
MITRE Tech ID	Click to select
Severity	Medium
Status	New
Affected Endpoint	N/A
Description	
Assigned To	Click to select

Selected 0 (Total: 621)

- Reconnaissance
  - ☐ **T1589 Gather Victim Identity Information**
    - ☐ T1589.001 Credentials
    - ☐ T1589.002 Email Addresses
    - ☐ T1589.003 Employee Names
  - ☐ **T1590 Gather Victim Network Information**
    - ☐ T1590.001 Domain Properties
    - ☐ T1590.002 DNS

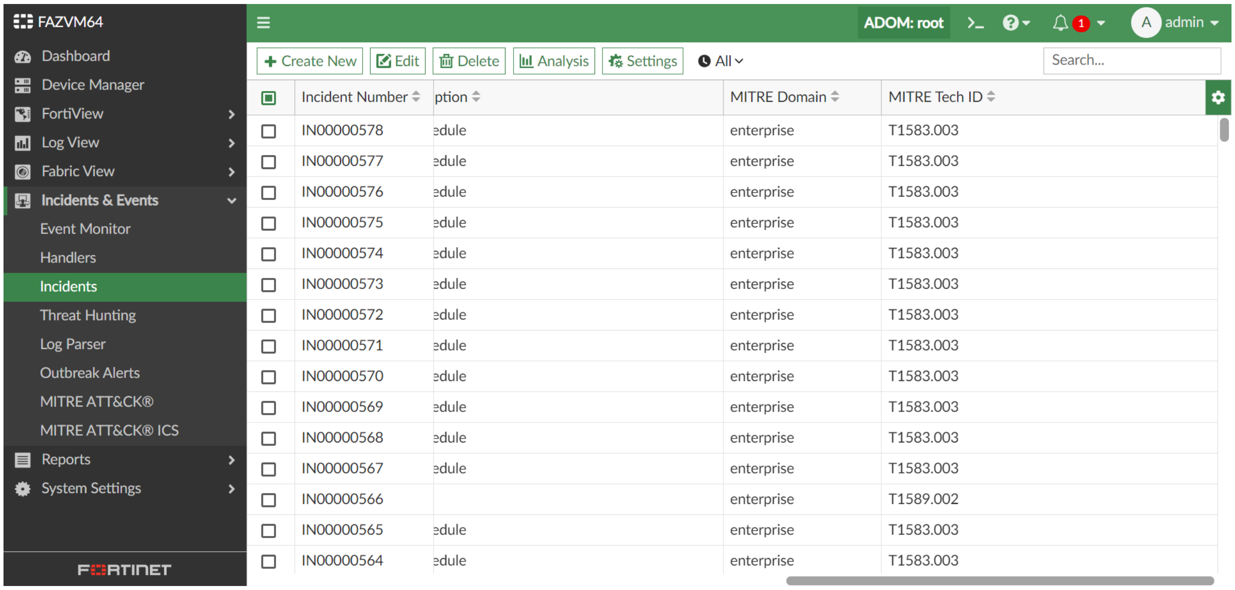
OK Cancel

The *MITRE Domain* and *MITRE Tech ID* can also be included for incidents via the *Create Incident* and *Update Incident* playbook task actions. In the example below, the *MITRE Domain* can be selected when *Action* = *Create Incident*.



Connector	Local Connector	
	This connector is auto-selected. You must click "OK" and save playbook to apply this selection.	
Action	Create Incident	
Endpoint ID	Playbook Starter	Click to select
End User ID	Playbook Starter	Click to select
Endpoint	Playbook Starter	Click to select
Category	Click to select	
	This field is required.	
Severity	Click to select	
Status	Click to select	
Description	Click to select	Click to select
MITRE Domain	N/A	

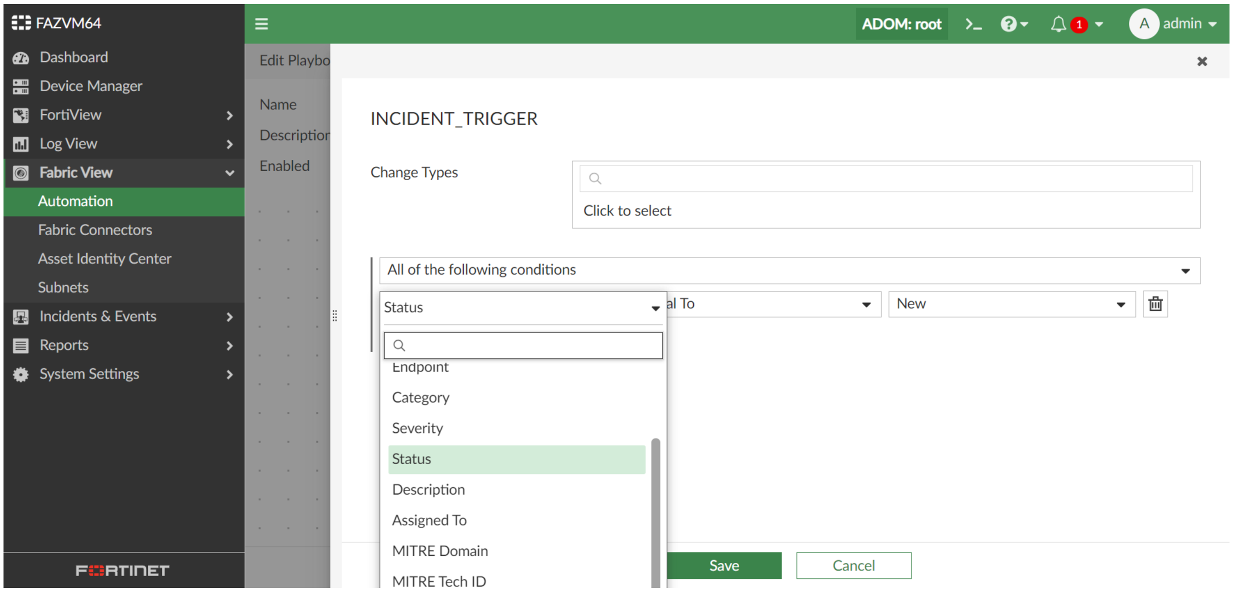
The *MITRE Domain* and *MITRE Tech ID* columns have been added to the table view in *Incidents & Events* > *Incidents*.



Incident Number	ption	MITRE Domain	MITRE Tech ID
IN00000578	edule	enterprise	T1583.003
IN00000577	edule	enterprise	T1583.003
IN00000576	edule	enterprise	T1583.003
IN00000575	edule	enterprise	T1583.003
IN00000574	edule	enterprise	T1583.003
IN00000573	edule	enterprise	T1583.003
IN00000572	edule	enterprise	T1583.003
IN00000571	edule	enterprise	T1583.003
IN00000570	edule	enterprise	T1583.003
IN00000569	edule	enterprise	T1583.003
IN00000568	edule	enterprise	T1583.003
IN00000567	edule	enterprise	T1583.003
IN00000566		enterprise	T1589.002
IN00000565	edule	enterprise	T1583.003
IN00000564	edule	enterprise	T1583.003

To use the MITRE Domain or MITRE Tech ID as part of a playbook trigger:

When configuring an *INCIDENT_TRIGGER* for a playbook, you can select *MITRE Domain* or *MITRE Tech ID* as a filter condition.



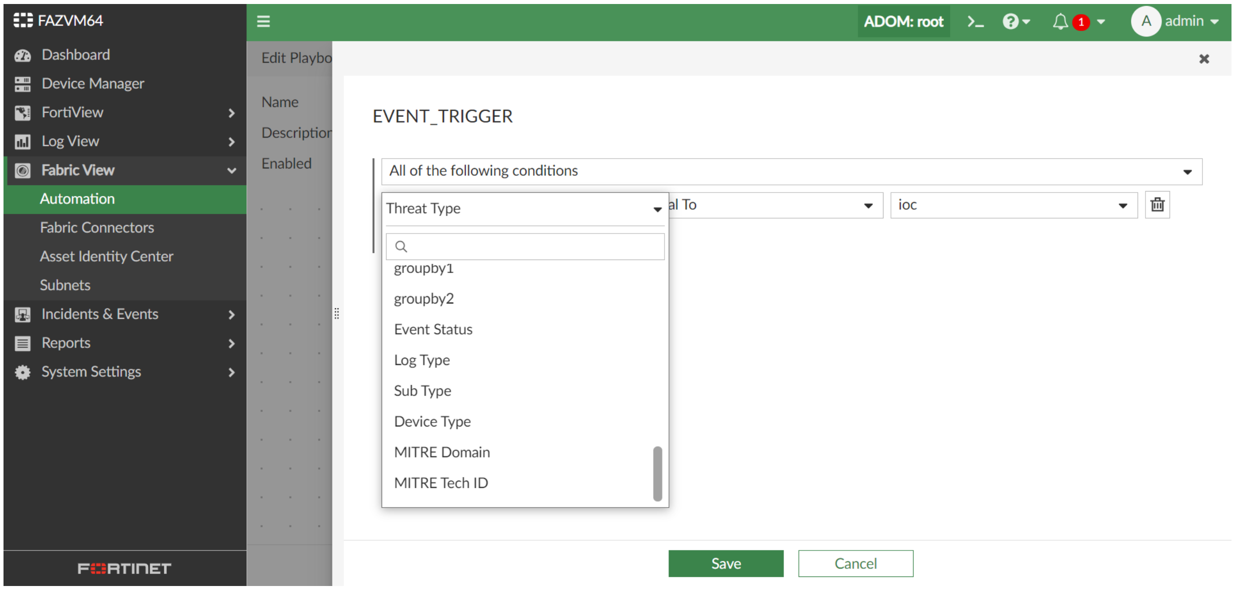
INCIDENT_TRIGGER

Change Types

All of the following conditions

Status | al To | New

Similarly, when configuring an *EVENT_TRIGGER* for a playbook, you can select *MITRE Domain* or *MITRE Tech ID* as a filter condition.



EVENT_TRIGGER

All of the following conditions

Threat Type | al To | ioc

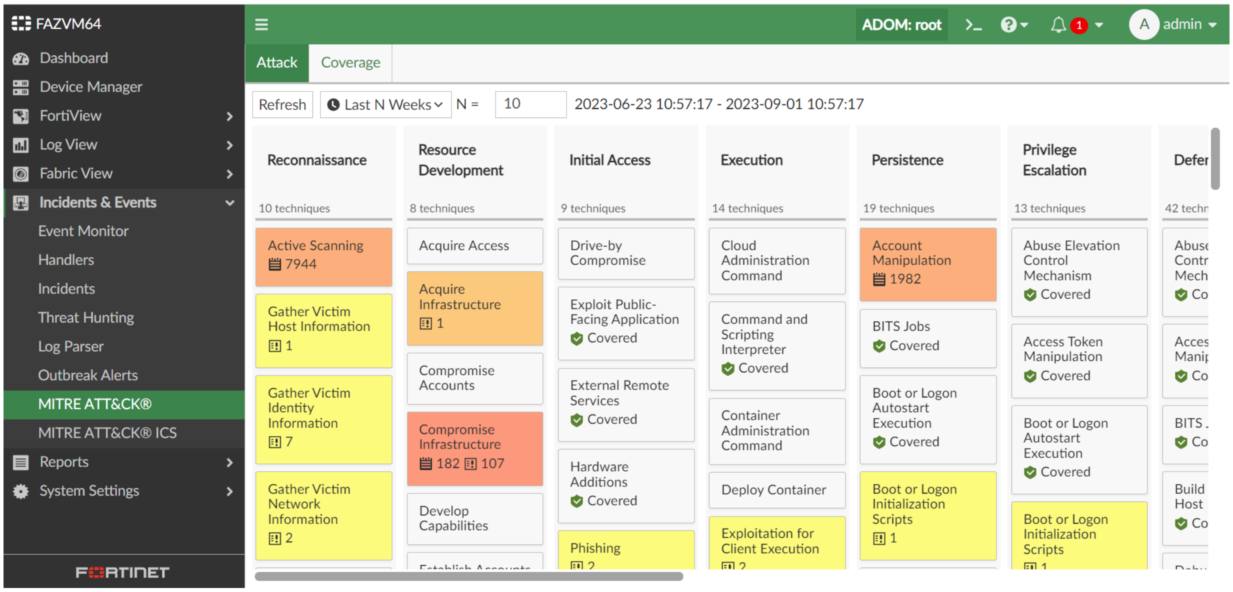
To use the *Attack* tab for a MITRE ATT&CK matrix in FortiAnalyzer:

Incidents & Events > MITRE ATT&CK® > Attack is used for the examples below, but the same information applies for *Incidents & Events > MITRE ATT&CK® ICS > Attack* when you have an OT Security Service license in FortiAnalyzer.

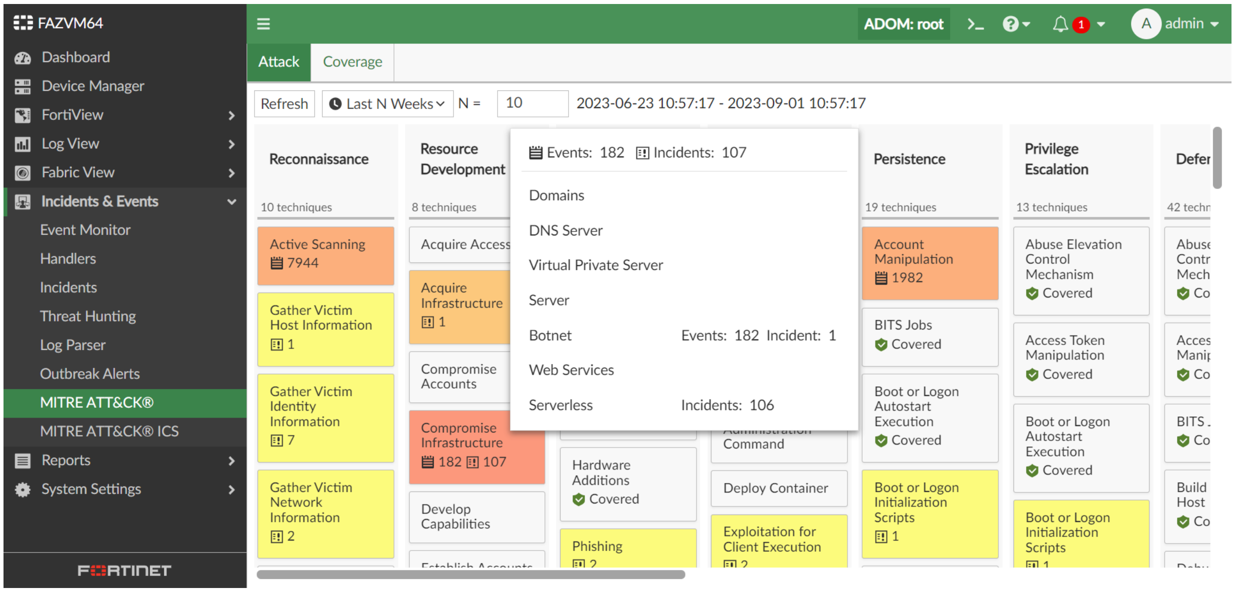
The *Attack* tab provides incident and event information associated with each technique in the matrix.

If there are events associated with the technique, an icon and count displays on the tile. A separate icon and count displays for the associated incidents as well.

You can refresh the matrix or view the attacks in the specific time range by using the time filter in the toolbar. In the example below, there are 182 events and 107 incidents associated with the *Compromise Infrastructure* technique in the last 10 weeks.



Mouse over a tile to display a tooltip with the number of events and/or incidents under each sub-technique. In the example below, the *Botnet* sub-technique has 182 events and 1 incident, while the *Serverless* sub-technique has 106 incidents.

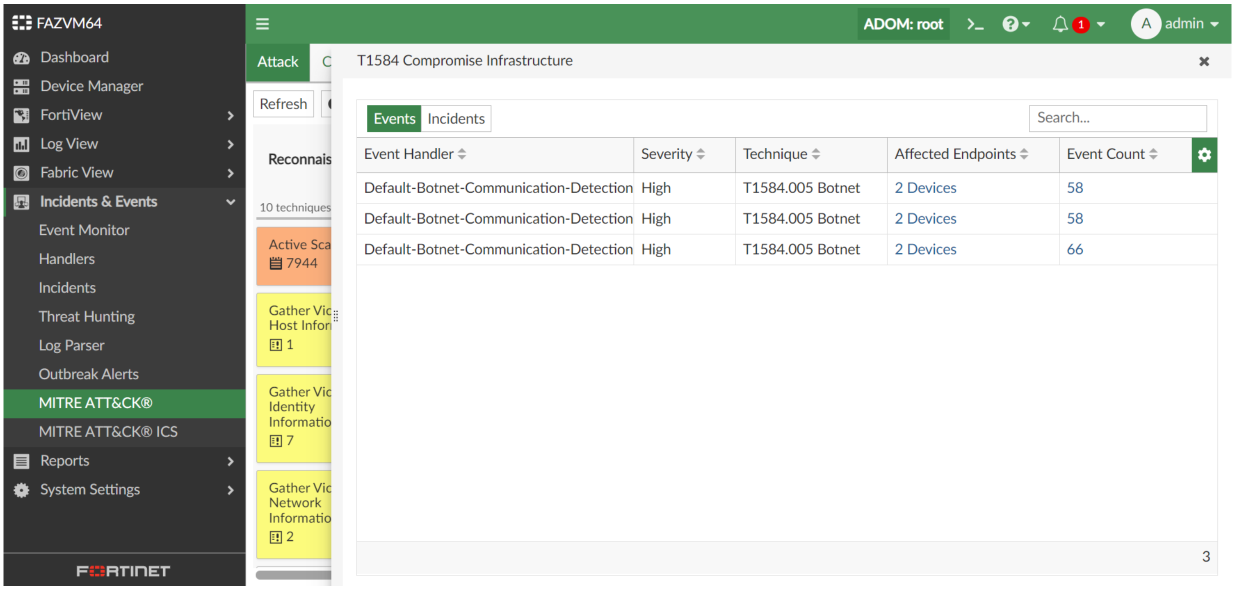

Events: 182 Incidents: 107

Domains
DNS Server
Virtual Private Server
Server
Botnet Events: 182 Incident: 1
Web Services
Serverless Incidents: 106

Click a tile with associated events or incidents to open a pane for that technique. In this pane, you can toggle between table views for associated *Events* and *Incidents*.

The table view for *Events* associated with the technique includes the following columns:

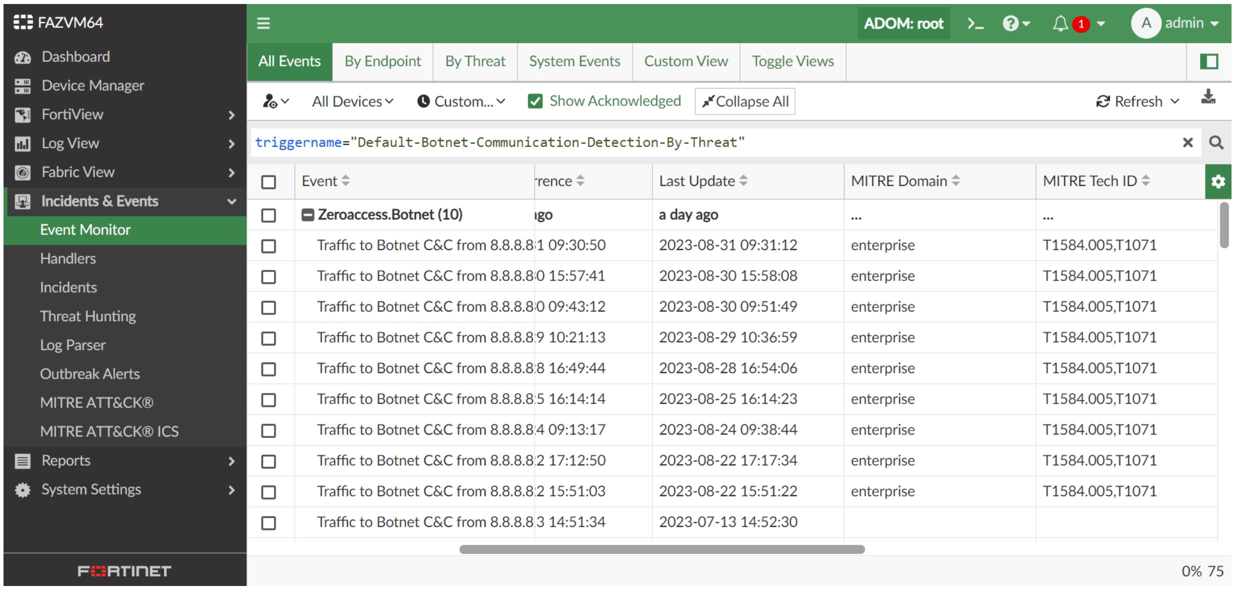
Column	Description
Event Handler	The event handler that generated the event(s).
Severity	The severity of the event(s).
Technique	The technique or sub-technique related to the event(s).
Affected Endpoints	The number of affected devices. Click the count for affected endpoints to open another pane with the list of endpoints found in the events.
Event Count	The event count related to that event handler and technique or sub-technique.



T1584 Compromise Infrastructure

Event Handler	Severity	Technique	Affected Endpoints	Event Count
Default-Botnet-Communication-Detection	High	T1584.005 Botnet	2 Devices	58
Default-Botnet-Communication-Detection	High	T1584.005 Botnet	2 Devices	58
Default-Botnet-Communication-Detection	High	T1584.005 Botnet	2 Devices	66

Click the event count to open *Incidents & Events* > *Event Monitor* in a new tab. The *Event Monitor* is filtered by the selected handler and time range from the matrix. Note that the *Event Monitor* now includes columns for the *MITRE Domain* and *MITRE Tech ID*.

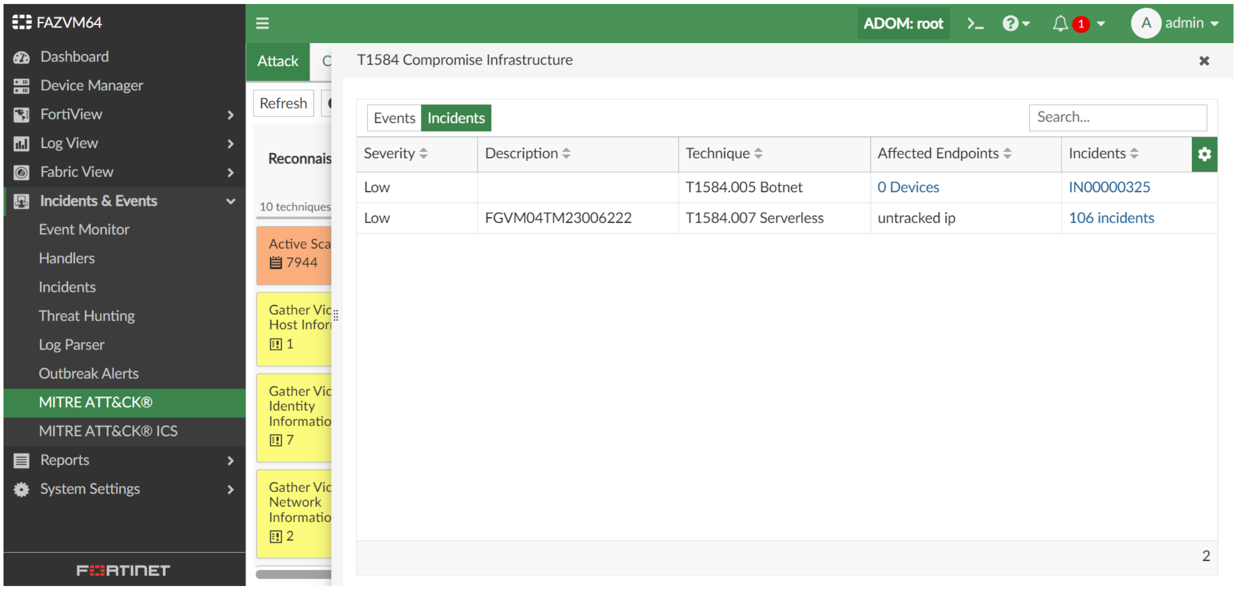


```
triggername="Default-Botnet-Communication-Detection-By-Threat"
```

□	Event	rence	Last Update	MITRE Domain	MITRE Tech ID
□	Zeroaccess.Botnet (10)	ıgo	a day ago	...	...
□	Traffic to Botnet C&C from 8.8.8.8	1 09:30:50	2023-08-31 09:31:12	enterprise	T1584.005,T1071
□	Traffic to Botnet C&C from 8.8.8.8	0 15:57:41	2023-08-30 15:58:08	enterprise	T1584.005,T1071
□	Traffic to Botnet C&C from 8.8.8.8	0 09:43:12	2023-08-30 09:51:49	enterprise	T1584.005,T1071
□	Traffic to Botnet C&C from 8.8.8.8	9 10:21:13	2023-08-29 10:36:59	enterprise	T1584.005,T1071
□	Traffic to Botnet C&C from 8.8.8.8	8 16:49:44	2023-08-28 16:54:06	enterprise	T1584.005,T1071
□	Traffic to Botnet C&C from 8.8.8.8	5 16:14:14	2023-08-25 16:14:23	enterprise	T1584.005,T1071
□	Traffic to Botnet C&C from 8.8.8.8	4 09:13:17	2023-08-24 09:38:44	enterprise	T1584.005,T1071
□	Traffic to Botnet C&C from 8.8.8.8	2 17:12:50	2023-08-22 17:17:34	enterprise	T1584.005,T1071
□	Traffic to Botnet C&C from 8.8.8.8	2 15:51:03	2023-08-22 15:51:22	enterprise	T1584.005,T1071
□	Traffic to Botnet C&C from 8.8.8.8	3 14:51:34	2023-07-13 14:52:30		

The table view for *Incidents* associated with the technique includes following columns:

Column	Description
Severity	The severity of the incident(s).
Description	The description for the incident.
Technique	The technique or sub-technique related to the incident(s).
Affected Endpoints	The number of affected endpoints. Click the count for affected endpoints to open another pane with the list of endpoints found in the incidents.
Incidents	The incident count related to that technique or sub-technique. Click the incident count to open the *Incidents* pane in a new tab. It is filtered by incidents of the selected technique.



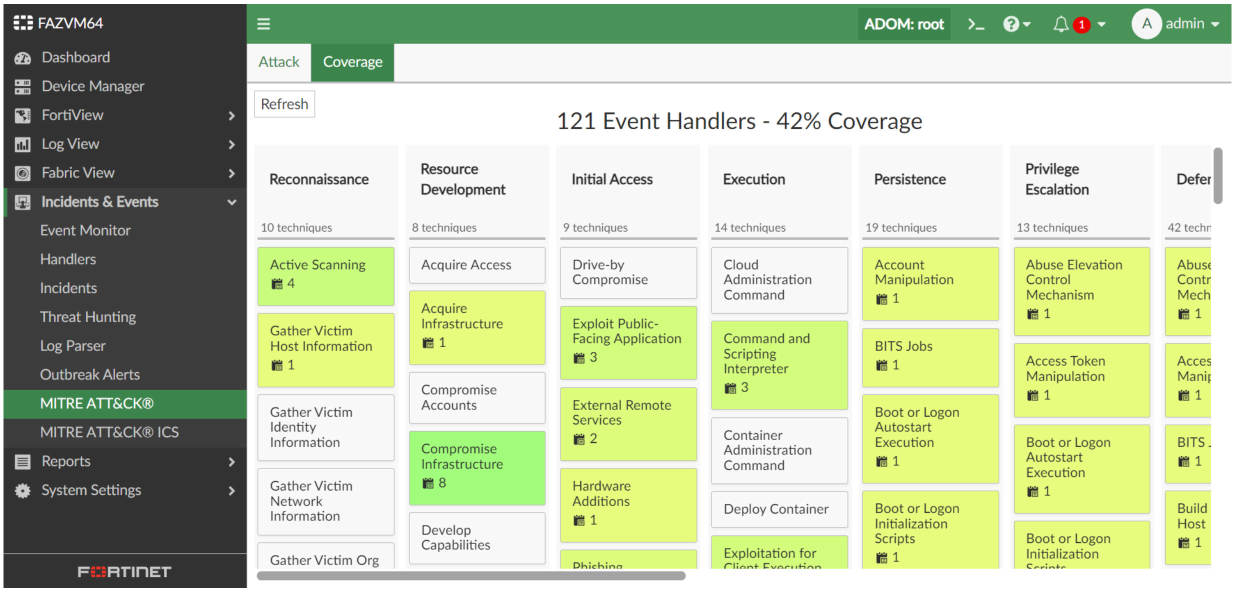
T1584 Compromise Infrastructure

Severity	Description	Technique	Affected Endpoints	Incidents
Low		T1584.005 Botnet	0 Devices	IN00000325
Low	FGVM04TM23006222	T1584.007 Serverless	untracked ip	106 incidents

To use the *Coverage* tab for a MITRE ATT&CK matrix in FortiAnalyzer:

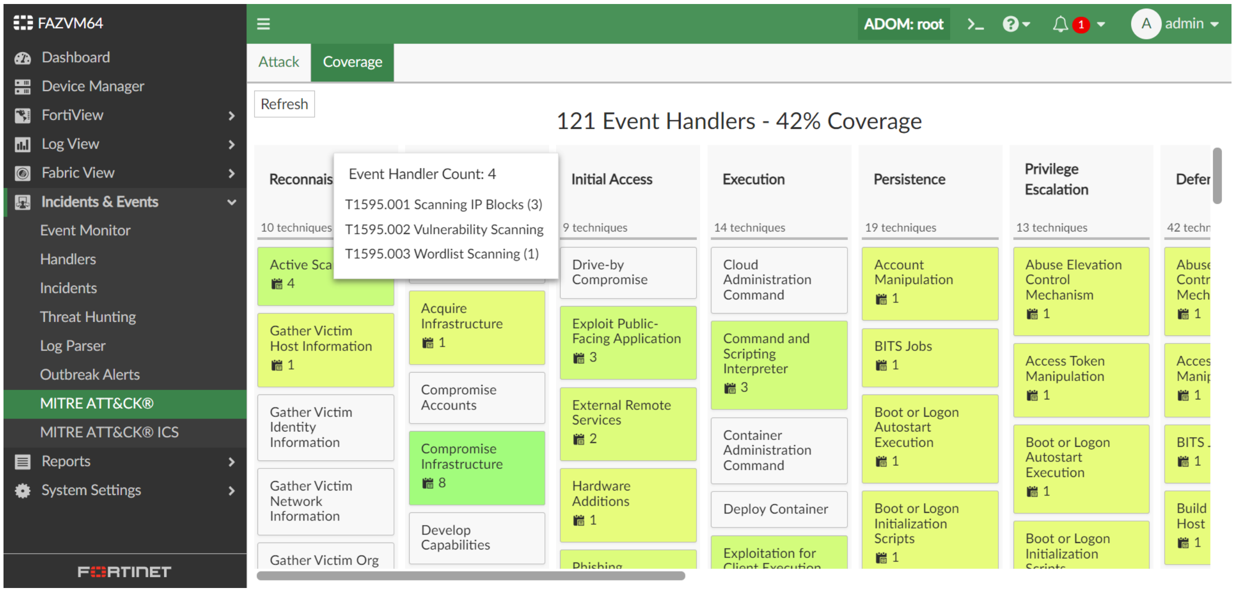
Incidents & Events > *MITRE ATT&CK®* > *Coverage* is used for the examples below, but the same information applies for *Incidents & Events* > *MITRE ATT&CK® ICS* > *Coverage* when you have an OT Security Service license in FortiAnalyzer.

The *Coverage* tab displays the number of event handlers associated with each technique in the matrix. This helps you to determine gaps in coverage where more event handlers could be configured to identify related attacks. The top of the pane displays the overall coverage. In the example below, the coverage is *121 Event Handlers - 42% Coverage*.



When a basic or correlation event handler is associated with a technique, it will be included as part of the coverage for that technique. The tile displays an icon and count for associated event handlers. Mouse over the tile to display the information in a tooltip. This includes the total event handler count and a breakdown of the count for each sub-technique, if they are available.

In the example below, the tooltip displays three event handlers associated with the *Scanning IP Blocks* sub-technique and one associated with the *Wordlist Scanning* sub-technique.

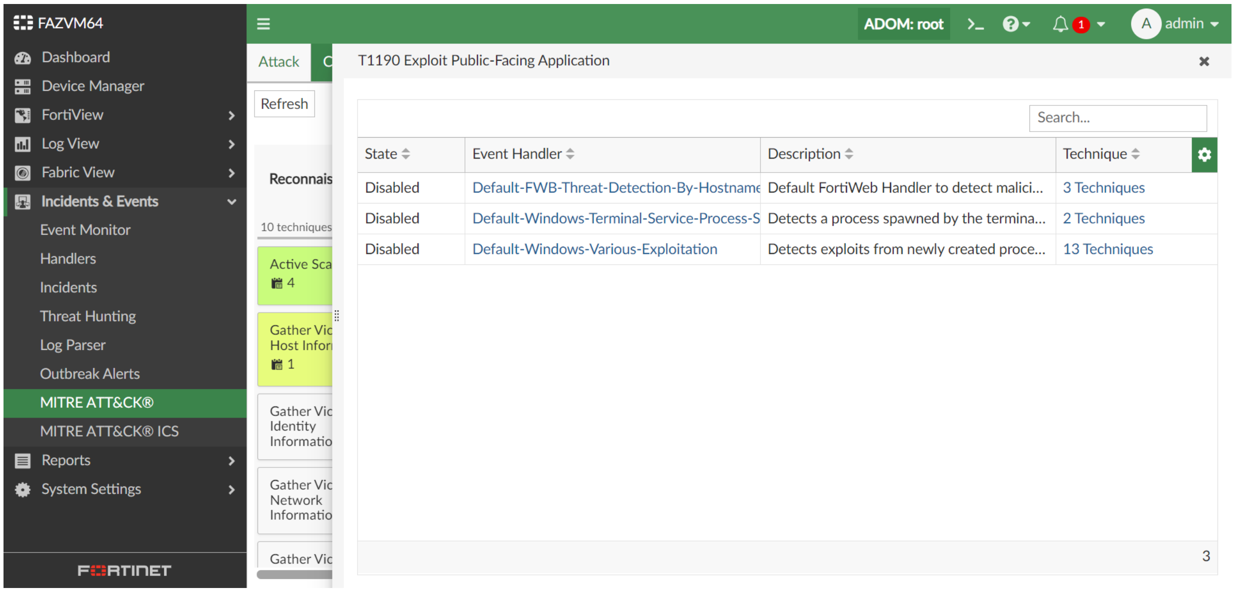


121 Event Handlers - 42% Coverage

Event Handler Count: 4
T1595.001 Scanning IP Blocks (3)
T1595.002 Vulnerability Scanning
T1595.003 Wordlist Scanning (1)

Click a tile with coverage to open a table view of event handlers for that technique. The table includes the following columns:

Column	Description
State	The state of the event handler: *Enabled* or *Disabled*.
Event Handlers	The name of the event handler.
Description	The description of the event handler.
Technique	The technique or sub-technique(s) associated with the event handler. If there are multiple sub-techniques associated with the event handler, the count will be provided in this column. Click the count to display which sub-techniques are associated with the event handler.

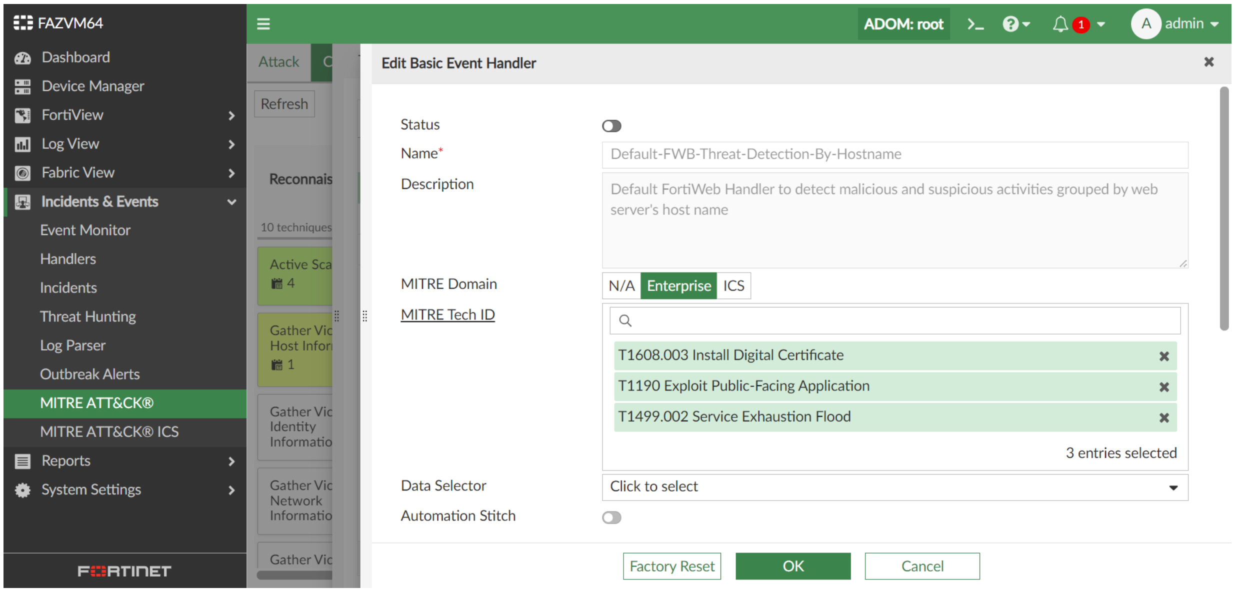


T1190 Exploit Public-Facing Application

State	Event Handler	Description	Technique
Disabled	Default-FWB-Threat-Detection-By-Hostname	Default FortiWeb Handler to detect malici...	3 Techniques
Disabled	Default-Windows-Terminal-Service-Process-S	Detects a process spawned by the termina...	2 Techniques
Disabled	Default-Windows-Various-Exploitation	Detects exploits from newly created proce...	13 Techniques

3

Click an event handler name in the table to view the event handler configuration. You can edit the *Status*, *MITRE Domain*, and *MITRE Tech ID* from this pane, if needed. After updating the coverage for an event handler, refresh the *MITRE ATT&CK®* matrix to display the changes.



Edit Basic Event Handler

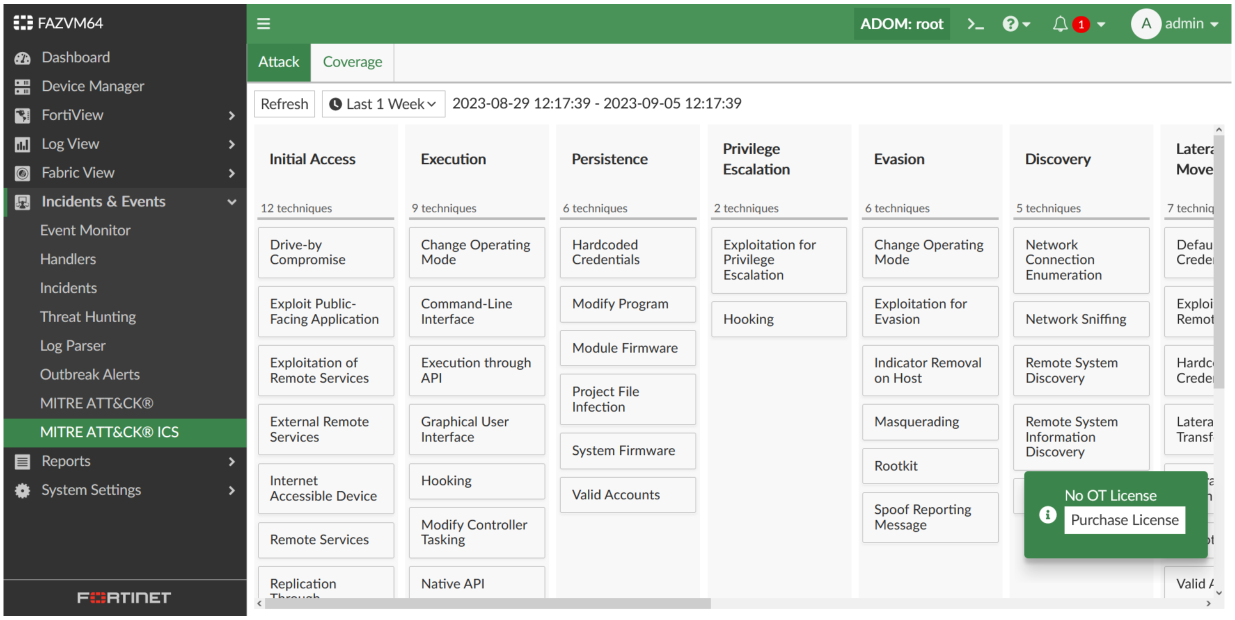
Status: ○
Name*: Default-FWB-Threat-Detection-By-Hostname
Description: Default FortiWeb Handler to detect malicious and suspicious activities grouped by web server's host name
MITRE Domain: N/A [✓ Enterprise] ICS
MITRE Tech ID:
- T1608.003 Install Digital Certificate
- T1190 Exploit Public-Facing Application
- T1499.002 Service Exhaustion Flood

3 entries selected
Data Selector: Click to select
Automation Stitch: ○

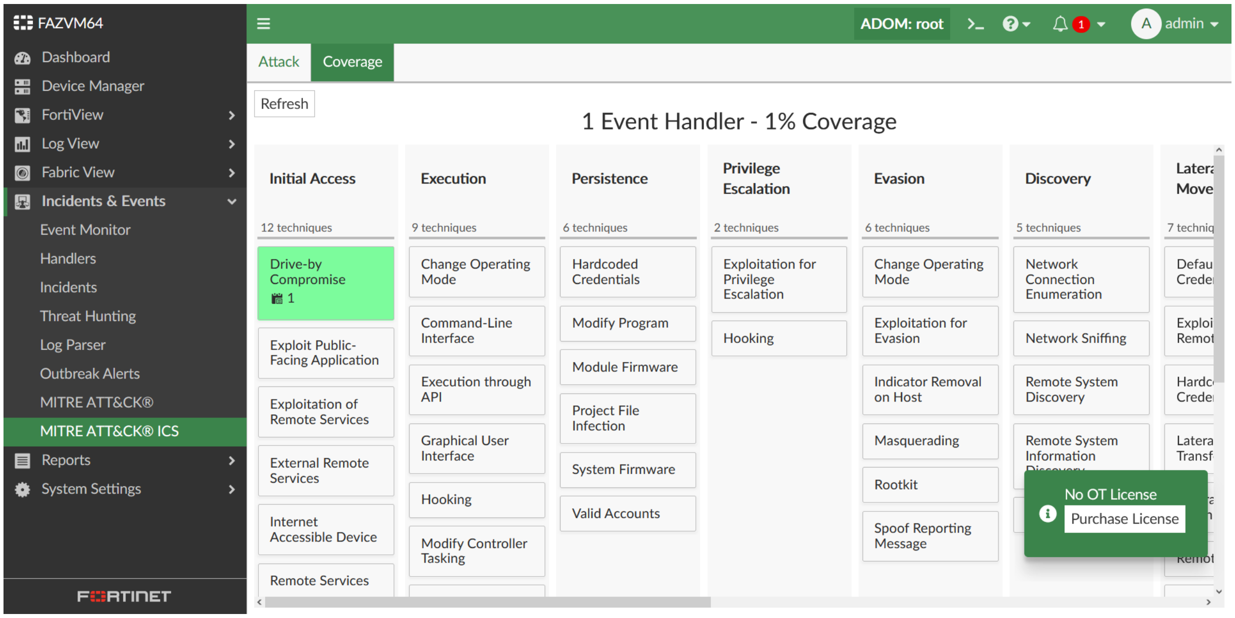
MITRE ATT&CK® ICS without an OT Security Service license:

If you do not have an OT Security Service license for FortiAnalyzer, the *MITRE ATT&CK® ICS* pane will display a notificaiton that the license is missing.

The *Attack* tab will not display any event or incident counts for the techniques in the matrix.



The *Coverage* tab will display the event handler counts for the techniques, but you will not be able to click the tiles to view their information or perform any actions.



Deliver reports, event handlers, and SIEM rules as FortiGuard packages - 7.4.2

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Security Automation Service objects

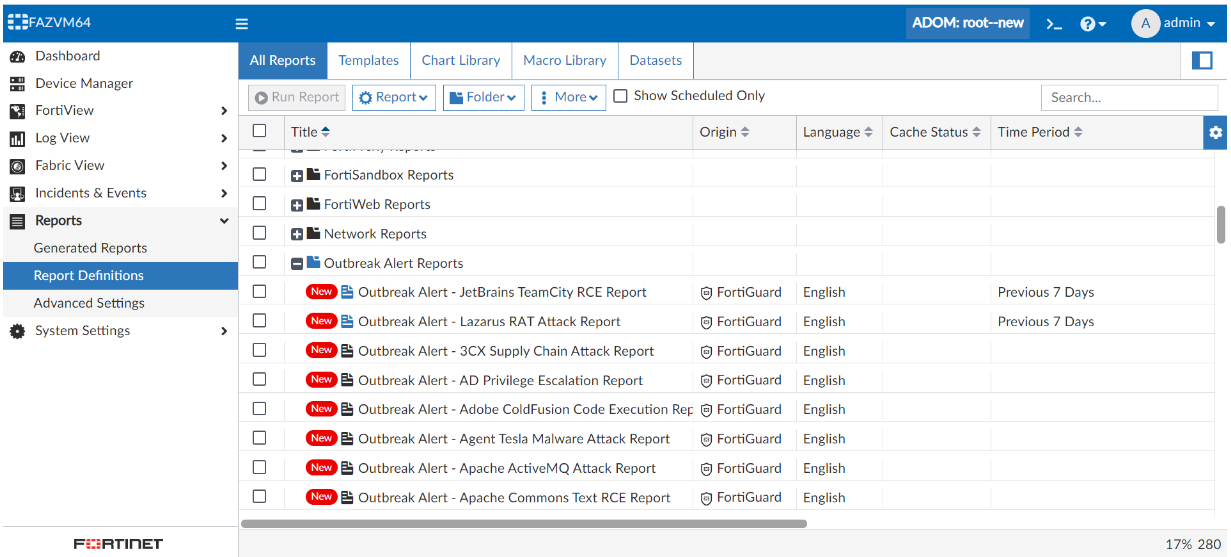
FortiAnalyzer 7.4.2 includes the following enhancements:

- *FortiGuard Outbreak Detection Service*: Outbreak Alert reports delivered in content packages are saved on the global level, reducing per-ADOM installation time.
- *FortiAnalyzer Security Automation Service*: The FortiAnalyzer Security Automation Service offers premium reports, event handlers, SIEM parsers, and playbooks as content packages. These RHSP FortiGuard package objects are only applied with a valid Security Automation Service license. For more information about this service, see the FortiGuard website.

To determine if you have a valid license for these services in your FortiAnalyzer GUI, see License Information widget in the FortiAnalyzer Administration Guide.

Reports:

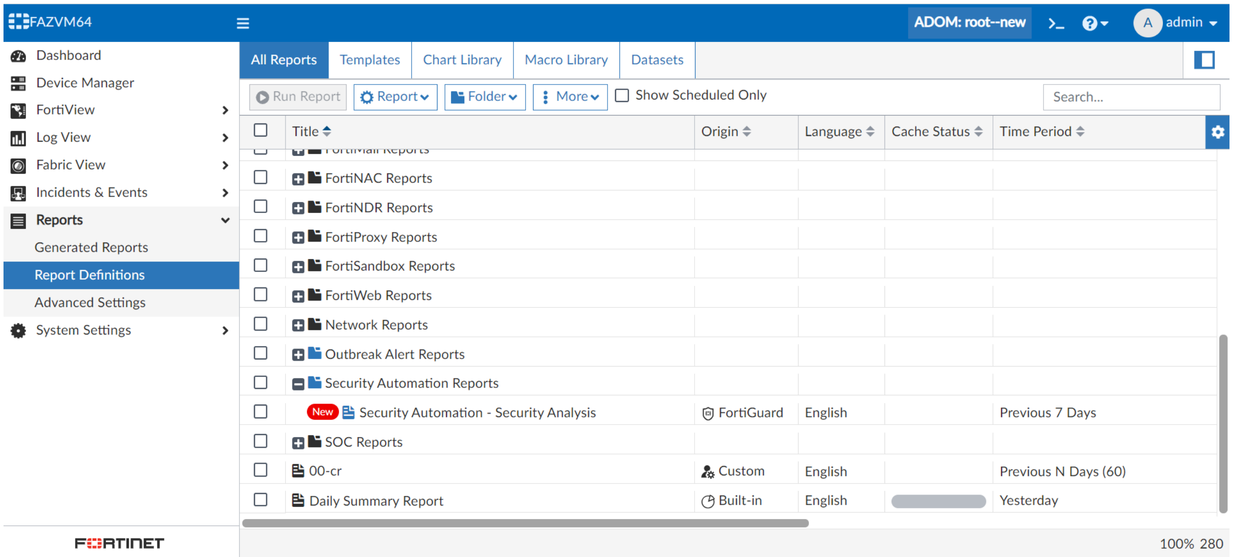
Reports delivered as part of licensed FortiGuard Outbreak Detection Service can be found in *Reports > Report Definitions > All Reports*. They are stored in the *Outbreak Alert Reports* folder at the global level. Outbreak Alert reports released prior to this release remain at the ADOM level.



☐ Show Scheduled Only

☐	Title	Origin	Language	Cache Status	Time Period
☐	FortiSandbox Reports				
☐	FortiWeb Reports				
☐	Network Reports				
☐	Outbreak Alert Reports				
☐	New Outbreak Alert - JetBrains TeamCity RCE Report	FortiGuard	English		Previous 7 Days
☐	New Outbreak Alert - Lazarus RAT Attack Report	FortiGuard	English		Previous 7 Days
☐	New Outbreak Alert - 3CX Supply Chain Attack Report	FortiGuard	English		
☐	New Outbreak Alert - AD Privilege Escalation Report	FortiGuard	English		
☐	New Outbreak Alert - Adobe ColdFusion Code Execution Rep	FortiGuard	English		
☐	New Outbreak Alert - Agent Tesla Malware Attack Report	FortiGuard	English		
☐	New Outbreak Alert - Apache ActiveMQ Attack Report	FortiGuard	English		
☐	New Outbreak Alert - Apache Commons Text RCE Report	FortiGuard	English		

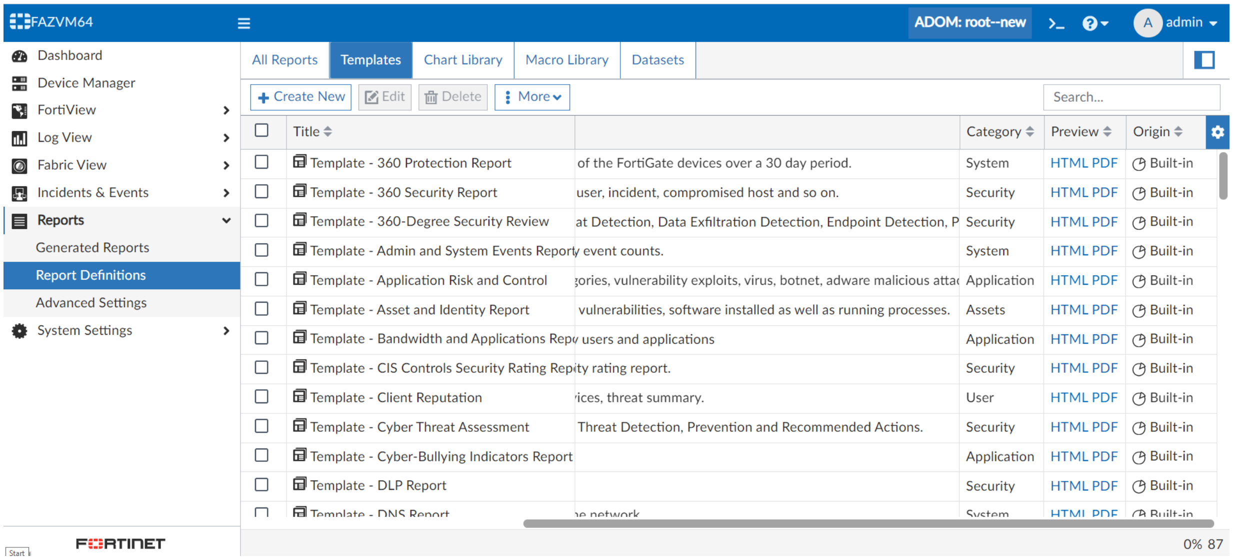
Reports included in the RHSP packages from the Security Automation Service are displayed in the global *Security Automation Reports* folder. Note that the global folder and global reports are identified with the system theme's color applied to the icon.



□	Title	Origin	Language	Cache Status	Time Period
□	FortiMail Reports				
□	FortiNAC Reports				
□	FortiNDR Reports				
□	FortiProxy Reports				
□	FortiSandbox Reports				
□	FortiWeb Reports				
□	Network Reports				
□	Outbreak Alert Reports				
□	Security Automation Reports				
□	New Security Automation - Security Analysis	FortiGuard	English		Previous 7 Days
□	SOC Reports				
□	00-cr	Custom	English		Previous N Days (60)
□	Daily Summary Report	Built-in	English		Yesterday

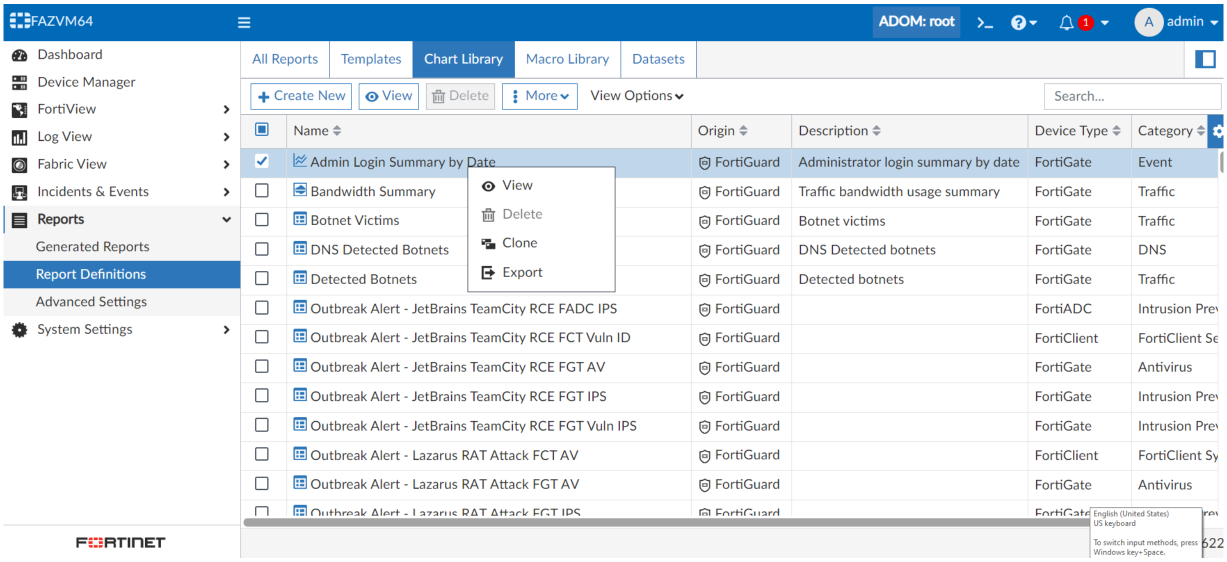
A new *Origin* column is added to the *All Reports*, *Templates*, *Chart Library*, *Macro Library*, and *Datasets* tables to indicate where the object originated:

- *FortiGuard*: Delivered by a FortiGuard package.
- *Built-in*: Included in the FortiAnalyzer by default.
- *Custom*: Created by a FortiAnalyzer administrator.



□	Title		Category	Preview	Origin
□	Template - 360 Protection Report	of the FortiGate devices over a 30 day period.	System	HTML PDF	Built-in
□	Template - 360 Security Report	user, incident, compromised host and so on.	Security	HTML PDF	Built-in
□	Template - 360-Degree Security Review	at Detection, Data Exfiltration Detection, Endpoint Detection, P	Security	HTML PDF	Built-in
□	Template - Admin and System Events Report	event counts.	System	HTML PDF	Built-in
□	Template - Application Risk and Control	gories, vulnerability exploits, virus, botnet, adware malicious atta	Application	HTML PDF	Built-in
□	Template - Asset and Identity Report	vulnerabilities, software installed as well as running processes.	Assets	HTML PDF	Built-in
□	Template - Bandwidth and Applications Rep	users and applications	Application	HTML PDF	Built-in
□	Template - CIS Controls Security Rating Rep	ity rating report.	Security	HTML PDF	Built-in
□	Template - Client Reputation	ices, threat summary.	User	HTML PDF	Built-in
□	Template - Cyber Threat Assessment	Threat Detection, Prevention and Recommended Actions.	Security	HTML PDF	Built-in
□	Template - Cyber-Bullying Indicators Report		Application	HTML PDF	Built-in
□	Template - DLP Report		Security	HTML PDF	Built-in
□	Template - DNS Report	ne network	System	HTML PDF	Built-in

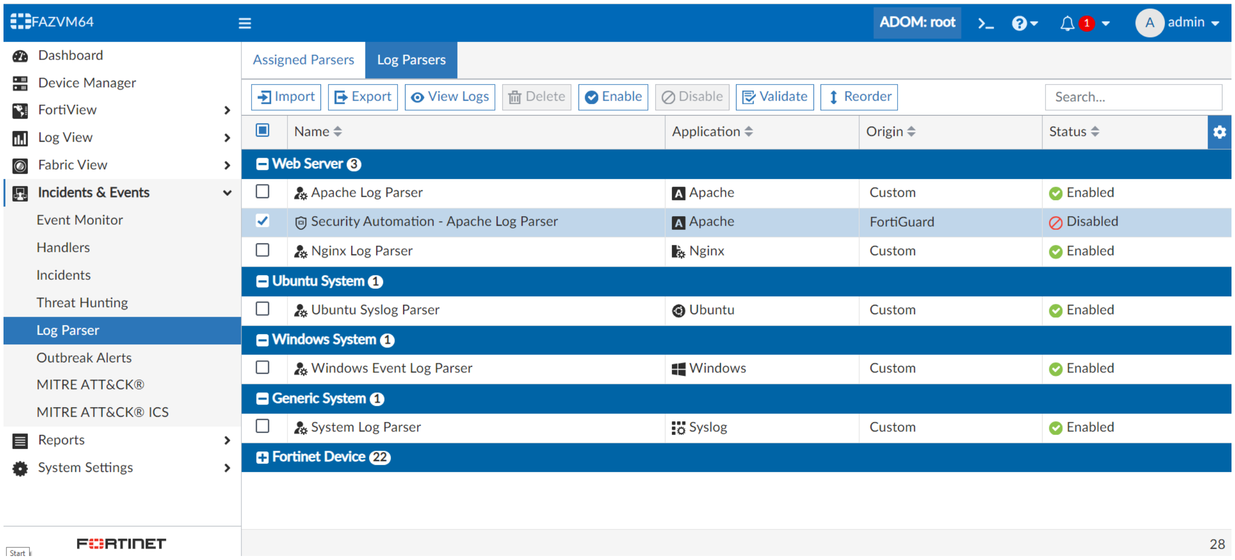
Global report's *Layout*, *Chart*, and *Dataset* cannot be edited or deleted. They are available for reference only.



☐	Name	Origin	Description	Device Type	Category
☑	Admin Login Summary by Date	FortiGuard	Administrator login summary by date	FortiGate	Event
☐	Bandwidth Summary	FortiGuard	Traffic bandwidth usage summary	FortiGate	Traffic
☐	Botnet Victims	FortiGuard	Botnet victims	FortiGate	Traffic
☐	DNS Detected Botnets	FortiGuard	DNS Detected botnets	FortiGate	DNS
☐	Detected Botnets	FortiGuard	Detected botnets	FortiGate	Traffic
☐	Outbreak Alert - JetBrains TeamCity RCE FADC IPS	FortiGuard		FortiADC	Intrusion Prev
☐	Outbreak Alert - JetBrains TeamCity RCE FCT Vuln ID	FortiGuard		FortiClient	FortiClient Se
☐	Outbreak Alert - JetBrains TeamCity RCE FGT AV	FortiGuard		FortiGate	Antivirus
☐	Outbreak Alert - JetBrains TeamCity RCE FGT IPS	FortiGuard		FortiGate	Intrusion Prev
☐	Outbreak Alert - JetBrains TeamCity RCE FGT Vuln IPS	FortiGuard		FortiGate	Intrusion Prev
☐	Outbreak Alert - Lazarus RAT Attack FCT AV	FortiGuard		FortiClient	FortiClient Sy
☐	Outbreak Alert - Lazarus RAT Attack FGT AV	FortiGuard		FortiGate	Antivirus
☐	Outbreak Alert - Lazarus RAT Attack FGT IPS	FortiGuard		FortiGate	

SIEM log parsers:

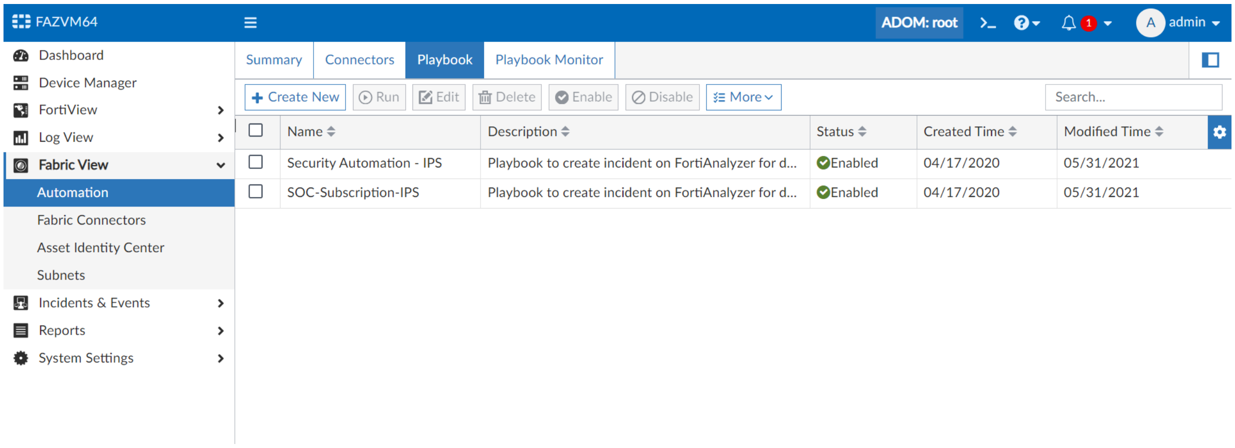
SIEM parsers delivered by the RHSP package are displayed in *Incidents & Events* > *Log Parsers*. They are stored at the global level and *FortiGuard* is displayed in the *Origin* column indicating that the parsers were delivered as part of a FortiGuard package.



☐	Name	Application	Origin	Status
	Web Server 3			
☐	Apache Log Parser	Apache	Custom	Enabled
☑	Security Automation - Apache Log Parser	Apache	FortiGuard	Disabled
☐	Nginx Log Parser	Nginx	Custom	Enabled
	Ubuntu System 1			
☐	Ubuntu Syslog Parser	Ubuntu	Custom	Enabled
	Windows System 1			
☐	Windows Event Log Parser	Windows	Custom	Enabled
	Generic System 1			
☐	System Log Parser	Syslog	Custom	Enabled
	Fortinet Device 22			

Playbooks:

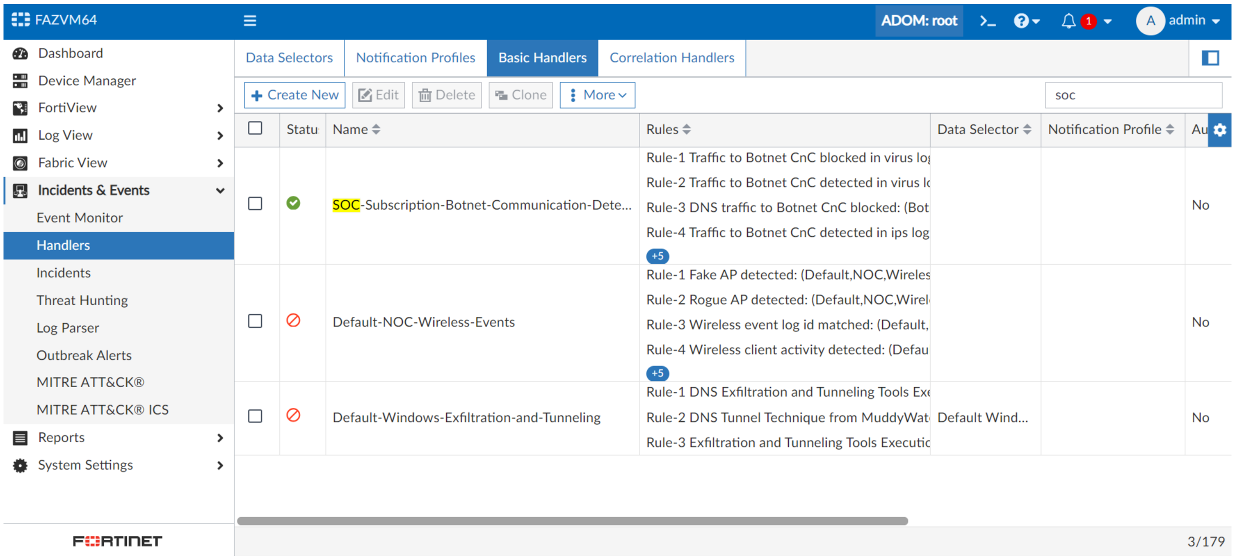
Playbooks delivered by the RHSP package are displayed in *Fabric View > Automation > Playbook*.



	Name	Description	Status	Created Time	Modified Time
□	Security Automation - IPS	Playbook to create incident on FortiAnalyzer for d...	✓Enabled	04/17/2020	05/31/2021
□	SOC-Subscription-IPS	Playbook to create incident on FortiAnalyzer for d...	✓Enabled	04/17/2020	05/31/2021

Event handlers:

Handlers delivered by the RHSP package are displayed in *Incidents & Events > Handlers > Basic Handlers*.

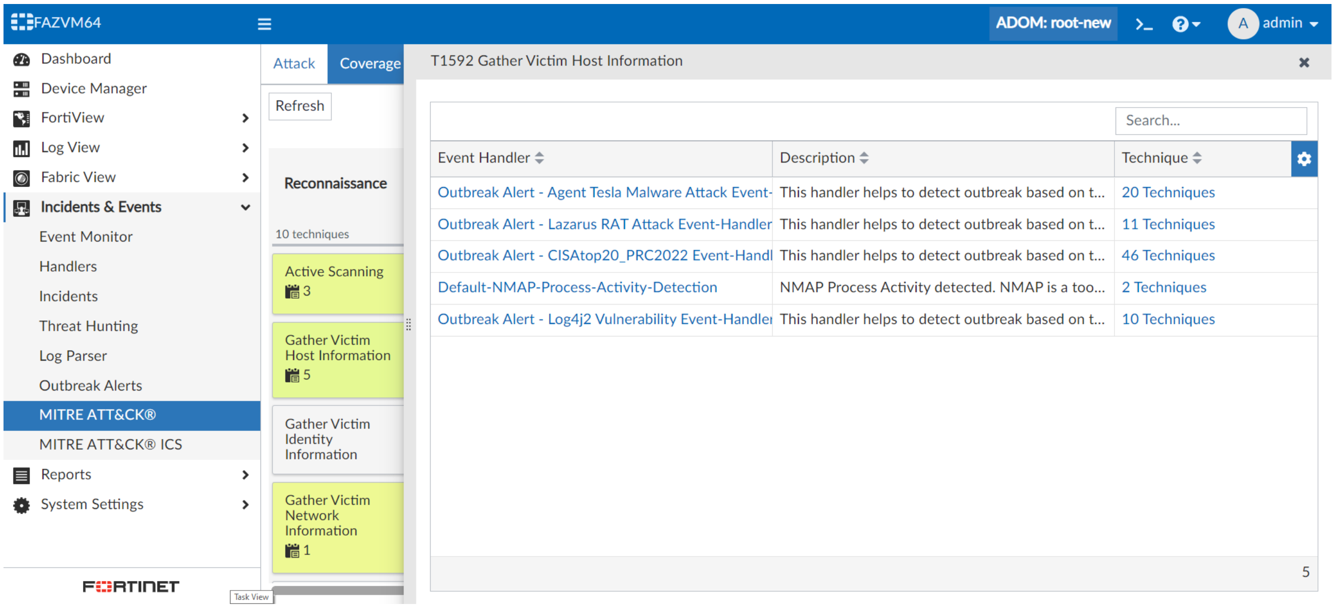


	Statu	Name	Rules	Data Selector	Notification Profile	Au
□	✓	SOC-Subscription-Botnet-Communication-Dete...	Rule-1 Traffic to Botnet CnC blocked in virus lo Rule-2 Traffic to Botnet CnC detected in virus l Rule-3 DNS traffic to Botnet CnC blocked: (Bot Rule-4 Traffic to Botnet CnC detected in ips log +5			No
□	⊘	Default-NOC-Wireless-Events	Rule-1 Fake AP detected: (Default,NOC,Wireles Rule-2 Rogue AP detected: (Default,NOC,Wirel Rule-3 Wireless event log id matched: (Default, Rule-4 Wireless client activity detected: (Defau +5			No
□	⊘	Default-Windows-Exfiltration-and-Tunneling	Rule-1 DNS Exfiltration and Tunneling Tools Ex Rule-2 DNS Tunnel Technique from MuddyWat Rule-3 Exfiltration and Tunneling Tools Executic	Default Wind...		No

MITRE information included in outbreak detection - 7.4.2

The *MITRE Domain* and *MITRE Tech ID* are now included in Outbreak Alert event handlers. For more information about Outbreak Alerts, see *Outbreak Alerts* in the FortiAnalyzer Administration Guide.

As a result, the relevant Outbreak Alert event handlers display in the appropriate techniques in *MITRE ATT&CK® > Coverage*. For example, see the image below.



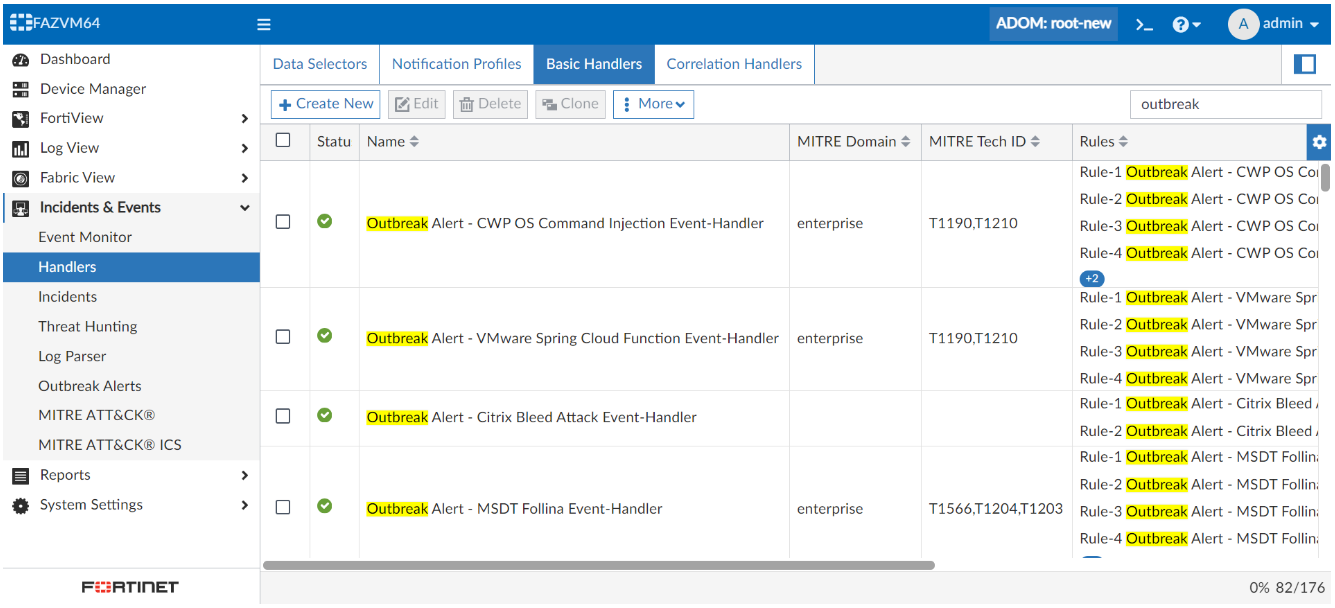
T1592 Gather Victim Host Information

Event Handler	Description	Technique
Outbreak Alert - Agent Tesla Malware Attack Event-	This handler helps to detect outbreak based on t...	20 Techniques
Outbreak Alert - Lazarus RAT Attack Event-Handler	This handler helps to detect outbreak based on t...	11 Techniques
Outbreak Alert - CISAtop20_PRC2022 Event-Handl	This handler helps to detect outbreak based on t...	46 Techniques
Default-NMAP-Process-Activity-Detection	NMAP Process Activity detected. NMAP is a too...	2 Techniques
Outbreak Alert - Log4j2 Vulnerability Event-Handler	This handler helps to detect outbreak based on t...	10 Techniques

For more information about the *MITRE ATT&CK®* pane, see the FortiAnalyzer Administration Guide.

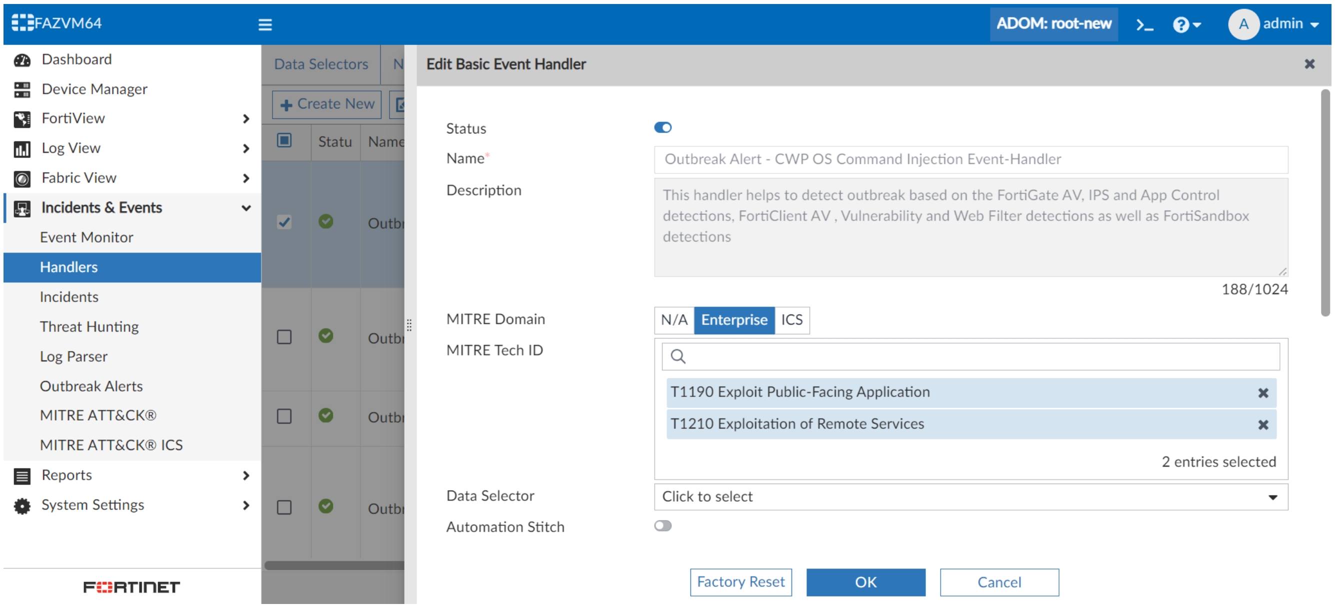
To view the MITRE information in the Outbreak Alert event handlers:

In *Incidents & Events > Basic Handlers*, the *MITRE Domain* and *MITRE Tech ID* columns display the information for Outbreak Alert event handlers.



□	Statu	Name	MITRE Domain	MITRE Tech ID	Rules
□	✓	Outbreak Alert - CWP OS Command Injection Event-Handler	enterprise	T1190,T1210	Rule-1 Outbreak Alert - CWP OS Coı Rule-2 Outbreak Alert - CWP OS Coı Rule-3 Outbreak Alert - CWP OS Coı Rule-4 Outbreak Alert - CWP OS Coı +2
□	✓	Outbreak Alert - VMware Spring Cloud Function Event-Handler	enterprise	T1190,T1210	Rule-1 Outbreak Alert - VMware Spr Rule-2 Outbreak Alert - VMware Spr Rule-3 Outbreak Alert - VMware Spr Rule-4 Outbreak Alert - VMware Spr
□	✓	Outbreak Alert - Citrix Bleed Attack Event-Handler			Rule-1 Outbreak Alert - Citrix Bleed Rule-2 Outbreak Alert - Citrix Bleed
□	✓	Outbreak Alert - MSDT Follina Event-Handler	enterprise	T1566,T1204,T1203	Rule-1 Outbreak Alert - MSDT Follin Rule-2 Outbreak Alert - MSDT Follin Rule-3 Outbreak Alert - MSDT Follin Rule-4 Outbreak Alert - MSDT Follin

You can also review and update this information when editing an Outbreak Alert event handler. For example, see the *MITRE Domain* and *MITRE Tech ID* fields in the image below.



Edit Basic Event Handler

Status: ●

Name*: Outbreak Alert - CWP OS Command Injection Event-Handler

Description: This handler helps to detect outbreak based on the FortiGate AV, IPS and App Control detections, FortiClient AV , Vulnerability and Web Filter detections as well as FortiSandbox detections

188/1024

MITRE Domain: N/A [✓ Enterprise] ICS

MITRE Tech ID:
- T1190 Exploit Public-Facing Application
- T1210 Exploitation of Remote Services

2 entries selected

Data Selector: Click to select

Automation Stitch: ○

Log and Report

This section lists the new features added to FortiAnalyzer for logs and reports:

- Logging on page 69
- Log Forwarding on page 89
- Reports on page 93
- Others on page 115

Logging

This section lists the new features added to FortiAnalyzer for logging:

- FortiAnalyzer supports FortiWeb Cloud attack logs on page 69
- Support parsing and addition of third-party application logs to the SIEM DB on page 70
- Per-ADOM log rate on page 76
- Support EMS multitenancy via FortiAnalyzer ADOMs 7.4.1 on page 78
- Logging support for FortiCASB 7.4.1 on page 80
- Logging support for FortiPAM 7.4.1 on page 82
- Logging support for FortiToken Cloud 7.4.1 on page 83
- Support parsing and addition of third-party application logs to the SIEM DB in JSON format 7.4.1 on page 84
- FortiAnalyzer supports packet header information for FortiWeb traffic log 7.4.1 on page 86
- Support additional log fields for long live session logs 7.4.2 on page 88

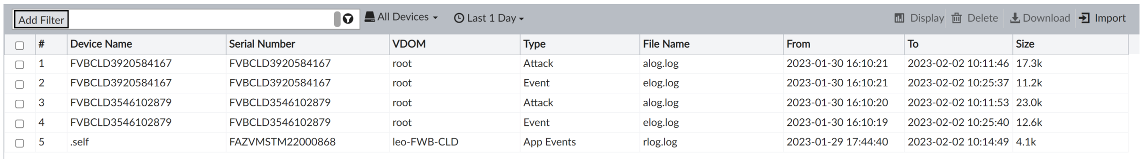
FortiAnalyzer supports FortiWeb Cloud attack logs

FortiAnalyzer now supports FortiWeb Cloud attack logs, and additional event/attack log fields have been added.

After adding and authorizing a FortiWeb Cloud device in FortiAnalyzer, you can view Attack and Event logs from this device in *Log View*.

To view FortiWeb Cloud logs in FortiAnalyzer:

1. In *Device Manager*, add and authorize the FortiWeb Cloud device.
2. To view logs from the FortiWeb Cloud device, go to *Log View* > *Log Browse*.

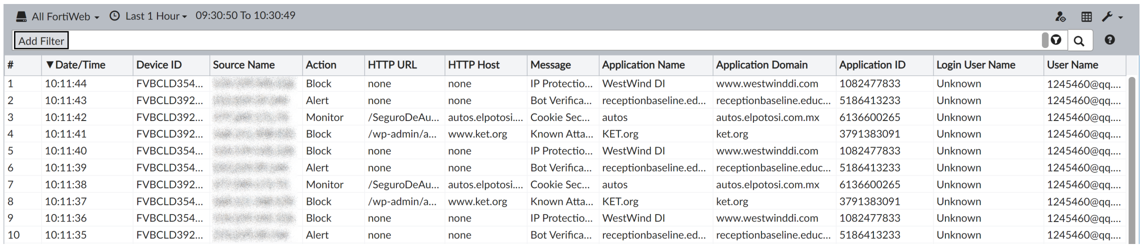


□	#	Device Name	Serial Number	VDOM	Type	File Name	From	To	Size
□	1	FVBCLD3920584167	FVBCLD3920584167	root	Attack	alog.log	2023-01-30 16:10:21	2023-02-02 10:11:46	17.3k
□	2	FVBCLD3920584167	FVBCLD3920584167	root	Event	elog.log	2023-01-30 16:10:21	2023-02-02 10:25:37	11.2k
□	3	FVBCLD3546102879	FVBCLD3546102879	root	Attack	alog.log	2023-01-30 16:10:20	2023-02-02 10:11:53	23.0k
□	4	FVBCLD3546102879	FVBCLD3546102879	root	Event	elog.log	2023-01-30 16:10:19	2023-02-02 10:25:40	12.6k
□	5	.self	FAZVMSTM22000868	leo-FWB-CLD	App Events	rlog.log	2023-01-29 17:44:40	2023-02-02 10:14:49	4.1k

You can also go to *Log View* > *FortiWeb* > *Attack*. This includes FortiWeb Cloud attack logs, as well as four new fields:

- *user_id*, which corresponds to the *User ID* column
- *app_id*, which corresponds to the *Application ID* column
- *app_name*, which corresponds to the *Application Name* column
- *app_domain*, which corresponds to the *Application Domain* column

See an example of *Log View > FortiWeb > Attack* below.

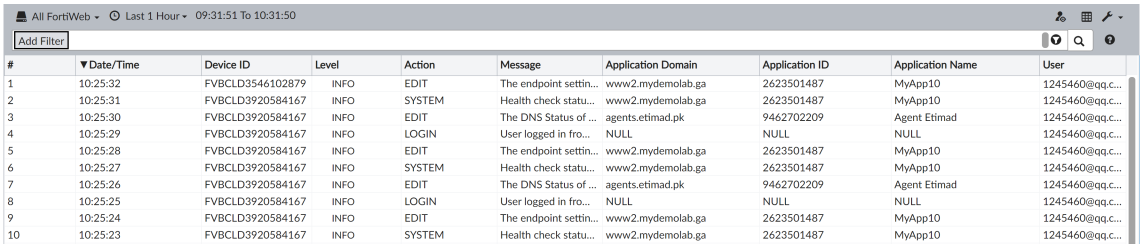


#	▼Date/Time	Device ID	Source Name	Action	HTTP URL	HTTP Host	Message	Application Name	Application Domain	Application ID	Login User Name	User Name
1	10:11:44	FVBCLD354...	[redacted]	Block	none	none	IP Protectio...	WestWind DI	www.westwinddi.com	1082477833	Unknown	1245460@qq....
2	10:11:43	FVBCLD392...	[redacted]	Alert	none	none	Bot Verifica...	receptionbaseline.ed...	receptionbaseline.educ...	5186413233	Unknown	1245460@qq....
3	10:11:42	FVBCLD392...	[redacted]	Monitor	/SeguroDeAu...	autos.elpotosi....	Cookie Sec...	autos	autos.elpotosi.com.mx	6136600265	Unknown	1245460@qq....
4	10:11:41	FVBCLD392...	[redacted]	Block	/wp-admin/a...	www.ket.org	Known Atta...	KET.org	ket.org	3791383091	Unknown	1245460@qq....
5	10:11:40	FVBCLD354...	[redacted]	Block	none	none	IP Protectio...	WestWind DI	www.westwinddi.com	1082477833	Unknown	1245460@qq....
6	10:11:39	FVBCLD354...	[redacted]	Alert	none	none	Bot Verifica...	receptionbaseline.ed...	receptionbaseline.educ...	5186413233	Unknown	1245460@qq....
7	10:11:38	FVBCLD392...	[redacted]	Monitor	/SeguroDeAu...	autos.elpotosi....	Cookie Sec...	autos	autos.elpotosi.com.mx	6136600265	Unknown	1245460@qq....
8	10:11:37	FVBCLD354...	[redacted]	Block	/wp-admin/a...	www.ket.org	Known Atta...	KET.org	ket.org	3791383091	Unknown	1245460@qq....
9	10:11:36	FVBCLD354...	[redacted]	Block	none	none	IP Protectio...	WestWind DI	www.westwinddi.com	1082477833	Unknown	1245460@qq....
10	10:11:35	FVBCLD392...	[redacted]	Alert	none	none	Bot Verifica...	receptionbaseline.ed...	receptionbaseline.educ...	5186413233	Unknown	1245460@qq....

Finally, you can also go to *Log View > FortiWeb > Event*. This includes FortiWeb Cloud event logs, as well as five new fields:

- *user_id*, which corresponds to the *User ID* column
- *login_user*, which corresponds to the *User* column
- *app_id*, which corresponds to the *Application ID* column
- *app_name*, which corresponds to the *Application Name* column
- *app_domain*, which corresponds to the *Application Domain* column

See an example of *Log View > FortiWeb > Event* below.



#	▼Date/Time	Device ID	Level	Action	Message	Application Domain	Application ID	Application Name	User
1	10:25:32	FVBCLD3546102879	INFO	EDIT	The endpoint settin...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...
2	10:25:31	FVBCLD3920584167	INFO	SYSTEM	Health check statu...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...
3	10:25:30	FVBCLD3920584167	INFO	EDIT	The DNS Status of ...	agents.etimad.pk	9462702209	Agent Etimad	1245460@qq.c...
4	10:25:29	FVBCLD3920584167	INFO	LOGIN	User logged in fro...	NULL	NULL	NULL	1245460@qq.c...
5	10:25:28	FVBCLD3920584167	INFO	EDIT	The endpoint settin...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...
6	10:25:27	FVBCLD3920584167	INFO	SYSTEM	Health check statu...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...
7	10:25:26	FVBCLD3920584167	INFO	EDIT	The DNS Status of ...	agents.etimad.pk	9462702209	Agent Etimad	1245460@qq.c...
8	10:25:25	FVBCLD3920584167	INFO	LOGIN	User logged in fro...	NULL	NULL	NULL	1245460@qq.c...
9	10:25:24	FVBCLD3920584167	INFO	EDIT	The endpoint settin...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...
10	10:25:23	FVBCLD3920584167	INFO	SYSTEM	Health check statu...	www2.mydemolab.ga	2623501487	MyApp10	1245460@qq.c...

Support parsing and addition of third-party application logs to the SIEM DB

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- SIEM log parsers

FortiAnalyzer supports parsing and addition of third-party application logs to the SIEM DB.

There are two types of log parsers:

- Predefined parsers
- Custom parsers

You can find predefined SIEM log parsers in *Incidents & Events > Log Parser > Log Parsers*. There are predefined parsers for all fabric related Fortinet products. Predefined Apache and Nginx web server log parsers have also been added to this list of predefined SIEM log parsers.

The configuration of each SIEM log parser (predefined and custom) is specific to the ADOM that you are in. Any changes to an existing parser or any newly added parsers will only affect the ADOM that the action was completed in. Ensure you are in the correct ADOM when working with log parsers.

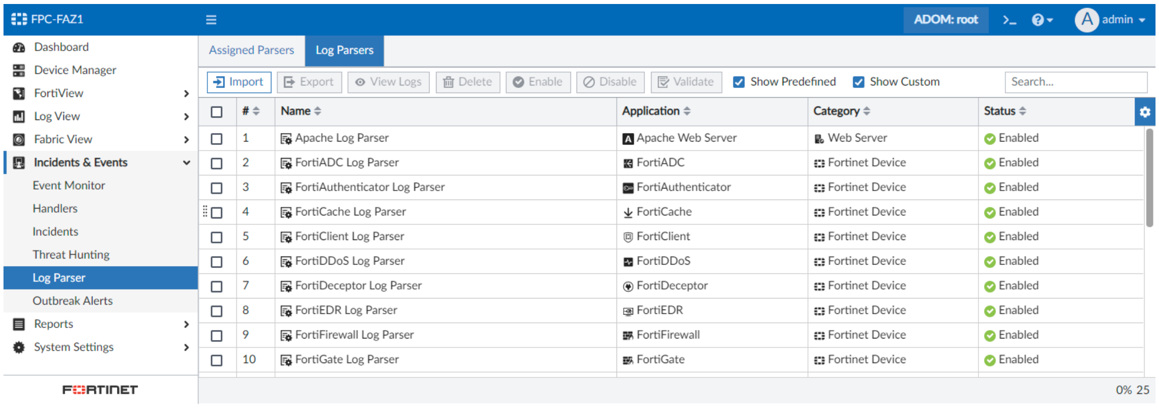
The following information is provided in this topic:

- To view the log parsers: on page 71
- The Apache web server log parser: on page 72
- The Nginx web server log parser: on page 73
- To import a custom log parser: on page 74
- To validate if the original logs can be parsed: on page 74
- To assign devices to a log parser: on page 75

To view the log parsers:

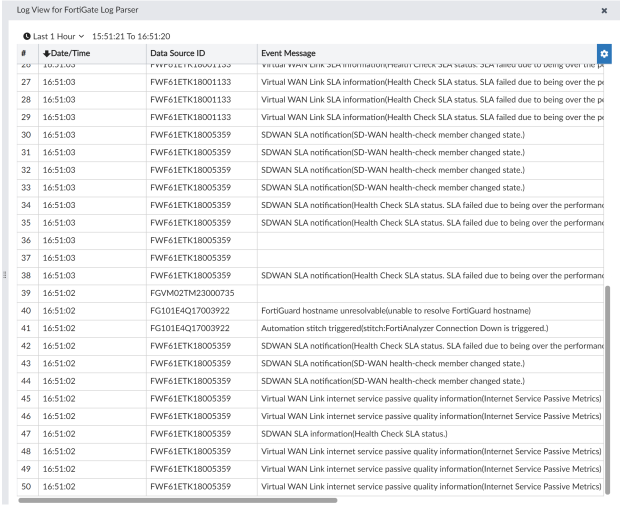
1. In *Incidents & Events* > *Log Parser* > *Log Parsers*, select *Show Predefined* and/or *Show Custom* to show the available log parsers in the table view.
   Each predefined log parser is assigned a default *Application* and *Category*. Custom log parsers are assigned a default *Application* and *Category* when they are imported.

   The # column is the priority of each Siem Log_Parser from highest (`1`) to lowest. By default, newly imported custom log parsers are assigned the lowest priority. To change the priority, click the left edge of the row and drag and drop it to the desired area in the table. See below.



□	#	Name	Application	Category	Status
□	1	Apache Log Parser	Apache Web Server	Web Server	✓ Enabled
□	2	FortiADC Log Parser	FortiADC	Fortinet Device	✓ Enabled
□	3	FortiAuthenticator Log Parser	FortiAuthenticator	Fortinet Device	✓ Enabled
□	4	FortiCache Log Parser	FortiCache	Fortinet Device	✓ Enabled
□	5	FortiClient Log Parser	FortiClient	Fortinet Device	✓ Enabled
□	6	FortiDDoS Log Parser	FortiDDoS	Fortinet Device	✓ Enabled
□	7	FortiDeceptor Log Parser	FortiDeceptor	Fortinet Device	✓ Enabled
□	8	FortiEDR Log Parser	FortiEDR	Fortinet Device	✓ Enabled
□	9	FortiFirewall Log Parser	FortiFirewall	Fortinet Device	✓ Enabled
□	10	FortiGate Log Parser	FortiGate	Fortinet Device	✓ Enabled

2. Double-click a log parser in the table view to display all related SIEM logs. Alternatively, you can select the checkbox for the log parser and click *View Logs*.



Log View for FortiGate Log Parser ✖

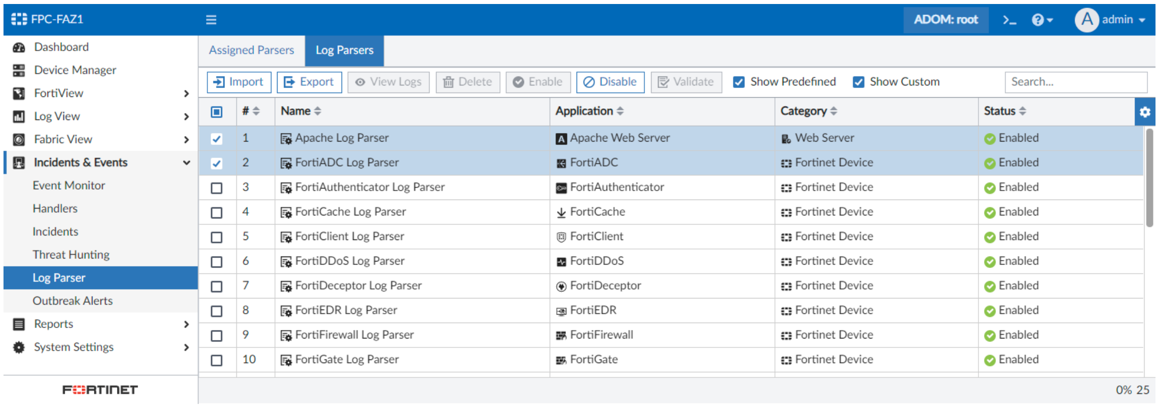
Last 1 Hour ⌄ 15:51:21 To 16:51:20

#	Date/Time	Data Source ID	Event Message
26	16:51:03	FWF61ETK18001133	Virtual WAN Link SLA information(Health Check SLA status. SLA failed due to being over the pe
27	16:51:03	FWF61ETK18001133	Virtual WAN Link SLA information(Health Check SLA status. SLA failed due to being over the pe
28	16:51:03	FWF61ETK18001133	Virtual WAN Link SLA information(Health Check SLA status. SLA failed due to being over the pe
29	16:51:03	FWF61ETK18001133	Virtual WAN Link SLA information(Health Check SLA status. SLA failed due to being over the pe
30	16:51:03	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
31	16:51:03	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
32	16:51:03	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
33	16:51:03	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
34	16:51:03	FWF61ETK18005359	SDWAN SLA notification(Health Check SLA status. SLA failed due to being over the performanc
35	16:51:03	FWF61ETK18005359	SDWAN SLA notification(Health Check SLA status. SLA failed due to being over the performanc
36	16:51:03	FWF61ETK18005359	
37	16:51:03	FWF61ETK18005359	
38	16:51:03	FWF61ETK18005359	SDWAN SLA notification(Health Check SLA status. SLA failed due to being over the performanc
39	16:51:02	FGVM02TM23000735	
40	16:51:02	FG101E4Q17003922	FortiGuard hostname unresolvable(unable to resolve FortiGuard hostname)
41	16:51:02	FG101E4Q17003922	Automation stitch triggered(stitch:FortiAnalyzer Connection Down is triggered.)
42	16:51:02	FWF61ETK18005359	SDWAN SLA notification(Health Check SLA status. SLA failed due to being over the performanc
43	16:51:02	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
44	16:51:02	FWF61ETK18005359	SDWAN SLA notification(SD-WAN health-check member changed state.)
45	16:51:02	FWF61ETK18005359	Virtual WAN Link internet service passive quality information(Internet Service Passive Metrics)
46	16:51:02	FWF61ETK18005359	Virtual WAN Link internet service passive quality information(Internet Service Passive Metrics)
47	16:51:02	FWF61ETK18005359	SDWAN SLA information(Health Check SLA status.)
48	16:51:02	FWF61ETK18005359	Virtual WAN Link internet service passive quality information(Internet Service Passive Metrics)
49	16:51:02	FWF61ETK18005359	Virtual WAN Link internet service passive quality information(Internet Service Passive Metrics)
50	16:51:02	FWF61ETK18005359	Virtual WAN Link internet service passive quality information(Internet Service Passive Metrics)

3. Select the checkbox for one or more log parsers in the table to perform an action from the toolbar. For example, you can *Export* in JSON format, *Enable*, *Disable*, *Delete*, or *Validate* the log parsers.

   Some actions will be unavailable if they cannot be performed on the selected log parser(s).

   - You cannot *Disable* a log parser if it is assigned and in use.
   - You cannot *Delete* predefined log parsers. They can only be disabled.
   - You cannot perform the *Validate* action on more than one parser at a time.

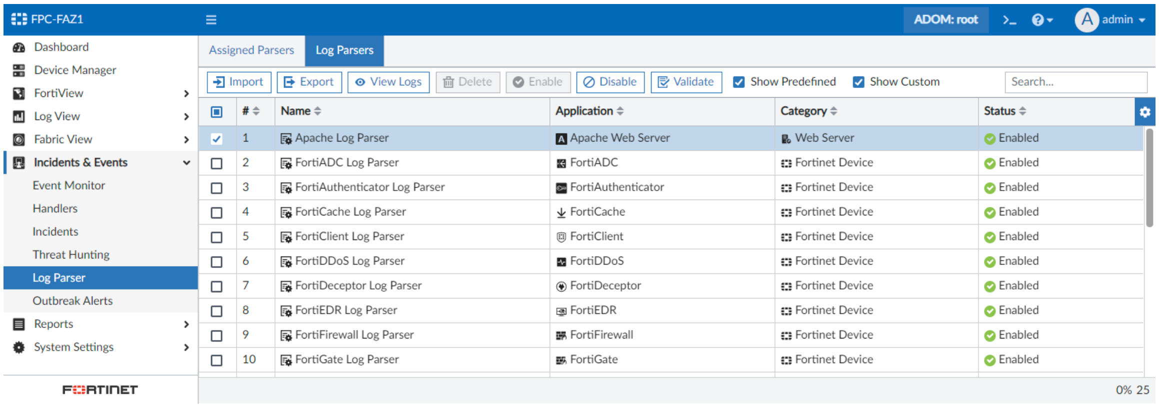


☑ Show Predefined ☑ Show Custom

☐	#	Name	Application	Category	Status
☑	1	Apache Log Parser	Apache Web Server	Web Server	Enabled
☑	2	FortiADC Log Parser	FortiADC	Fortinet Device	Enabled
☐	3	FortiAuthenticator Log Parser	FortiAuthenticator	Fortinet Device	Enabled
☐	4	FortiCache Log Parser	FortiCache	Fortinet Device	Enabled
☐	5	FortiClient Log Parser	FortiClient	Fortinet Device	Enabled
☐	6	FortiDDoS Log Parser	FortiDDoS	Fortinet Device	Enabled
☐	7	FortiDeceptor Log Parser	FortiDeceptor	Fortinet Device	Enabled
☐	8	FortiEDR Log Parser	FortiEDR	Fortinet Device	Enabled
☐	9	FortiFirewall Log Parser	FortiFirewall	Fortinet Device	Enabled
☐	10	FortiGate Log Parser	FortiGate	Fortinet Device	Enabled

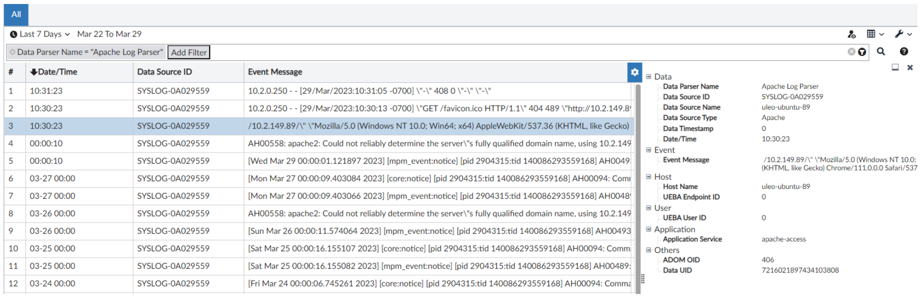
The Apache web server log parser:

Go to *Incidents & Events > Log Parser > Log Parsers* to find the Apache Log Parser in the predefined SIEM log parsers. Double-click the parser to view the related logs.



	#	Name	Application	Category	Status
☑	1	Apache Log Parser	Apache Web Server	Web Server	Enabled
□	2	FortiADC Log Parser	FortiADC	Fortinet Device	Enabled
□	3	FortiAuthenticator Log Parser	FortiAuthenticator	Fortinet Device	Enabled
□	4	FortiCache Log Parser	FortiCache	Fortinet Device	Enabled
□	5	FortiClient Log Parser	FortiClient	Fortinet Device	Enabled
□	6	FortiDDoS Log Parser	FortiDDoS	Fortinet Device	Enabled
□	7	FortiDeceptor Log Parser	FortiDeceptor	Fortinet Device	Enabled
□	8	FortiEDR Log Parser	FortiEDR	Fortinet Device	Enabled
□	9	FortiFirewall Log Parser	FortiFirewall	Fortinet Device	Enabled
□	10	FortiGate Log Parser	FortiGate	Fortinet Device	Enabled

The Apache logs are also parsed in *Log View > Fabric > All*. You can filter by `Data Parser Name = Apache Log Parser`.



Data Parser Name = "Apache Log Parser"

#	Date/Time	Data Source ID	Event Message
1	10:31:23	SYSLOG-0A029559	10.2.0.250 - - [29/Mar/2023:10:31:05 -0700] \"-\" 408 0 \"-\" \"-\"
2	10:30:23	SYSLOG-0A029559	10.2.0.250 - - [29/Mar/2023:10:30:13 -0700] \"GET /favicon.ico HTTP/1.1\" 404 489 \"http://10.2.149.8
3	10:30:23	SYSLOG-0A029559	/10.2.149.89/\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
4	00:00:10	SYSLOG-0A029559	AH00558: apache2: Could not reliably determine the server\"s fully qualified domain name, using 10.2.149
5	00:00:10	SYSLOG-0A029559	[Wed Mar 29 00:00:01.121897 2023] [mpm_event:notice] [pid 2904315:tid 140086293559168] AH0049
6	03-27 00:00	SYSLOG-0A029559	[Mon Mar 27 00:00:09.403084 2023] [core:notice] [pid 2904315:tid 140086293559168] AH00094: Comr
7	03-27 00:00	SYSLOG-0A029559	[Mon Mar 27 00:00:09.403066 2023] [mpm_event:notice] [pid 2904315:tid 140086293559168] AH0048
8	03-26 00:00	SYSLOG-0A029559	AH00558: apache2: Could not reliably determine the server\"s fully qualified domain name, using 10.2.149
9	03-26 00:00	SYSLOG-0A029559	[Sun Mar 26 00:00:11.574064 2023] [mpm_event:notice] [pid 2904315:tid 140086293559168] AH00493
10	03-25 00:00	SYSLOG-0A029559	[Sat Mar 25 00:00:16.155107 2023] [core:notice] [pid 2904315:tid 140086293559168] AH00094: Comm
11	03-25 00:00	SYSLOG-0A029559	[Sat Mar 25 00:00:16.155082 2023] [mpm_event:notice] [pid 2904315:tid 140086293559168] AH00489:
12	03-24 00:00	SYSLOG-0A029559	[Fri Mar 24 00:00:06.745261 2023] [core:notice] [pid 2904315:tid 140086293559168] AH00094: Comma

Data
- Data Parser Name: Apache Log Parser
- Data Source ID: SYSLOG-0A029559
- Data Source Name: uleo-ubuntu-89
- Data Source Type: Apache
- Data Timestamp: 0
- Date/Time: 10:30:23

Event
- Event Message: /10.2.149.89/\" \"Mozilla/5.0 (Windows NT 10.0; (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537

Host
- Host Name: uleo-ubuntu-89
- UEBA Endpoint ID: 0

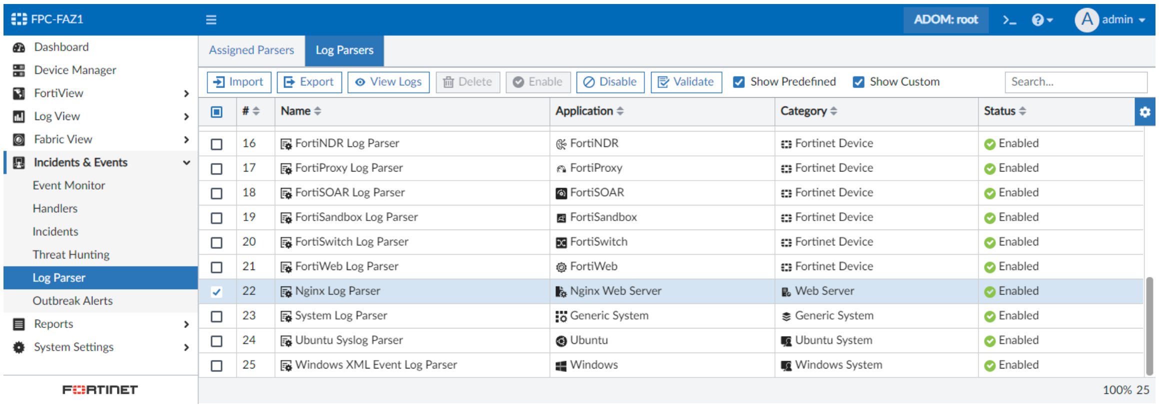
User
- UEBA User ID: 0

Application
- Application Service: apache-access

Others
- ADOM OID: 406
- Data UID: 7216021897434103808

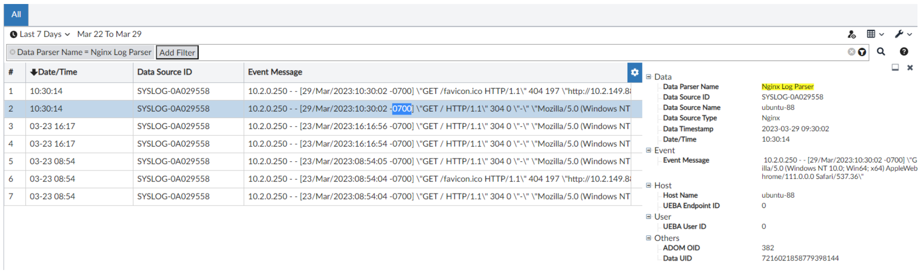
The Nginx web server log parser:

Go to *Incidents & Events > Log Parser > Log Parsers* to find the Nginx Log Parser in the predefined SIEM log parsers. Double-click the parser to view the related logs.



	#	Name	Application	Category	Status
□	16	FortiNDR Log Parser	FortiNDR	Fortinet Device	Enabled
□	17	FortiProxy Log Parser	FortiProxy	Fortinet Device	Enabled
□	18	FortiSOAR Log Parser	FortiSOAR	Fortinet Device	Enabled
□	19	FortiSandbox Log Parser	FortiSandbox	Fortinet Device	Enabled
□	20	FortiSwitch Log Parser	FortiSwitch	Fortinet Device	Enabled
□	21	FortiWeb Log Parser	FortiWeb	Fortinet Device	Enabled
☑	22	Nginx Log Parser	Nginx Web Server	Web Server	Enabled
□	23	System Log Parser	Generic System	Generic System	Enabled
□	24	Ubuntu Syslog Parser	Ubuntu	Ubuntu System	Enabled
□	25	Windows XML Event Log Parser	Windows	Windows System	Enabled

The Nginx logs are also parsed in *Log View > Fabric > All*. You can filter by `Data Parser Name = Nginx Log Parser`.

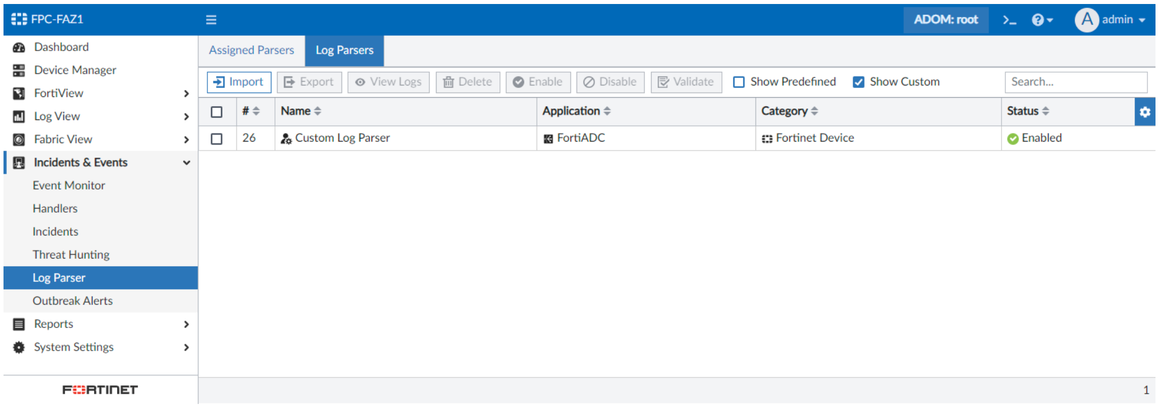


#	Date/Time	Data Source ID	Event Message
1	10:30:14	SYSLOG-0A029558	10.2.0.250 - - [29/Mar/2023:10:30:02 -0700] \"GET /favicon.ico HTTP/1.1\" 404 197 \"http://10.2.149.8
2	10:30:14	SYSLOG-0A029558	10.2.0.250 - - [29/Mar/2023:10:30:02 -0700] \"GET / HTTP/1.1\" 304 0 \"-\" \"Mozilla/5.0 (Windows NT
3	03-23 16:17	SYSLOG-0A029558	10.2.0.250 - - [23/Mar/2023:16:16:56 -0700] \"GET / HTTP/1.1\" 304 0 \"-\" \"Mozilla/5.0 (Windows NT
4	03-23 16:17	SYSLOG-0A029558	10.2.0.250 - - [23/Mar/2023:16:16:54 -0700] \"GET / HTTP/1.1\" 304 0 \"-\" \"Mozilla/5.0 (Windows NT
5	03-23 08:54	SYSLOG-0A029558	10.2.0.250 - - [23/Mar/2023:08:54:05 -0700] \"GET / HTTP/1.1\" 304 0 \"-\" \"Mozilla/5.0 (Windows NT
6	03-23 08:54	SYSLOG-0A029558	10.2.0.250 - - [23/Mar/2023:08:54:04 -0700] \"GET /favicon.ico HTTP/1.1\" 404 197 \"http://10.2.149.8
7	03-23 08:54	SYSLOG-0A029558	10.2.0.250 - - [23/Mar/2023:08:54:04 -0700] \"GET / HTTP/1.1\" 304 0 \"-\" \"Mozilla/5.0 (Windows NT

⊟ Data	
Data Parser Name	Nginx Log Parser
Data Source ID	SYSLOG-0A029558
Data Source Name	ubuntu-88
Data Source Type	Nginx
Data Timestamp	2023-03-29 09:30:02
Date/Time	10:30:14
⊟ Event	
Event Message	10.2.0.250 - - [29/Mar/2023:10:30:02 -0700] \"G illa/5.0 (Windows NT 10.0; Win64; x64) AppleWeb hrome/111.0.0.0 Safari/537.36\"
⊟ Host	
Host Name	ubuntu-88
UEBA Endpoint ID	0
⊟ User	
UEBA User ID	0
⊟ Others	
ADOM OID	382
Data UID	7216021858779398144

To import a custom log parser:

1. In *Incidents & Events > Log Parser > Log Parsers*, click *Import*.
   The *Import Log Parser* dialog displays.
2. Drag and drop or select the log parser.
   The log parser must be in the correct format as a JSON file to meet the requirements checked during the import.
3. Click *OK*.
   Once added, the custom log parser will be included in the table view when *Show Custom* is selected.

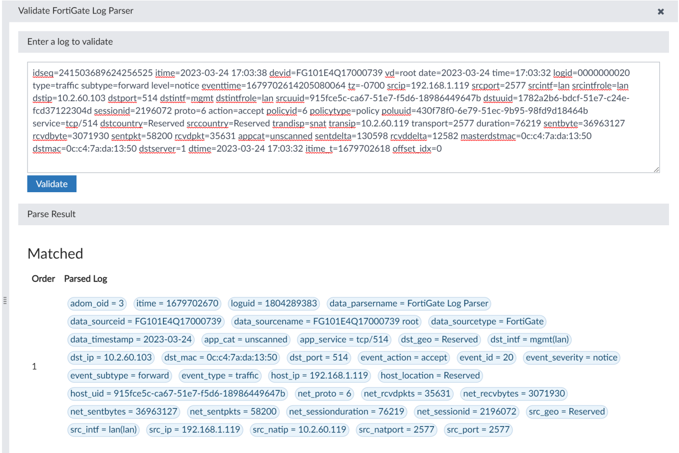


□ Show Predefined ☑ Show Custom

□	#	Name	Application	Category	Status
□	26	Custom Log Parser	FortiADC	Fortinet Device	✓ Enabled

To validate if the original logs can be parsed:

1. In *Incidents & Events > Log Parser > Log Parsers*, select the checkbox for a log parser.
2. Click *Validate*.
   The *Validate Log Parser* pane opens.
3. Enter a log to validate and click *Validate*.
   A *Parse Result* will display in the same pane.



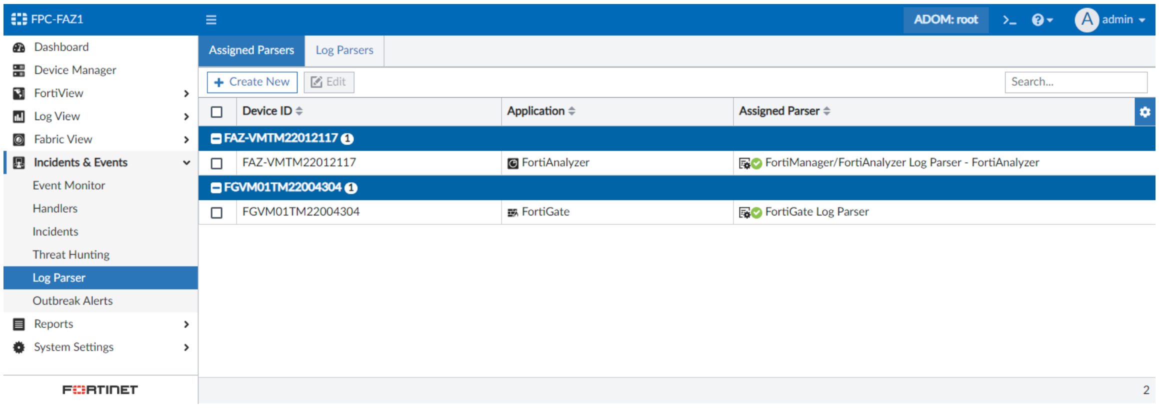
```
idseq=241503689624256525 itime=2023-03-24 17:03:38 devid=FG101E4Q17000739 vd=root date=2023-03-24 time=17:03:32 logid=0000000020
type=traffic subtype=forward level=notice eventtime=1679702614205080064 tz=-0700 srcip=192.168.1.119 srcport=2577 srcintf=lan srcintfrole=lan
dstip=10.2.60.103 dstport=514 dstintf=mgmt dstintfrole=lan srcuuid=915fce5c-ca67-51e7-f5d6-18986449647b dstuuid=1782a2b6-bdcf-51e7-c24e-
fcd37122304d sessionid=2196072 proto=6 action=accept policyid=6 policytype=policy poluuid=430f78f0-6e79-51ec-9b95-98fd9d18464b
service=tcp/514 dstcountry=Reserved srccountry=Reserved trandisp=snat transip=10.2.60.119 transport=2577 duration=76219 sentbyte=36963127
rcvdbyte=3071930 sentpkt=58200 rcvdpkt=35631 appcat=unscanned sentdelta=130598 rcvddelta=12582 masterdstmac=0c:c4:7a:da:13:50
dstmac=0c:c4:7a:da:13:50 dstserver=1 dtime=2023-03-24 17:03:32 itime_t=1679702618 offset_idx=0
```

Matched

Order	Parsed Log
1	adom_oid = 3 itime = 1679702670 loguid = 1804289383 data_parsername = FortiGate Log Parser data_sourceid = FG101E4Q17000739 data_sourcename = FG101E4Q17000739 root data_sourcetype = FortiGate data_timestamp = 2023-03-24 app_cat = unscanned app_service = tcp/514 dst_geo = Reserved dst_intf = mgmt(lan) dst_ip = 10.2.60.103 dst_mac = 0c:c4:7a:da:13:50 dst_port = 514 event_action = accept event_id = 20 event_severity = notice event_subtype = forward event_type = traffic host_ip = 192.168.1.119 host_location = Reserved host_uid = 915fce5c-ca67-51e7-f5d6-18986449647b net_proto = 6 net_rcvdpkts = 35631 net_recvbytes = 3071930 net_sentbytes = 36963127 net_sentpkts = 58200 net_sessionduration = 76219 net_sessionid = 2196072 src_geo = Reserved src_intf = lan(lan) src_ip = 192.168.1.119 src_natip = 10.2.60.119 src_natport = 2577 src_port = 2577

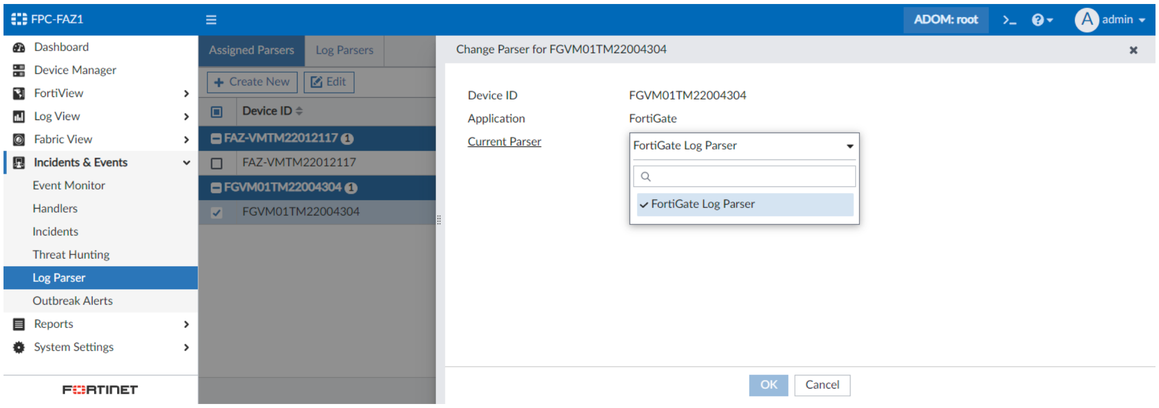
To assign devices to a log parser:

1. Go to *Incidents & Events > Log Parser > Assigned Parsers*.
   The existing log parser assignments display in a table view.



□	Device ID	Application	Assigned Parser
FAZ-VMTM22012117			
□	FAZ-VMTM22012117	FortiAnalyzer	FortiManager/FortiAnalyzer Log Parser - FortiAnalyzer
FGVM01TM22004304			
□	FGVM01TM22004304	FortiGate	FortiGate Log Parser

2. Select the checkbox for an existing log parser assignment and click *Edit*.
   Alternatively, you can click *Create New* to create a new log parser assignment.
   The *Change Parser* pane displays.
3. From the *Current Parser* dropdown, select the log parser to assign the device/application to.
4. Click *OK*.



Change Parser for FGVM01TM22004304

Device ID	FGVM01TM22004304
Application	FortiGate
Current Parser	FortiGate Log Parser

✓ FortiGate Log Parser

Per-ADOM log rate

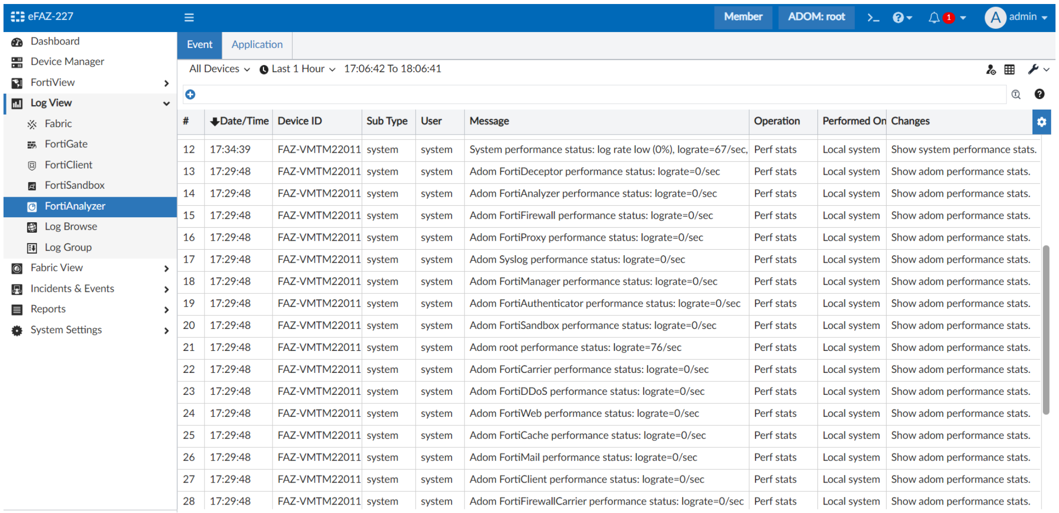
To better fit multi-tenancy deployment, FortiAnalyzer provides a per-ADOM log rate that the administrator can monitor to prevent one ADOM/customer from impacting the stability of the entire unit.

An additional diskquota log has been introduced to inform the administrator when an ADOM reaches the configured quota threshold.

To view the logs in the GUI:

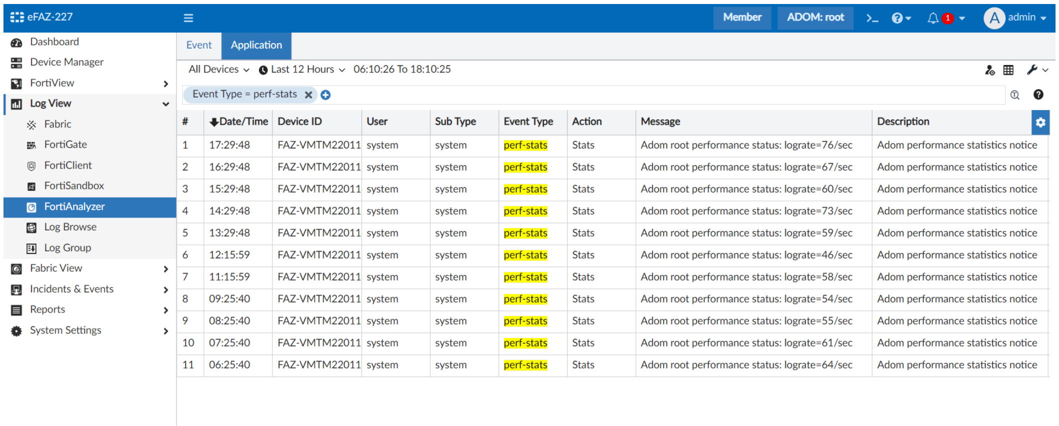
A log message for ADOM performance statistics (log rate) is added to both FortiAnalyzer Event logs and Application logs. FortiAnalyzer Event logs will generate this message for all ADOMs, while Application logs will generate this message for the current ADOM only.

For example, see the below log messages in *Log View > FortiAnalyzer > Event*:



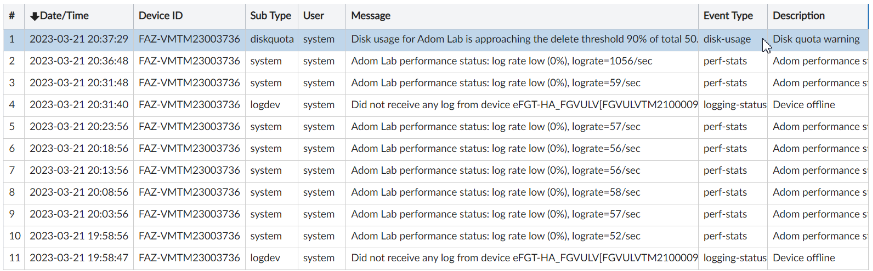
#	Date/Time	Device ID	Sub Type	User	Message	Operation	Performed On	Changes
12	17:34:39	FAZ-VMTM22011	system	system	System performance status: log rate low (0%), lograte=67/sec,	Perf stats	Local system	Show system performance stats.
13	17:29:48	FAZ-VMTM22011	system	system	Adom FortiDeceptor performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
14	17:29:48	FAZ-VMTM22011	system	system	Adom FortiAnalyzer performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
15	17:29:48	FAZ-VMTM22011	system	system	Adom FortiFirewall performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
16	17:29:48	FAZ-VMTM22011	system	system	Adom FortiProxy performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
17	17:29:48	FAZ-VMTM22011	system	system	Adom Syslog performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
18	17:29:48	FAZ-VMTM22011	system	system	Adom FortiManager performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
19	17:29:48	FAZ-VMTM22011	system	system	Adom FortiAuthenticator performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
20	17:29:48	FAZ-VMTM22011	system	system	Adom FortiSandbox performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
21	17:29:48	FAZ-VMTM22011	system	system	Adom root performance status: lograte=76/sec	Perf stats	Local system	Show adom performance stats.
22	17:29:48	FAZ-VMTM22011	system	system	Adom FortiCarrier performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
23	17:29:48	FAZ-VMTM22011	system	system	Adom FortiDDoS performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
24	17:29:48	FAZ-VMTM22011	system	system	Adom FortiWeb performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
25	17:29:48	FAZ-VMTM22011	system	system	Adom FortiCache performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
26	17:29:48	FAZ-VMTM22011	system	system	Adom FortiMail performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
27	17:29:48	FAZ-VMTM22011	system	system	Adom FortiClient performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.
28	17:29:48	FAZ-VMTM22011	system	system	Adom FortiFirewallCarrier performance status: lograte=0/sec	Perf stats	Local system	Show adom performance stats.

For example, see the below log messages in *Log View > FortiAnalyzer > Application*:



#	Date/Time	Device ID	User	Sub Type	Event Type	Action	Message	Description
1	17:29:48	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=76/sec	Adom performance statistics notice
2	16:29:48	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=67/sec	Adom performance statistics notice
3	15:29:48	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=60/sec	Adom performance statistics notice
4	14:29:48	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=73/sec	Adom performance statistics notice
5	13:29:48	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=59/sec	Adom performance statistics notice
6	12:15:59	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=46/sec	Adom performance statistics notice
7	11:15:59	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=58/sec	Adom performance statistics notice
8	09:25:40	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=54/sec	Adom performance statistics notice
9	08:25:40	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=55/sec	Adom performance statistics notice
10	07:25:40	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=61/sec	Adom performance statistics notice
11	06:25:40	FAZ-VMTM22011	system	system	perf-stats	Stats	Adom root performance status: lograte=64/sec	Adom performance statistics notice

A log message is also added for ADOM archive usage to Local Application Logs. See below example taken from *Log View > FortiAnalyzer > Application*:



#	Date/Time	Device ID	Sub Type	User	Message	Event Type	Description
1	2023-03-21 20:37:29	FAZ-VMTM23003736	diskquota	system	Disk usage for Adom Lab is approaching the delete threshold 90% of total 50.	disk-usage	Disk quota warning
2	2023-03-21 20:36:48	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=1056/sec	perf-stats	Adom performance s
3	2023-03-21 20:31:48	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=59/sec	perf-stats	Adom performance s
4	2023-03-21 20:31:40	FAZ-VMTM23003736	logdev	system	Did not receive any log from device eFGT-HA_FGVULV[FGVULVTM2100009	logging-status	Device offline
5	2023-03-21 20:23:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=57/sec	perf-stats	Adom performance s
6	2023-03-21 20:18:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=56/sec	perf-stats	Adom performance s
7	2023-03-21 20:13:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=56/sec	perf-stats	Adom performance s
8	2023-03-21 20:08:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=58/sec	perf-stats	Adom performance s
9	2023-03-21 20:03:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=57/sec	perf-stats	Adom performance s
10	2023-03-21 19:58:56	FAZ-VMTM23003736	system	system	Adom Lab performance status: log rate low (0%), lograte=52/sec	perf-stats	Adom performance s
11	2023-03-21 19:58:47	FAZ-VMTM23003736	logdev	system	Did not receive any log from device eFGT-HA_FGVULV[FGVULVTM2100009	logging-status	Device offline

To set the interval for the ADOM performance statistics logs:

CLI configuration is added for the interval time to log performance state.

In the FortiAnalyzer CLI, enter the following command:

```
config system locallog setting
   set log-interval-adom-perf-stats <integer>
end
```

For the `log-interval-adom-perf-stats` setting, enter the interval in minutes. The range should be `5`-`2880`. Enter `0` to disable the logs.

Example logs:

Event log message for ADOM performance statistics (log rate):

```
id=7231962960615178247 bid=865533 dvid=1040 itime=1683822591 euid=1 epid=1 dsteuid=1
     dstepid=1 log_id="0001010093" subtype="system" type="event" level="notice"
     time="09:29:51" date="2023-05-11" user="system" action="Stats" msg="Adom root
     performance status: lograte=54/sec" userfrom="system" desc="Adom performance
     statistics notice" operation="Perf stats" performed_on="Local system" changes="Show
     adom performance stats." lograte=54 logratelimit=0 tz="-0700" devid="FAZ-VMTM22011553"
     devname="eFAZ-227"
```

Application log message for ADOM performance statistics (log rate):

```
id=7207521362594958664 bid=101707 dvid=1059 itime=1678131838 euid=1 epid=1 dsteuid=1
     dstepid=1 vd="fortinet" logid="220004" type="appevent" subtype="system"
     eventtype="perf-stats" action="Stats" level="notice" date="2023-03-06" time="11:43:58"
     user="system" user_from="system" desc="Adom performance statistics notice" msg="Adom
     fortinet performance status: log rate low (0%), lograte=49/sec" tz="-0800"
     adom="fortinet" operation="Perf stats" lograte=49 performed_on="Local system"
     changes="Show adom performance stats." logratelimit=0 devid="FAZ-VMTM23003360"
     devname="eFAZ-54"
```

Log message for ADOM archive usage:

```
id=7207519107737128256 bid=100933 dvid=1059 itime=1678131313 euid=1 epid=1 dsteuid=1
     dstepid=1 vd="fortinet" logid="220003" type="appevent" subtype="diskquota"
     eventtype="disk-usage" level="warning" date="2023-03-06" time="11:35:14" user="system"
     user_from="system" desc="Disk quota warning" msg="Disk usage for Adom fortinet is
     approaching the delete threshold 90% of total 50.0MB.  Archive Usage at 196.7%(29.5MB)
     and Analytics Usage at 41.6%(14.6MB)." tz="-0800" adom="fortinet" diskusage=88
     devid="FAZ-VMTM23003360" devname="eFAZ-54"
```

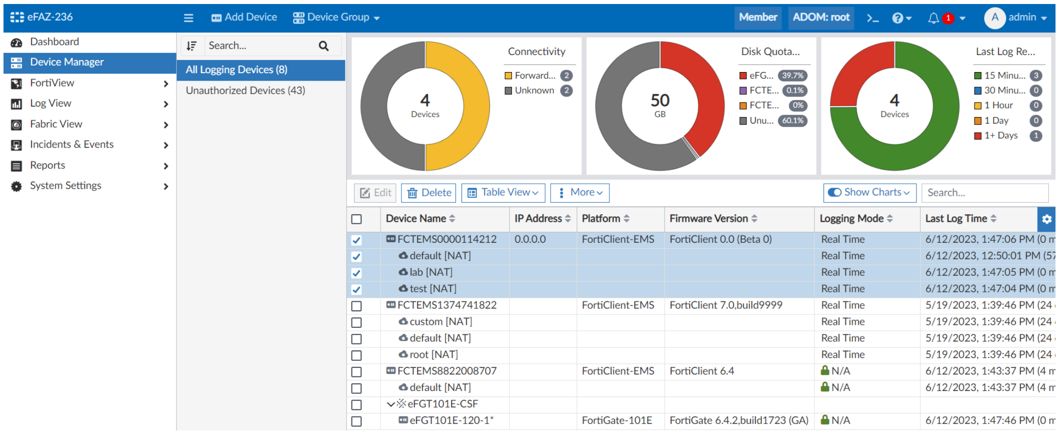
Support EMS multitenancy via FortiAnalyzer ADOMs - 7.4.1

With FortiClient EMS multitenancy, you can create multiple sites, providing granular access to different sites and separating endpoint data and configurations.

FortiAnalyzer has added support to EMS multitenancy by providing the following:

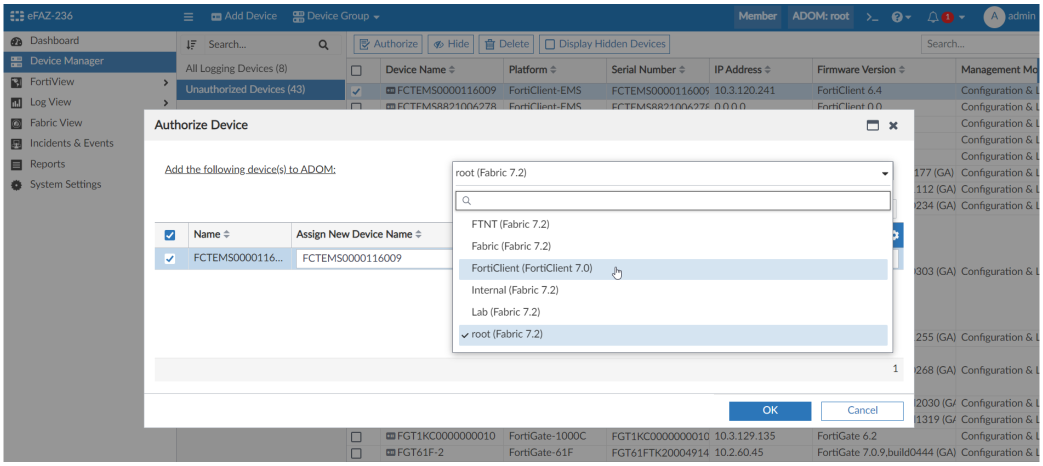
- Each log is mapped to its corresponding site using the `vd` log field
- EMS sites can be assigned to different FortiAnalyzer ADOMs

EMS logs (with multiple FCT logs) can be received by FortiAnalyzer directly with required fields added.



☐	Device Name	IP Address	Platform	Firmware Version	Logging Mode	Last Log Time
☑	FCTEMS0000114212	0.0.0.0	FortiClient-EMS	FortiClient 0.0 (Beta 0)	Real Time	6/12/2023, 1:47:06 PM (0 m
☑	default [NAT]				Real Time	6/12/2023, 12:50:01 PM (57
☑	lab [NAT]				Real Time	6/12/2023, 1:47:05 PM (0 m
☑	test [NAT]				Real Time	6/12/2023, 1:47:04 PM (0 m
☐	FCTEMS1374741822		FortiClient-EMS	FortiClient 7.0,build9999	Real Time	5/19/2023, 1:39:46 PM (24
☐	custom [NAT]				Real Time	5/19/2023, 1:39:46 PM (24
☐	default [NAT]				Real Time	5/19/2023, 1:39:46 PM (24
☐	root [NAT]				Real Time	5/19/2023, 1:39:46 PM (24
☐	FCTEMS8822008707		FortiClient-EMS	FortiClient 6.4	N/A	6/12/2023, 1:43:37 PM (4 m
☐	default [NAT]				N/A	6/12/2023, 1:43:37 PM (4 m
☐	eFGT101E-CSF					
☐	eFGT101E-120-1*		FortiGate-101E	FortiGate 6.4.2,build1723 (GA)	N/A	6/12/2023, 1:47:46 PM (0 m

FortiClient can be promoted into Fabric ADOM or FortiClient ADOM in FortiAnalyzer.



Authorize Device

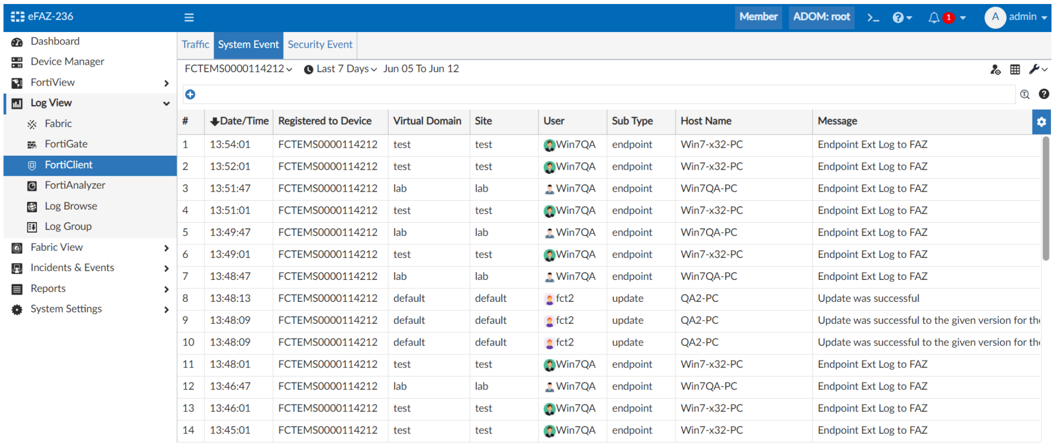
Add the following device(s) to ADOM: root (Fabric 7.2)

☑	Name	Assign New Device Name
☑	FCTEMS0000116...	FCTEMS0000116009

1

☐	Device Name	Platform	Serial Number	IP Address	Firmware Version	Management Mo
☑	FCTEMS0000116009	FortiClient-EMS	FCTEMS000011600	10.3.120.241	FortiClient 6.4	Configuration & L
☐	FCTEMS8821006278	FortiClient-EMS	FCTEMS882100627	0.0.0.0	FortiClient 0.0	Configuration & L
☐	FGT1KC0000000010	FortiGate-1000C	FGT1KC0000000010	10.3.129.135	FortiGate 6.2	Configuration & L
☐	FGT61F-2	FortiGate-61F	FGT61FTK20004914	10.2.60.45	FortiGate 7.0.9,build0444 (GA)	Configuration & L

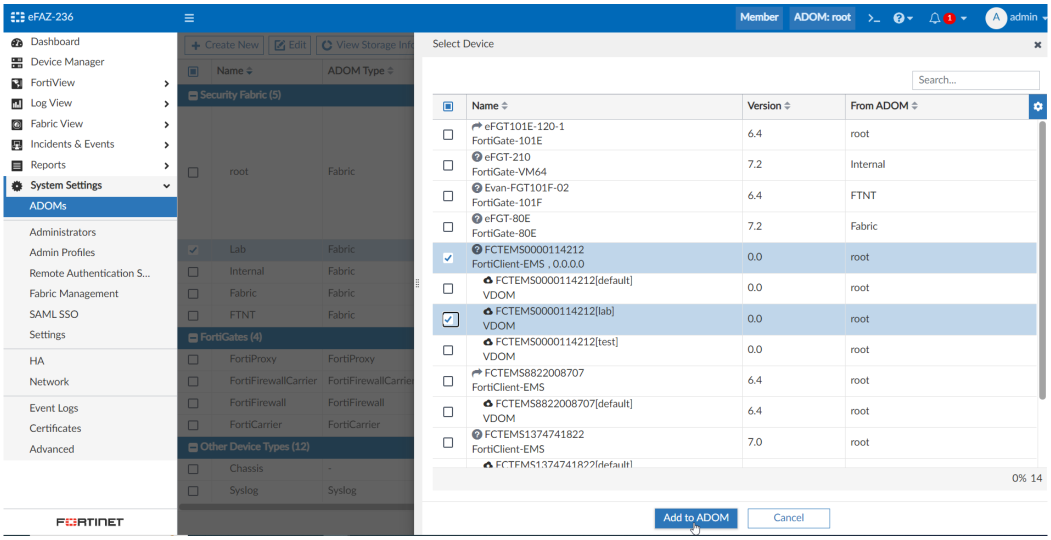
The FortiClient logs from multitenancy logs can be converted to `vd=sitename` when receiving logs.



FCTEMS0000114212 Last 7 Days Jun 05 To Jun 12

#	Date/Time	Registered to Device	Virtual Domain	Site	User	Sub Type	Host Name	Message
1	13:54:01	FCTEMS0000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
2	13:52:01	FCTEMS0000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
3	13:51:47	FCTEMS0000114212	lab	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
4	13:51:01	FCTEMS0000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
5	13:49:47	FCTEMS0000114212	lab	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
6	13:49:01	FCTEMS0000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
7	13:48:47	FCTEMS0000114212	lab	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
8	13:48:13	FCTEMS0000114212	default	default	fct2	update	QA2-PC	Update was successful
9	13:48:09	FCTEMS0000114212	default	default	fct2	update	QA2-PC	Update was successful to the given version for th
10	13:48:09	FCTEMS0000114212	default	default	fct2	update	QA2-PC	Update was successful to the given version for th
11	13:48:01	FCTEMS0000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
12	13:46:47	FCTEMS0000114212	lab	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
13	13:46:01	FCTEMS0000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
14	13:45:01	FCTEMS0000114212	test	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ

The multitenancy logs can be assigned to different ADOMs based on its VDOM when the *ADOM Mode* is set to *Advanced*.



Select Device

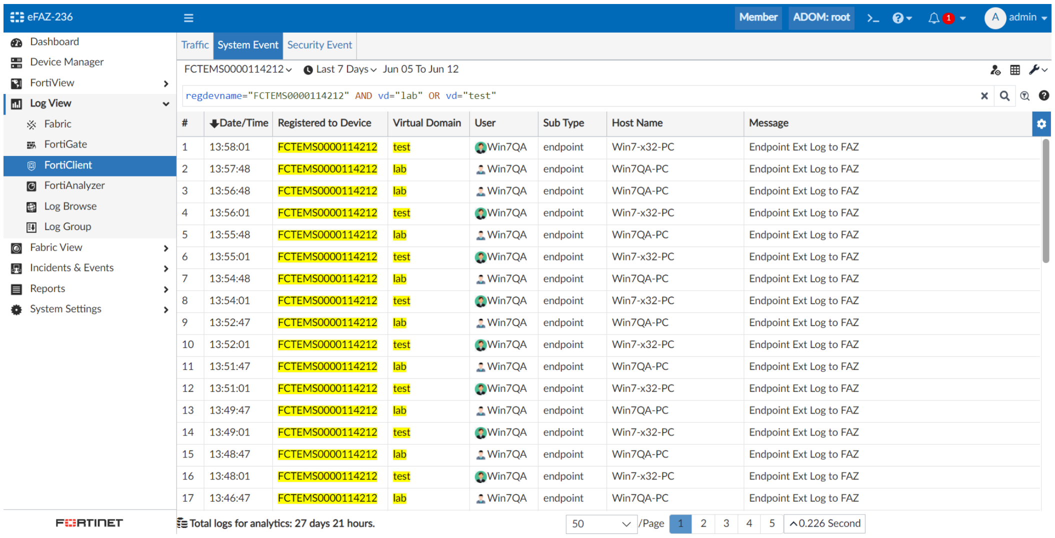
■	Name	Version	From ADOM
□	eFGT101E-120-1 FortiGate-101E	6.4	root
□	eFGT-210 FortiGate-VM64	7.2	Internal
□	Evan-FGT101F-02 FortiGate-101F	6.4	FTNT
□	eFGT-80E FortiGate-80E	7.2	Fabric
☑	FCTEMS0000114212 FortiClient-EMS , 0.0.0.0	0.0	root
□	FCTEMS0000114212[default] VDOM	0.0	root
☑	FCTEMS0000114212[lab] VDOM	0.0	root
□	FCTEMS0000114212[test] VDOM	0.0	root
□	FCTEMS8822008707 FortiClient-EMS	6.4	root
□	FCTEMS8822008707[default] VDOM	6.4	root
□	FCTEMS1374741822 FortiClient-EMS	7.0	root
	FCTEMS1374741822[default]		

0% 14

Two new fields are added to FortiClient logs:

- `vd`
- `regdevname`

The FortiClient logs can be filtered by these fields in *Log View*. For example, see below.



```
regdevname="FCTEMS0000114212" AND vd="lab" OR vd="test"
```

#	Date/Time	Registered to Device	Virtual Domain	User	Sub Type	Host Name	Message
1	13:58:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
2	13:57:48	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
3	13:56:48	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
4	13:56:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
5	13:55:48	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
6	13:55:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
7	13:54:48	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
8	13:54:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
9	13:52:47	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
10	13:52:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
11	13:51:47	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
12	13:51:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
13	13:49:47	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
14	13:49:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
15	13:48:47	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ
16	13:48:01	FCTEMS0000114212	test	Win7QA	endpoint	Win7-x32-PC	Endpoint Ext Log to FAZ
17	13:46:47	FCTEMS0000114212	lab	Win7QA	endpoint	Win7QA-PC	Endpoint Ext Log to FAZ

Total logs for analytics: 27 days 21 hours.

50 /Page 1 2 3 4 5 0.226 Second

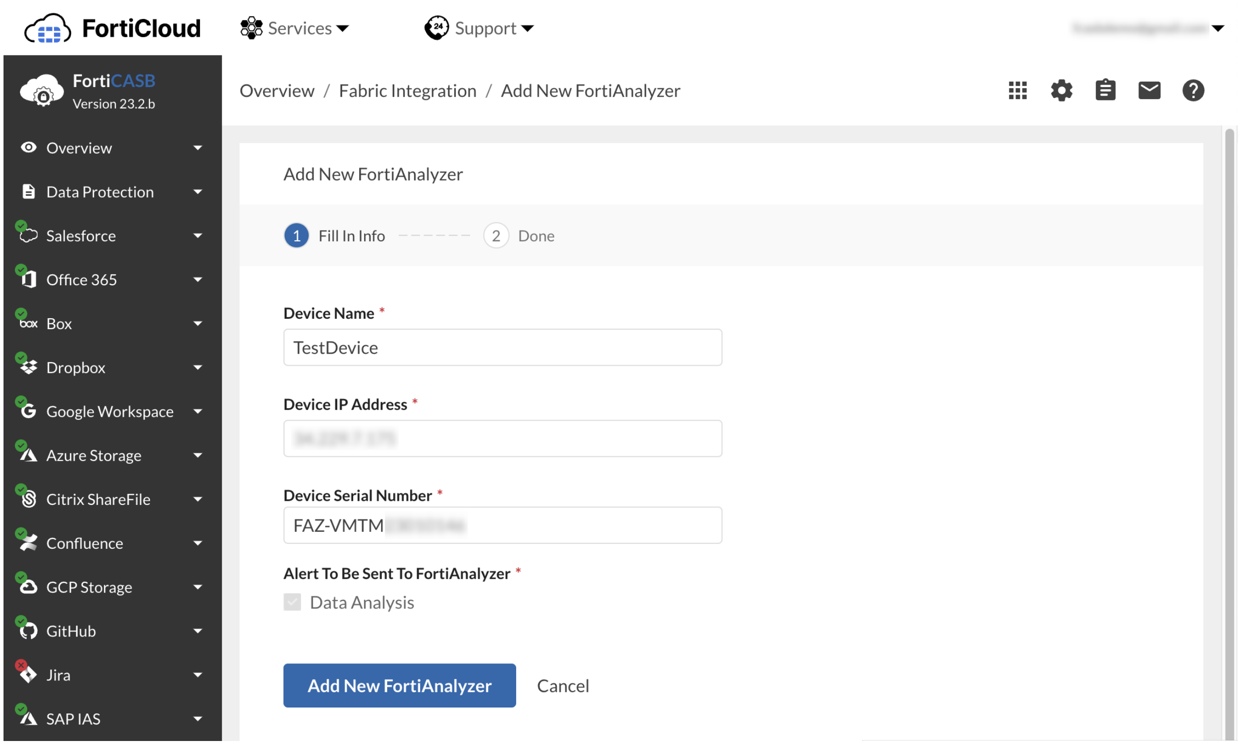
Logging support for FortiCASB - 7.4.1

FortiAnalyzer v7.4.1 recognizes FortiCASB devices as device type.

FortiAnalyzer can now receive, store, and display logs from authorized FortiCASB devices in *Log View*.

To configure FortiCASB logging to FortiAnalyzer:

1. In the FortiCASB GUI, go to *Overview* > *Fabric Integration* > *Add New FortiAnalyzer*.
2. Configure the following settings for the FortiAnalyzer device and click *Add New FortiAnalyzer*:
   - *Device Name*
   - *Device IP Address*
   - *Device Serial Number*



Add New FortiAnalyzer

Device Name *
TestDevice

Device IP Address *
[redacted]

Device Serial Number *
FAZ-VMTM[redacted]

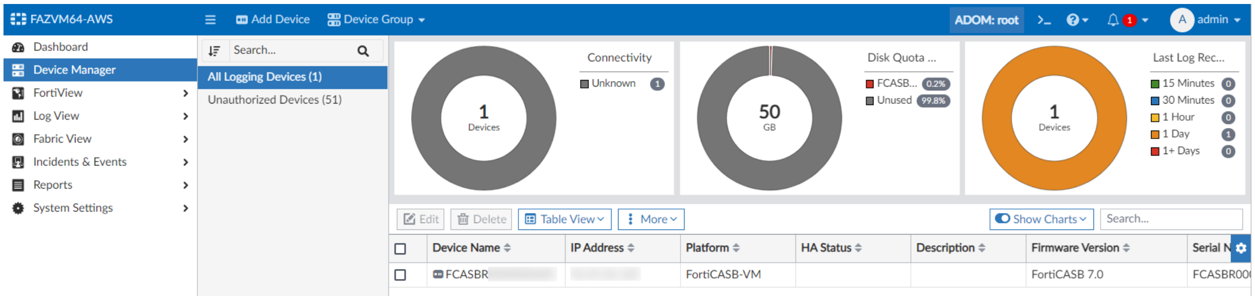
Alert To Be Sent To FortiAnalyzer *
☑ Data Analysis

3. In the FortiAnalyzer GUI, go to *Device Manager* in the root ADOM.

   The FortiCASB displays in the *Unauthorized Devices* list.

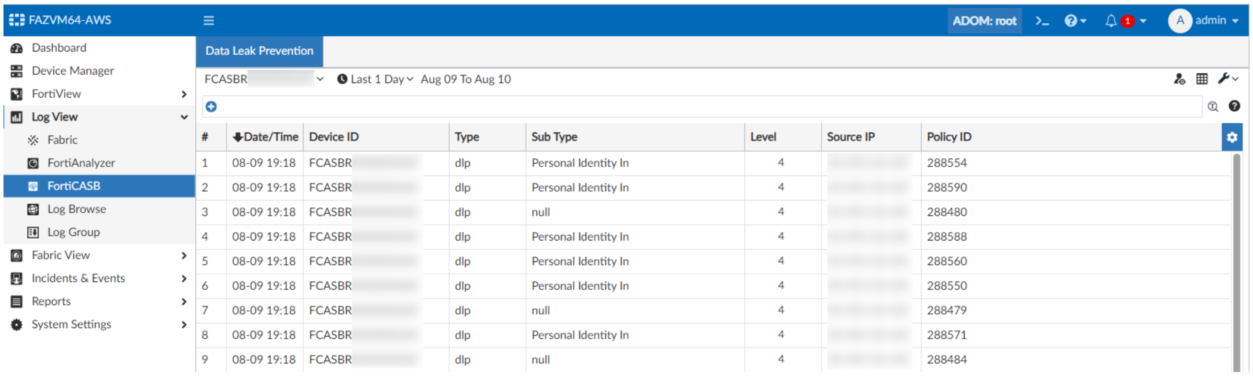
4. Select the FortiCASB device and click *Authorize*.

   The FortiCASB device now displays in *All Logging Devices* list.



	Device Name	IP Address	Platform	HA Status	Description	Firmware Version	Serial N
□	FCASBR[redacted]	[redacted]	FortiCASB-VM			FortiCASB 7.0	FCASBR00

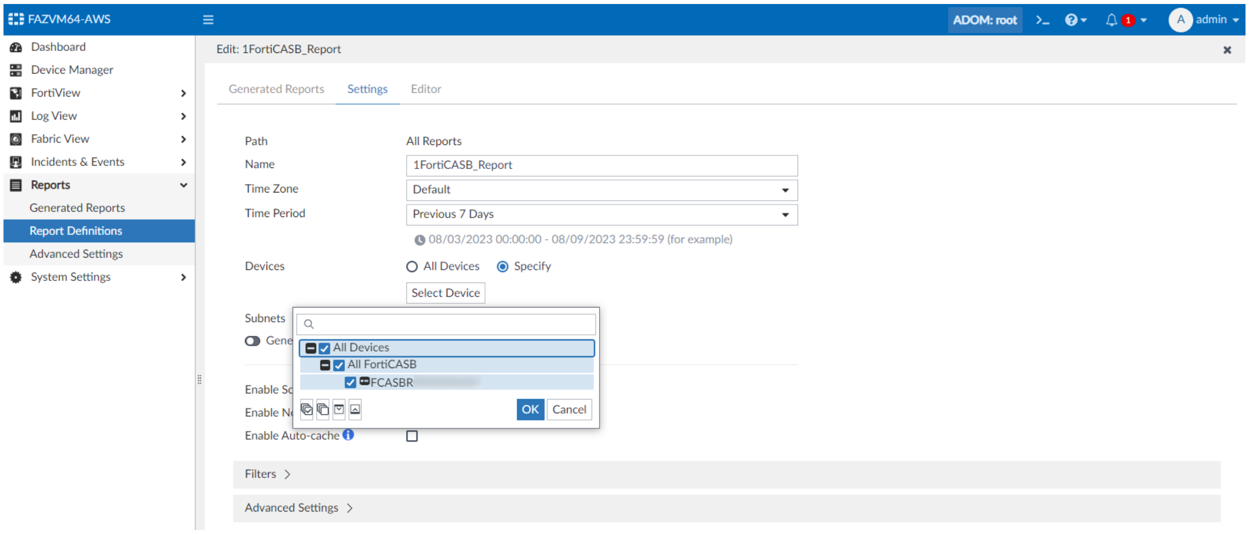
The FortiCASB logs display in *Log View > FortiCASB*.



FCASBR[redacted]

#	Date/Time	Device ID	Type	Sub Type	Level	Source IP	Policy ID
1	08-09 19:18	FCASBR[redacted]	dlp	Personal Identity In	4	[redacted]	288554
2	08-09 19:18	FCASBR[redacted]	dlp	Personal Identity In	4	[redacted]	288590
3	08-09 19:18	FCASBR[redacted]	dlp	null	4	[redacted]	288480
4	08-09 19:18	FCASBR[redacted]	dlp	Personal Identity In	4	[redacted]	288588
5	08-09 19:18	FCASBR[redacted]	dlp	Personal Identity In	4	[redacted]	288560
6	08-09 19:18	FCASBR[redacted]	dlp	Personal Identity In	4	[redacted]	288550
7	08-09 19:18	FCASBR[redacted]	dlp	null	4	[redacted]	288479
8	08-09 19:18	FCASBR[redacted]	dlp	Personal Identity In	4	[redacted]	288571
9	08-09 19:18	FCASBR[redacted]	dlp	null	4	[redacted]	288484

The FortiCASB device can now be used in *Reports*.



Edit: 1FortiCASB_Report

Path	All Reports
Name	1FortiCASB_Report
Time Zone	Default
Time Period	Previous 7 Days
	08/03/2023 00:00:00 - 08/09/2023 23:59:59 (for example)
Devices	○ All Devices ● Specify
	Select Device
Subnets	
Enable Auto-cache	□

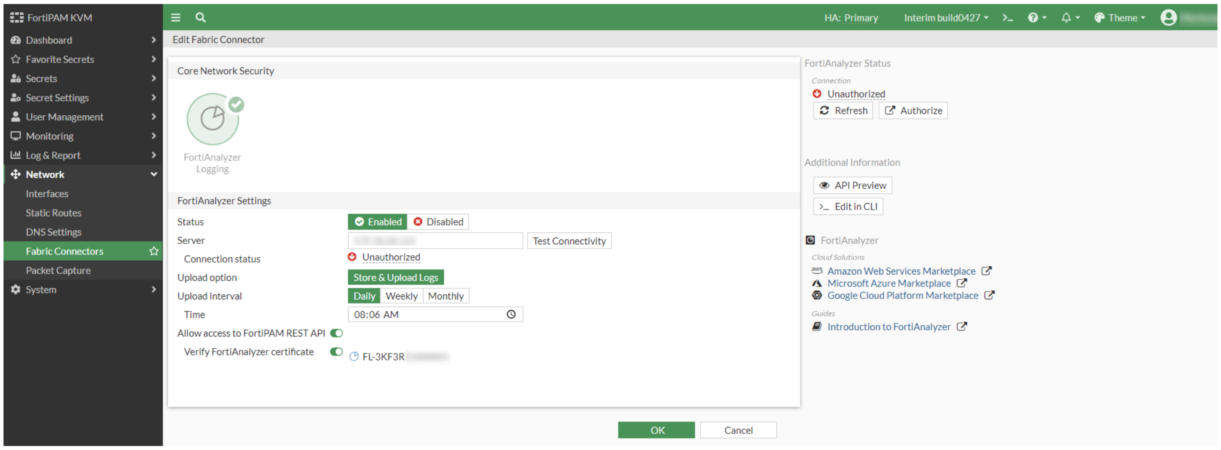
☑ All Devices
☑ All FortiCASB
☑ FCASBR[redacted]

Logging support for FortiPAM - 7.4.1

FortiAnalyzer v7.4.1 recognizes FortiPAM devices as device type.

To configure FortiPAM logging to FortiAnalyzer:

1. In the FortiPAM GUI, go to *Network > Fabric Connectors*, and edit *FortiAnalyzer Logging*. In the *Server* field, enter the FortiAnalyzer IP address.



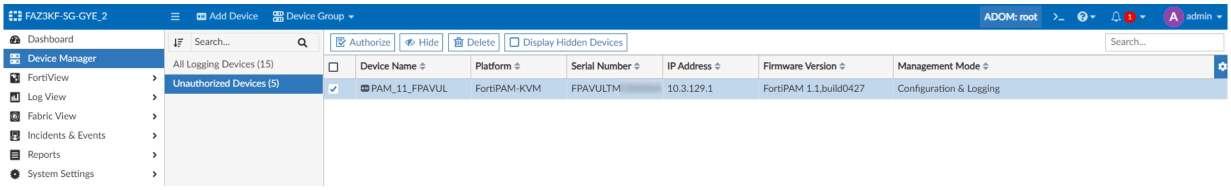
Edit Fabric Connector

FortiAnalyzer Status
Connection: Unauthorized

FortiAnalyzer Settings

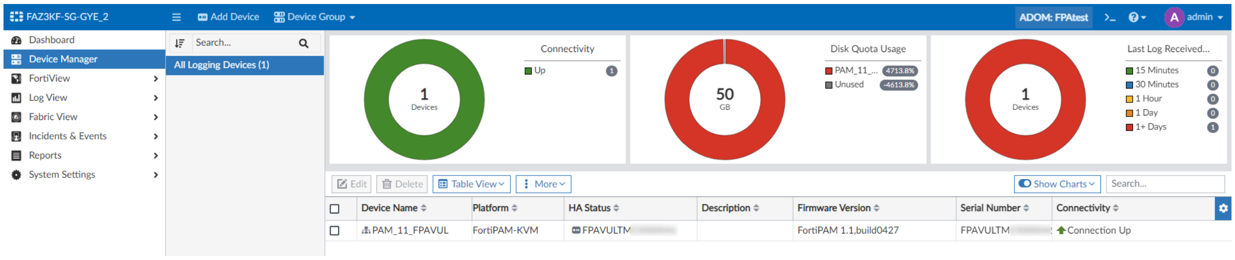
Status	Enabled / Disabled (Enabled selected)
Server	[redacted] Test Connectivity
Connection status	Unauthorized
Upload option	Store & Upload Logs
Upload interval	Daily / Weekly / Monthly (Daily selected)
Time	08:06 AM
Allow access to FortiPAM REST API	on
Verify FortiAnalyzer certificate	on FL-3KF3R[redacted]

2. In the FortiAnalyzer GUI root ADOM, go to *Device Manager > Unauthorized Devices*. Select the FortiPAM device and click *Authorize*.



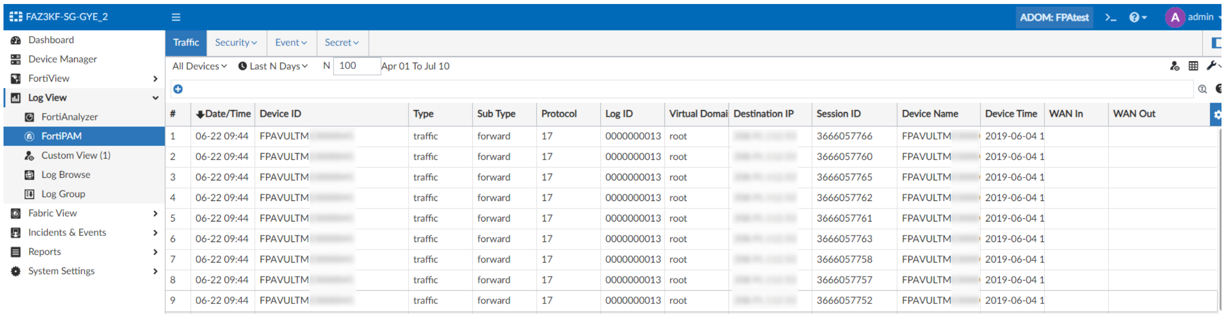
	Device Name	Platform	Serial Number	IP Address	Firmware Version	Management Mode
☑	PAM_11_FPAVUL	FortiPAM-KVM	FPAVULTM[redacted]	10.3.129.1	FortiPAM 1.1,build0427	Configuration & Logging

The FortiPAM device is now authorized in *Device Manager*.



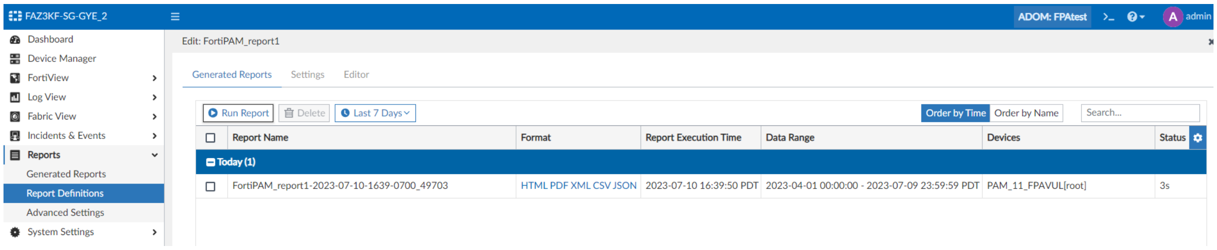
Device Name	Platform	HA Status	Description	Firmware Version	Serial Number	Connectivity
PAM_11_FPAVUL	FortiPAM-KVM	FPAVULTM[redacted]		FortiPAM 1.1,build0427	FPAVULTM[redacted]	Connection Up

3. To view logs from the FortiPAM device, go to *Log View* > *FortiPAM*.



#	Date/Time	Device ID	Type	Sub Type	Protocol	Log ID	Virtual Domai	Destination IP	Session ID	Device Name	Device Time	WAN In	WAN Out
1	06-22 09:44	FPAVULTM[redacted]	traffic	forward	17	0000000013	root	[redacted]	3666057766	FPAVULTM[redacted]	2019-06-04 1		
2	06-22 09:44	FPAVULTM[redacted]	traffic	forward	17	0000000013	root	[redacted]	3666057760	FPAVULTM[redacted]	2019-06-04 1		
3	06-22 09:44	FPAVULTM[redacted]	traffic	forward	17	0000000013	root	[redacted]	3666057765	FPAVULTM[redacted]	2019-06-04 1		
4	06-22 09:44	FPAVULTM[redacted]	traffic	forward	17	0000000013	root	[redacted]	3666057762	FPAVULTM[redacted]	2019-06-04 1		
5	06-22 09:44	FPAVULTM[redacted]	traffic	forward	17	0000000013	root	[redacted]	3666057761	FPAVULTM[redacted]	2019-06-04 1		
6	06-22 09:44	FPAVULTM[redacted]	traffic	forward	17	0000000013	root	[redacted]	3666057763	FPAVULTM[redacted]	2019-06-04 1		
7	06-22 09:44	FPAVULTM[redacted]	traffic	forward	17	0000000013	root	[redacted]	3666057758	FPAVULTM[redacted]	2019-06-04 1		
8	06-22 09:44	FPAVULTM[redacted]	traffic	forward	17	0000000013	root	[redacted]	3666057757	FPAVULTM[redacted]	2019-06-04 1		
9	06-22 09:44	FPAVULTM[redacted]	traffic	forward	17	0000000013	root	[redacted]	3666057752	FPAVULTM[redacted]	2019-06-04 1		

You can create a FortiPAM report in FortiAnalyzer.



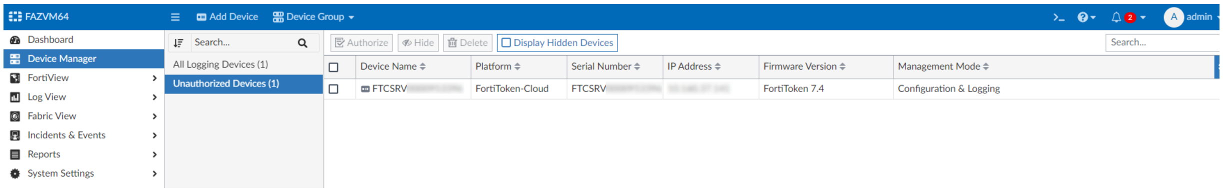
Report Name	Format	Report Execution Time	Data Range	Devices	Status
FortiPAM_report1-2023-07-10-1639-0700_49703	HTML PDF XML CSV JSON	2023-07-10 16:39:50 PDT	2023-04-01 00:00:00 - 2023-07-09 23:59:59 PDT	PAM_11_FPAVUL[root]	3s

Logging support for FortiToken Cloud - 7.4.1

FortiAnalyzer can now receive, store, and display logs from authorized FortiToken Cloud devices in *Log View*.

To configure FortiToken Cloud logging on FortiAnalyzer:

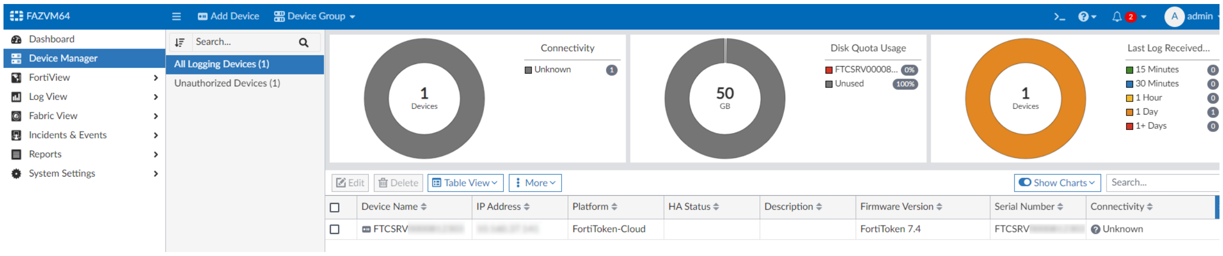
1. Configure the FortiToken Cloud device to send logs to FortiAnalyzer.
2. In the FortiAnalyzer GUI, go to *Device Manager* in the root ADOM.
   The FortiToken Cloud displays in the *Unauthorized Devices* list.



Device Name	Platform	Serial Number	IP Address	Firmware Version	Management Mode
FTCSRV[redacted]	FortiToken-Cloud	FTCSRV[redacted]	[redacted]	FortiToken 7.4	Configuration & Logging

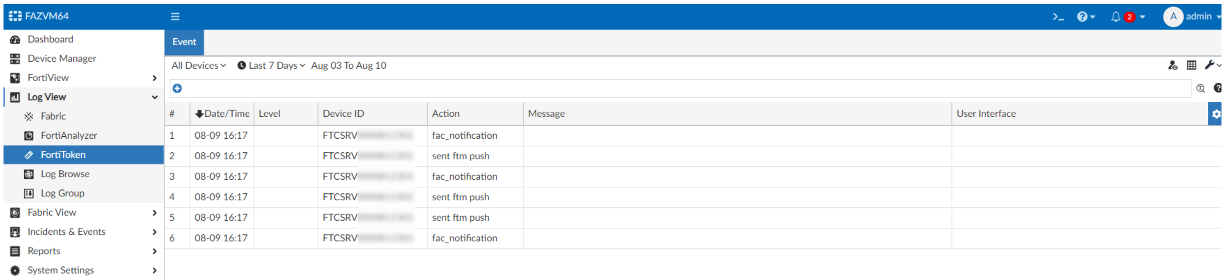
3. Select the FortiToken Cloud device and click *Authorize*.

The FortiToken Cloud device now displays in *All Logging Devices* list.



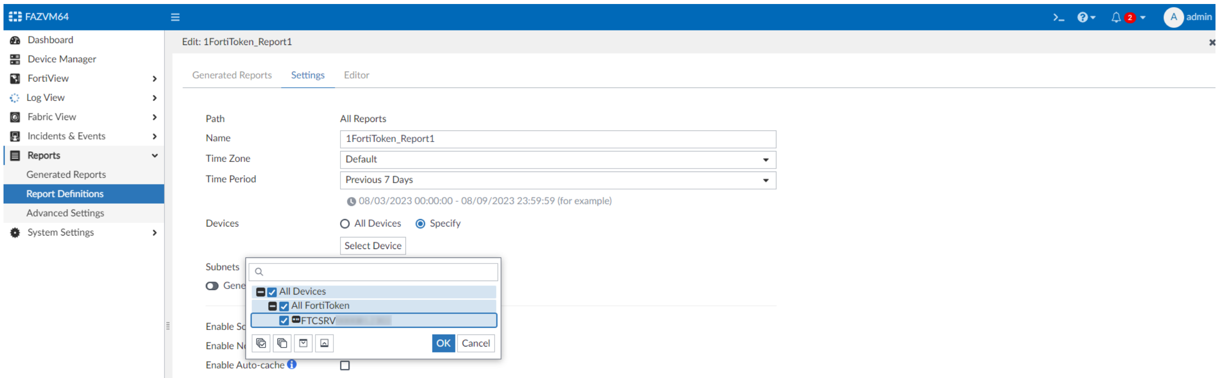
☐	Device Name	IP Address	Platform	HA Status	Description	Firmware Version	Serial Number	Connectivity
☐	FTCSRV[redacted]	[redacted]	FortiToken-Cloud			FortiToken 7.4	FTCSRV[redacted]	Unknown

The FortiToken Cloud logs display in *Log View > FortiToken*.



#	Date/Time	Level	Device ID	Action	Message	User Interface
1	08-09 16:17		FTCSRV[redacted]	fac_notification		
2	08-09 16:17		FTCSRV[redacted]	sent ftm push		
3	08-09 16:17		FTCSRV[redacted]	fac_notification		
4	08-09 16:17		FTCSRV[redacted]	sent ftm push		
5	08-09 16:17		FTCSRV[redacted]	sent ftm push		
6	08-09 16:17		FTCSRV[redacted]	fac_notification		

The FortiToken Cloud device can now be used in *Reports*.



Edit: 1FortiToken_Report1

Path	All Reports
Name	1FortiToken_Report1
Time Zone	Default
Time Period	Previous 7 Days
	08/03/2023 00:00:00 - 08/09/2023 23:59:59 (for example)
Devices	○ All Devices ● Specify
Subnets	
Gene	
Enable Sc	
Enable N	
Enable Auto-cache	☐

☑ All Devices
☑ All FortiToken
☑ FTCSRV[redacted]

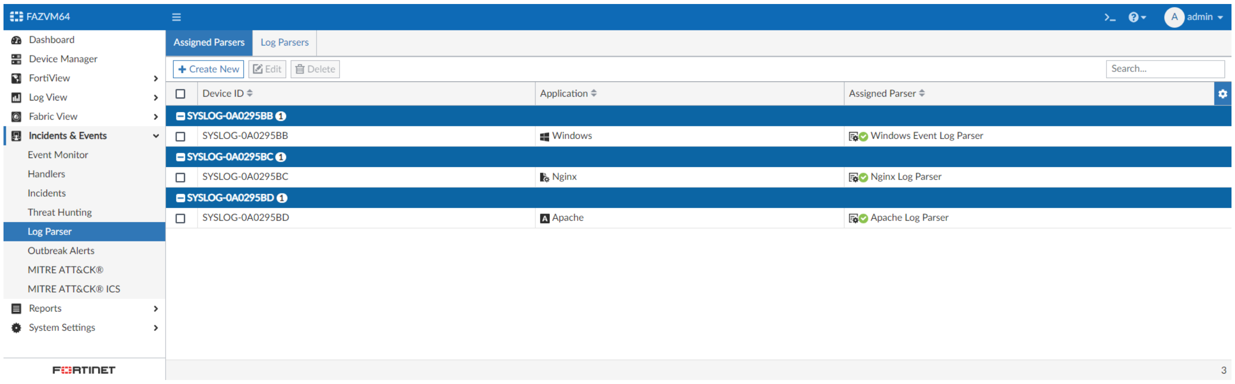
Support parsing and addition of third-party application logs to the SIEM DB in JSON format - 7.4.1

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- SIEM log parsers

If third-party logs are in JSON format, the default Windows, Apache, and Nginx log parsers can parse generic field data from them. These default log parsers can also be updated in the GUI, if needed.

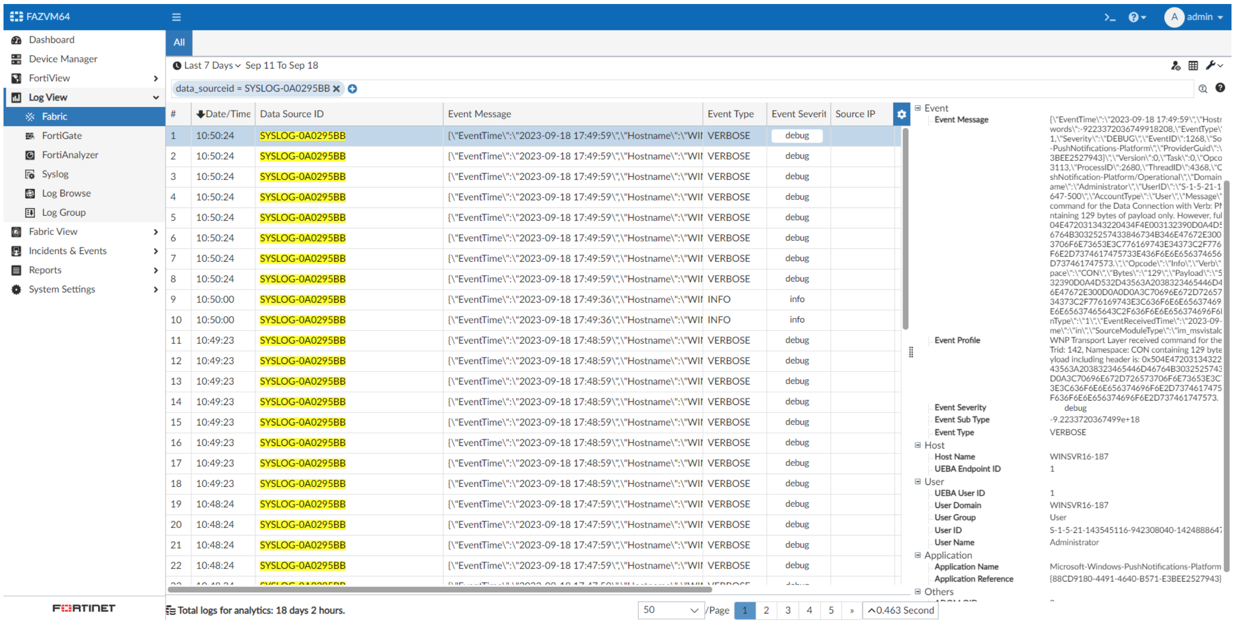
In *Incidents & Events > Log Parser > Assigned Parsers*, the third-party devices are automatically assigned to the appropriate log parser according to their logs in JSON format.



	Device ID	Application	Assigned Parser
	SYSLOG-0A0295BB 1		
□	SYSLOG-0A0295BB	Windows	Windows Event Log Parser
	SYSLOG-0A0295BC 1		
□	SYSLOG-0A0295BC	Nginx	Nginx Log Parser
	SYSLOG-0A0295BD 1		
□	SYSLOG-0A0295BD	Apache	Apache Log Parser

3

The *Windows Event Log Parser* can parse Windows logs in JSON format. For example, Event_Profile, Event_Serverity, and Host_Name. The complete content of JSON is inserted into Event_Msg field for future reference, if needed.



Last 7 Days Sep 11 To Sep 18

data_sourceid = SYSLOG-0A0295BB

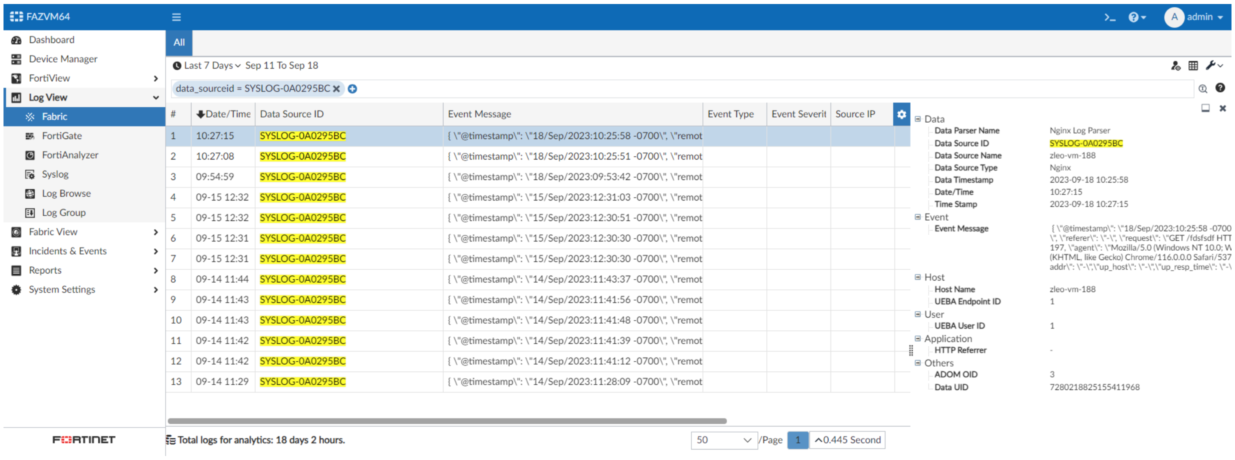
#	Date/Time	Data Source ID	Event Message	Event Type	Event Severit	Source IP
1	10:50:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:49:59\",\"Hostname\":\"WII	VERBOSE	debug	
2	10:50:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:49:59\",\"Hostname\":\"WII	VERBOSE	debug	
3	10:50:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:49:59\",\"Hostname\":\"WII	VERBOSE	debug	
4	10:50:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:49:59\",\"Hostname\":\"WII	VERBOSE	debug	
5	10:50:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:49:59\",\"Hostname\":\"WII	VERBOSE	debug	
6	10:50:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:49:59\",\"Hostname\":\"WII	VERBOSE	debug	
7	10:50:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:49:59\",\"Hostname\":\"WII	VERBOSE	debug	
8	10:50:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:49:59\",\"Hostname\":\"WII	VERBOSE	debug	
9	10:50:00	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:49:36\",\"Hostname\":\"WII	INFO	info	
10	10:50:00	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:49:36\",\"Hostname\":\"WII	INFO	info	
11	10:49:23	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:48:59\",\"Hostname\":\"WII	VERBOSE	debug	
12	10:49:23	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:48:59\",\"Hostname\":\"WII	VERBOSE	debug	
13	10:49:23	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:48:59\",\"Hostname\":\"WII	VERBOSE	debug	
14	10:49:23	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:48:59\",\"Hostname\":\"WII	VERBOSE	debug	
15	10:49:23	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:48:59\",\"Hostname\":\"WII	VERBOSE	debug	
16	10:49:23	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:48:59\",\"Hostname\":\"WII	VERBOSE	debug	
17	10:49:23	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:48:59\",\"Hostname\":\"WII	VERBOSE	debug	
18	10:49:23	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:48:59\",\"Hostname\":\"WII	VERBOSE	debug	
19	10:48:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:47:59\",\"Hostname\":\"WII	VERBOSE	debug	
20	10:48:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:47:59\",\"Hostname\":\"WII	VERBOSE	debug	
21	10:48:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:47:59\",\"Hostname\":\"WII	VERBOSE	debug	
22	10:48:24	SYSLOG-0A0295BB	{\"EventTime\":\"2023-09-18 17:47:59\",\"Hostname\":\"WII	VERBOSE	debug	

Event	
Event Message	{\"EventTime\":\"2023-09-18 17:49:59\",\"Hostr words\":-9223372036749918208,\"EventType\' 1,\"Severity\":\"DEBUG\",\"EventID\":1268,\"So -PushNotifications-Platform\",\"ProviderGuid\":\ 3BEE2527943}\",\"Version\":0,\"Task\":0,\"Opco 3113,\"ProcessID\":2680,\"ThreadID\":4368,\"C shNotification-Platform/Operational\",\"Domain ame\":\"Administrator\",\"UserID\":\"S-1-5-21-1 647-500\",\"AccountType\":\"User\",\"Message\" command for the Data Connection with Verb: PI ntaining 129 bytes of payload only. However, ful 04E472031343220434F4E003132390D0A4D5 6764B30325257433846734B346E47672E300 3706F6E73653E3C776169743E34373C2F776 F6E2D7374617475733E436F6E6E656374656 D737461747573.\",\"Opcode\":\"Info\",\"Verb\": pace\":\"CON\",\"Bytes\":\"129\",\"Payload\":\"5 32390D0A4D532D43563A2038323465446D4 6E47672E300D0A0D0A3C70696E672D72657 34373C2F776169743E3C636F6E6E65637469 E6E65637465643C2F636F6E6E656374696F6I nType\":\"1\",\"EventReceivedTime\":\"2023-09- me\":\"in\",\"SourceModuleType\":\"im_msvistalc
Event Profile	WNP Transport Layer received command for the Trid: 142, Namespace: CON containing 129 byte yload including header is: 0x504E47203134322 43563A2038323465446D46764B3032525743 D0A3C70696E672D726573706F6E73653E3C 3E3C636F6E6E656374696F6E2D7374617475 F636F6E6E656374696F6E2D737461747573.
Event Severity	debug
Event Sub Type	-9.2233720367499e+18
Event Type	VERBOSE
Host	
Host Name	WINSVR16-187
UEBA Endpoint ID	1
User	
UEBA User ID	1
User Domain	WINSVR16-187
User Group	User
User ID	S-1-5-21-143545116-942308040-1424888647
User Name	Administrator
Application	
Application Name	Microsoft-Windows-PushNotifications-Platform
Application Reference	{88CD9180-4491-4640-B571-E3BEE2527943}
Others	

Total logs for analytics: 18 days 2 hours.

50 /Page 1 2 3 4 5 » 0.463 Second

The *Nginx Log Parser* can parse Nginx server logs in JSON format. For example, Data_TimeStamp, Host_Name, and HTTP_Referrer. The complete content of JSON is inserted into Event_Msg field for future reference, if needed.



Last 7 Days Sep 11 To Sep 18

data_sourceid = SYSLOG-0A0295BC

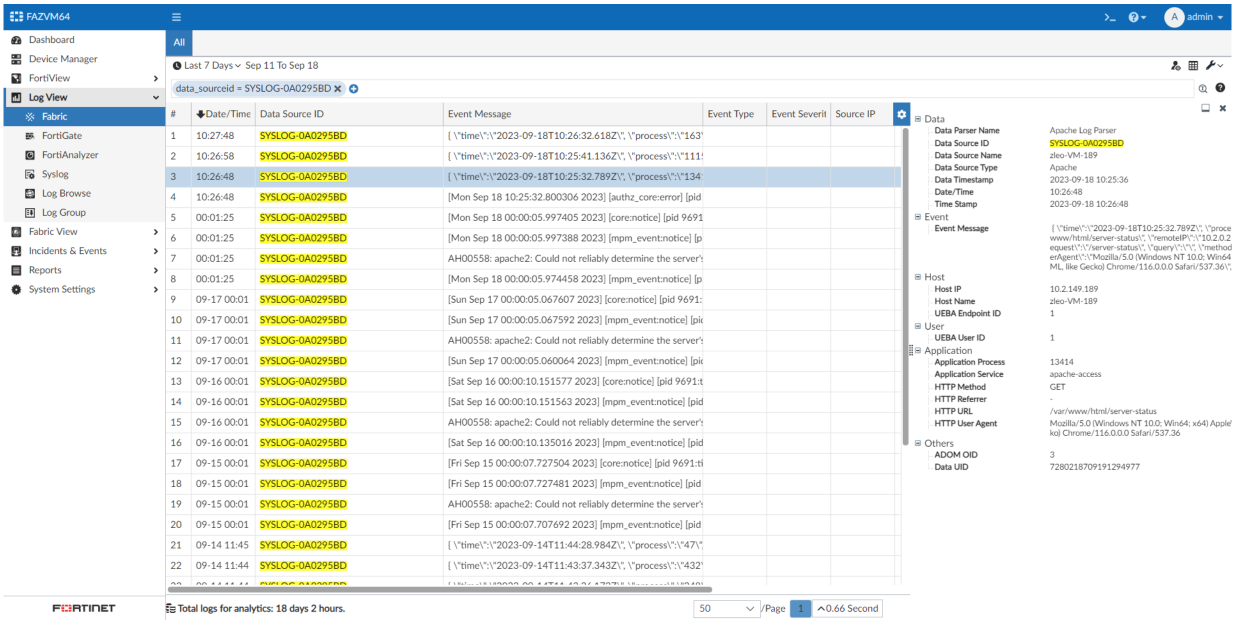
#	Date/Time	Data Source ID	Event Message	Event Type	Event Severit	Source IP
1	10:27:15	SYSLOG-0A0295BC	{ \"@timestamp\": \"18/Sep/2023:10:25:58 -0700\", \"remot			
2	10:27:08	SYSLOG-0A0295BC	{ \"@timestamp\": \"18/Sep/2023:10:25:51 -0700\", \"remot			
3	09:54:59	SYSLOG-0A0295BC	{ \"@timestamp\": \"18/Sep/2023:09:53:42 -0700\", \"remot			
4	09-15 12:32	SYSLOG-0A0295BC	{ \"@timestamp\": \"15/Sep/2023:12:31:03 -0700\", \"remot			
5	09-15 12:32	SYSLOG-0A0295BC	{ \"@timestamp\": \"15/Sep/2023:12:30:51 -0700\", \"remot			
6	09-15 12:31	SYSLOG-0A0295BC	{ \"@timestamp\": \"15/Sep/2023:12:30:30 -0700\", \"remot			
7	09-15 12:31	SYSLOG-0A0295BC	{ \"@timestamp\": \"15/Sep/2023:12:30:30 -0700\", \"remot			
8	09-14 11:44	SYSLOG-0A0295BC	{ \"@timestamp\": \"14/Sep/2023:11:43:37 -0700\", \"remot			
9	09-14 11:43	SYSLOG-0A0295BC	{ \"@timestamp\": \"14/Sep/2023:11:41:56 -0700\", \"remot			
10	09-14 11:43	SYSLOG-0A0295BC	{ \"@timestamp\": \"14/Sep/2023:11:41:48 -0700\", \"remot			
11	09-14 11:42	SYSLOG-0A0295BC	{ \"@timestamp\": \"14/Sep/2023:11:41:39 -0700\", \"remot			
12	09-14 11:42	SYSLOG-0A0295BC	{ \"@timestamp\": \"14/Sep/2023:11:41:12 -0700\", \"remot			
13	09-14 11:29	SYSLOG-0A0295BC	{ \"@timestamp\": \"14/Sep/2023:11:28:09 -0700\", \"remot			

Data	
Data Parser Name	Nginx Log Parser
Data Source ID	SYSLOG-0A0295BC
Data Source Name	zleo-vm-188
Data Source Type	Nginx
Data Timestamp	2023-09-18 10:25:58
Date/Time	10:27:15
Time Stamp	2023-09-18 10:27:15
Event	
Event Message	{ \"@timestamp\": \"18/Sep/2023:10:25:58 -0700 \", \"referer\": \"-\", \"request\": \"GET /fdsfsdf HTT 197, \"agent\": \"Mozilla/5.0 (Windows NT 10.0; W (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537 addr\": \"-\",\"up_host\": \"-\",\"up_resp_time\": \"-\
Host	
Host Name	zleo-vm-188
UEBA Endpoint ID	1
User	
UEBA User ID	1
Application	
HTTP Referrer	-
Others	
ADOM OID	3
Data UID	7280218825155411968

Total logs for analytics: 18 days 2 hours.

50 /Page 1 0.445 Second

The *Apache Log Parser* can parse Apache server logs in JSON format. For example, Host_IP, Host_Name, and Application_Service. The complete content of JSON is inserted into Event_Msg field for future reference, if needed.



Last 7 Days Sep 11 To Sep 18

data_sourceid = SYSLOG-0A0295BD

#	Date/Time	Data Source ID	Event Message	Event Type	Event Severit	Source IP
1	10:27:48	SYSLOG-0A0295BD	{ \"time\":\"2023-09-18T10:26:32.618Z\", \"process\":\"163'			
2	10:26:58	SYSLOG-0A0295BD	{ \"time\":\"2023-09-18T10:25:41.136Z\", \"process\":\"111!			
3	10:26:48	SYSLOG-0A0295BD	{ \"time\":\"2023-09-18T10:25:32.789Z\", \"process\":\"134:			
4	10:26:48	SYSLOG-0A0295BD	[Mon Sep 18 10:25:32.800306 2023] [authz_core:error] [pid			
5	00:01:25	SYSLOG-0A0295BD	[Mon Sep 18 00:00:05.997405 2023] [core:notice] [pid 9691			
6	00:01:25	SYSLOG-0A0295BD	[Mon Sep 18 00:00:05.997388 2023] [mpm_event:notice] [p			
7	00:01:25	SYSLOG-0A0295BD	AH00558: apache2: Could not reliably determine the server's			
8	00:01:25	SYSLOG-0A0295BD	[Mon Sep 18 00:00:05.974458 2023] [mpm_event:notice] [p			
9	09-17 00:01	SYSLOG-0A0295BD	[Sun Sep 17 00:00:05.067607 2023] [core:notice] [pid 9691:			
10	09-17 00:01	SYSLOG-0A0295BD	[Sun Sep 17 00:00:05.067592 2023] [mpm_event:notice] [pic			
11	09-17 00:01	SYSLOG-0A0295BD	AH00558: apache2: Could not reliably determine the server's			
12	09-17 00:01	SYSLOG-0A0295BD	[Sun Sep 17 00:00:05.060064 2023] [mpm_event:notice] [pic			
13	09-16 00:01	SYSLOG-0A0295BD	[Sat Sep 16 00:00:10.151577 2023] [core:notice] [pid 9691:t			
14	09-16 00:01	SYSLOG-0A0295BD	[Sat Sep 16 00:00:10.151563 2023] [mpm_event:notice] [pid			
15	09-16 00:01	SYSLOG-0A0295BD	AH00558: apache2: Could not reliably determine the server's			
16	09-16 00:01	SYSLOG-0A0295BD	[Sat Sep 16 00:00:10.135016 2023] [mpm_event:notice] [pid			
17	09-15 00:01	SYSLOG-0A0295BD	[Fri Sep 15 00:00:07.727504 2023] [core:notice] [pid 9691:ti			
18	09-15 00:01	SYSLOG-0A0295BD	[Fri Sep 15 00:00:07.727481 2023] [mpm_event:notice] [pid			
19	09-15 00:01	SYSLOG-0A0295BD	AH00558: apache2: Could not reliably determine the server's			
20	09-15 00:01	SYSLOG-0A0295BD	[Fri Sep 15 00:00:07.707692 2023] [mpm_event:notice] [pid			
21	09-14 11:45	SYSLOG-0A0295BD	{ \"time\":\"2023-09-14T11:44:28.984Z\", \"process\":\"47\",			
22	09-14 11:44	SYSLOG-0A0295BD	{ \"time\":\"2023-09-14T11:43:37.343Z\", \"process\":\"432'			

Data	
Data Parser Name	Apache Log Parser
Data Source ID	SYSLOG-0A0295BD
Data Source Name	zleo-VM-189
Data Source Type	Apache
Data Timestamp	2023-09-18 10:25:36
Date/Time	10:26:48
Time Stamp	2023-09-18 10:26:48
Event	
Event Message	{ \"time\":\"2023-09-18T10:25:32.789Z\", \"proce www/html/server-status\", \"remoteIP\":\"10.2.0.2 equest\":\"/server-status\", \"query\":\"\", \"method erAgent\":\"Mozilla/5.0 (Windows NT 10.0; Win64 ML, like Gecko) Chrome/116.0.0.0 Safari/537.36\",
Host	
Host IP	10.2.149.189
Host Name	zleo-VM-189
UEBA Endpoint ID	1
User	
UEBA User ID	1
Application	
Application Process	13414
Application Service	apache-access
HTTP Method	GET
HTTP Referrer	-
HTTP URL	/var/www/html/server-status
HTTP User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple' ko) Chrome/116.0.0.0 Safari/537.36
Others	
ADOM OID	3
Data UID	7280218709191294977

Total logs for analytics: 18 days 2 hours.

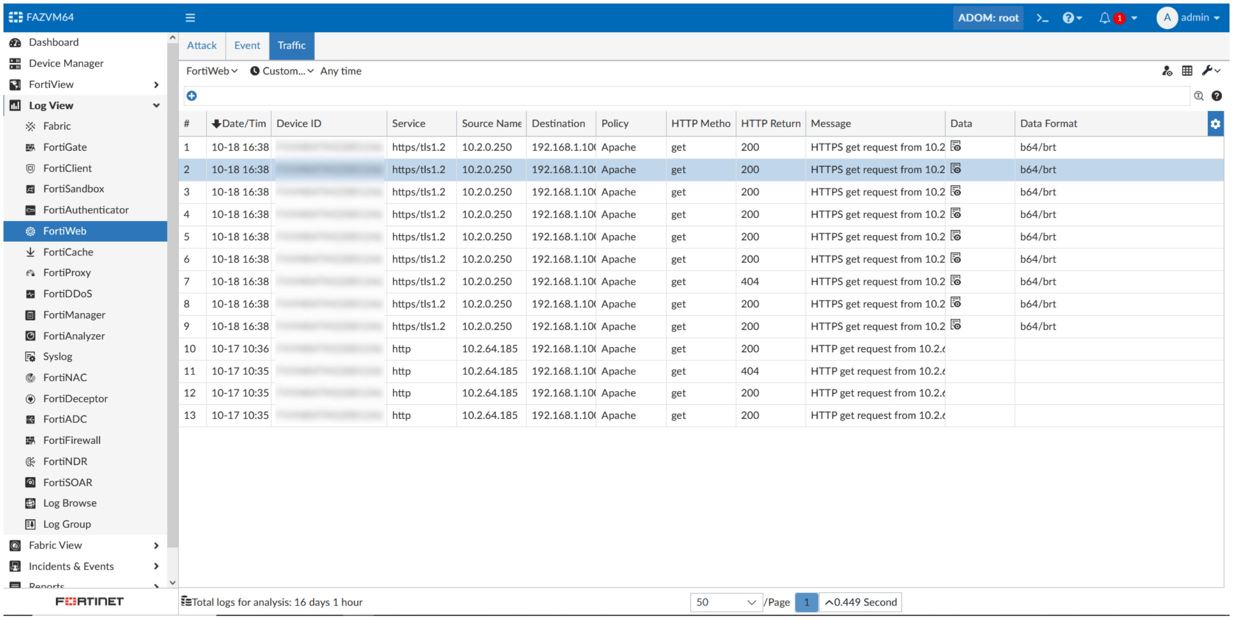
50 /Page 1 ^0.66 Second

FortiAnalyzer supports packet header information for FortiWeb traffic log - 7.4.1

FortiAnalyzer supports packet header information for FortiWeb traffic log to centralize the troubleshooting. This feature requires field "`set traffic_packet`" to be enabled.

To view packet header information for FortiWeb traffic logs on FortiAnalyzer:

1. On FortiAnalyzer, go to *Log View* > *FortiWeb*.



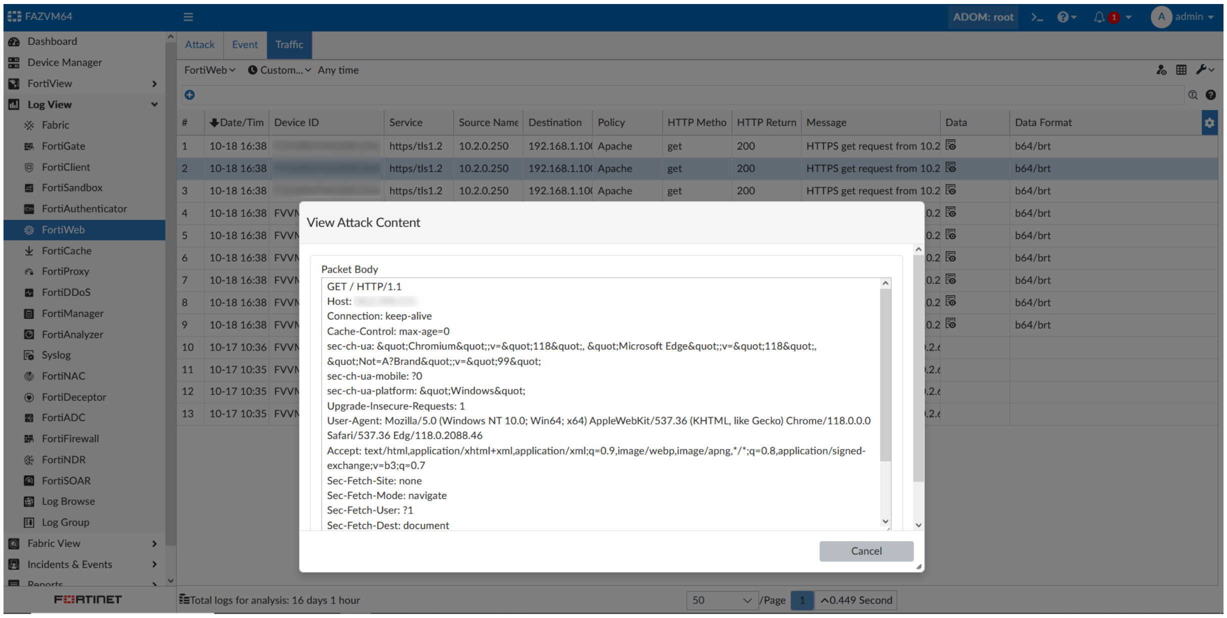
FortiWeb Custom... Any time

#	Date/Tim	Device ID	Service	Source Name	Destination	Policy	HTTP Metho	HTTP Return	Message	Data	Data Format
1	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	▤	b64/brt
2	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	▤	b64/brt
3	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	▤	b64/brt
4	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	▤	b64/brt
5	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	▤	b64/brt
6	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	▤	b64/brt
7	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	404	HTTPS get request from 10.2	▤	b64/brt
8	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	▤	b64/brt
9	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	▤	b64/brt
10	10-17 10:36	[redacted]	http	10.2.64.185	192.168.1.10(	Apache	get	200	HTTP get request from 10.2.(		
11	10-17 10:35	[redacted]	http	10.2.64.185	192.168.1.10(	Apache	get	404	HTTP get request from 10.2.(		
12	10-17 10:35	[redacted]	http	10.2.64.185	192.168.1.10(	Apache	get	200	HTTP get request from 10.2.(		
13	10-17 10:35	[redacted]	http	10.2.64.185	192.168.1.10(	Apache	get	200	HTTP get request from 10.2.(		

Total logs for analysis: 16 days 1 hour

50 /Page 1 ^0.449 Second

2. View the packet header dialog window by one of the following methods:
   - Click the icon in the *Data* column.



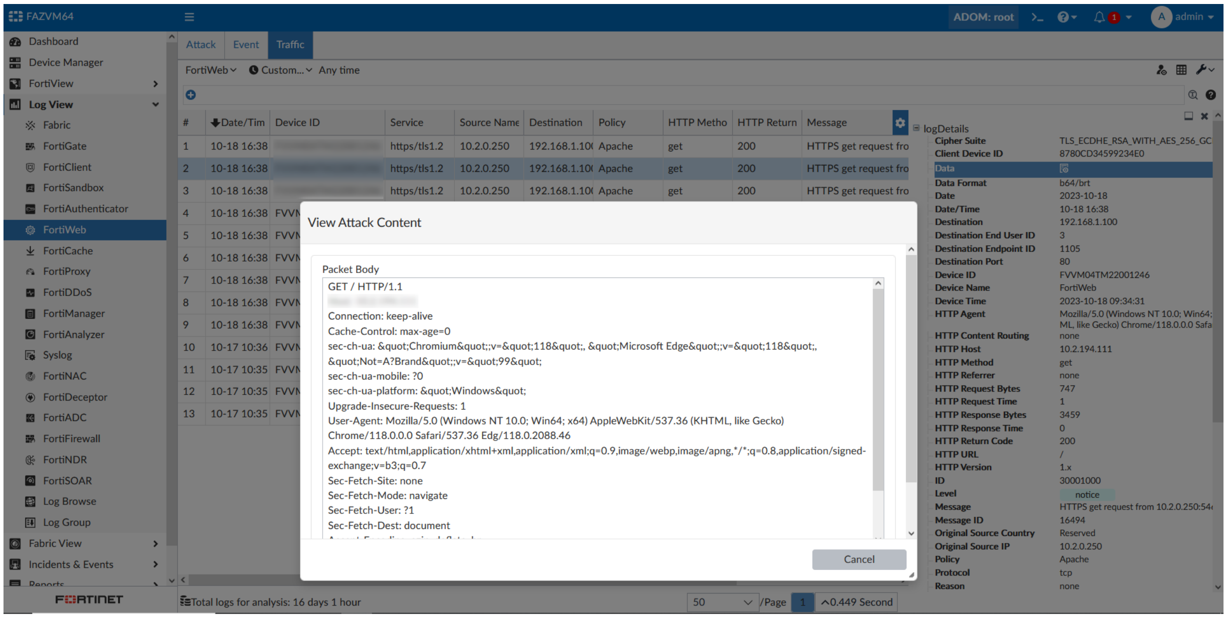
#	Date/Tim	Device ID	Service	Source Name	Destination	Policy	HTTP Metho	HTTP Return	Message	Data	Data Format
1	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	🗎	b64/brt
2	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	🗎	b64/brt
3	10-18 16:38	[redacted]	https/tls1.2	10.2.0.250	192.168.1.10(	Apache	get	200	HTTPS get request from 10.2	🗎	b64/brt
4	10-18 16:38	FVVN							0.2	🗎	b64/brt
5	10-18 16:38	FVVN							0.2	🗎	b64/brt
6	10-18 16:38	FVVN							0.2	🗎	b64/brt
7	10-18 16:38	FVVN							0.2	🗎	b64/brt
8	10-18 16:38	FVVN							0.2	🗎	b64/brt
9	10-18 16:38	FVVN							0.2	🗎	b64/brt
10	10-17 10:36	FVVN							.2.(		
11	10-17 10:35	FVVN							.2.(		
12	10-17 10:35	FVVN							.2.(		
13	10-17 10:35	FVVN							.2.(		

View Attack Content

Packet Body

```
GET / HTTP/1.1
Host: [redacted]
Connection: keep-alive
Cache-Control: max-age=0
sec-ch-ua: &quot;Chromium&quot;;v=&quot;118&quot;, &quot;Microsoft Edge&quot;;v=&quot;118&quot;,
&quot;Not=A?Brand&quot;;v=&quot;99&quot;
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: &quot;Windows&quot;
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0
Safari/537.36 Edg/118.0.2088.46
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
```

   - Click the icon in the detail panel.



View Attack Content

Packet Body

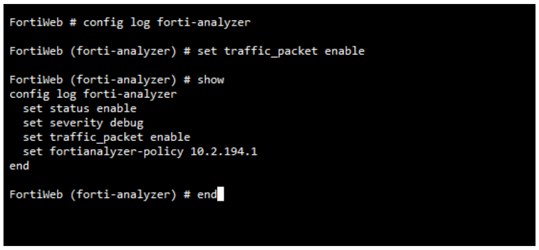
```
GET / HTTP/1.1
[redacted]
Connection: keep-alive
Cache-Control: max-age=0
sec-ch-ua: &quot;Chromium&quot;;v=&quot;118&quot;, &quot;Microsoft Edge&quot;;v=&quot;118&quot;,
&quot;Not=A?Brand&quot;;v=&quot;99&quot;
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: &quot;Windows&quot;
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/118.0.0.0 Safari/537.36 Edg/118.0.2088.46
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
```

Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_GC
Client Device ID	8780CD34599234E0
Data	🗎
Data Format	b64/brt
Date	2023-10-18
Date/Time	10-18 16:38
Destination	192.168.1.100
Destination End User ID	3
Destination Endpoint ID	1105
Destination Port	80
Device ID	FVVM04TM22001246
Device Name	FortiWeb
Device Time	2023-10-18 09:34:31
HTTP Agent	Mozilla/5.0 (Windows NT 10.0; Win64; ML, like Gecko) Chrome/118.0.0.0 Safa
HTTP Content Routing	none
HTTP Host	10.2.194.111
HTTP Method	get
HTTP Referrer	none
HTTP Request Bytes	747
HTTP Request Time	1
HTTP Response Bytes	3459
HTTP Response Time	0
HTTP Return Code	200
HTTP URL	/
HTTP Version	1.x
ID	30001000
Level	notice
Message	HTTPS get request from 10.2.0.250:54
Message ID	16494
Original Source Country	Reserved
Original Source IP	10.2.0.250
Policy	Apache
Protocol	tcp
Reason	none

To enable the traffic packet setting on FortiWeb:

1. In the FortiWeb CLI, enable the `traffic_packet` setting. For example:

```
config log forti-analyzer
   set traffic_packet enable
end
```



```
FortiWeb # config log forti-analyzer

FortiWeb (forti-analyzer) # set traffic_packet enable

FortiWeb (forti-analyzer) # show
config log forti-analyzer
  set status enable
  set severity debug
  set traffic_packet enable
  set fortianalyzer-policy 10.2.194.1
end

FortiWeb (forti-analyzer) # end
```

Support additional log fields for long live session logs - 7.4.2

In FortiAnalyzer 7.4.2, three new log fields are supported for FortiGate long live session logs:

- *Duration Delta*
- *Sent Packet Delta*
- *Received Packet Delta*

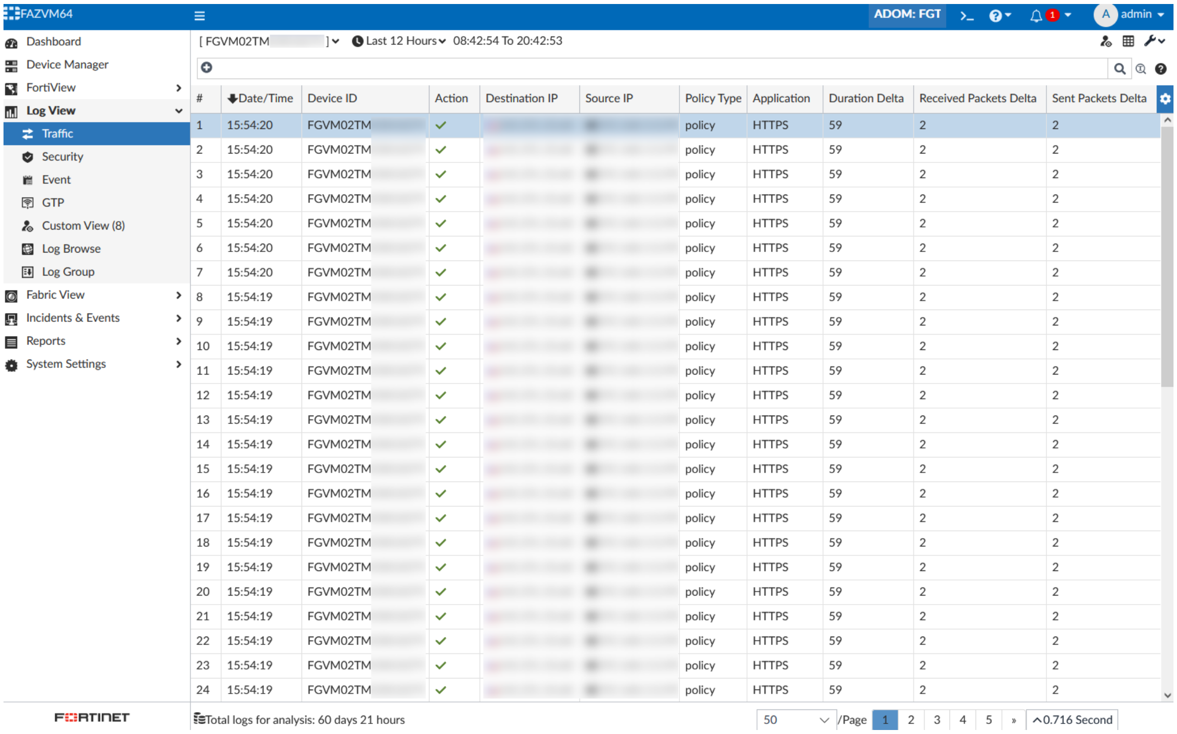
These fields are only available when the FortiGate is v7.4.2 or higher.

To view the new fields in the FortiAnalyzer GUI:

1. Go to *Log View > Traffic*.

   In the table view, there are three new columns:

   - *Duration Delta*
   - *Received Packet Delta*
   - *Sent Packet Delta*



[FGVM02TM[redacted]] Last 12 Hours 08:42:54 To 20:42:53

#	Date/Time	Device ID	Action	Destination IP	Source IP	Policy Type	Application	Duration Delta	Received Packets Delta	Sent Packets Delta
1	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
2	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
3	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
4	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
5	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
6	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
7	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
8	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
9	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
10	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
11	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
12	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
13	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
14	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
15	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
16	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
17	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
18	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
19	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
20	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
21	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
22	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
23	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
24	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2

Total logs for analysis: 60 days 21 hours

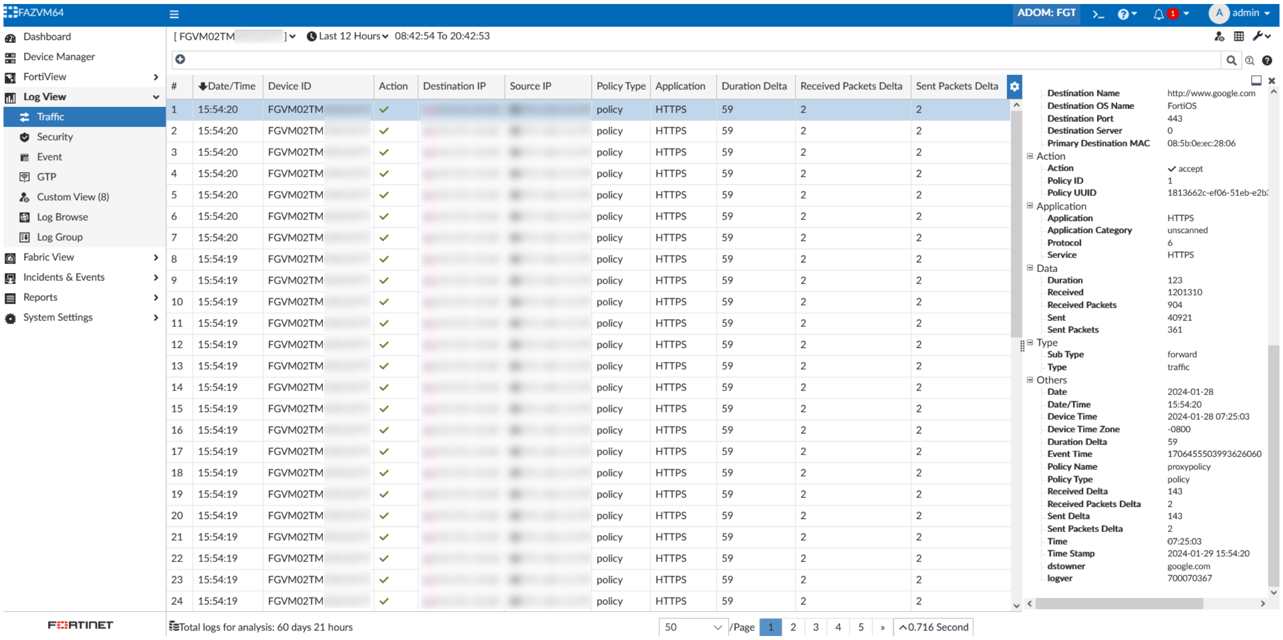
50 /Page 1 2 3 4 5 » 0.716 Second

If these columns are not visible, click the *Column Settings* icon and add the columns to the table view. For more information, see Customizing displayed columns in the FortiAnalyzer Administration Guide.

2. To open the log detail pane, double-click a long live session log in the table.

   In the *Others* section, the three new fields are available:

   - *Duration Delta*
   - *Received Packet Delta*
   - *Sent Packet Delta*



[FGVM02TM[redacted]] Last 12 Hours 08:42:54 To 20:42:53

#	Date/Time	Device ID	Action	Destination IP	Source IP	Policy Type	Application	Duration Delta	Received Packets Delta	Sent Packets Delta
1	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
2	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
3	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
4	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
5	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
6	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
7	15:54:20	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
8	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
9	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
10	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
11	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
12	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
13	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
14	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
15	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
16	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
17	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
18	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
19	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
20	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
21	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
22	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
23	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2
24	15:54:19	FGVM02TM[redacted]	✓	[redacted]	[redacted]	policy	HTTPS	59	2	2

Destination Name	http://www.google.com
Destination OS Name	FortiOS
Destination Port	443
Destination Server	0
Primary Destination MAC	08:5b:0e:ec:28:06
⊟ Action	
Action	✓ accept
Policy ID	1
Policy UUID	1813662c-ef06-51eb-e2b
⊟ Application	
Application	HTTPS
Application Category	unscanned
Protocol	6
Service	HTTPS
⊟ Data	
Duration	123
Received	1201310
Received Packets	904
Sent	40921
Sent Packets	361
⊟ Type	
Sub Type	forward
Type	traffic
⊟ Others	
Date	2024-01-28
Date/Time	15:54:20
Device Time	2024-01-28 07:25:03
Device Time Zone	-0800
Duration Delta	59
Event Time	1706455503993626060
Policy Name	proxypolicy
Policy Type	policy
Received Delta	143
Received Packets Delta	2
Sent Delta	143
Sent Packets Delta	2
Time	07:25:03
Time Stamp	2024-01-29 15:54:20
dstowner	google.com
logver	700070367

Total logs for analysis: 60 days 21 hours 50 /Page 1 2 3 4 5 » 0.716 Second

The fields are also available when viewing the raw log in FortiAnalyzer.

Log Forwarding

This section lists the new features added to FortiAnalyzer for log forwarding:

- Fluentd support for public cloud integration on page 89

Fluentd support for public cloud integration

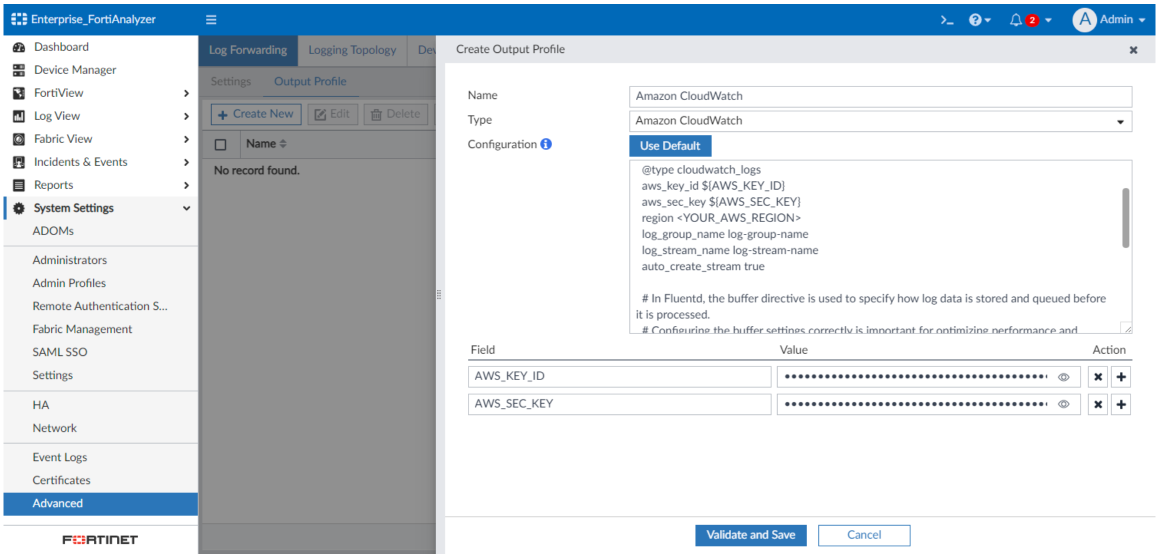
Support is added for log streaming to multiple destinations via Fluentd. This allows log forwarding to public cloud services.

You can create output profiles to configure log forwarding to public cloud services.

To create an output profile for log forwarding:

1. Go to *System Settings* > *Advanced* > *Log Forwarding* > *Output Profile*.
2. Click *Create New*.

   The *Create Output Profile* pane displays.



Name: Amazon CloudWatch

Type: Amazon CloudWatch

Configuration:

```
 @type cloudwatch_logs
 aws_key_id ${AWS_KEY_ID}
 aws_sec_key ${AWS_SEC_KEY}
 region <YOUR_AWS_REGION>
 log_group_name log-group-name
 log_stream_name log-stream-name
 auto_create_stream true

 # In Fluentd, the buffer directive is used to specify how log data is stored and queued before
it is processed.
 # Configuring the buffer settings correctly is important for optimizing performance and
```

Field	Value	Action
AWS_KEY_ID	••	✖ +
AWS_SEC_KEY	••	✖ +

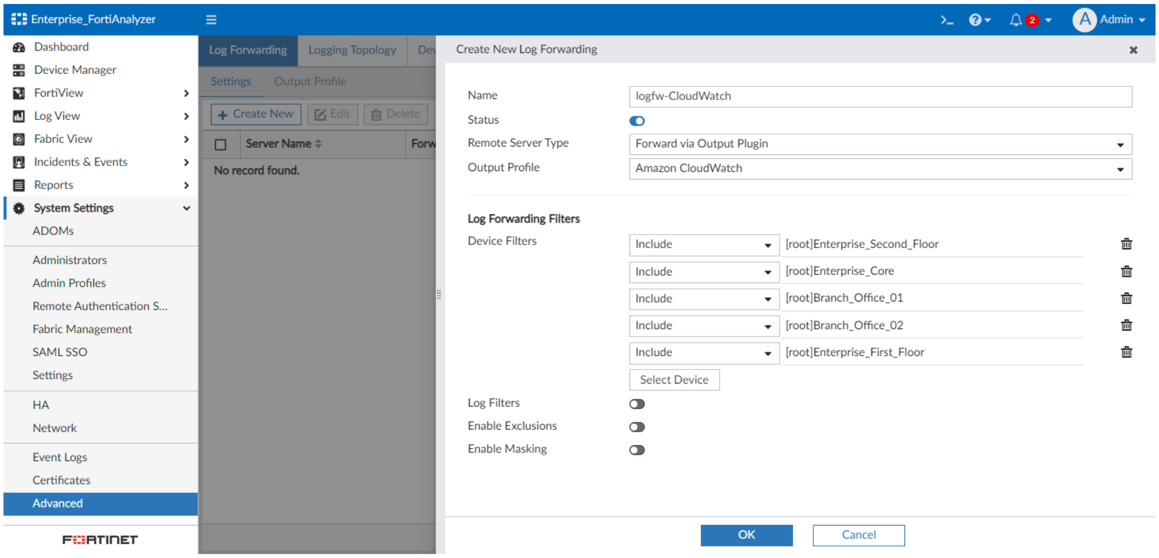
3. Configure the following options:

Name	Enter a name for the output profile.
Type	Select the public cloud service for the output profile.
Configuration	Click *Use Default* to use the default Fluentd configuration for the selected public cloud service. Alternatively, copy and paste the Fluentd configuration into this field for the selected public cloud service.
Field	Fields will automatically be added into the configuration if a keyword matches the placeholder in the configuration to provide encryption for you to hide the credentials. For example, a password placeholder in the configuration would be "`${password}`". In the field, you can define *Field*: `password`, *Value*: `actual_password`.

4. Click *Validate and Save*.

To configure log forwarding to the output profile:

1. Go to *System Settings* > *Advanced Log Forwarding* > *Settings*.
2. Click *Create New*.
   The *Create New Log Forwarding* pane displays.



Create New Log Forwarding

Name	logfw-CloudWatch
Status	●
Remote Server Type	Forward via Output Plugin
Output Profile	Amazon CloudWatch

Log Forwarding Filters

Device Filters

Include	[root]Enterprise_Second_Floor
Include	[root]Enterprise_Core
Include	[root]Branch_Office_01
Include	[root]Branch_Office_02
Include	[root]Enterprise_First_Floor

Select Device

Log Filters ○

Enable Exclusions ○

Enable Masking ○

3. Configure the following options:

Name		Enter a name for the remote server.
Status		Enable log forwarding.
Remote Server Type		Select *Forward via Output Plugin*.
Output Profile		Select the output profile.
Log Forwarding Filters		
	Device Filters	Click *Select Device*, then select the devices whose logs will be forwarded.
	Log Filters	Enable to configure filters for the logs that are forwarded.
	Enable Exclusions	Enable to configure filter on the logs that are forwarded.
	Enable Masking	Enable log field masking, if needed.

4. Click *OK*.

To troubleshoot the Fluentd connection with the FortiAnalyzer CLI:

1. In the FortiAnalyzer CLI, enter the following command to check the Fluentd write status:

```
FAZVM64 # diagnose test application fwdplugind 4
   Stats for plugin:
   lfw_name: logfw-CloudWatch
   plugin_name: Amazon CloudWatch
   type: AMAZON_CLOUDWATCH
   fd-plug-id: tcp_1_3da_6af_922_1c3
   fluentd emit stats(emit_calls|emit_rec_calls|emit_size): 3685, 88677, 0
   fluentd write stats(write|retry|rollback): 3, 0, 0
   fluentd buffer queue(byte_size|total_queue_size|queue_len|ratio): 49842536,
         52433884, 2, 0
   fluentd buffer stage(byte_size|stage_length): 4325288, 1
   fluentd flush stats(flush_time|slow_flush_count): 0, 0
```

2. In the FortiAnalyzer CLI, enter the following command to determine if the Fluentd log files are present:

```
FAZVM64 # diagnose sql fluentd log-tail
   Fluentd log files are not present. Please turn on Fluentd log first if you need to
         test it.
```

3. In the FortiAnalyzer CLI, enter the following command to enable Fluentd logging:

```
FAZVM64 # diagnose test application fwdplugind 201 log enable
  Warning: This will enable Fluentd logging.
  Fluentd requires a restart for changes to take effect. The restart will disrupt
       Fluentd's current log handling.
  Execute the command again in one minute for the changes to take effect.
FAZVM64 # diagnose test application fwdplugind 201 log enable
  Fluentd logging is enabled, Fluentd will be restarted.
```

4. In the FortiAnalyzer CLI, enter the following command again to show the processed events:

```
FAZVM64 # diagnose sql fluentd log-tail
  File /drive0/private/fwdplugind/fluentd/logs/faz-td-agent.log, is present, will
       open it.
  Please press Control+C to exit.
  ======================================
  aws_sec_key xxxxxx
  region "us-west-2"
  log_group_name "Log-Group-Test"
  log_stream_name "Log-Stream-test"
  auto_create_stream true
  @id tcp_1_3da_6af_922_1c3
  <buffer tag,time>
  @type "memory"
  chunk_limit_size 10M
  total_limit_size 50M
  timekey 5m
  timekey_wait 30s
  timekey_use_utc true
  flush_thread_count 3
  flush_at_shutdown true
  overflow_action block
  retry_forever true
  disable_chunk_backup true
  </buffer>
  </match>
  </worker>
  </ROOT>
  2023-04-24 16:05:20 -0700 [info]: starting fluentd-1.15.2 pid=12376 ruby="2.7.6"
  2023-04-24 16:05:20 -0700 [info]: spawn command to main: cmdline=
       ["/usr/local/fluentd/td-agent/bin/ruby", "-Eascii-8bit:ascii-8bit",
       "/usr/sbin/td-agent", "-d", "/drive0/private/fwdplugind/fluentd/faz-td-
       agent.pid", "-c", "/drive0/private/fwdplugind/fluentd/faz-td-agent.conf", "-
       o", "/drive0/private/fwdplugind/fluentd/logs/faz-td-agent.log", "--log-rotate-
       size", "5120000", "--under-supervisor"]
  2023-04-24 16:05:20 -0700 [info]: #0 adding match pattern="tcp_1" type="cloudwatch_
       logs"
  2023-04-24 16:05:21 -0700 [info]: adding source type="monitor_agent"
  2023-04-24 16:05:21 -0700 [info]: #0 adding source type="tcp"
  2023-04-24 16:05:21 -0700 [info]: #0 starting fluentd worker pid=12390 ppid=12387
       worker=0
  2023-04-24 16:05:21 -0700 [info]: #0 listening tcp socket bind="127.0.0.1"
       port=10000
  2023-04-24 16:05:21 -0700 [info]: #0 fluentd worker is now running worker=0
```

Reports

This section lists the new features added to FortiAnalyzer for reports:

Report guidance

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Report guidance

FortiAnalyzer provides many factory default reports that use charts relying on specific log types and log fields to provide valuable output. When running a full report, you may see "`No Data`" returned in sections if:

- logging was not enabled correctly
- the report element is for a different Device/Log Type
- there are no matching logs

Debugging such scenarios can be time consuming because it requires navigating through charts, macros, and datasets.

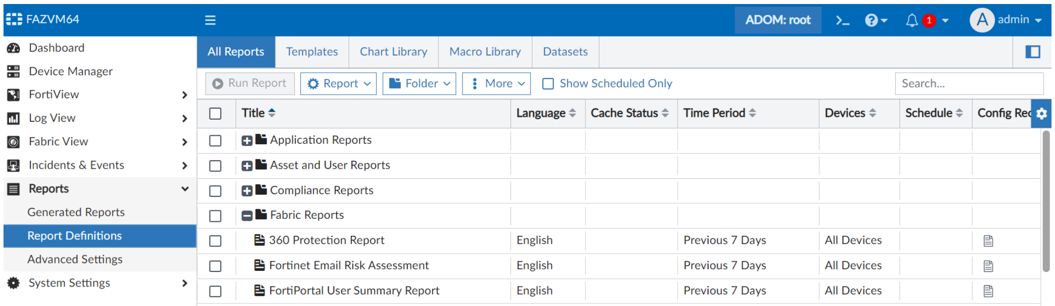
To improve the overall reporting experience, a new *Report Guidance* feature has been implemented to provide full visibility for each report element in terms of:

- Device Type (e.g. Fortigate)
- Log Type (e.g. traffic)
- Log Fields (e.g. action, itime)

In short, you can use the *Report Guidance* feature to troubleshoot and determine if FortiAnalyzer has the appropriate Analytics logs available for a report.

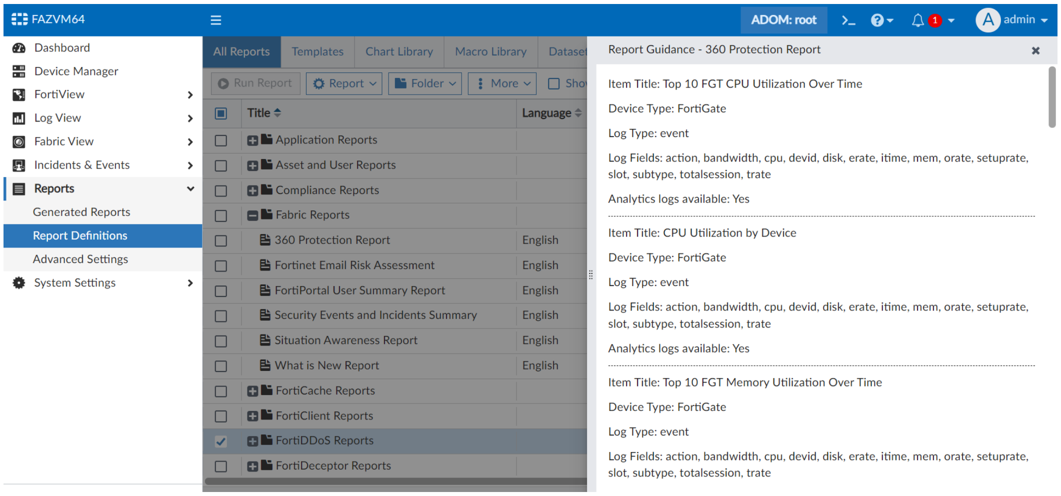
To use the Report Guidance feature:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
   There is a new *Config Recommendation* column.



☐	Title	Language	Cache Status	Time Period	Devices	Schedule	Config Rec
☐	Application Reports						
☐	Asset and User Reports						
☐	Compliance Reports						
☐	Fabric Reports						
☐	360 Protection Report	English		Previous 7 Days	All Devices		🗎
☐	Fortinet Email Risk Assessment	English		Previous 7 Days	All Devices		🗎
☐	FortiPortal User Summary Report	English		Previous 7 Days	All Devices		🗎

2. Click the icon in the *Config Recommendation* column.
   The *Report Guidance* pane opens for that report. This pane provides the `Item Title` (chart or macro name), `Device Type`, `Log Type`, and the relevant `Log Fields` and Analytics log availability.



☐	Title	Language
☐	Application Reports	
☐	Asset and User Reports	
☐	Compliance Reports	
☐	Fabric Reports	
☐	360 Protection Report	English
☐	Fortinet Email Risk Assessment	English
☐	FortiPortal User Summary Report	English
☐	Security Events and Incidents Summary	English
☐	Situation Awareness Report	English
☐	What is New Report	English
☐	FortiCache Reports	
☐	FortiClient Reports	
☑	FortiDDoS Reports	
☐	FortiDeceptor Reports	

Report Guidance - 360 Protection Report

Item Title: Top 10 FGT CPU Utilization Over Time

Device Type: FortiGate

Log Type: event

Log Fields: action, bandwidth, cpu, devid, disk, erate, itime, mem, orate, setuprate, slot, subtype, totalsession, trate

Analytics logs available: Yes

Item Title: CPU Utilization by Device

Device Type: FortiGate

Log Type: event

Log Fields: action, bandwidth, cpu, devid, disk, erate, itime, mem, orate, setuprate, slot, subtype, totalsession, trate

Analytics logs available: Yes

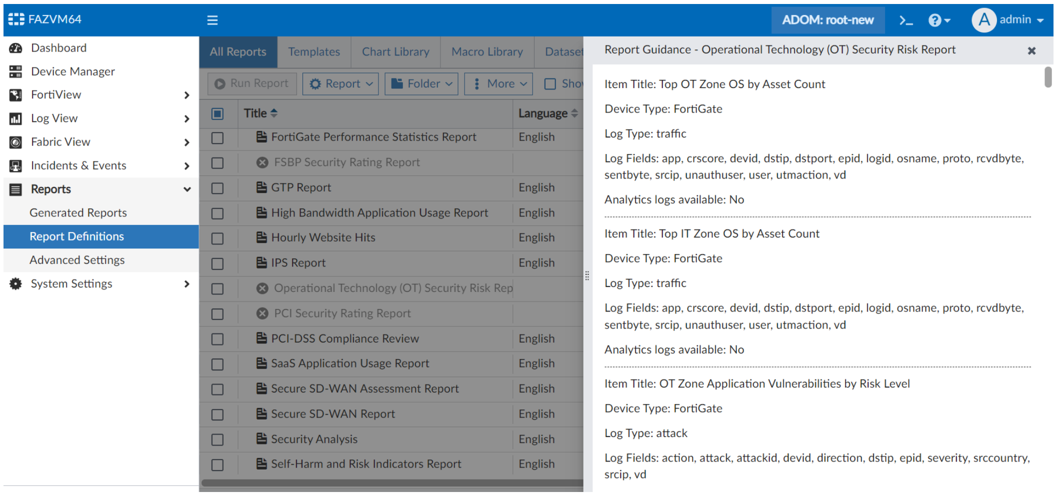
Item Title: Top 10 FGT Memory Utilization Over Time

Device Type: FortiGate

Log Type: event

Log Fields: action, bandwidth, cpu, devid, disk, erate, itime, mem, orate, setuprate, slot, subtype, totalsession, trate

The *Report Guidance* pane is available for license-controlled reports, but the report cannot be generated without a valid license.



☐	Title	Language
☐	FortiGate Performance Statistics Report	English
☐	FSBP Security Rating Report	
☐	GTP Report	English
☐	High Bandwidth Application Usage Report	English
☐	Hourly Website Hits	English
☐	IPS Report	English
☐	Operational Technology (OT) Security Risk Rep	
☐	PCI Security Rating Report	
☐	PCI-DSS Compliance Review	English
☐	SaaS Application Usage Report	English
☐	Secure SD-WAN Assessment Report	English
☐	Secure SD-WAN Report	English
☐	Security Analysis	English
☐	Self-Harm and Risk Indicators Report	English

Report Guidance - Operational Technology (OT) Security Risk Report

Item Title: Top OT Zone OS by Asset Count

Device Type: FortiGate

Log Type: traffic

Log Fields: app, crscore, devid, dstip, dstport, epid, logid, osname, proto, rcvdbyte, sentbyte, srcip, unauthuser, user, utmaction, vd

Analytics logs available: No

Item Title: Top IT Zone OS by Asset Count

Device Type: FortiGate

Log Type: traffic

Log Fields: app, crscore, devid, dstip, dstport, epid, logid, osname, proto, rcvdbyte, sentbyte, srcip, unauthuser, user, utmaction, vd

Analytics logs available: No

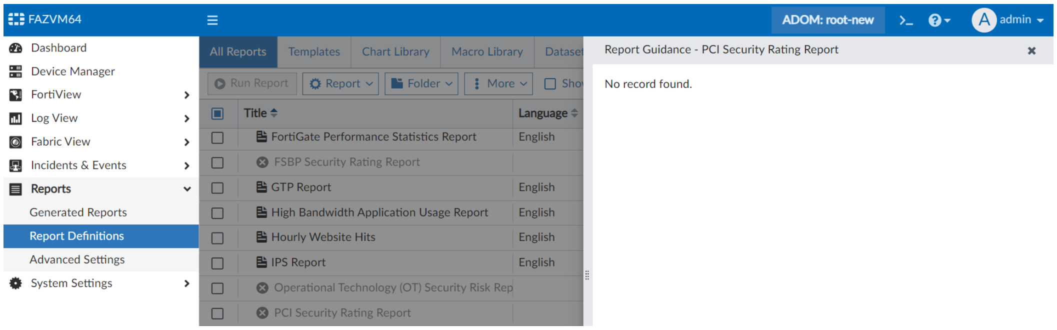
Item Title: OT Zone Application Vulnerabilities by Risk Level

Device Type: FortiGate

Log Type: attack

Log Fields: action, attack, attackid, devid, direction, dstip, epid, severity, srccountry, srcip, vd

For reports that are not generated with log tables, such as the FSBP/PCI or CIS Security Rating Reports, the *Report Guidance* pane will indicate `No record found`.



Title	Language
FortiGate Performance Statistics Report	English
FSBP Security Rating Report	
GTP Report	English
High Bandwidth Application Usage Report	English
Hourly Website Hits	English
IPS Report	English
Operational Technology (OT) Security Risk Rep	
PCI Security Rating Report	

Report Guidance - PCI Security Rating Report

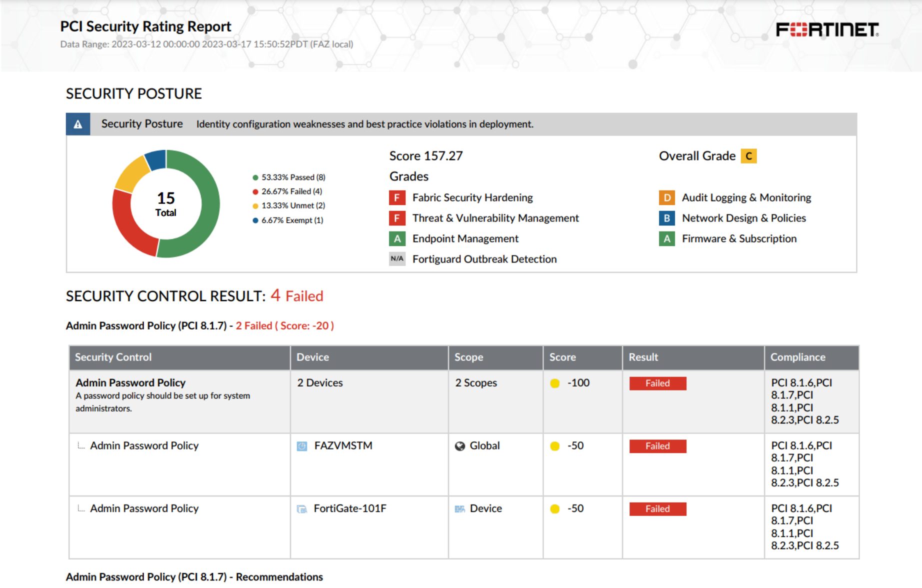
No record found.

PCI Security Rating Report

A *PCI Security Rating Report* is now available on FortiAnalyzer to optimize the deployed FortiGates in terms of *Security Posture*, *Fabric Coverage*, and *Optimization* based on PCI DSS 3.2 standards. This report consolidates security ratings performed on fabric deployments.

Each category includes the *Failed*, *Unmet*, *Passed*, and *Exempt* security control results. Recommendations are provided as well.

For example, see a sample of page 1 from the report in PDF format below.



PCI Security Rating Report

Data Range: 2023-03-12 00:00:00 2023-03-17 15:50:52PDT (FAZ local)

SECURITY POSTURE

Security Posture Identity configuration weaknesses and best practice violations in deployment.

Score 157.27

Overall Grade C

Grades

F Fabric Security Hardening

F Threat & Vulnerability Management

A Endpoint Management

N/A Fortiguard Outbreak Detection

D Audit Logging & Monitoring

B Network Design & Policies

A Firmware & Subscription

SECURITY CONTROL RESULT: 4 Failed

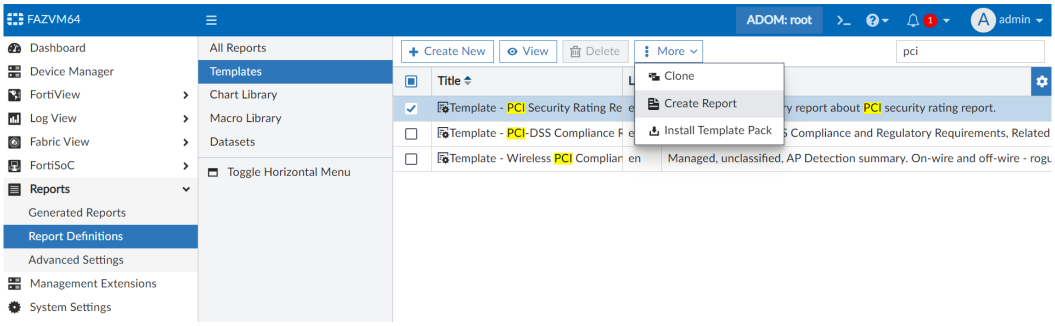
Admin Password Policy (PCI 8.1.7) - 2 Failed (Score: -20)

Security Control	Device	Scope	Score	Result	Compliance
Admin Password Policy A password policy should be set up for system administrators.	2 Devices	2 Scopes	● -100	Failed	PCI 8.1.6,PCI 8.1.7,PCI 8.1.1,PCI 8.2.3,PCI 8.2.5
Admin Password Policy	FAZVMSTM	Global	● -50	Failed	PCI 8.1.6,PCI 8.1.7,PCI 8.1.1,PCI 8.2.3,PCI 8.2.5
Admin Password Policy	FortiGate-101F	Device	● -50	Failed	PCI 8.1.6,PCI 8.1.7,PCI 8.1.1,PCI 8.2.3,PCI 8.2.5

Admin Password Policy (PCI 8.1.7) - Recommendations

To create the report from the template:

1. Go to *Reports > Report Definitions > Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - PCI Security Rating Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



☐	Title	L	
☑	Template - PCI Security Rating Re	e	y report about PCI security rating report.
☐	Template - PCI-DSS Compliance R	e	S Compliance and Regulatory Requirements, Related
☐	Template - Wireless PCI Complian	en	Managed, unclassified, AP Detection summary. On-wire and off-wire - rogu

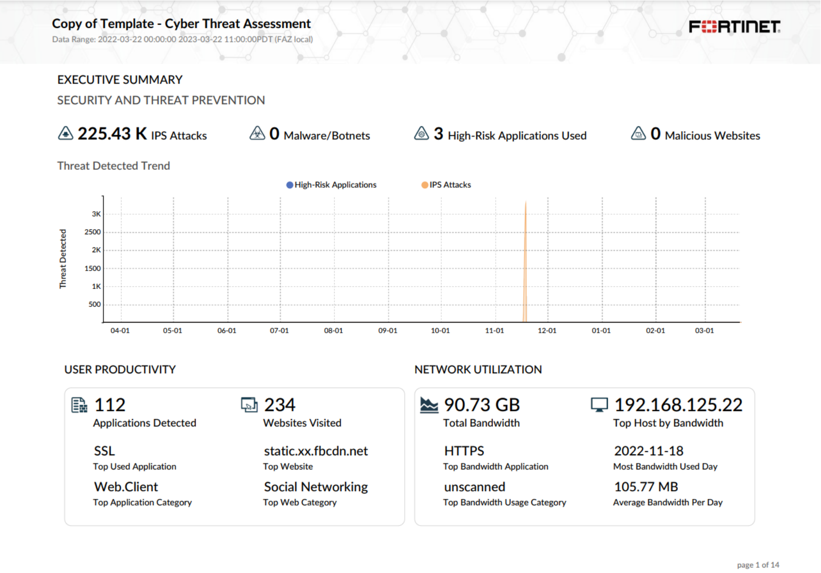
To run the PCI Security Rating Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *PCI Security Rating Report*.
   The *Edit: PCI Security Rating Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Cyber Threats Assessment Report update

The existing *Cyber Threats Assessment Report* has been updated with new style and content to enhance the visibility of the provided data.

For example, see a sample of the report in PDF format below:



Copy of Template - Cyber Threat Assessment
Data Range: 2022-03-22 00:00:00 2023-03-22 11:00:00PDT (FAZ local)

EXECUTIVE SUMMARY
SECURITY AND THREAT PREVENTION

225.43 K IPS Attacks · 0 Malware/Botnets · 3 High-Risk Applications Used · 0 Malicious Websites

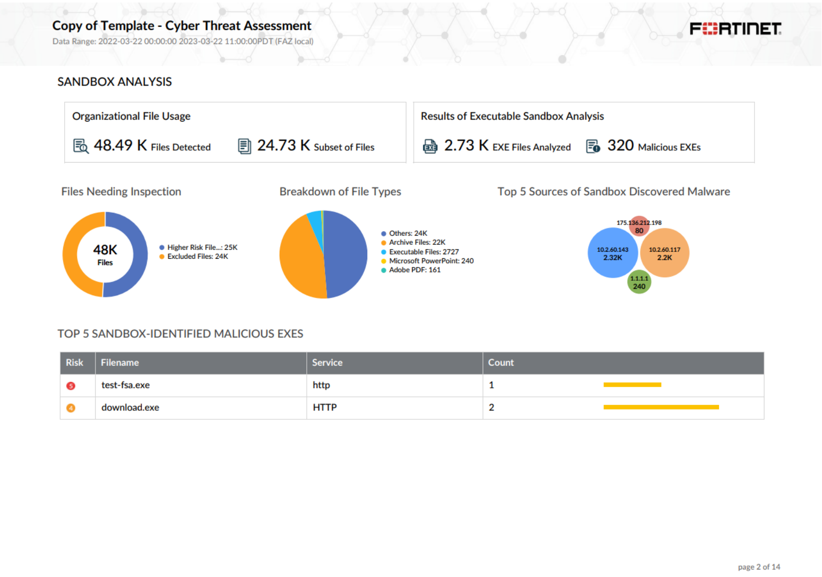
USER PRODUCTIVITY

112 Applications Detected
234 Websites Visited
SSL Top Used Application
static.xx.fbcdn.net Top Website
Web.Client Top Application Category
Social Networking Top Web Category

NETWORK UTILIZATION

90.73 GB Total Bandwidth
192.168.125.22 Top Host by Bandwidth
HTTPS Top Bandwidth Application
2022-11-18 Most Bandwidth Used Day
unscanned Top Bandwidth Usage Category
105.77 MB Average Bandwidth Per Day

page 1 of 14



Copy of Template - Cyber Threat Assessment

Data Range: 2022-03-22 00:00:00 2023-03-22 11:00:00PDT (FAZ local)

SANDBOX ANALYSIS

Organizational File Usage

48.49 K Files Detected   24.73 K Subset of Files

Results of Executable Sandbox Analysis

2.73 K EXE Files Analyzed   320 Malicious EXEs

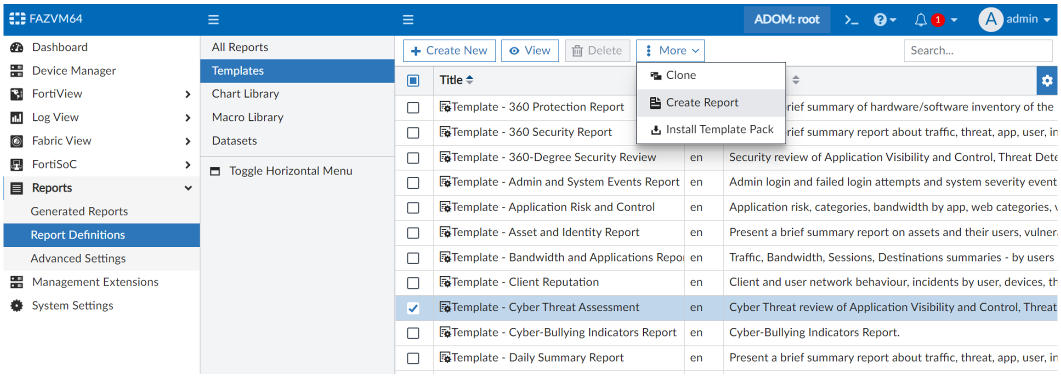
TOP 5 SANDBOX-IDENTIFIED MALICIOUS EXES

Risk	Filename	Service	Count
5	test-fsa.exe	http	1
4	download.exe	HTTP	2

page 2 of 14

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Cyber Threats Assessment Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



■	Title		
□	Template - 360 Protection Report		rief summary of hardware/software inventory of the
□	Template - 360 Security Report		rief summary report about traffic, threat, app, user, in
□	Template - 360-Degree Security Review	en	Security review of Application Visibility and Control, Threat Dete
□	Template - Admin and System Events Report	en	Admin login and failed login attempts and system severity event
□	Template - Application Risk and Control	en	Application risk, categories, bandwidth by app, web categories, v
□	Template - Asset and Identity Report	en	Present a brief summary report on assets and their users, vulner
□	Template - Bandwidth and Applications Repor	en	Traffic, Bandwidth, Sessions, Destinations summaries - by users
□	Template - Client Reputation	en	Client and user network behaviour, incidents by user, devices, th
☑	Template - Cyber Threat Assessment	en	Cyber Threat review of Application Visibility and Control, Threat
□	Template - Cyber-Bullying Indicators Report	en	Cyber-Bullying Indicators Report.
□	Template - Daily Summary Report	en	Present a brief summary report about traffic, threat, app, user, in

To run the Cyber Threats Assessment Report:

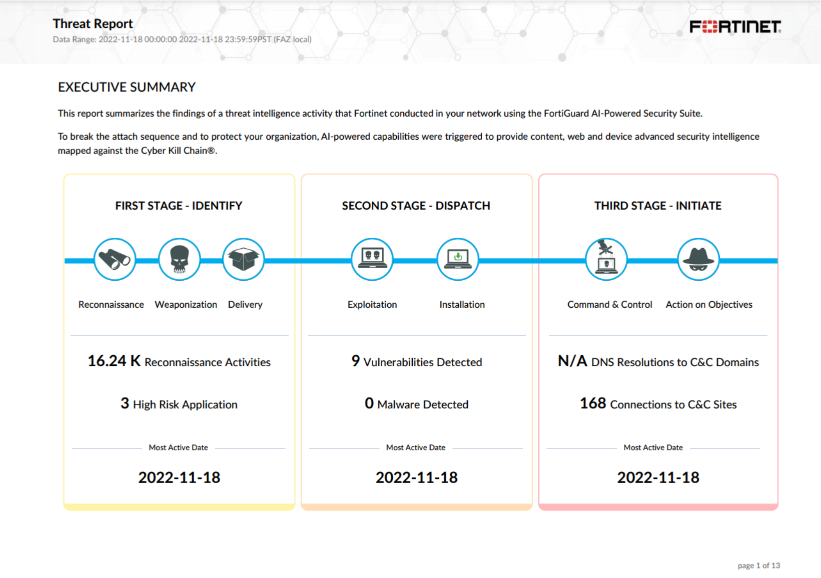
1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *Cyber Threats Assessment Report*.
   The *Edit: Cyber Threats Assessment Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Threat Report update

The *Threat Report* has been updated to provide the following:

- New style and content to better present threat data
- Threats are mapped to the Cyber Kill Chain stages for correlation and pattern identification

For example, see a sample of the report in PDF format below:



Threat Report

Data Range: 2022-11-18 00:00:00 2022-11-18 23:59:59PST (FAZ local)

EXECUTIVE SUMMARY

This report summarizes the findings of a threat intelligence activity that Fortinet conducted in your network using the FortiGuard AI-Powered Security Suite.

To break the attach sequence and to protect your organization, AI-powered capabilities were triggered to provide content, web and device advanced security intelligence mapped against the Cyber Kill Chain®.

FIRST STAGE - IDENTIFY

Reconnaissance Weaponization Delivery

16.24 K Reconnaissance Activities

3 High Risk Application

Most Active Date

2022-11-18

SECOND STAGE - DISPATCH

Exploitation Installation

9 Vulnerabilities Detected

0 Malware Detected

Most Active Date

2022-11-18

THIRD STAGE - INITIATE

Command & Control Action on Objectives

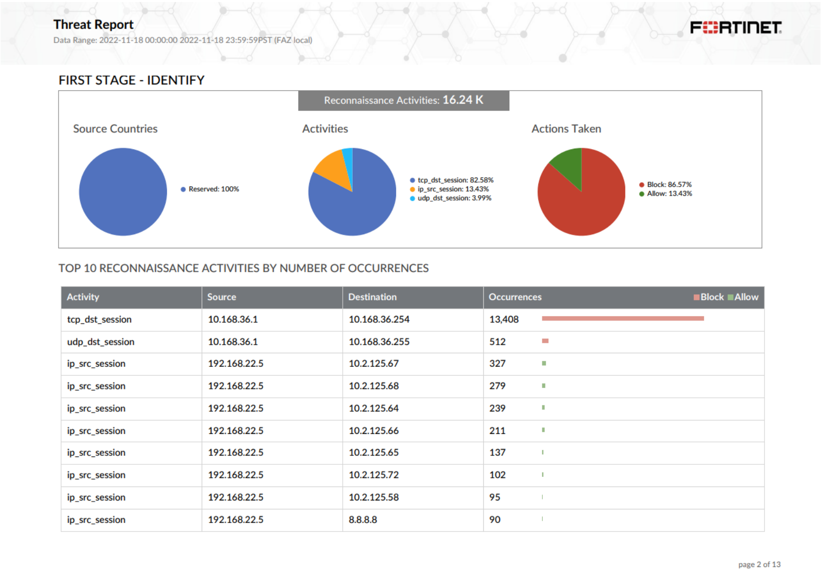
N/A DNS Resolutions to C&C Domains

168 Connections to C&C Sites

Most Active Date

2022-11-18

page 1 of 13



Threat Report

Data Range: 2022-11-18 00:00:00 2022-11-18 23:59:59PST (FAZ local)

FIRST STAGE - IDENTIFY

Reconnaissance Activities: 16.24 K

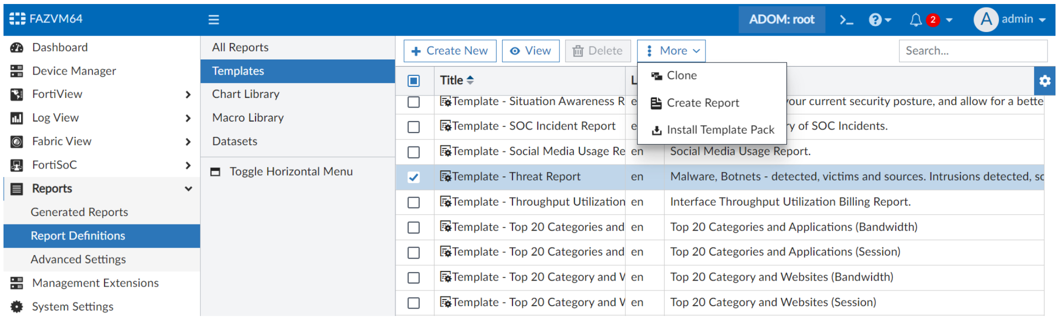
TOP 10 RECONNAISSANCE ACTIVITIES BY NUMBER OF OCCURRENCES

Activity	Source	Destination	Occurrences ■Block ■Allow
tcp_dst_session	10.168.36.1	10.168.36.254	13,408
udp_dst_session	10.168.36.1	10.168.36.255	512
ip_src_session	192.168.22.5	10.2.125.67	327
ip_src_session	192.168.22.5	10.2.125.68	279
ip_src_session	192.168.22.5	10.2.125.64	239
ip_src_session	192.168.22.5	10.2.125.66	211
ip_src_session	192.168.22.5	10.2.125.65	137
ip_src_session	192.168.22.5	10.2.125.72	102
ip_src_session	192.168.22.5	10.2.125.58	95
ip_src_session	192.168.22.5	8.8.8.8	90

page 2 of 13

To create the report from the template:

1. Go to *Reports > Report Definitions > Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Threat Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



☐	Title	L	
☐	Template - Situation Awareness R	e	our current security posture, and allow for a bette
☐	Template - SOC Incident Report	e	y of SOC Incidents.
☐	Template - Social Media Usage Re	en	Social Media Usage Report.
☑	Template - Threat Report	en	Malware, Botnets - detected, victims and sources. Intrusions detected, sc
☐	Template - Throughput Utilization	en	Interface Throughput Utilization Billing Report.
☐	Template - Top 20 Categories and	en	Top 20 Categories and Applications (Bandwidth)
☐	Template - Top 20 Categories and	en	Top 20 Categories and Applications (Session)
☐	Template - Top 20 Category and V	en	Top 20 Category and Websites (Bandwidth)
☐	Template - Top 20 Category and V	en	Top 20 Category and Websites (Session)

To run the Threat Report:

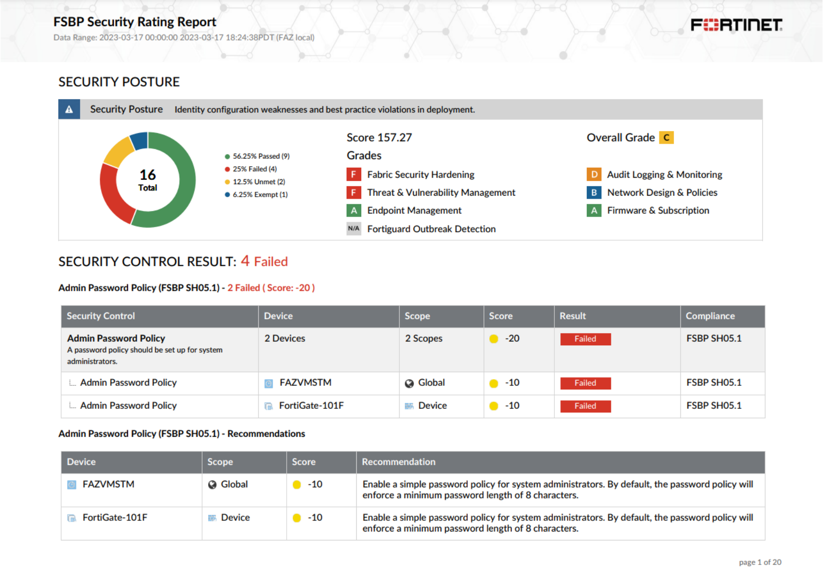
1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *Threat Report*.
   The *Edit: Threat Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

FSBP Security Rating Report

A FSBP (Fortinet Security Best Practices) Security Rating Report is available on FortiAnalyzer to optimize the deployed FortiGates in terms of *Security Posture*, *Fabric Coverage*, and *Optimization*. This report consolidates security ratings performed on fabric deployments.

Each category includes the *Failed*, *Unmet*, *Passed*, and *Exempt* security control results. Recommendations are provided as well.

For example, see a sample of page 1 from the report in PDF format below.



FSBP Security Rating Report

Data Range: 2023-03-17 00:00:00 2023-03-17 18:24:38PDT (FAZ local)

SECURITY POSTURE

Security Posture Identity configuration weaknesses and best practice violations in deployment.

Score 157.27

Overall Grade C

Grades

F	Fabric Security Hardening	D	Audit Logging & Monitoring
F	Threat & Vulnerability Management	B	Network Design & Policies
A	Endpoint Management	A	Firmware & Subscription
N/A	Fortiguard Outbreak Detection		

SECURITY CONTROL RESULT: 4 Failed

Admin Password Policy (FSBP SH05.1) - 2 Failed (Score: -20)

Security Control	Device	Scope	Score	Result	Compliance
Admin Password Policy A password policy should be set up for system administrators.	2 Devices	2 Scopes	● -20	Failed	FSBP SH05.1
Admin Password Policy	FAZVMSTM	Global	● -10	Failed	FSBP SH05.1
Admin Password Policy	FortiGate-101F	Device	● -10	Failed	FSBP SH05.1

Admin Password Policy (FSBP SH05.1) - Recommendations

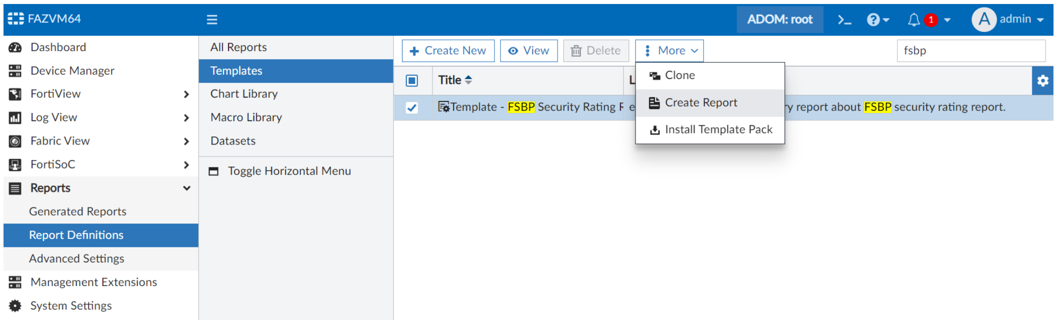
Device	Scope	Score	Recommendation
FAZVMSTM	Global	● -10	Enable a simple password policy for system administrators. By default, the password policy will enforce a minimum password length of 8 characters.
FortiGate-101F	Device	● -10	Enable a simple password policy for system administrators. By default, the password policy will enforce a minimum password length of 8 characters.

page 1 of 20

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.

2. Select the checkbox for *Template - FSBP Security Rating Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



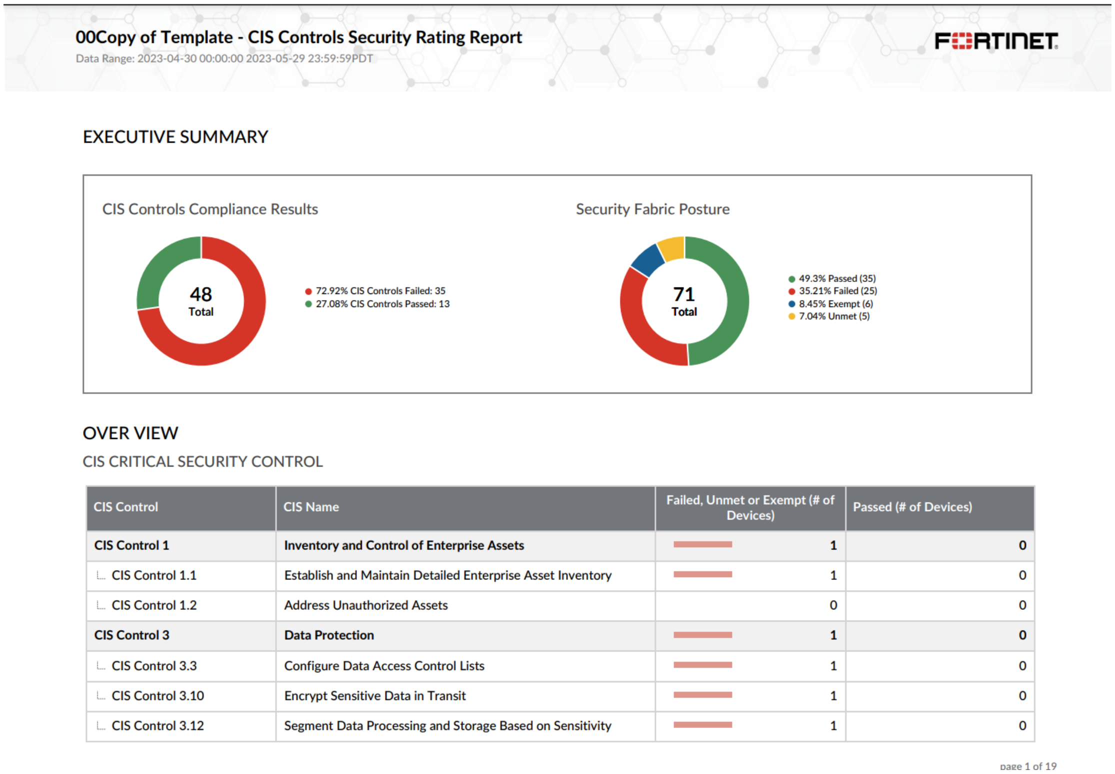
To run the FSBP Security Rating Report:

1. Go to *Reports > Report Definitions > All Reports*, and double-click the row for the *FSBP Security Rating Report*.
   The *Edit: FSBP Security Rating Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

CIS Controls Security Rating report

A *CIS Controls Security Rating Report* is now available on FortiAnalyzer. This report includes CIS mapping information.

For example, see a sample of the report in PDF format below.



00Copy of Template - CIS Controls Security Rating Report

Data Range: 2023-04-30 00:00:00 2023-05-29 23:59:59PDT

EXECUTIVE SUMMARY

CIS Controls Compliance Results

Security Fabric Posture

OVER VIEW

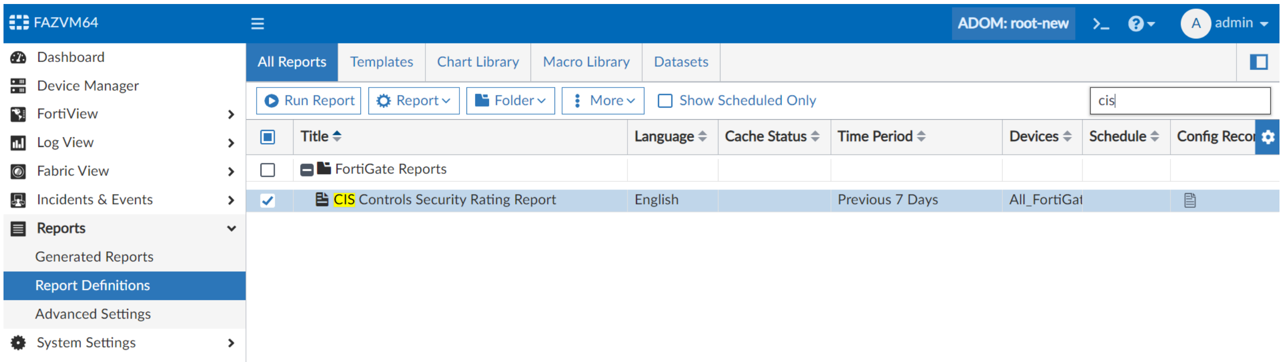
CIS CRITICAL SECURITY CONTROL

CIS Control	CIS Name	Failed, Unmet or Exempt (# of Devices)	Passed (# of Devices)
CIS Control 1	**Inventory and Control of Enterprise Assets**	**1**	**0**
∟ CIS Control 1.1	Establish and Maintain Detailed Enterprise Asset Inventory	1	0
∟ CIS Control 1.2	Address Unauthorized Assets	0	0
CIS Control 3	**Data Protection**	**1**	**0**
∟ CIS Control 3.3	Configure Data Access Control Lists	1	0
∟ CIS Control 3.10	Encrypt Sensitive Data in Transit	1	0
∟ CIS Control 3.12	Segment Data Processing and Storage Based on Sensitivity	1	0

page 1 of 19

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - CIS Controls Security Rating Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



☐	Title	Language	Cache Status	Time Period	Devices	Schedule	Config Recor
☐	FortiGate Reports						
☑	CIS Controls Security Rating Report	English		Previous 7 Days	All_FortiGat		

To run the CIS Controls Security Rating Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *CIS Controls Security Rating Report*.
   The *Edit: CIS Controls Security Rating Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Shadow IT Report

The *Shadow IT Report* is now available on FortiAnalyzer.

This report provides enhanced visibility and control for cloud based applications.

Detected applications are classified as:

- `Managed`: Allowed applications.
- `Unmanaged`: Blocked, quarantined, or reset applications.

Information about the applications, including their Category and Compliance Standard, is provided by the Shadow IT database (SIDB).

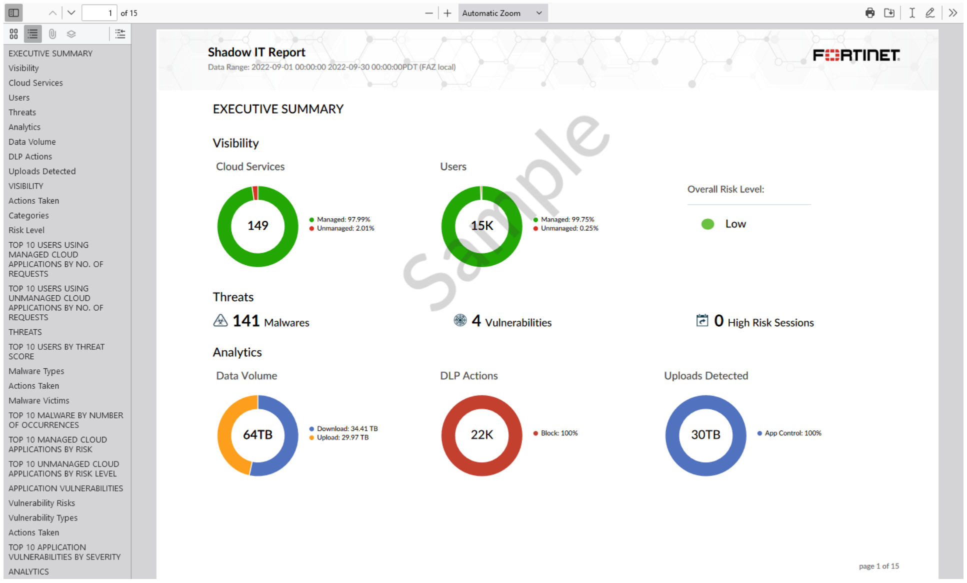
Application risk is determined by a numerical score provided by the SIDB for each application. The Risk Levels in the report are as follows:

- `Low`: Score is 1 to 15.
- `Guarded`: Score is 16 to 30.
- `Elevated`: Score is 31 to 50.
- `High`: Score is 51 to 70.
- `Severe`: Score is 71 to 100.

The `Overall Risk Level` is the average application risk score for all detected managed applications.

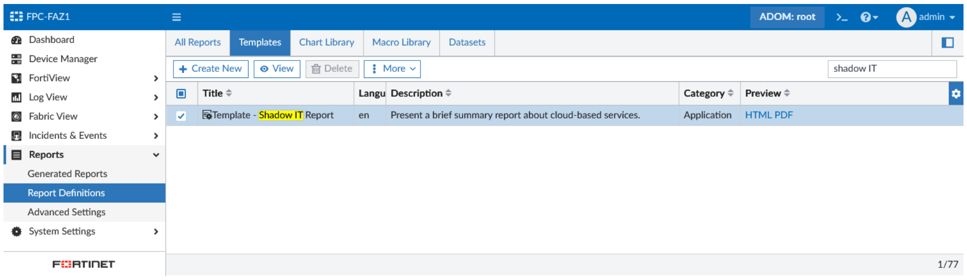
The `High Risk Sessions` are the number of sessions from managed applications with a risk score of `High` or `Severe`.

For example, see a sample of page 1 from the report in PDF format below.



To create the report from the template:

1. Go to *Reports > Report Definitions > Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Shadow IT Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



☐	Title	Langu	Description	Category	Preview
☑	Template - Shadow IT Report	en	Present a brief summary report about cloud-based services.	Application	HTML PDF

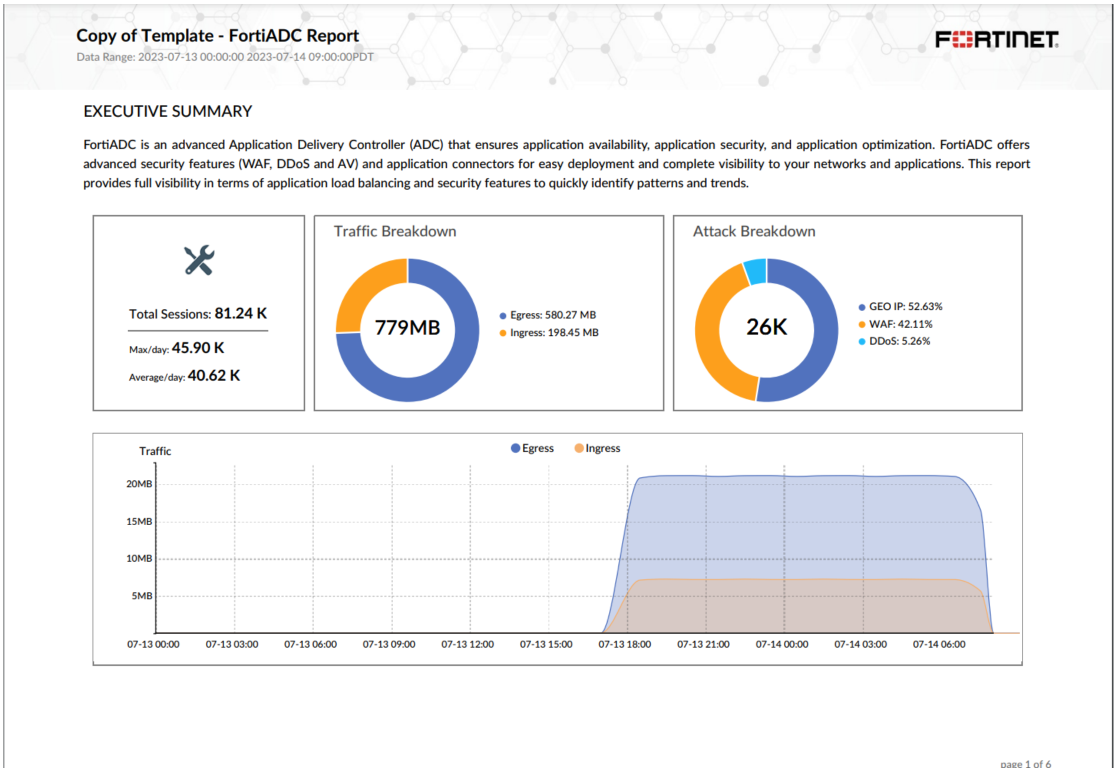
To run the Shadow IT Report:

1. Go to *Reports > Report Definitions > All Reports*, and double-click the row for the *Shadow IT Report*.
   The *Edit: Shadow IT Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

FortiADC Report - 7.4.1

The *FortiADC Report* is available on FortiAnalyzer to offer comprehensive visibility into application load balancing and security features, enabling rapid identification of security patterns and trends associated with the use of the product.

For example, see a sample of page 1 from the report in PDF format below.



Copy of Template - FortiADC Report

Data Range: 2023-07-13 00:00:00 2023-07-14 09:00:00PDT

EXECUTIVE SUMMARY

FortiADC is an advanced Application Delivery Controller (ADC) that ensures application availability, application security, and application optimization. FortiADC offers advanced security features (WAF, DDoS and AV) and application connectors for easy deployment and complete visibility to your networks and applications. This report provides full visibility in terms of application load balancing and security features to quickly identify patterns and trends.

Total Sessions: 81.24 K

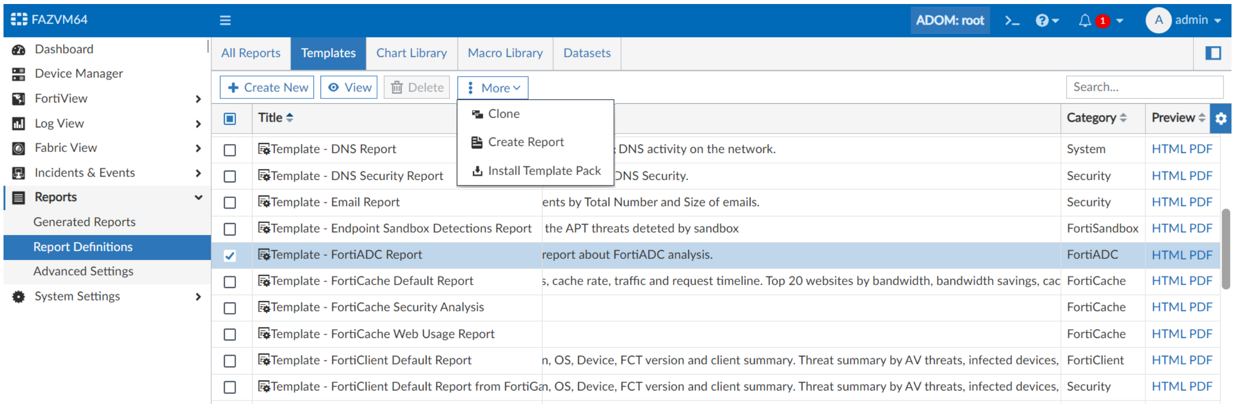
Max/day: 45.90 K

Average/day: 40.62 K

This report requires that a FortiADC device has been added and authorized to the FortiAnalyzer.

To create the report from the template:

1. Go to *Reports > Report Definitions > Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - FortiADC Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



☐	Title		Category	Preview
☐	Template - DNS Report	DNS activity on the network.	System	HTML PDF
☐	Template - DNS Security Report	DNS Security.	Security	HTML PDF
☐	Template - Email Report	ents by Total Number and Size of emails.	Security	HTML PDF
☐	Template - Endpoint Sandbox Detections Report	the APT threats deteted by sandbox	FortiSandbox	HTML PDF
☑	Template - FortiADC Report	report about FortiADC analysis.	FortiADC	HTML PDF
☐	Template - FortiCache Default Report	s, cache rate, traffic and request timeline. Top 20 websites by bandwidth, bandwidth savings, cac	FortiCache	HTML PDF
☐	Template - FortiCache Security Analysis		FortiCache	HTML PDF
☐	Template - FortiCache Web Usage Report		FortiCache	HTML PDF
☐	Template - FortiClient Default Report	n, OS, Device, FCT version and client summary. Threat summary by AV threats, infected devices,	FortiClient	HTML PDF
☐	Template - FortiClient Default Report from FortiGa	n, OS, Device, FCT version and client summary. Threat summary by AV threats, infected devices,	Security	HTML PDF

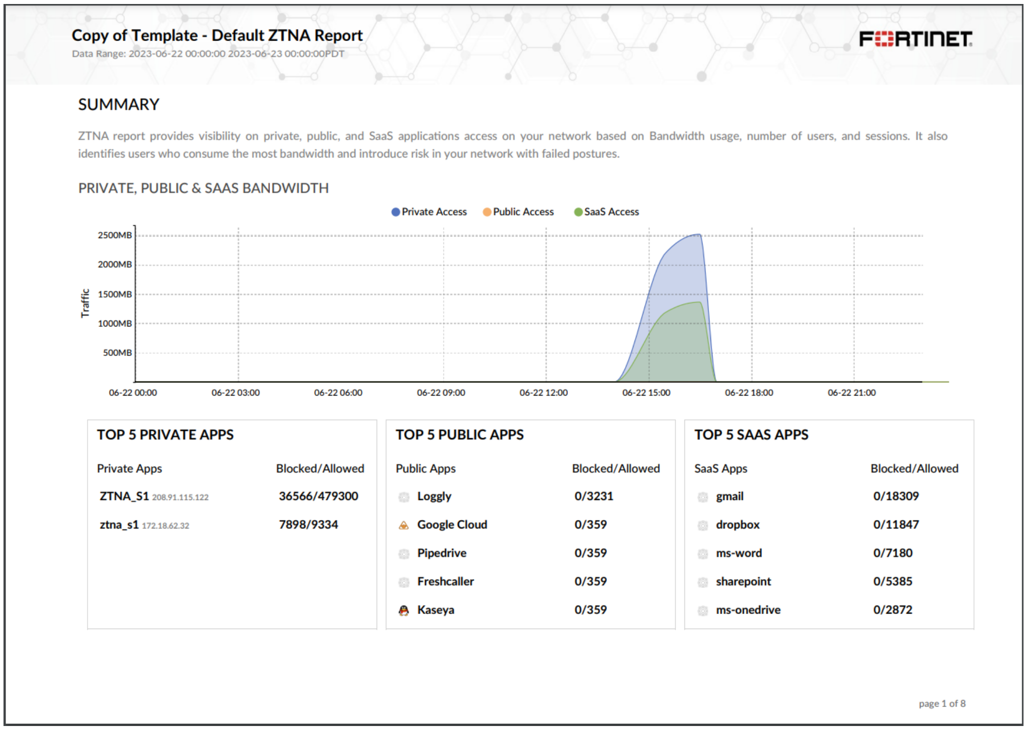
To run the FortiADC Report:

1. Go to *Reports > Report Definitions > All Reports*, and double-click the row for the *FortiADC Report*.
   The *Edit: FortiADC Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

ZTNA Report - 7.4.1

The *Default ZTNA Report* is now available on FortiAnalyzer to enhance visibility in terms of applications being used with the corresponding bandwidth used and sessions. To better differentiate accessibility and deployments, applications are grouped as private, public, and SaaS. Users that present security risks due to failing security postures can be quickly identified.

For example, see a sample of page 1 from the report in PDF format below.



Copy of Template - Default ZTNA Report

Data Range: 2023-06-22 00:00:00 2023-06-23 00:00:00PDT

SUMMARY

ZTNA report provides visibility on private, public, and SaaS applications access on your network based on Bandwidth usage, number of users, and sessions. It also identifies users who consume the most bandwidth and introduce risk in your network with failed postures.

PRIVATE, PUBLIC & SAAS BANDWIDTH

TOP 5 PRIVATE APPS

Private Apps	Blocked/Allowed
ZTNA_S1 208.91.115.122	36566/479300
ztna_s1 172.18.62.32	7898/9334

TOP 5 PUBLIC APPS

Public Apps	Blocked/Allowed
Loggly	0/3231
Google Cloud	0/359
Pipedrive	0/359
Freshcaller	0/359
Kaseya	0/359

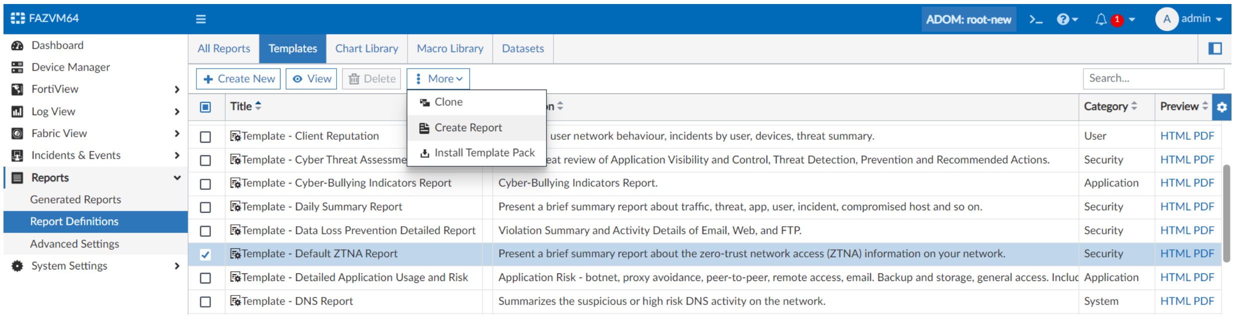
TOP 5 SAAS APPS

SaaS Apps	Blocked/Allowed
gmail	0/18309
dropbox	0/11847
ms-word	0/7180
sharepoint	0/5385
ms-onedrive	0/2872

page 1 of 8

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Default ZTNA Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



☐	Title	n	Category	Preview
☐	Template - Client Reputation	user network behaviour, incidents by user, devices, threat summary.	User	HTML PDF
☐	Template - Cyber Threat Assessme	eat review of Application Visibility and Control, Threat Detection, Prevention and Recommended Actions.	Security	HTML PDF
☐	Template - Cyber-Bullying Indicators Report	Cyber-Bullying Indicators Report.	Application	HTML PDF
☐	Template - Daily Summary Report	Present a brief summary report about traffic, threat, app, user, incident, compromised host and so on.	Security	HTML PDF
☐	Template - Data Loss Prevention Detailed Report	Violation Summary and Activity Details of Email, Web, and FTP.	Security	HTML PDF
☑	Template - Default ZTNA Report	Present a brief summary report about the zero-trust network access (ZTNA) information on your network.	Security	HTML PDF
☐	Template - Detailed Application Usage and Risk	Application Risk - botnet, proxy avoidance, peer-to-peer, remote access, email. Backup and storage, general access. Incluc	Application	HTML PDF
☐	Template - DNS Report	Summarizes the suspicious or high risk DNS activity on the network.	System	HTML PDF

To run the Default ZTNA Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *Default ZTNA Report*.
   The *Edit: Default ZTNA Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

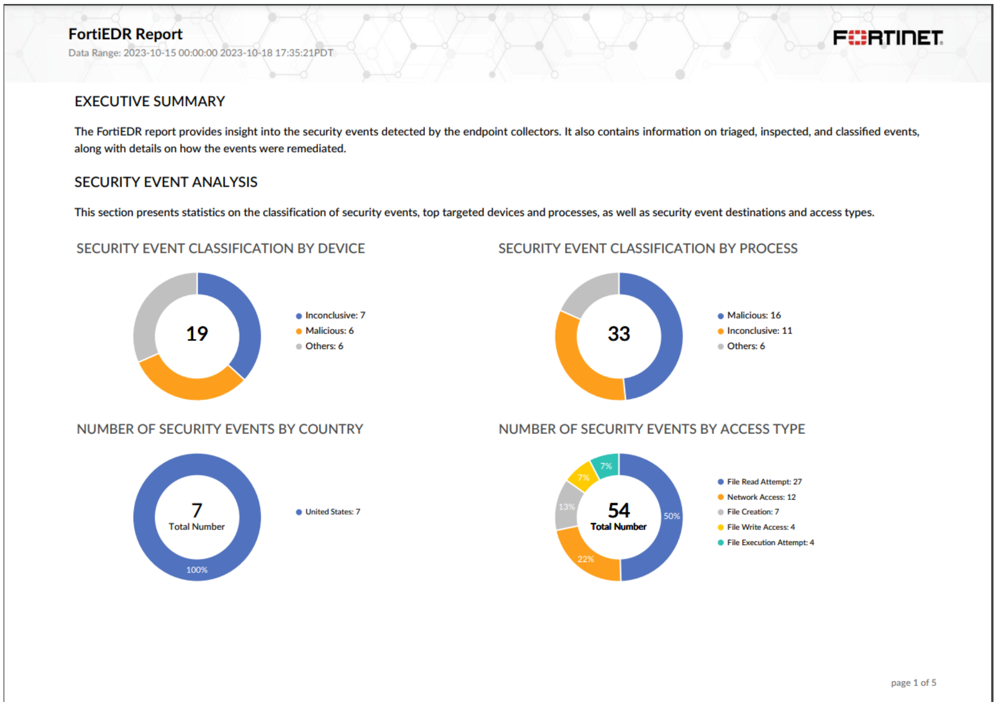
FortiEDR Report - 7.4.1

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- List of Report Templates

A FortiEDR report is available on FortiAnalyzer to provide insight into the security events detected by the endpoint collectors. It also contains information on triaged, inspected, and classified events, along with details on how the events were remediated.

For example, see a sample of page 1 from the report in PDF format below.



FortiEDR Report

Data Range: 2023-10-15 00:00:00 2023-10-18 17:35:21PDT

EXECUTIVE SUMMARY

The FortiEDR report provides insight into the security events detected by the endpoint collectors. It also contains information on triaged, inspected, and classified events, along with details on how the events were remediated.

SECURITY EVENT ANALYSIS

This section presents statistics on the classification of security events, top targeted devices and processes, as well as security event destinations and access types.

SECURITY EVENT CLASSIFICATION BY DEVICE

SECURITY EVENT CLASSIFICATION BY PROCESS

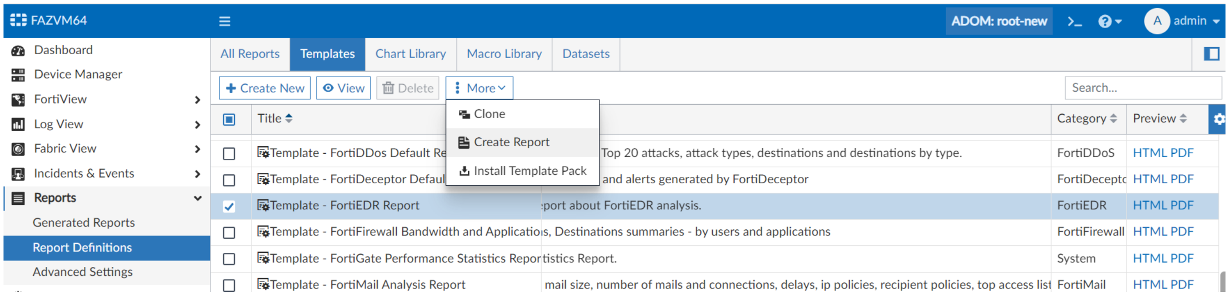
NUMBER OF SECURITY EVENTS BY COUNTRY

NUMBER OF SECURITY EVENTS BY ACCESS TYPE

page 1 of 5

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - FortiEDR Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



	Title		Category	Preview
☐	Template - FortiDDos Default Re	Top 20 attacks, attack types, destinations and destinations by type.	FortiDDoS	HTML PDF
☐	Template - FortiDeceptor Defaul	and alerts generated by FortiDeceptor	FortiDeceptc	HTML PDF
☑	Template - FortiEDR Report	:port about FortiEDR analysis.	FortiEDR	HTML PDF
☐	Template - FortiFirewall Bandwidth and Applicatio	s, Destinations summaries - by users and applications	FortiFirewall	HTML PDF
☐	Template - FortiGate Performance Statistics Repor	tistics Report.	System	HTML PDF
☐	Template - FortiMail Analysis Report	mail size, number of mails and connections, delays, ip policies, recipient policies, top access list	FortiMail	HTML PDF

To run the FortiEDR Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *FortEDR Report*.
   The *Edit: FortiEDR Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

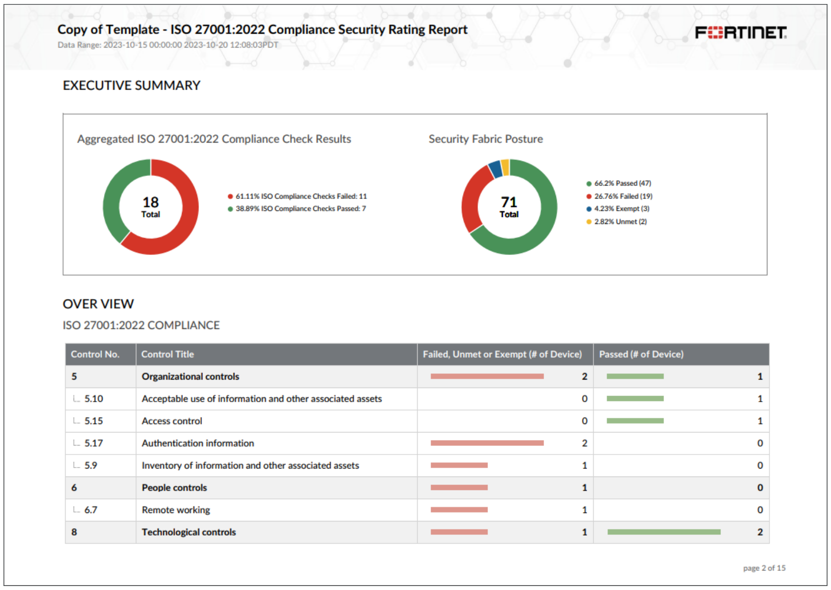
ISO 27001:2022 Compliance Security Rating Report - 7.4.1

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- List of Report Templates

FortiAnalyzer v7.4.1 includes an *ISO 27001:2022 Compliance Security Rating Report* to help customers optimize their deployed FortiGates and other fabric devices to be aligned with the technical requirements of common industry compliance framework.

For example, see a sample of page 2 from the report in PDF format below.



Copy of Template - ISO 27001:2022 Compliance Security Rating Report

Data Range: 2023-10-15 00:00:00 2023-10-20 12:08:03PDT

EXECUTIVE SUMMARY

FORTINET
Aggregated ISO 27001:2022 Compliance Check Results
18
Total
61.11% ISO Compliance Checks Failed: 11
38.89% ISO Compliance Checks Passed: 7
Security Fabric Posture
71
Total
66.2% Passed (47)
26.76% Failed (19)
4.23% Exempt (3)
2.82% Unmet (2)

OVER VIEW

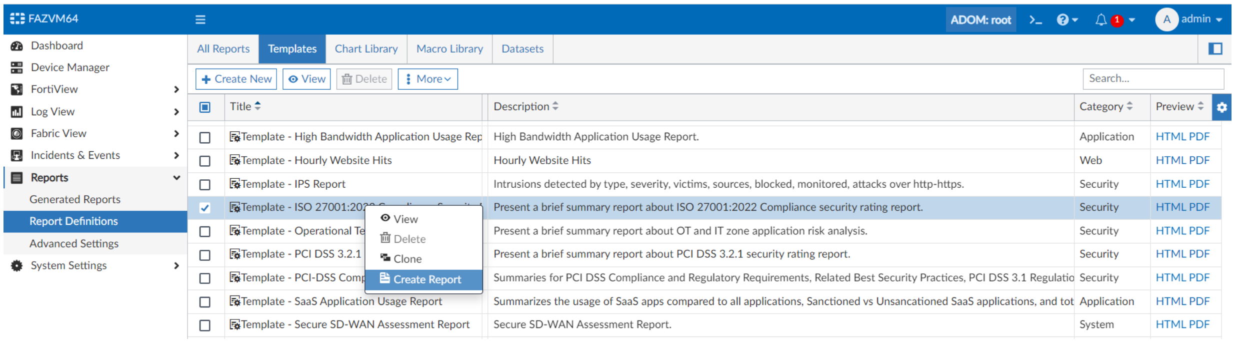
ISO 27001:2022 COMPLIANCE

Control No.	Control Title	Failed, Unmet or Exempt (# of Device)	Passed (# of Device)
5	**Organizational controls**	2	1
└ 5.10	Acceptable use of information and other associated assets	0	1
└ 5.15	Access control	0	1
└ 5.17	Authentication information	2	0
└ 5.9	Inventory of information and other associated assets	1	0
6	**People controls**	1	0
└ 6.7	Remote working	1	0
8	**Technological controls**	1	2

page 2 of 15

To create the report from the template:

1. Go to *Reports > Report Definitions > Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - ISO 27001:2022 Compliance Security Rating Report* .
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



☐	Title	Description	Category	Preview
☐	Template - High Bandwidth Application Usage Rep	High Bandwidth Application Usage Report.	Application	HTML PDF
☐	Template - Hourly Website Hits	Hourly Website Hits	Web	HTML PDF
☐	Template - IPS Report	Intrusions detected by type, severity, victims, sources, blocked, monitored, attacks over http-https.	Security	HTML PDF
☑	Template - ISO 27001:20	Present a brief summary report about ISO 27001:2022 Compliance security rating report.	Security	HTML PDF
☐	Template - Operational Te	Present a brief summary report about OT and IT zone application risk analysis.	Security	HTML PDF
☐	Template - PCI DSS 3.2.1	Present a brief summary report about PCI DSS 3.2.1 security rating report.	Security	HTML PDF
☐	Template - PCI-DSS Comp	Summaries for PCI DSS Compliance and Regulatory Requirements, Related Best Security Practices, PCI DSS 3.1 Regulatio	Security	HTML PDF
☐	Template - SaaS Application Usage Report	Summarizes the usage of SaaS apps compared to all applications, Sanctioned vs Unsancationed SaaS applications, and tot	Application	HTML PDF
☐	Template - Secure SD-WAN Assessment Report	Secure SD-WAN Assessment Report.	System	HTML PDF

To run the ISO 27001:2022 Compliance Security Rating Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *ISO 27001:2022 Compliance Security Rating Report* .
   The *Edit: ISO 27001:2022 Compliance Security Rating Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Exporting a report with settings - 7.4.1

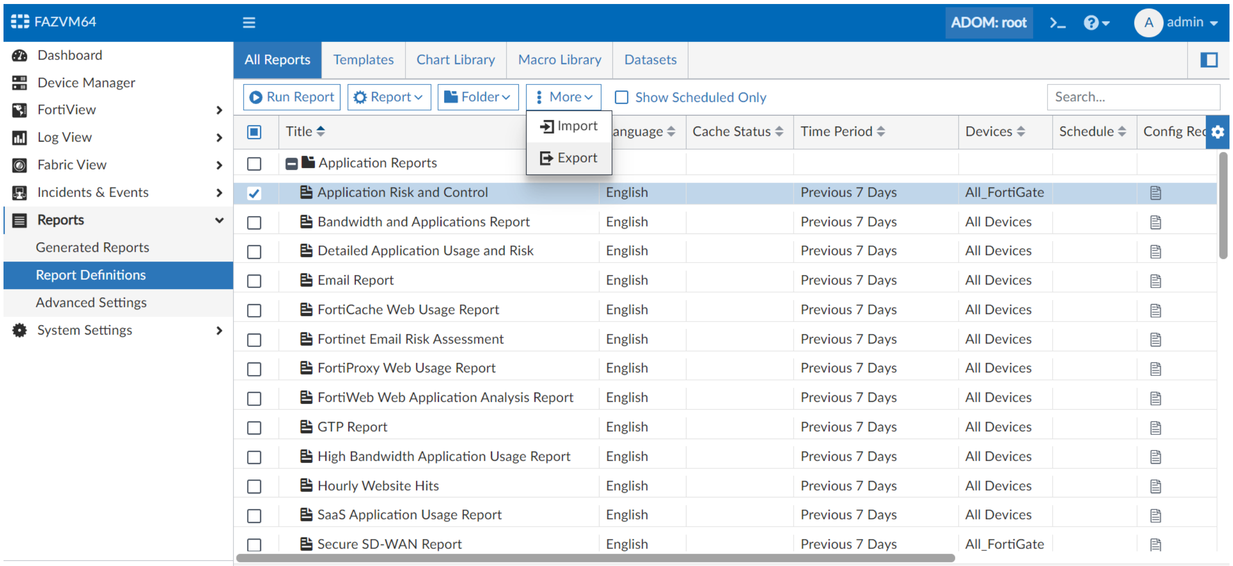
This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Importing and exporting reports

In FortiAnalyzer 7.4.1, the report settings, subnets, LDAP server, and output profile configurations are included in exported report files. You can then import the report file, including the configurations, to another FortiAnalyzer unit or ADOM.

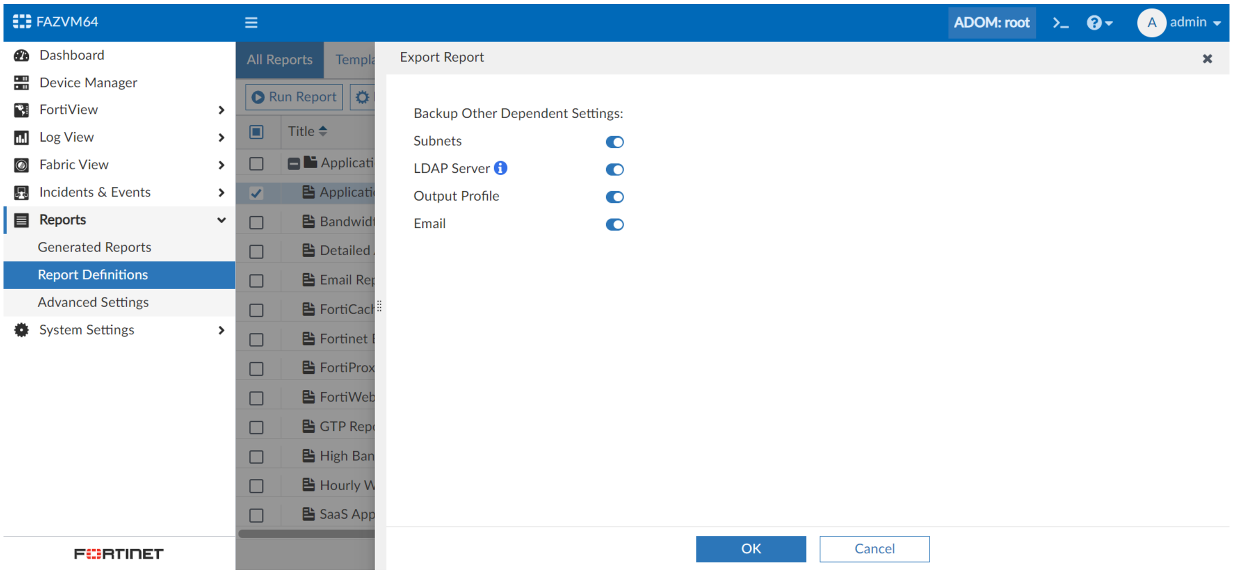
To export a report:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. Select a report, and click *More* > *Export*.
   In this example, the admin is exporting the `Application Risk and Control` report.



☐	Title	Language	Cache Status	Time Period	Devices	Schedule	Config Rec
☐	Application Reports						
☑	Application Risk and Control	English		Previous 7 Days	All_FortiGate		🗎
☐	Bandwidth and Applications Report	English		Previous 7 Days	All Devices		🗎
☐	Detailed Application Usage and Risk	English		Previous 7 Days	All Devices		🗎
☐	Email Report	English		Previous 7 Days	All Devices		🗎
☐	FortiCache Web Usage Report	English		Previous 7 Days	All Devices		🗎
☐	Fortinet Email Risk Assessment	English		Previous 7 Days	All Devices		🗎
☐	FortiProxy Web Usage Report	English		Previous 7 Days	All Devices		🗎
☐	FortiWeb Web Application Analysis Report	English		Previous 7 Days	All Devices		🗎
☐	GTP Report	English		Previous 7 Days	All Devices		🗎
☐	High Bandwidth Application Usage Report	English		Previous 7 Days	All Devices		🗎
☐	Hourly Website Hits	English		Previous 7 Days	All Devices		🗎
☐	SaaS Application Usage Report	English		Previous 7 Days	All Devices		🗎
☐	Secure SD-WAN Report	English		Previous 7 Days	All_FortiGate		🗎

The *Export Report* pane displays.



Export Report

Backup Other Dependent Settings:

Subnets

LDAP Server

Output Profile

Email

4. Use the toggles to *Backup Other Dependent Settings* in the exported file, as needed:
   - *Subnets*
   - *LDAP Server* (the export will remove the ADOM setting from the LDAP configuration)
   - *Output Profile*
   - *Email*

   By default, all of these options are disabled.
5. Click *OK* to export the report.

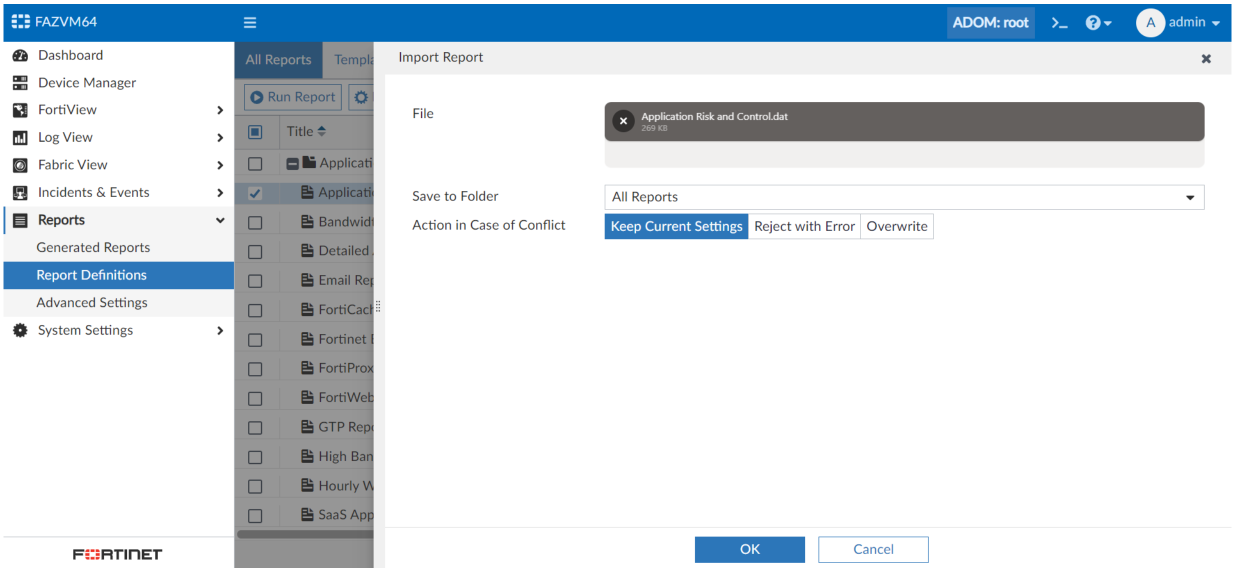
   The report configuration is saved as a .dat file on the management computer. This includes the charts, datasets, images, and report settings.

To import a report:

1. If using ADOMs, ensure that you are in the correct ADOM.

   If the device type used in the charts and datasets for the report does not match the ADOM type, the import will be rejected with an error. For more information, see How ADOMs affect reports in the FortiAnalyzer Administration Guide.
2. Go to *Reports > Report Definitions > All Reports*.
3. Click *More > Import*.

   The *Import Report* pane displays.



Import Report

File: Application Risk and Control.dat 269 KB

Save to Folder: All Reports

Action in Case of Conflict: [✓ Keep Current Settings] Reject with Error Overwrite

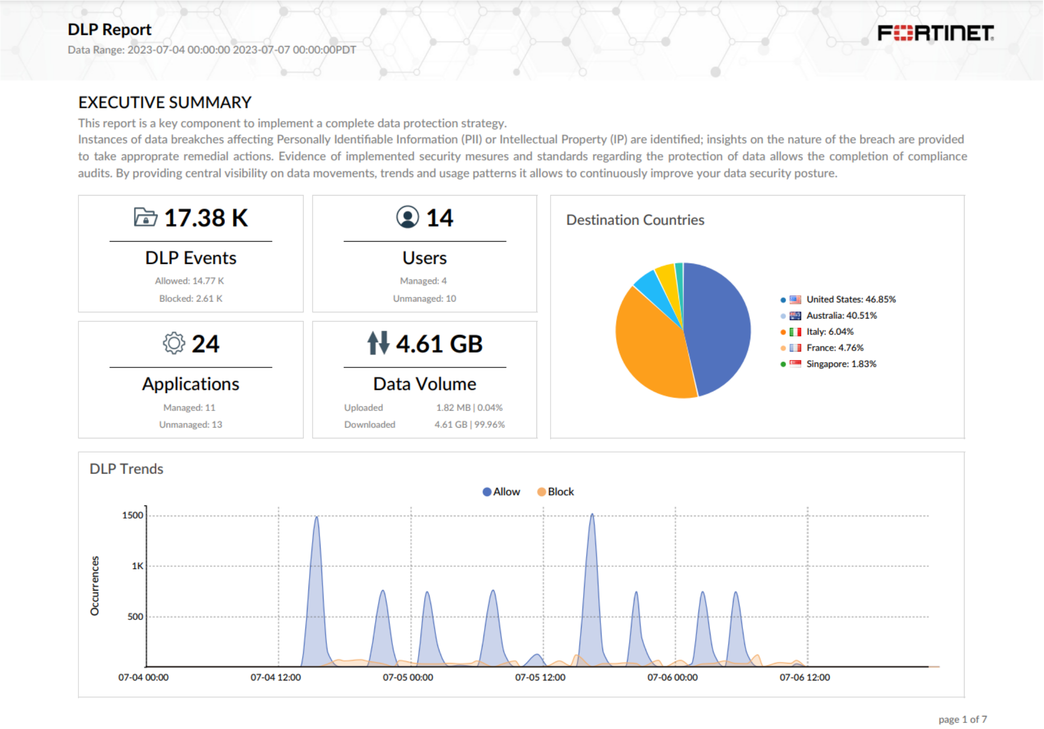
4. In the *File* field, drag and drop the .dat report file, or click *Browse* and select the file.

   In the example pictured above, the admin is importing the previously exported `Application Risk and Control` report.
5. From the *Save to Folder* dropdown, select the folder to save the report in.
6. Select the *Action in Case of Conflict*:
   - *Keep Current Settings* (default)
   - *Reject with Error*
   - *Overwrite*
7. Click *OK* to import the report.

DLP report - 7.4.1

A *DLP Report* is available on FortiAnalyzer to enhance visibility and to implement a comprehensive data protection policy.

For example, see a sample of page 1 from the report in PDF format below.



DLP Report
Data Range: 2023-07-04 00:00:00 2023-07-07 00:00:00PDT

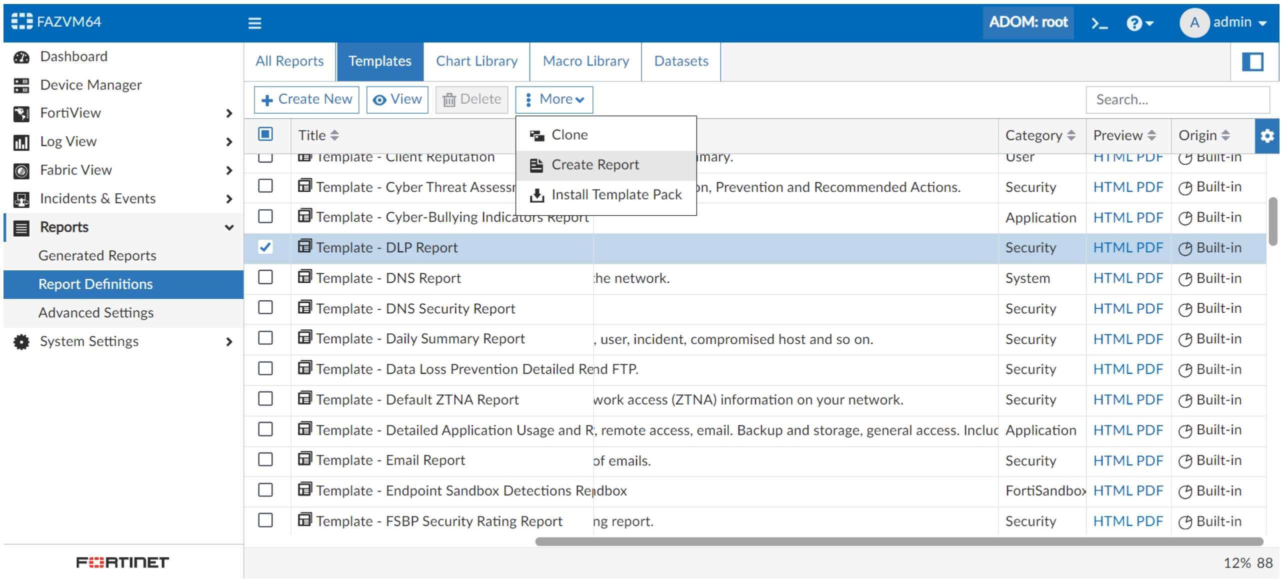
EXECUTIVE SUMMARY

This report is a key component to implement a complete data protection strategy.
Instances of data breakches affecting Personally Identifiable Information (PII) or Intellectual Property (IP) are identified; insights on the nature of the breach are provided to take approprate remedial actions. Evidence of implemented security mesures and standards regarding the protection of data allows the completion of compliance audits. By providing central visibility on data movements, trends and usage patterns it allows to continuously improve your data security posture.

17.38 K DLP Events Allowed: 14.77 K Blocked: 2.61 K	14 Users Managed: 4 Unmanaged: 10
24 Applications Managed: 11 Unmanaged: 13	4.61 GB Data Volume Uploaded 1.82 MB | 0.04% Downloaded 4.61 GB | 99.96%

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - DLP Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



☐	Title		Category	Preview	Origin
☐	Template - Client Reputation	mary.	User	HTML PDF	Built-in
☐	Template - Cyber Threat Assessr	on, Prevention and Recommended Actions.	Security	HTML PDF	Built-in
☐	Template - Cyber-Bullying Indicators Report		Application	HTML PDF	Built-in
☑	Template - DLP Report		Security	HTML PDF	Built-in
☐	Template - DNS Report	he network.	System	HTML PDF	Built-in
☐	Template - DNS Security Report		Security	HTML PDF	Built-in
☐	Template - Daily Summary Report	, user, incident, compromised host and so on.	Security	HTML PDF	Built-in
☐	Template - Data Loss Prevention Detailed Re	nd FTP.	Security	HTML PDF	Built-in
☐	Template - Default ZTNA Report	work access (ZTNA) information on your network.	Security	HTML PDF	Built-in
☐	Template - Detailed Application Usage and R	, remote access, email. Backup and storage, general access. Incluc	Application	HTML PDF	Built-in
☐	Template - Email Report	of emails.	Security	HTML PDF	Built-in
☐	Template - Endpoint Sandbox Detections Re	dbox	FortiSandbox	HTML PDF	Built-in
☐	Template - FSBP Security Rating Report	ng report.	Security	HTML PDF	Built-in

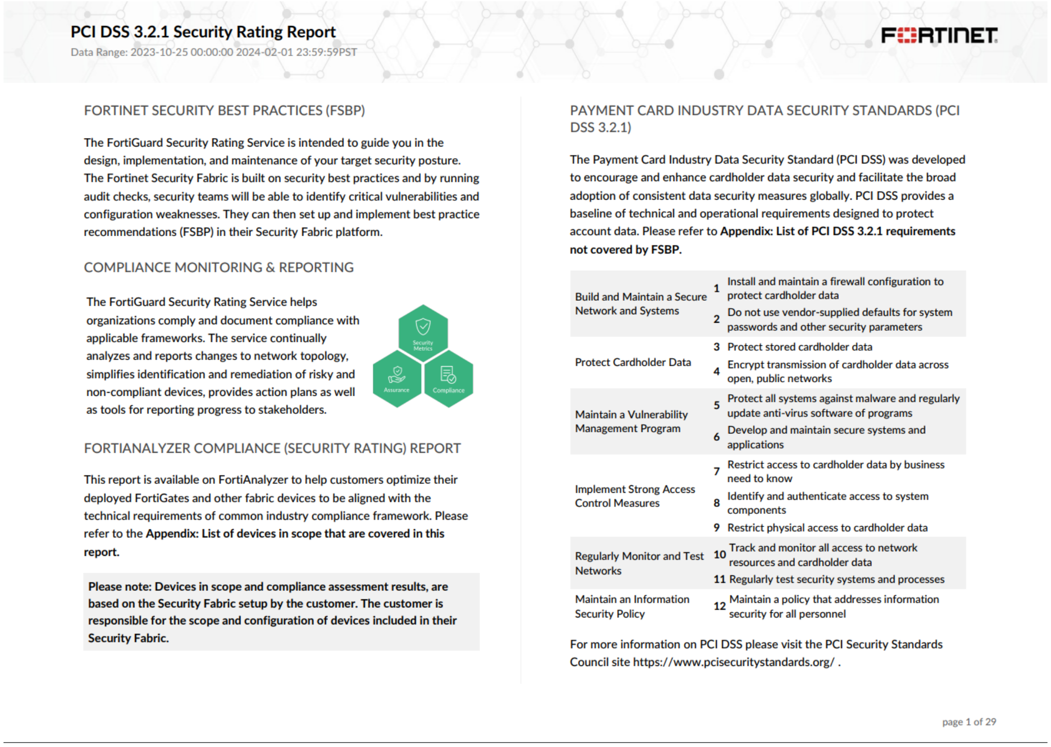
To run the DLP Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *DLP Report*.
   The *Edit: DLP Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

PCI DSS security rating report update - 7.4.1

The PCI DSS report has been updated to match the PCI DSS 3.2.1 requirements. It is now call the *PCI DSS Security Rating Report*.

For example, see a sample of page 1 and 2 from the report in PDF format below.



PCI DSS 3.2.1 Security Rating Report

Data Range: 2023-10-25 00:00:00 2024-02-01 23:59:59PST

FORTINET SECURITY BEST PRACTICES (FSBP)

The FortiGuard Security Rating Service is intended to guide you in the design, implementation, and maintenance of your target security posture. The Fortinet Security Fabric is built on security best practices and by running audit checks, security teams will be able to identify critical vulnerabilities and configuration weaknesses. They can then set up and implement best practice recommendations (FSBP) in their Security Fabric platform.

COMPLIANCE MONITORING & REPORTING

The FortiGuard Security Rating Service helps organizations comply and document compliance with applicable frameworks. The service continually analyzes and reports changes to network topology, simplifies identification and remediation of risky and non-compliant devices, provides action plans as well as tools for reporting progress to stakeholders.

FORTIANALYZER COMPLIANCE (SECURITY RATING) REPORT

This report is available on FortiAnalyzer to help customers optimize their deployed FortiGates and other fabric devices to be aligned with the technical requirements of common industry compliance framework. Please refer to the **Appendix: List of devices in scope that are covered in this report.**

Please note: Devices in scope and compliance assessment results, are based on the Security Fabric setup by the customer. The customer is responsible for the scope and configuration of devices included in their Security Fabric.

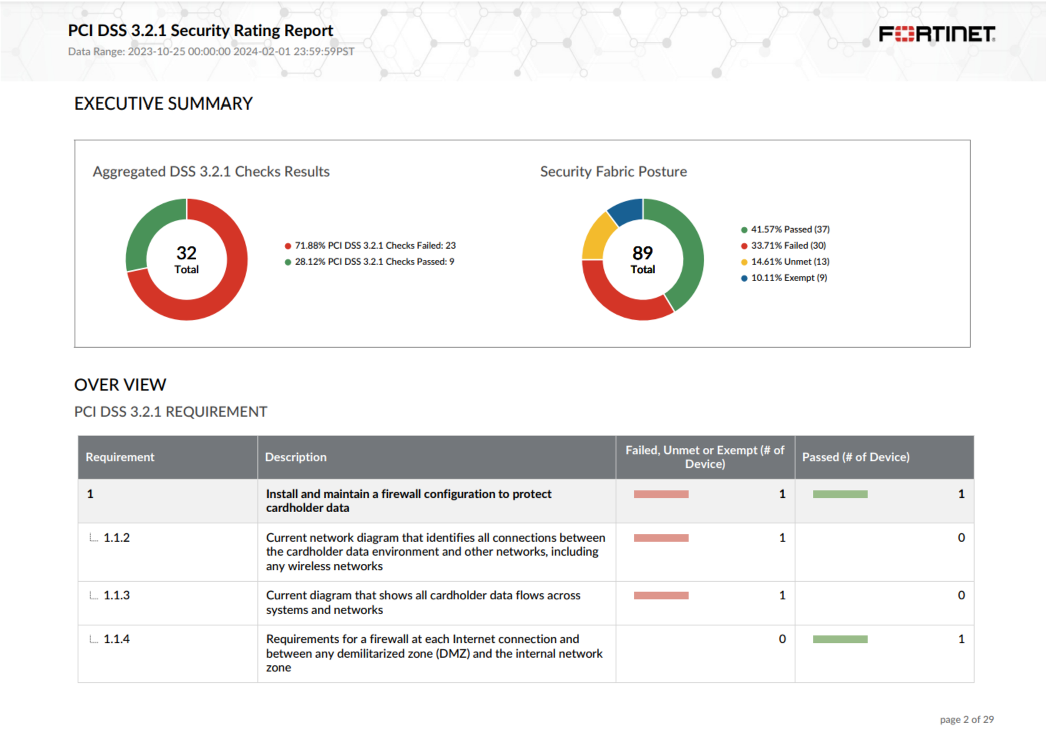
PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS 3.2.1)

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. Please refer to **Appendix: List of PCI DSS 3.2.1 requirements not covered by FSBP.**

Build and Maintain a Secure Network and Systems	1	Install and maintain a firewall configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5	Protect all systems against malware and regularly update anti-virus software of programs
	6	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7	Restrict access to cardholder data by business need to know
	8	Identify and authenticate access to system components
	9	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an Information Security Policy	12	Maintain a policy that addresses information security for all personnel

For more information on PCI DSS please visit the PCI Security Standards Council site https://www.pcisecuritystandards.org/ .

page 1 of 29



PCI DSS 3.2.1 Security Rating Report

Data Range: 2023-10-25 00:00:00 2024-02-01 23:59:59PST

EXECUTIVE SUMMARY

Aggregated DSS 3.2.1 Checks Results

32
Total
71.88% PCI DSS 3.2.1 Checks Failed: 23
28.12% PCI DSS 3.2.1 Checks Passed: 9

Security Fabric Posture

OVER VIEW

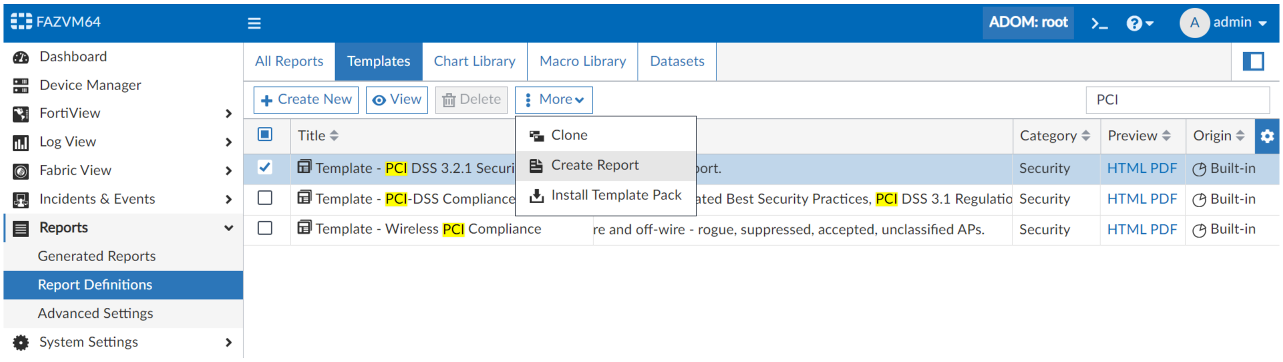
PCI DSS 3.2.1 REQUIREMENT

Requirement	Description	Failed, Unmet or Exempt (# of Device)	Passed (# of Device)
1	**Install and maintain a firewall configuration to protect cardholder data**	**1**	**1**
1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1	0
1.1.3	Current diagram that shows all cardholder data flows across systems and networks	1	0
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	0	1

page 2 of 29

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - PCI DSS 3.2.1 Security Rating Report*.
3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



	Title		Category	Preview	Origin
☑	Template - PCI DSS 3.2.1 Securi	ort.	Security	HTML PDF	Built-in
☐	Template - PCI-DSS Compliance	ated Best Security Practices, PCI DSS 3.1 Regulatio	Security	HTML PDF	Built-in
☐	Template - Wireless PCI Compliance	re and off-wire - rogue, suppressed, accepted, unclassified APs.	Security	HTML PDF	Built-in

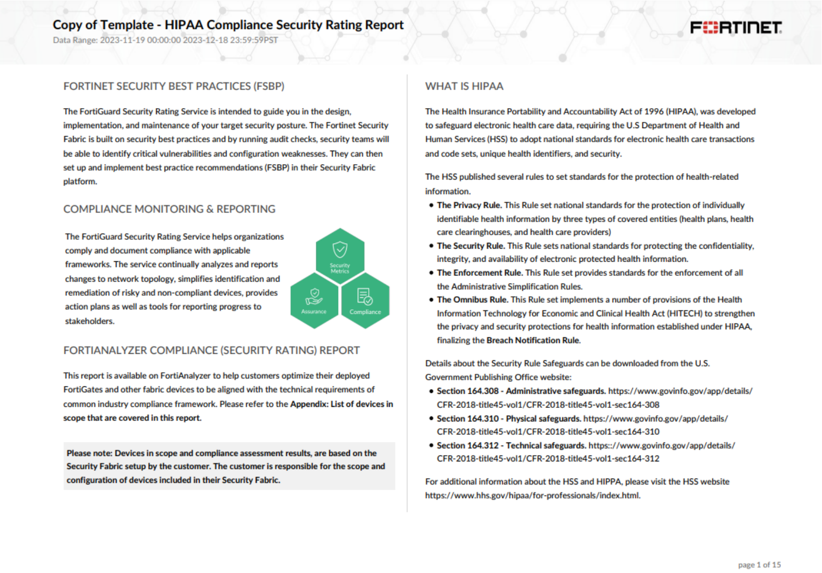
To run the PCI DSS 3.2.1 Security Rating Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *PCI DSS 3.2.1 Security Rating Report*.
   The *Edit: PCI DSS 3.2.1 Security Rating Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

HIPAA report - 7.4.2

The *HIPAA Compliance Security Rating Report* is now available on FortiAnalyzer to provide a security and compliance posture assessment of the security fabric against HIPAA compliance requirements.

For example, see a sample of page 1 and 2 from the report in PDF format below.



Copy of Template - HIPAA Compliance Security Rating Report
Data Range: 2023-11-19 00:00:00 2023-12-18 23:59:59PST

FORTINET SECURITY BEST PRACTICES (FSBP)

The FortiGuard Security Rating Service is intended to guide you in the design, implementation, and maintenance of your target security posture. The Fortinet Security Fabric is built on security best practices and by running audit checks, security teams will be able to identify critical vulnerabilities and configuration weaknesses. They can then set up and implement best practice recommendations (FSBP) in their Security Fabric platform.

COMPLIANCE MONITORING & REPORTING

The FortiGuard Security Rating Service helps organizations comply and document compliance with applicable frameworks. The service continually analyzes and reports changes to network topology, simplifies identification and remediation of risky and non-compliant devices, provides action plans as well as tools for reporting progress to stakeholders.

FORTIANALYZER COMPLIANCE (SECURITY RATING) REPORT

This report is available on FortiAnalyzer to help customers optimize their deployed FortiGates and other fabric devices to be aligned with the technical requirements of common industry compliance framework. Please refer to the **Appendix: List of devices in scope that are covered in this report.**

Please note: Devices in scope and compliance assessment results, are based on the Security Fabric setup by the customer. The customer is responsible for the scope and configuration of devices included in their Security Fabric.

WHAT IS HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), was developed to safeguard electronic health care data, requiring the U.S Department of Health and Human Services (HSS) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security.

The HSS published several rules to set standards for the protection of health-related information.

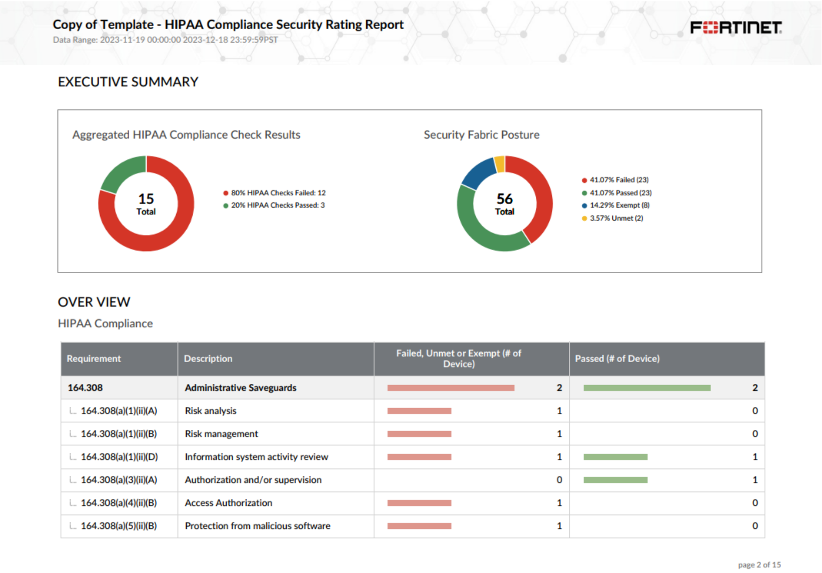
- **The Privacy Rule.** This Rule set national standards for the protection of individually identifiable health information by three types of covered entities (health plans, health care clearinghouses, and health care providers)
- **The Security Rule.** This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information.
- **The Enforcement Rule.** This Rule set provides standards for the enforcement of all the Administrative Simplification Rules.
- **The Omnibus Rule.** This Rule set implements a number of provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH) to strengthen the privacy and security protections for health information established under HIPAA, finalizing the **Breach Notification Rule**.

Details about the Security Rule Safeguards can be downloaded from the U.S. Government Publishing Office website:

- **Section 164.308 - Administrative safeguards.** https://www.govinfo.gov/app/details/CFR-2018-title45-vol1/CFR-2018-title45-vol1-sec164-308
- **Section 164.310 - Physical safeguards.** https://www.govinfo.gov/app/details/CFR-2018-title45-vol1/CFR-2018-title45-vol1-sec164-310
- **Section 164.312 - Technical safeguards.** https:://www.govinfo.gov/app/details/CFR-2018-title45-vol1/CFR-2018-title45-vol1-sec164-312

For additional information about the HSS and HIPPA, please visit the HSS website https://www.hhs.gov/hipaa/for-professionals/index.html.

page 1 of 15



Copy of Template - HIPAA Compliance Security Rating Report
Data Range: 2023-11-19 00:00:00 2023-12-18 23:59:59PST

EXECUTIVE SUMMARY

Aggregated HIPAA Compliance Check Results

- 🟥 80% HIPAA Checks Failed: 12
- 🟩 20% HIPAA Checks Passed: 3

Security Fabric Posture

- 🟥 41.07% Failed (23)
- 🟩 41.07% Passed (23)
- 🟦 14.29% Exempt (8)
- 🟨 3.57% Unmet (2)

OVER VIEW

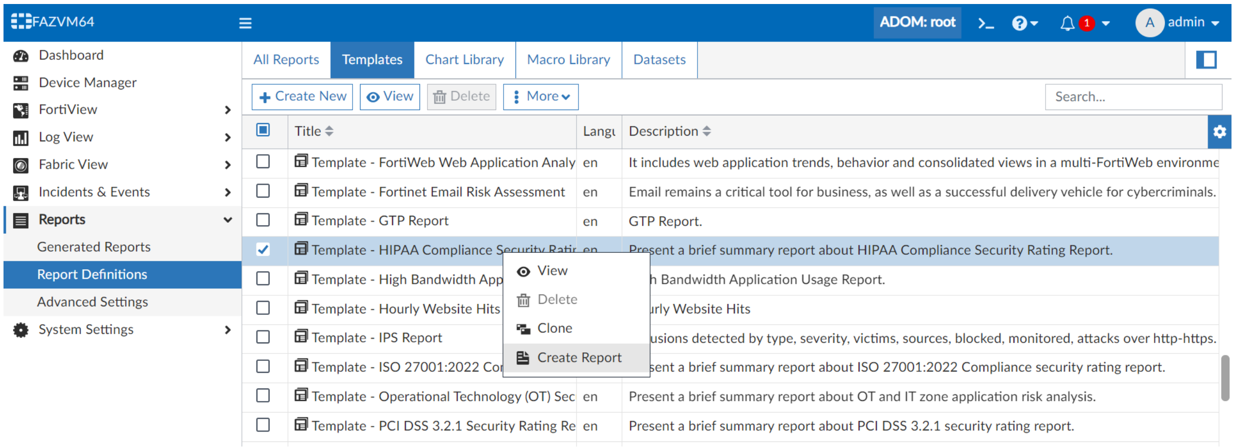
HIPAA Compliance

Requirement	Description	Failed, Unmet or Exempt (# of Device)	Passed (# of Device)
164.308	**Administrative Saveguards**	**2**	**2**
└ 164.308(a)(1)(ii)(A)	Risk analysis	1	0
└ 164.308(a)(1)(ii)(B)	Risk management	1	0
└ 164.308(a)(1)(ii)(D)	Information system activity review	1	1
└ 164.308(a)(3)(ii)(A)	Authorization and/or supervision	0	1
└ 164.308(a)(4)(ii)(B)	Access Authorization	1	0
└ 164.308(a)(5)(ii)(B)	Protection from malicious software	1	0

page 2 of 15

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - HIPAA Compliance Security Rating Report*.
3. Right-click the report and select *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.



	Title	Langu	Description
□	Template - FortiWeb Web Application Analy	en	It includes web application trends, behavior and consolidated views in a multi-FortiWeb environme
□	Template - Fortinet Email Risk Assessment	en	Email remains a critical tool for business, as well as a successful delivery vehicle for cybercriminals.
□	Template - GTP Report	en	GTP Report.
☑	Template - HIPAA Compliance Security Ratir	en	Present a brief summary report about HIPAA Compliance Security Rating Report.
□	Template - High Bandwidth App		h Bandwidth Application Usage Report.
□	Template - Hourly Website Hits		urly Website Hits
□	Template - IPS Report		usions detected by type, severity, victims, sources, blocked, monitored, attacks over http-https.
□	Template - ISO 27001:2022 Co		sent a brief summary report about ISO 27001:2022 Compliance security rating report.
□	Template - Operational Technology (OT) Sec	en	Present a brief summary report about OT and IT zone application risk analysis.
□	Template - PCI DSS 3.2.1 Security Rating Re	en	Present a brief summary report about PCI DSS 3.2.1 security rating report.

To run the report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *HIPAA Compliance Security Rating Report*.
   The *Edit: HIPAA Compliance Security Rating Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Others

This section lists the new features added to FortiAnalyzer for other topics relating to logging and reporting:

- Time zone settings per ADOMs/Reports on page 115
- New API to restore logs on page 118

Time zone settings per ADOMs/Reports

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

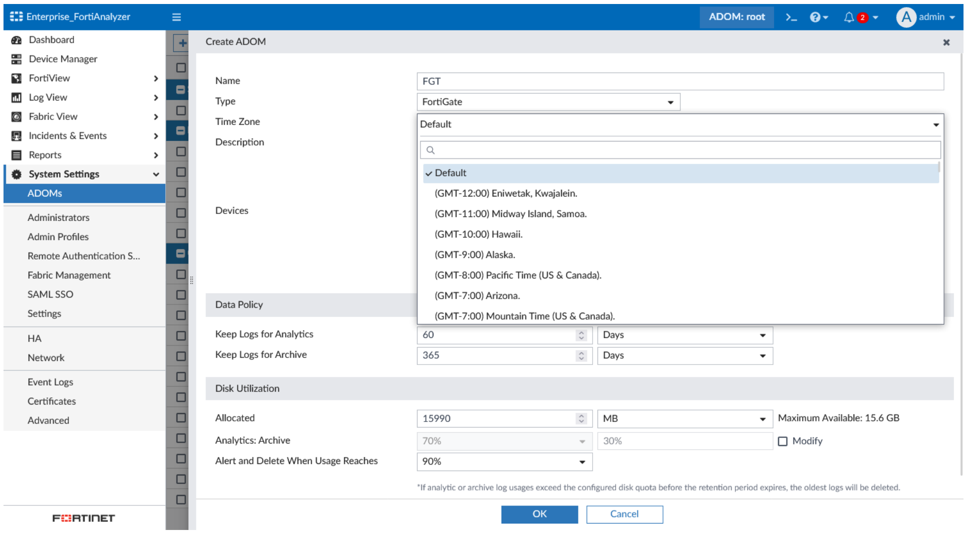
- Creating ADOMs
- Report Settings tab

To allow a more granular reporting experience for Global deployment, different timezones can be configured on each ADOM/Report.

The *Default* time zone used for this setting is the time zone set for the FortiAnalyzer.

To configure the time zone for an ADOM:

1. Go to *System Settings* > *ADOMs*.
2. Edit or create a new ADOM.
3. From the *Time Zone* dropdown, select a time zone for the ADOM.
   This time zone will be used when displaying data in *Log View* and *FortiView* for this ADOM.



Create ADOM

Name	FGT
Type	FortiGate
Time Zone	Default
Description	
Devices	

Time Zone list:
- ✓ Default
- (GMT-12:00) Eniwetak, Kwajalein.
- (GMT-11:00) Midway Island, Samoa.
- (GMT-10:00) Hawaii.
- (GMT-9:00) Alaska.
- (GMT-8:00) Pacific Time (US & Canada).
- (GMT-7:00) Arizona.
- (GMT-7:00) Mountain Time (US & Canada).

Data Policy

Keep Logs for Analytics	60	Days
Keep Logs for Archive	365	Days

Disk Utilization

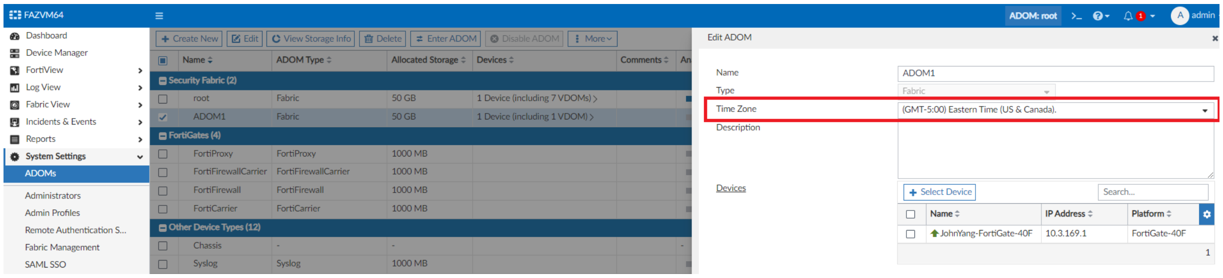
Allocated	15990	MB	Maximum Available: 15.6 GB
Analytics: Archive	70%	30%	□ Modify
Alert and Delete When Usage Reaches	90%		

*If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted.

4. Click *OK* to save.

Example:

In this example, the system time zone is (GMT-8:00) Pacific Time, which is used by the root ADOM. The admin creates a new adom (ADOM1) and sets the time zone to (GMT-5:00) Eastern Time:



	Name	ADOM Type	Allocated Storage	Devices	Comments
Security Fabric (2)					
□	root	Fabric	50 GB	1 Device (including 7 VDOMs)	
☑	ADOM1	Fabric	50 GB	1 Device (including 1 VDOM)	
FortiGates (4)					
□	FortiProxy	FortiProxy	1000 MB		
□	FortiFirewallCarrier	FortiFirewallCarrier	1000 MB		
□	FortiFirewall	FortiFirewall	1000 MB		
□	FortiCarrier	FortiCarrier	1000 MB		
Other Device Types (12)					
□	Chassis	-	-		
□	Syslog	Syslog	1000 MB		

Edit ADOM

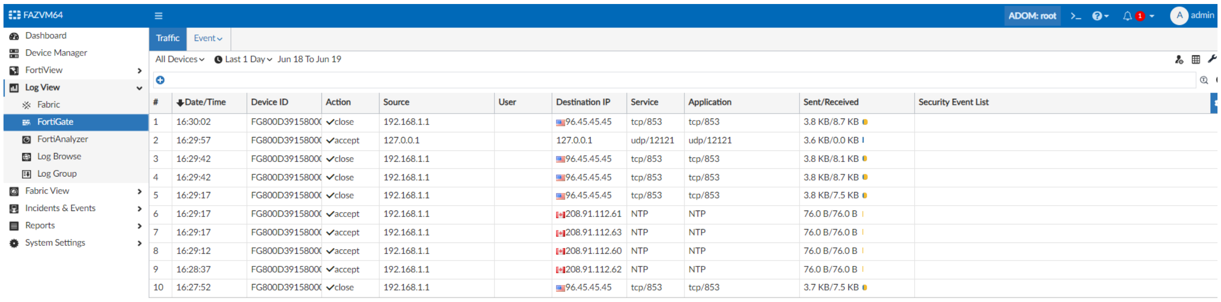
Name	ADOM1
Type	Fabric
Time Zone	(GMT-5:00) Eastern Time (US & Canada).
Description	
Devices	

	Name	IP Address	Platform
□	JohnYang-FortiGate-40F	10.3.169.1	FortiGate-40F

1

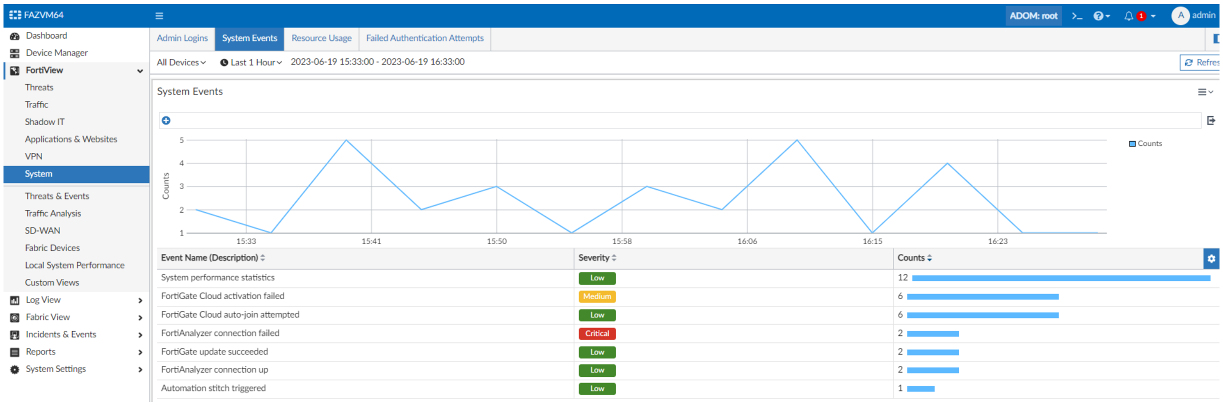
In the root ADOM, the *Log View*, *FortiView*, and *Generated Reports* panes are displayed according to the default system time zone: (GMT-8:00) Pacific Time.

For example, the admin is reviewing the panes below at approximately 16:30 Pacific Time.



All Devices · Last 1 Day · Jun 18 To Jun 19

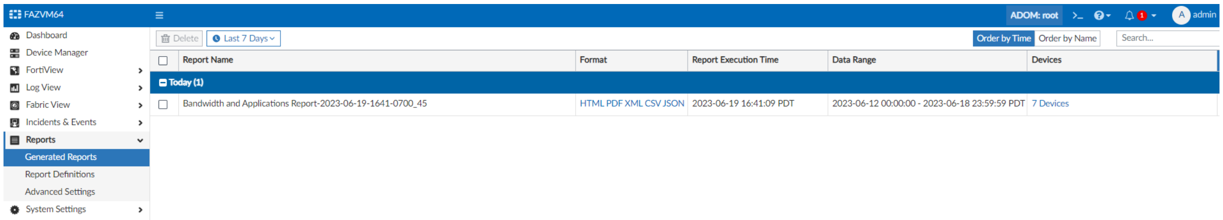
#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security Event List
1	16:30:02	FG800D3915800(	✓close	192.168.1.1		96.45.45.45	tcp/853	tcp/853	3.8 KB/8.7 KB	
2	16:29:57	FG800D3915800(	✓accept	127.0.0.1		127.0.0.1	udp/12121	udp/12121	3.6 KB/0.0 KB	
3	16:29:42	FG800D3915800(	✓close	192.168.1.1		96.45.45.45	tcp/853	tcp/853	3.8 KB/8.1 KB	
4	16:29:42	FG800D3915800(	✓close	192.168.1.1		96.45.45.45	tcp/853	tcp/853	3.8 KB/8.7 KB	
5	16:29:17	FG800D3915800(	✓close	192.168.1.1		96.45.45.45	tcp/853	tcp/853	3.8 KB/7.5 KB	
6	16:29:17	FG800D3915800(	✓accept	192.168.1.1		208.91.112.61	NTP	NTP	76.0 B/76.0 B	
7	16:29:17	FG800D3915800(	✓accept	192.168.1.1		208.91.112.63	NTP	NTP	76.0 B/76.0 B	
8	16:29:12	FG800D3915800(	✓accept	192.168.1.1		208.91.112.60	NTP	NTP	76.0 B/76.0 B	
9	16:28:37	FG800D3915800(	✓accept	192.168.1.1		208.91.112.62	NTP	NTP	76.0 B/76.0 B	
10	16:27:52	FG800D3915800(	✓close	192.168.1.1		96.45.45.45	tcp/853	tcp/853	3.7 KB/7.5 KB	



All Devices | Last 1 Hour | 2023-06-19 15:33:00 - 2023-06-19 16:33:00

System Events

Event Name (Description)	Severity	Counts
System performance statistics	Low	12
FortiGate Cloud activation failed	Medium	6
FortiGate Cloud auto-join attempted	Low	6
FortiAnalyzer connection failed	Critical	2
FortiGate update succeeded	Low	2
FortiAnalyzer connection up	Low	2
Automation stitch triggered	Low	1

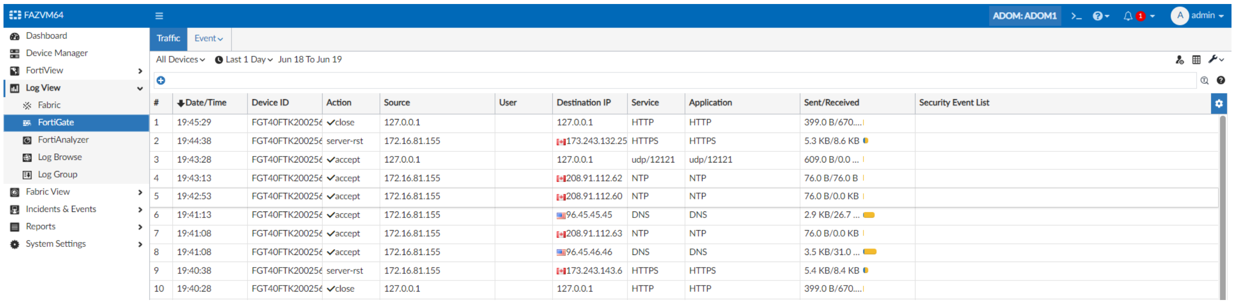


Last 7 Days

□	Report Name	Format	Report Execution Time	Data Range	Devices
Today (1)					
□	Bandwidth and Applications Report-2023-06-19-1641-0700_45	HTML PDF XML CSV JSON	2023-06-19 16:41:09 PDT	2023-06-12 00:00:00 - 2023-06-18 23:59:59 PDT	7 Devices

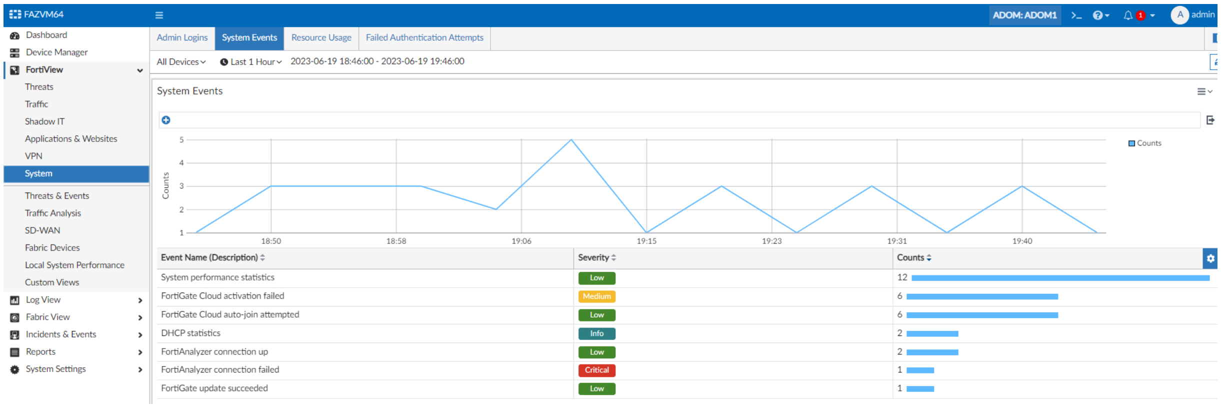
In ADOM1, the *Log View*, *FortiView*, and *Generated Reports* panes are displayed according the ADOM's specified time zone: (GMT-5:00) Eastern Time.

For example, the admin is reviewing the panes below at approximately 16:40 Pacific Time (19:40 Eastern Time).



All Devices | Last 1 Day | Jun 18 To Jun 19

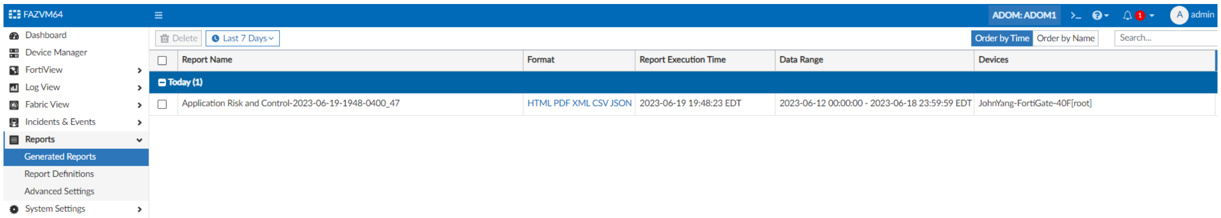
#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security Event List
1	19:45:29	FGT40FTK20025€	✓close	127.0.0.1		127.0.0.1	HTTP	HTTP	399.0 B/670....	
2	19:44:38	FGT40FTK20025€	server-rst	172.16.81.155		173.243.132.25	HTTPS	HTTPS	5.3 KB/8.6 KB	
3	19:43:28	FGT40FTK20025€	✓accept	127.0.0.1		127.0.0.1	udp/12121	udp/12121	609.0 B/0.0 ...	
4	19:43:13	FGT40FTK20025€	✓accept	172.16.81.155		208.91.112.62	NTP	NTP	76.0 B/76.0 B	
5	19:42:53	FGT40FTK20025€	✓accept	172.16.81.155		208.91.112.60	NTP	NTP	76.0 B/0.0 KB	
6	19:41:13	FGT40FTK20025€	✓accept	172.16.81.155		96.45.45.45	DNS	DNS	2.9 KB/26.7 ...	
7	19:41:08	FGT40FTK20025€	✓accept	172.16.81.155		208.91.112.63	NTP	NTP	76.0 B/0.0 KB	
8	19:41:08	FGT40FTK20025€	✓accept	172.16.81.155		96.45.46.46	DNS	DNS	3.5 KB/31.0 ...	
9	19:40:38	FGT40FTK20025€	server-rst	172.16.81.155		173.243.143.6	HTTPS	HTTPS	5.4 KB/8.4 KB	
10	19:40:28	FGT40FTK20025€	✓close	127.0.0.1		127.0.0.1	HTTP	HTTP	399.0 B/670....	



All Devices | Last 1 Hour | 2023-06-19 18:46:00 - 2023-06-19 19:46:00

System Events

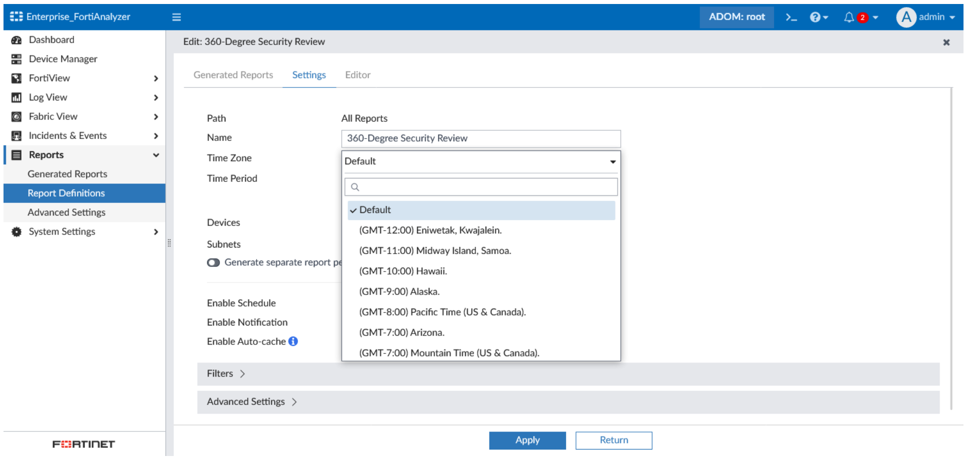
Event Name (Description)	Severity	Counts
System performance statistics	Low	12
FortiGate Cloud activation failed	Medium	6
FortiGate Cloud auto-join attempted	Low	6
DHCP statistics	Info	2
FortiAnalyzer connection up	Low	2
FortiAnalyzer connection failed	Critical	1
FortiGate update succeeded	Low	1



Report Name	Format	Report Execution Time	Data Range	Devices
Today (1)				
Application Risk and Control-2023-06-19-1948-0400_47	HTML PDF XML CSV JSON	2023-06-19 19:48:23 EDT	2023-06-12 00:00:00 - 2023-06-18 23:59:59 EDT	JohnYang-FortiGate-40F[root]

To configure the time zone for a report:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. Double-click the report, or right-click the report and select *Edit*.
3. Go to the *Settings* tab.
4. From the *Time Zone* dropdown, select a time zone to use for data in the report output.



Edit: 360-Degree Security Review

Path: All Reports
Name: 360-Degree Security Review
Time Zone: Default
Time Period

✓ Default
(GMT-12:00) Eniwetak, Kwajalein.
(GMT-11:00) Midway Island, Samoa.
(GMT-10:00) Hawaii.
(GMT-9:00) Alaska.
(GMT-8:00) Pacific Time (US & Canada).
(GMT-7:00) Arizona.
(GMT-7:00) Mountain Time (US & Canada).

5. Click *Apply* to save.

New API to restore logs

In FortiAnalyzer 7.4.0, a new JSON API endpoint has been created to allow logrestore:

```
/logview/logrestore
```

In addition, the `execute restore logs` command in the CLI is now a non-blocking task.

To implement non-blocking "restoring logs" via the CLI:

1. To run the "restoring logs" command via the CLI, enter the following command:

```
execute restore logs <device name(s)> {ftp | scp | sftp} <ip> <username> <password>
    <directory> [vdlist]
  Note: This command restores all logs from a specified server which were backed up
      prior to changing the RAID level or formatting the disks. Executing it
      frequently is not recommended!
  Do you want to continue? (y/n)y
  The restore operation will overwrite any logs already on the FortiAnalyzer.
  For following up:
    diagnose log restore status
    diagnose log restore cancel
```

2. To view the last log restore result or to check the status via the CLI, enter the following command:

```
diagnose log restore status
   Request for log restore for device "<device>" from IP "<IP>" at <date and time>
   Stopping processes.
   Downloading files for device <device>...
      Restore log file: <device>[root].dlog.1611248549.log.gz
      Restore log file: <device>[root].elog.1611250406.log.gz
      Restore log file: <device>[root].tlog.1611250406.log.gz
      Restore log file: <device>[root].vlog.1611250406.log.gz
      Restore log file: <device>[root].wlog.1611191194.log.gz
   Update device <device> log files disk usage...
   Restoration completed successfully.
   Recommend to rebuild log database by 'exec sql-local rebuild-db'.
   Restarting processes.
```

3. If the task is not complete yet, it can be stopped using the following command in the CLI:

```
diagnose log restore cancel
```

To implement "restoring logs" via the JSON API:

1. Add `logrestore` API:

```
request={
   'jsonrpc': '2.0',
   'params': [{
         'username': 'string',
         'service': 'ftp', 'filepath': 'string',
         'url': '/logview/logrestore', 'ip': 'ip_address',
         'logs-type': 'logs-only',
         'apiver': 3,
         'device': [{
            'devname': 'All_Device'
         }],
         'password': 'string'
      }],
      'id': '1',
      'method': 'add'
}
logs-type: logs-only logs-archive
   response={jsonrpc': '2.0', 'result': {'status': {'message': 'succeeded', 'code': 0},
         'reqid': xxxxx, u'logs-only': 0}, 'id': '1'}
```

2. Get `logrestore` status by reqid:

```
request={"jsonrpc": "2.0", "session": "<session>", "params": [{"url": "/logview/log
      restore/${reqid}", "apiver": 3}], "id": "1", "method": "get"}
The ${reqid} refer to the reqid in the response of "add logrestore".
response={
   "jsonrpc": "2.0", "result": {
   "task-status": "finished",
   "reqid": 1495138327,
   "data": {
         "message": "Request for log restore for device \"All_FortiGate\" from IP \"<ip
               address>\" at 2023-06-13 10:58:58\n\nStopping processes. \n\nDownloading
               files for device <device> (<device>[*])... \n No backup fi sk
               usage...\nDownloading files for device <device> (<device>[*])... \n No
               backup files for device <device>.\n\nUpdate device <device> log files disk
               usage...\nDownloading files for device <device> (F e device <device> log
               files disk usage...\nDownloading files for device <device> (<device>[*])...
               \n No backup files for device <device>. \n\nUpdate device <device> log
               files disk usage...\n\nRestora
         "device-result": {
            "device": [{
               "devid": "<device>",
               "status": "No backup files"
            }]
      "status": "Restoration completed successfully."
         }
   },
   "status": {
      "code": 0,
      "message": "succeeded"
   }
},
"id": "1"
}
```

System

This section lists the new features added to FortiAnalyzer for system settings:

- High Availability (HA) on page 121
- Administrators on page 124
- Others on page 130

High Availability (HA)

This section lists the new features added to FortiAnalyzer for high availability (HA):

- Geo-redundant High Availability (HA) on page 121

Geo-redundant High Availability (HA)

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Geo-redundant HA

An active-active mode is now available on FortiAnalyzer HA to help create a geo-redundant solution.

In FortiAnalyzer HA active-passive mode, a layer 2 connection is required between HA members in order to set up the HA cluster virtual IP. In active-active mode, however, a layer 2 connection is not required between data centers at different locations.

Below is a brief comparison between FortiAnalyzer HA in active-passive and active-active mode.

active-passive	active-active
Only the HA primary can receive logs and archive files from its directly connected device and forward them to HA secondary.	All HA members can receive logs and archive files from its directly connected device and forward logs and archive files to its HA peer.
Only the HA primary can forward data to the remote server.	All HA members can forward its directly received logs and archive file to the remote server.

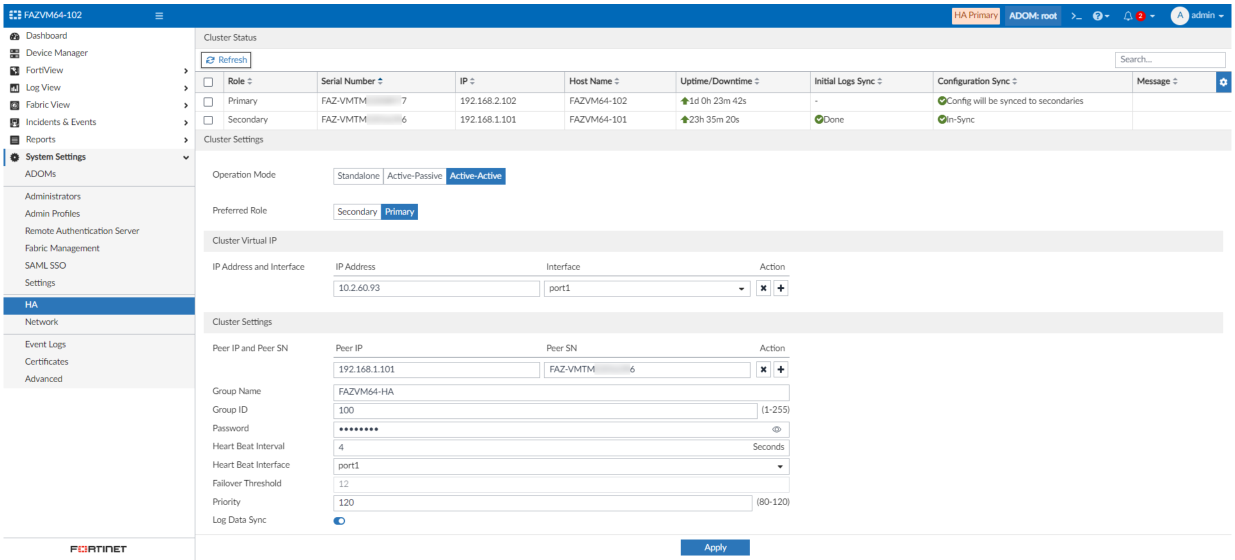
In the examples below, the goal is to build an active-active geo-redundant layer 3 FortiAnalyzer HA cluster between two data centers. The FortiAnalyzer HA members are located in different places. They are communicating with each other via routers. There is no layer 2 connection.

Unicast must be enabled for the HA heartbeat in order for the cluster to operate in this mode. This setting can only be configured from the CLI. For more information on enabling the unicast heartbeat setting, see the FortiAnalyzer CLI Reference.

When unicast is enabled, VRRP packets are sent to the peer address instead of the multicast address. VRRP (IP protocol 112) must be allowed through any connecting firewalls.

To build a geo-redundant FortiAnalyzer HA via the GUI:

1. In the first FortiAnalyzer, configure the primary in *System Settings* > *HA*.
   - For *Operation Mode*, select *Active-Active*.
   - For *Preferred Role*, select *Primary*.
   - Complete the other fields, including *Peer IP* and *Peer SN*.
   - Cluster Virtual IP (VIP) is optional. It requires a layer 2 connection between HA members. If VIP is not configured, select the interface which is used to communicate with the peer as *Heart Beat Interface*. You can click the *X* icon next to the VIP entry to remove it.



Cluster Status

	Role	Serial Number	IP	Host Name	Uptime/Downtime	Initial Logs Sync	Configuration Sync	Message
□	Primary	FAZ-VMTM[redacted]7	192.168.2.102	FAZVM64-102	1d 0h 23m 42s	-	✓Config will be synced to secondaries	
□	Secondary	FAZ-VMTM[redacted]6	192.168.1.101	FAZVM64-101	23h 35m 20s	✓Done	✓In-Sync	

Cluster Settings

Operation Mode: Standalone | Active-Passive | [✓ Active-Active]

Preferred Role: Secondary | [✓ Primary]

Cluster Virtual IP

IP Address and Interface	IP Address	Interface	Action
	10.2.60.93	port1	✖ ✚

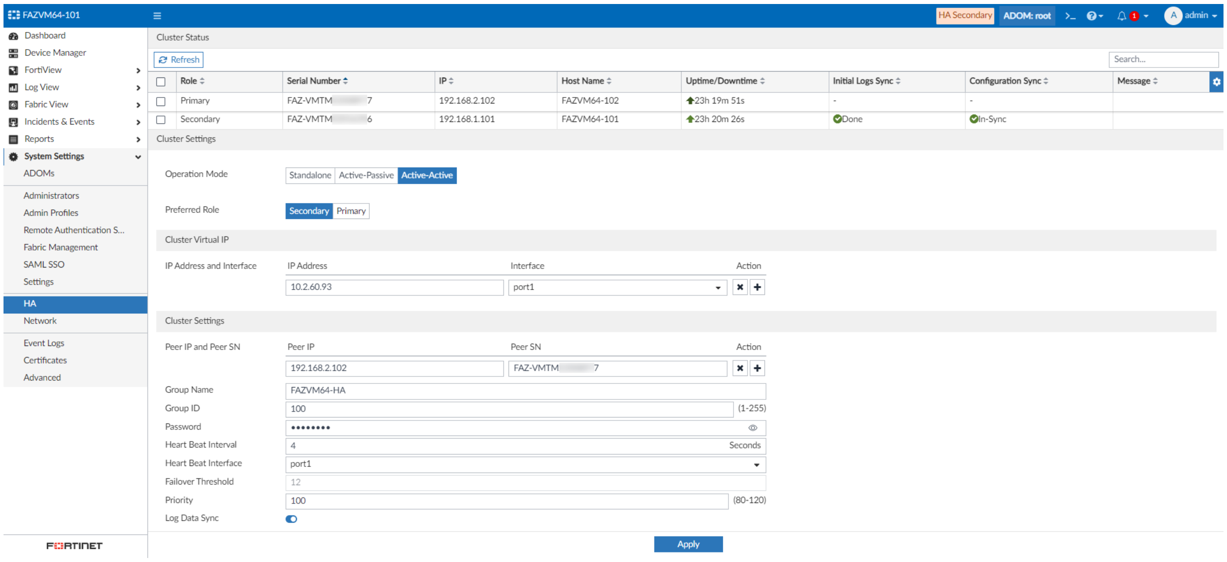
Cluster Settings

Peer IP and Peer SN	Peer IP	Peer SN	Action
	192.168.1.101	FAZ-VMTM[redacted]6	✖ ✚

Group Name: FAZVM64-HA
Group ID: 100 (1-255)
Password: ••••••••
Heart Beat Interval: 4 Seconds
Heart Beat Interface: port1
Failover Threshold: 12
Priority: 120 (80-120)
Log Data Sync: ●

2. In the second FortiAnalyzer, configure the primary in *System Settings* > *HA*.
   - For *Operation Mode*, select *Active-Active*.
   - For *Preferred Role*, select *Secondary*.
   - Complete the other fields, including *Peer IP* and *Peer SN*.
   - Cluster VIP is optional. It requires a layer 2 connection between HA members. If VIP is not configured, select the interface which is used to communicate with the peer as *Heart Beat Interface*. You can click the *X* icon next

to the VIP entry to remove it.



Cluster Status

☐	Role	Serial Number	IP	Host Name	Uptime/Downtime	Initial Logs Sync	Configuration Sync	Message
☐	Primary	FAZ-VMTM[redacted]7	192.168.2.102	FAZVM64-102	23h 19m 51s	-	-	
☐	Secondary	FAZ-VMTM[redacted]6	192.168.1.101	FAZVM64-101	23h 20m 26s	✓Done	✓In-Sync	

Cluster Settings

Operation Mode: Standalone | Active-Passive | [✓ Active-Active]

Preferred Role: [✓ Secondary] | Primary

Cluster Virtual IP

IP Address and Interface	IP Address	Interface	Action
	10.2.60.93	port1	✖ ✚

Cluster Settings

Peer IP and Peer SN	Peer IP	Peer SN	Action
	192.168.2.102	FAZ-VMTM[redacted]7	✖ ✚

Group Name: FAZVM64-HA
Group ID: 100 (1-255)
Password: ••••••••
Heart Beat Interval: 4 Seconds
Heart Beat Interface: port1
Failover Threshold: 12
Priority: 100 (80-120)
Log Data Sync: ●

To build a geo-redundant FortiAnalyzer HA via the CLI:

For more information about the FortiAnalyzer CLI commands, see the FortiAnalyzer 7.4 CLI Reference.

1. Configure the FortiAnalyzer HA.

   When configuring the FortiAnalyzer `system ha`, set `mode` to `a-a`. The `vip` is optional; if there is no layer 2 connection between HA members, `vip` will not work. In this case, set `hb-interface` as the interface which is used to communicate with the peer.

   a. Configure the first FortiAnalyzer. In the CLI, enter the following commands:

```
config system ha
   set mode a-a
   set group-id 100
   set group-name "FAZVM64-HA"
   set hb-interface "port1"
   set unicast enable
   set password xxxxxx
      config peer
         edit 1
            set ip "192.168.1.101"
            set serial-number "FAZ-VMTM-----6"
         next
      end
   set preferred-role primary
   set priority 120
end
```

   b. Configure the second FortiAnalyzer. In the CLI, enter the following commands:

```
config system ha
   set mode a-a
   set group-id 100
   set group-name "FAZVM64-HA"
   set hb-interface "port1"
   set unicast enable
   set password xxxxxx
      config peer
```

```
            edit 1
               set ip "192.168.2.102"
               set serial-number "FAZ-VMTM-----7"
            next
         end
   end
```

2. If the alternate FortiAnalyzer can be configured on FortiGate, `set server` to the HA primary and `set alt-server` to the HA secondary. In the FortiGate CLI, enter:

```
config log fortianalyzer setting
   set status enable
   set ?
   ...
   *server                                The main remote FortiAnalyzer.
   alt-server                            The alternate remote FortiAnalyzer.
   ...
   set server 192.168.2.102
   set alt-server 192.168.1.101
   ...
end
```

3. If the alternate FortiAnalyzer cannot be configured on FortiGate, `set server` to a HA member which is reachable from the FortiGate or to the VIP address of the FortiAnalyzer HA, if any. In the FortiGate CLI, enter:

```
config log fortianalyzer setting
   set status enable
   ...
   set server 192.168.2.102 (or 10.2.60.93)
   ...
end
```

Administrators

This section lists the new features added to FortiAnalyzer for administrators:

- A new restricted admin profile can be used to only change the administrators passwords 7.4.2 on page 124
- Per-ADOM admin profile 7.4.2 on page 127

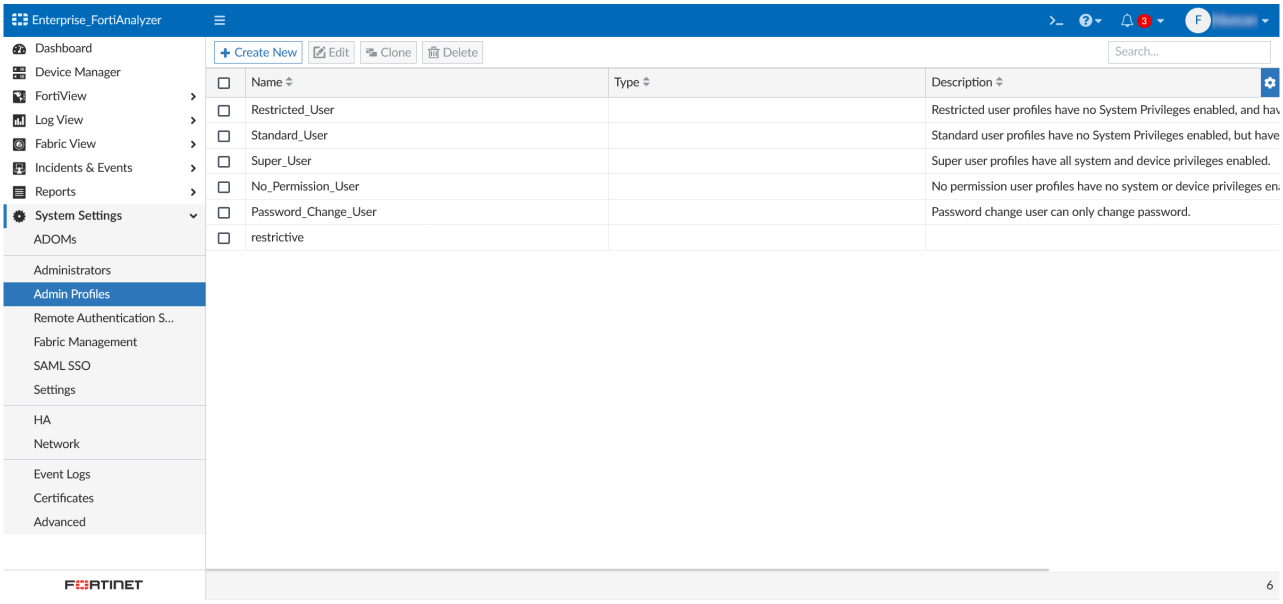
A new restricted admin profile can be used to only change the administrators passwords - 7.4.2

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Administrator profiles

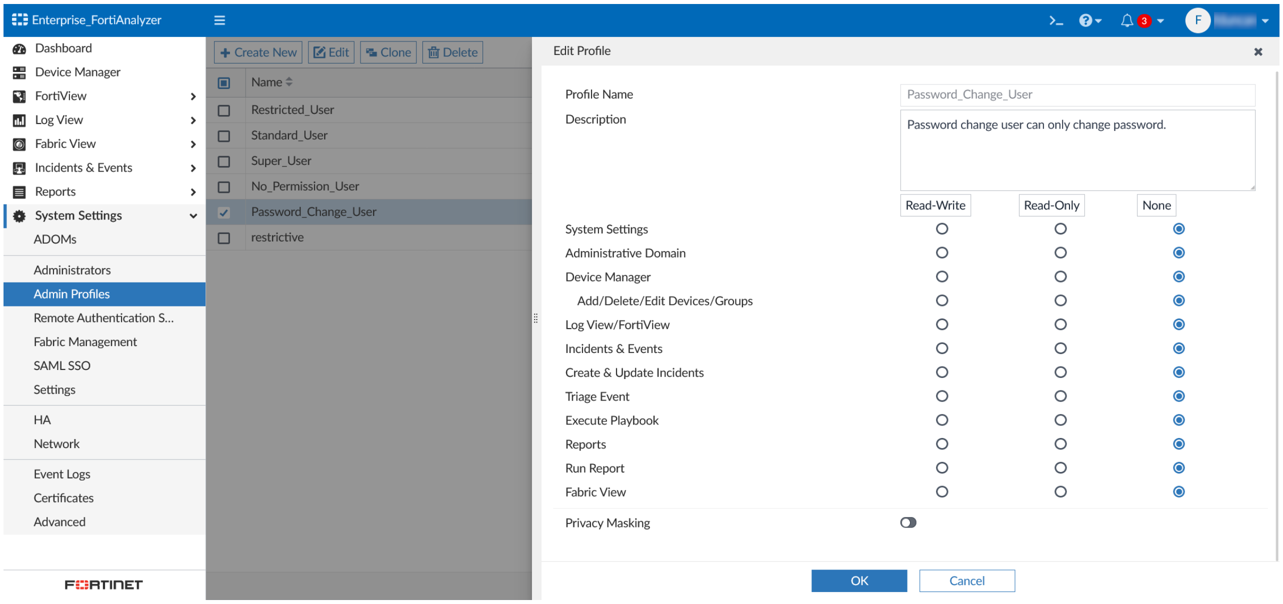
A new restricted admin profile can be used to only change the administrators passwords.

- A new admin profile called *Password_Change_User* has been added.



□	Name	Type	Description
□	Restricted_User		Restricted user profiles have no System Privileges enabled, and hav
□	Standard_User		Standard user profiles have no System Privileges enabled, but have
□	Super_User		Super user profiles have all system and device privileges enabled.
□	No_Permission_User		No permission user profiles have no system or device privileges en
□	Password_Change_User		Password change user can only change password.
□	restrictive		

- The admin profile has all permissions in the FortiAnalyzer GUI set to *None*.



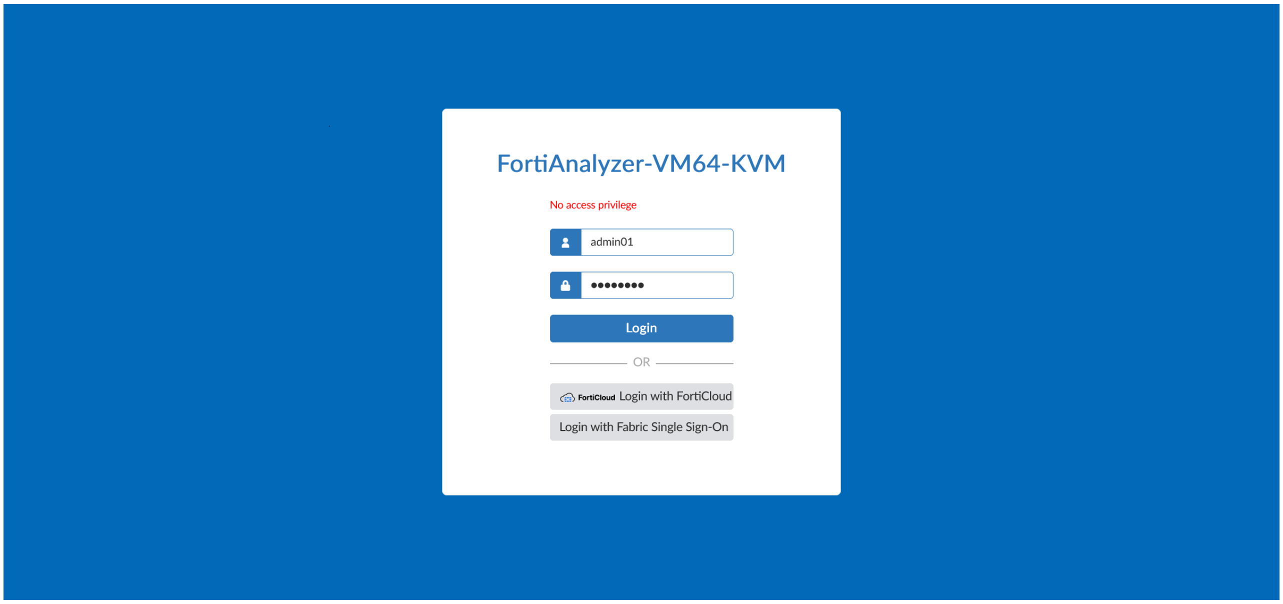
Profile Name: Password_Change_User

Description: Password change user can only change password.

	Read-Write	Read-Only	None
System Settings	○	○	●
Administrative Domain	○	○	●
Device Manager	○	○	●
Add/Delete/Edit Devices/Groups	○	○	●
Log View/FortiView	○	○	●
Incidents & Events	○	○	●
Create & Update Incidents	○	○	●
Triage Event	○	○	●
Execute Playbook	○	○	●
Reports	○	○	●
Run Report	○	○	●
Fabric View	○	○	●

Privacy Masking: off

- The admin profile has the following permissions in the CLI:
  - `write-passwd-access`: Read/Write.
  - `rpc-permit`: Read/Write.
- When the admin profile is applied to a user, the user will see "No access privilege" when attempting to log into the FortiAnalyzer GUI.



FortiAnalyzer-VM64-KVM
Login
OR
FortiCloud Login with FortiCloud
Login with Fabric Single Sign-On

No access privilege

admin01

••••••••

- The user can only access FortiAnalyzer using the CLI or API. When logging in via CLI or API, the admin is able to change user's passwords.

To specify which user/profile passwords can be changed:

1. In the FortiAnalyzer CLI, enter the following commands to configure `write-passwd-access`:

   ```
   config system admin profile
      edit Password_Change_User
         set write-passwd-access
            all All users.
            specify-by-profile Specify by profile.
            specify-by-user Specify by user.
         set write-passwd-access
   ```

   There are 3 options, by default allow to change all user's password.

   - **all**: *Password_Change_User* admins can change the password for all users.
   - **specify-by-profile**: Only allow the password of users who are using these profiles to be changed.

     ```
     set write-passwd-access specify-by-profile
        set write-passwd-profiles
           profileid Profile ID.
           Restricted_User profile
           Standard_User profile
           Super_User profile
           Package_User profile
           No_Permission_User profile
           Password_Change_User profile
           profile1 profile
        set write-passwd-profiles Restricted_User Standard_User profile1
     ```

     In this example, *Restricted_User*, *Standard_User*, and *profile1* are selected. *Password_Change_User* admins can only change the password of users who are using the *Restricted_User*, *Standard_User*, or *profile1* profile. The user can't change password of users who are using the *Super_User* profile for instance.
   - **specify-by-user**: Only allow the password of users in the list to be changed.

     ```
     set write-passwd-access specify-by-user
        set write-passwd-user-list
           <userid> users
     ```

```
                admin
                test
                test1
                test2
                test3
        set write-passwd-user-list test test3
```

In this example, test and test3 are selected. *Password_Change_User* admins can only change the password of the test and test3 user. Users cannot change the password of admin, test1, or test2.

Per-ADOM admin profile - 7.4.2

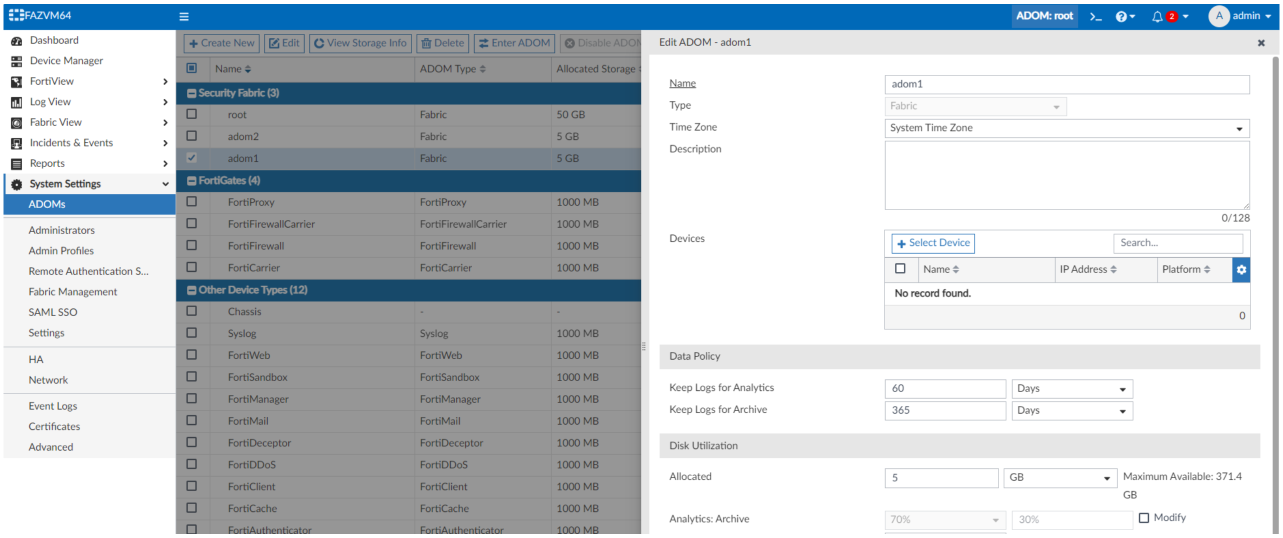
A per-ADOM admin profile allows the administrator to log in on different ADOMs with different admin profiles.

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Creating administrators

To assign a per-ADOM admin profile:

1. Create multiple ADOMs, as needed. In this example, `adom1` and `adom2` have been created.



Name	ADOM Type	Allocated Storage
Security Fabric (3)		
root	Fabric	50 GB
adom2	Fabric	5 GB
☑ adom1	Fabric	5 GB
FortiGates (4)		
FortiProxy	FortiProxy	1000 MB
FortiFirewallCarrier	FortiFirewallCarrier	1000 MB
FortiFirewall	FortiFirewall	1000 MB
FortiCarrier	FortiCarrier	1000 MB
Other Device Types (12)		
Chassis	-	-
Syslog	Syslog	1000 MB
FortiWeb	FortiWeb	1000 MB
FortiSandbox	FortiSandbox	1000 MB
FortiManager	FortiManager	1000 MB
FortiMail	FortiMail	1000 MB
FortiDeceptor	FortiDeceptor	1000 MB
FortiDDoS	FortiDDoS	1000 MB
FortiClient	FortiClient	1000 MB
FortiCache	FortiCache	1000 MB
FortiAuthenticator	FortiAuthenticator	1000 MB

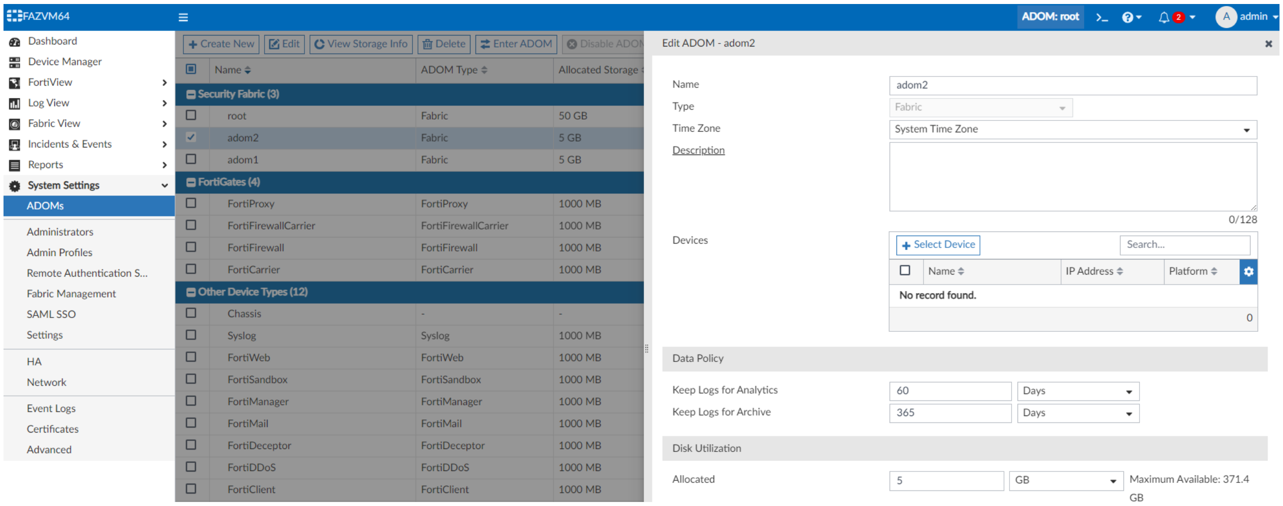
Name: adom1
Type: Fabric
Time Zone: System Time Zone
Description: 0/128
Devices:

□	Name	IP Address	Platform
No record found.			

0

Data Policy
Keep Logs for Analytics: 60 Days
Keep Logs for Archive: 365 Days

Disk Utilization
Allocated: 5 GB Maximum Available: 371.4 GB
Analytics: Archive: 70% 30% □ Modify



	Name	ADOM Type	Allocated Storage
	Security Fabric (3)		
□	root	Fabric	50 GB
☑	adom2	Fabric	5 GB
□	adom1	Fabric	5 GB
	FortiGates (4)		
□	FortiProxy	FortiProxy	1000 MB
□	FortiFirewallCarrier	FortiFirewallCarrier	1000 MB
□	FortiFirewall	FortiFirewall	1000 MB
□	FortiCarrier	FortiCarrier	1000 MB
	Other Device Types (12)		
□	Chassis	-	-
□	Syslog	Syslog	1000 MB
□	FortiWeb	FortiWeb	1000 MB
□	FortiSandbox	FortiSandbox	1000 MB
□	FortiManager	FortiManager	1000 MB
□	FortiMail	FortiMail	1000 MB
□	FortiDeceptor	FortiDeceptor	1000 MB
□	FortiDDoS	FortiDDoS	1000 MB
□	FortiClient	FortiClient	1000 MB

Edit ADOM - adom2

Name: adom2
Type: Fabric
Time Zone: System Time Zone
Description:
0/128

Devices: Select Device | Search...

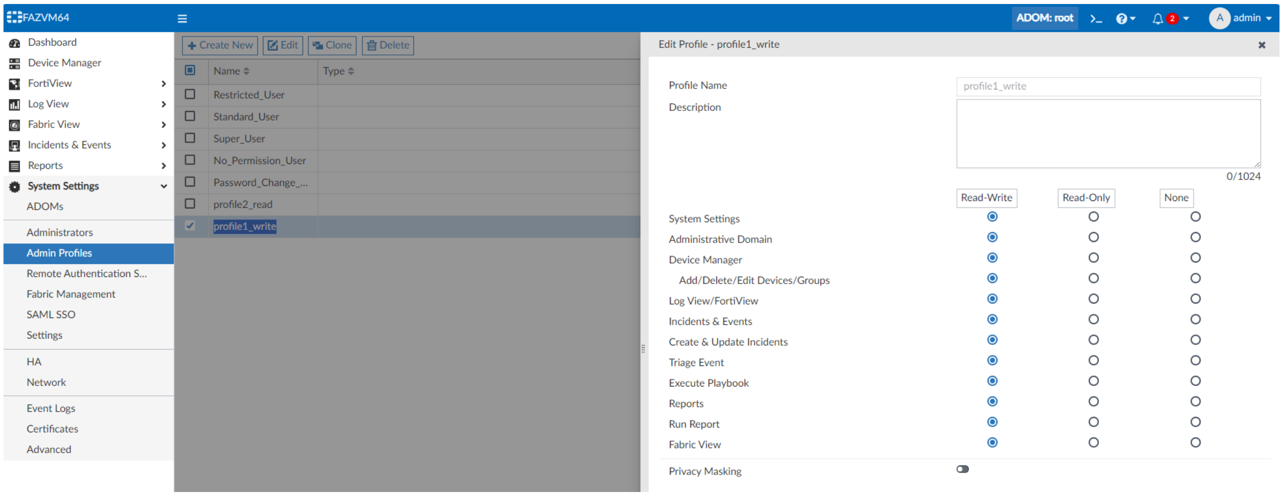
□	Name	IP Address	Platform

No record found.
0

Data Policy
Keep Logs for Analytics: 60 Days
Keep Logs for Archive: 365 Days

Disk Utilization
Allocated: 5 GB Maximum Available: 371.4 GB

2. Create multiple Admin Profiles with different access, as needed. In this example, `profile1_write` and `profile2_read` have been created.



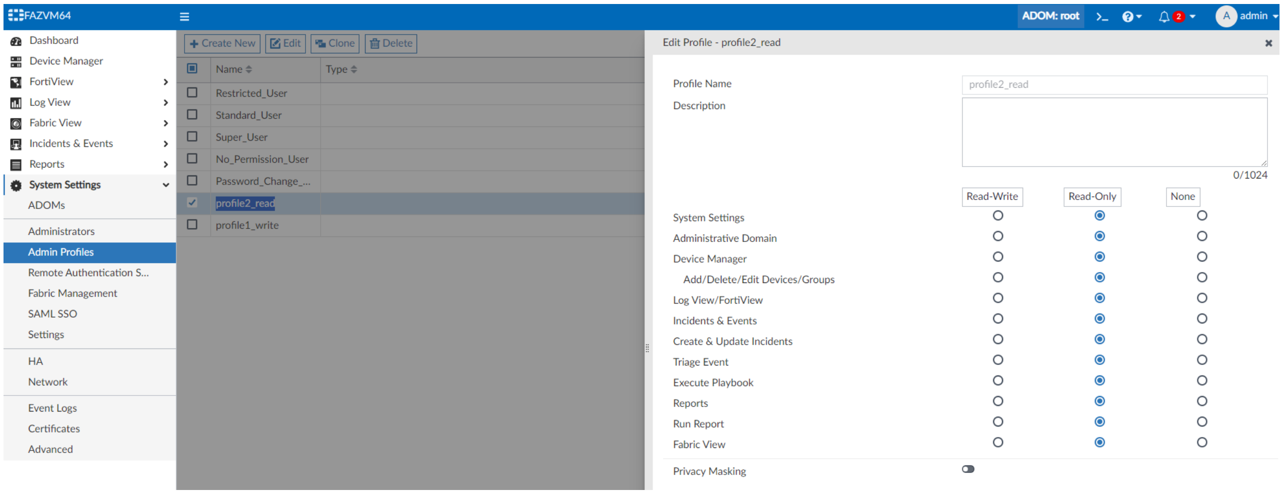
	Name	Type
□	Restricted_User	
□	Standard_User	
□	Super_User	
□	No_Permission_User	
□	Password_Change_...	
□	profile2_read	
☑	profile1_write	

Edit Profile - profile1_write

Profile Name: profile1_write
Description:
0/1024

	Read-Write	Read-Only	None
System Settings	●	○	○
Administrative Domain	●	○	○
Device Manager	●	○	○
Add/Delete/Edit Devices/Groups	●	○	○
Log View/FortiView	●	○	○
Incidents & Events	●	○	○
Create & Update Incidents	●	○	○
Triage Event	●	○	○
Execute Playbook	●	○	○
Reports	●	○	○
Run Report	●	○	○
Fabric View	●	○	○

Privacy Masking



	Name	Type
□	Restricted_User	
□	Standard_User	
□	Super_User	
□	No_Permission_User	
□	Password_Change_...	
☑	profile2_read	
□	profile1_write	

Edit Profile - profile2_read

Profile Name: profile2_read
Description:
0/1024

	Read-Write	Read-Only	None
System Settings	○	●	○
Administrative Domain	○	●	○
Device Manager	○	●	○
Add/Delete/Edit Devices/Groups	○	●	○
Log View/FortiView	○	●	○
Incidents & Events	○	●	○
Create & Update Incidents	○	●	○
Triage Event	○	●	○
Execute Playbook	○	●	○
Reports	○	●	○
Run Report	○	●	○
Fabric View	○	●	○

Privacy Masking

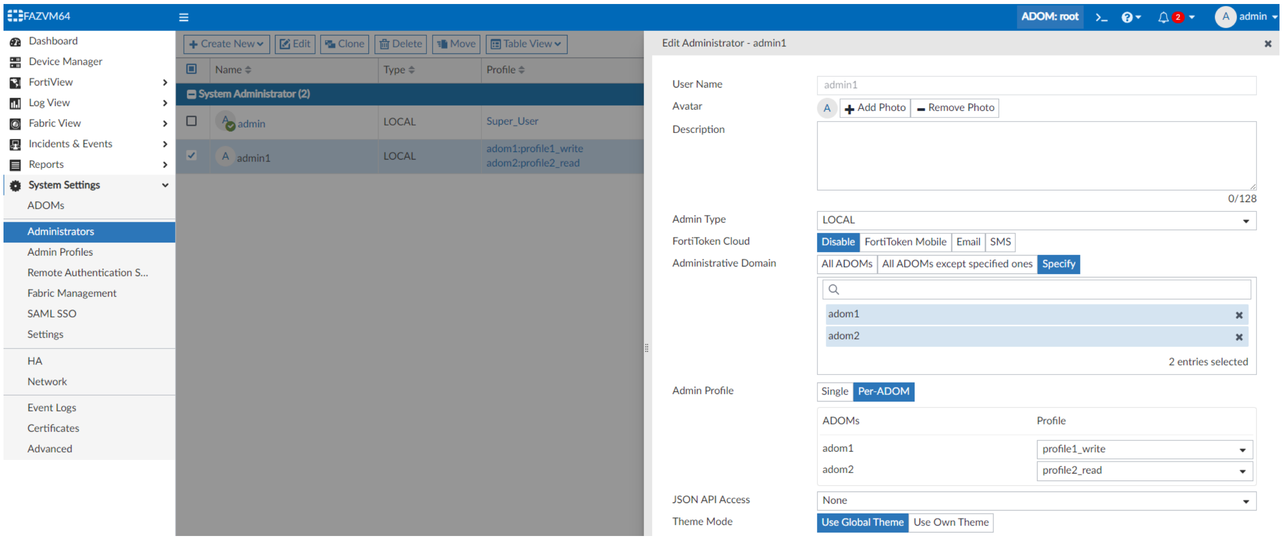
3. Go to *System Settings > Administrators*, and click *Create New*.
Alternatively, you can select an existing administrator and click *Edit*.

4. For *Administrative Domain*, select *Specify* and select the ADOMs the user should have access to.

5. For *Admin Profile*, select *Per-ADOM*.
   If *Single* is selected, the administrator will only have one admin profile for all ADOMs.

   When *Per-ADOM* is selected, the *Admin Profile* setting displays the list of ADOMs that you specified access to for the administrator. A *Profile* dropdown is available for each ADOM.
6. Using the *Profile* dropdowns, select an admin profile for each ADOM.
   The profile determines the administrator's access to the FortiAnalyzer features when they are in that ADOM.

   In the example below, a different profile is selected for each ADOM. The user `admin1` will have `profile1_write` access in `adom1` and `profile2_read` access in `adom2`.



Name	Type	Profile
System Administrator (2)		
admin	LOCAL	Super_User
admin1	LOCAL	adom1:profile1_write adom2:profile2_read

Edit Administrator - admin1

User Name: admin1

Admin Type: LOCAL

FortiToken Cloud: Disable

Administrative Domain: Specify

adom1

adom2

2 entries selected

Admin Profile: Per-ADOM

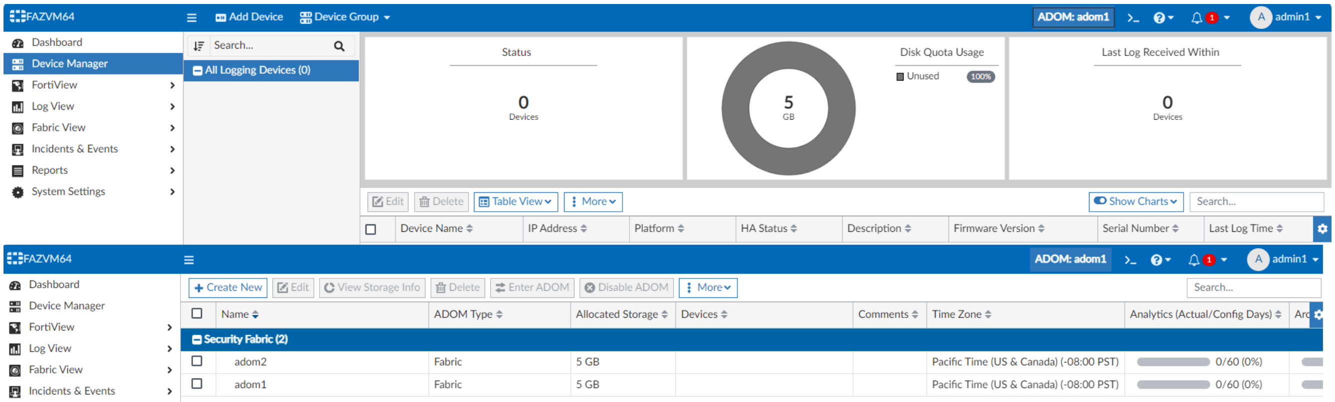
ADOMs	Profile
adom1	profile1_write
adom2	profile2_read

JSON API Access: None

Theme Mode: Use Global Theme

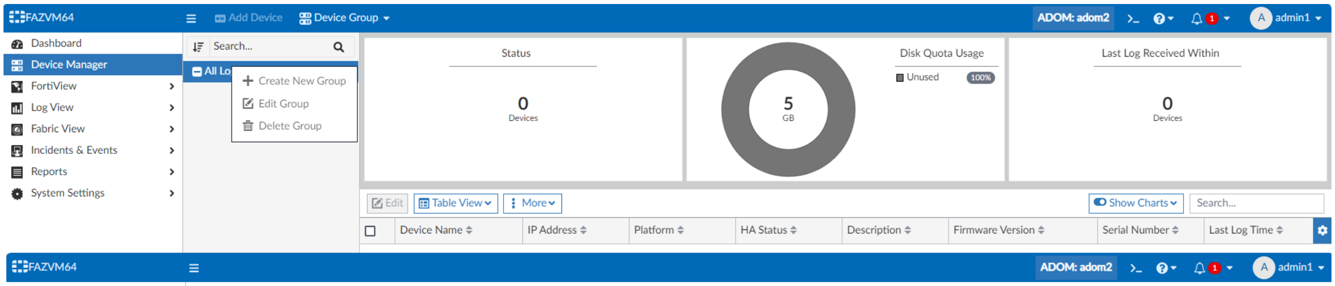
   In *System Settings* > *Administrators*, the *Profile* column lists the profiles selected per-ADOM.
7. Configure the other settings for the administrator, and click *OK*.

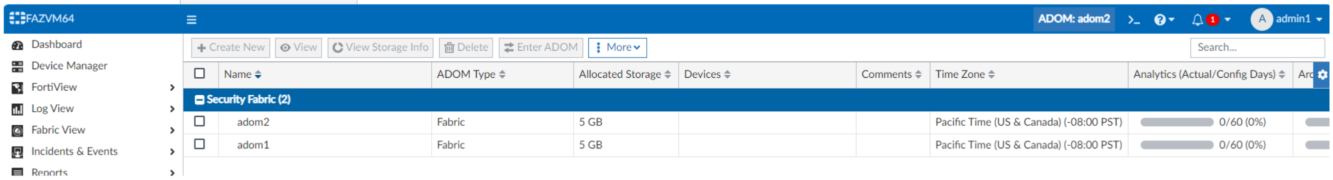
In this example, `admin1` has write access in `adom1` and read access in `adom2`. See below.



ADOM: adom1

Name	ADOM Type	Allocated Storage	Devices	Comments	Time Zone	Analytics (Actual/Config Days)
Security Fabric (2)						
adom2	Fabric	5 GB			Pacific Time (US & Canada) (-08:00 PST)	0/60 (0%)
adom1	Fabric	5 GB			Pacific Time (US & Canada) (-08:00 PST)	0/60 (0%)





Name	ADOM Type	Allocated Storage	Devices	Comments	Time Zone	Analytics (Actual/Config Days)	Arc
Security Fabric (2)							
adom2	Fabric	5 GB			Pacific Time (US & Canada) (-08:00 PST)	0/60 (0%)	
adom1	Fabric	5 GB			Pacific Time (US & Canada) (-08:00 PST)	0/60 (0%)	

Others

This section lists the new features added to FortiAnalyzer for other features relating to system settings:

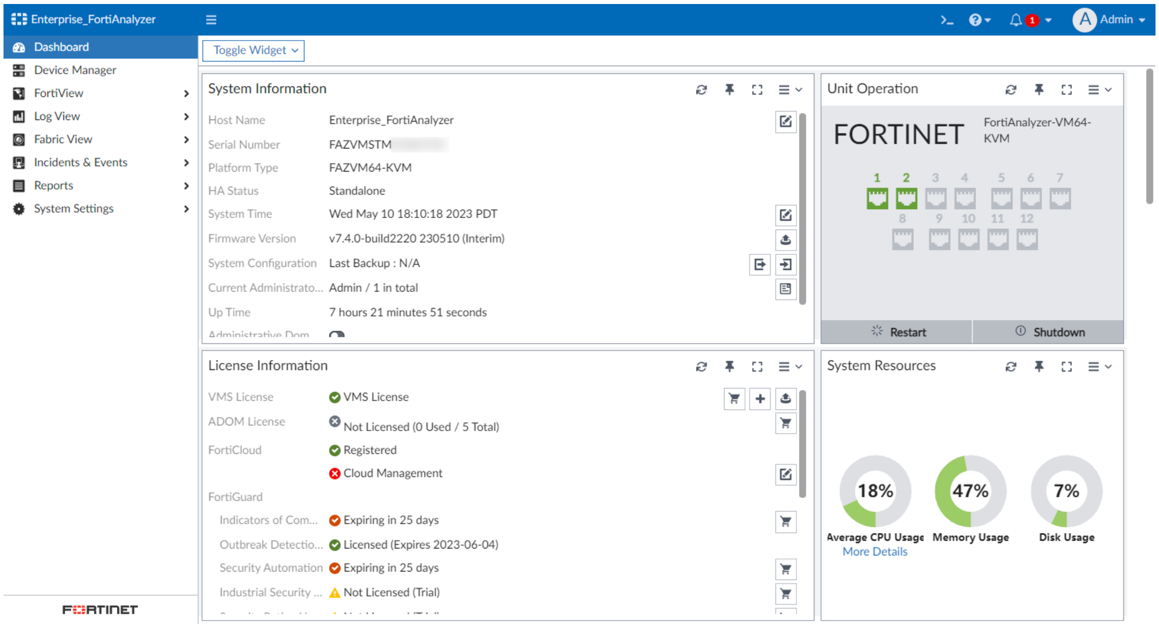
- FortiAnalyzer GUI enhancements on page 130
- Fabric of FAZ topology chart on page 134
- Fabric of FAZ: member authorization with supervisor on page 136
- Fabric of FAZ global FortiView support on page 141
- Fabric of FAZ: Central report support and creating Fabric groups on page 143
- Block out contract device from upgrading to next or major or minor release on page 146
- FortiManager and FortiAnalyzer support HTTP/2 for improved security, multiplexing, and reduced network latency 7.4.1 on page 148
- Backup strategy and configuration setup added to the FortiAnalyzer setup wizard 7.4.2 on page 150

FortiAnalyzer GUI enhancements

To enhance the user experience and to align to FortiOS, the following changes have been added to the FortiAnalyzer GUI:

- Uses a new and customizable landing page (*Dashboard*)
- Uses Neutrino framework
- Adopts a 3-layer navigation, making all menus accessible via a single click

The *Dashboard* includes widgets, such as *Log Status* and *Alert Message Console*. You can toggle which widgets display from the *Toggle Widget* dropdown.



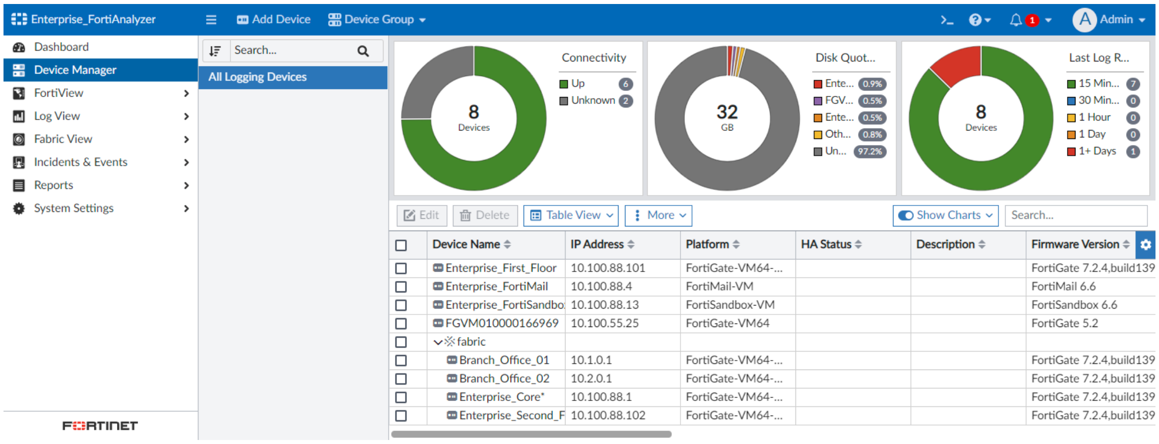
System Information

Host Name	Enterprise_FortiAnalyzer
Serial Number	FAZVMSTM[redacted]
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Wed May 10 18:10:18 2023 PDT
Firmware Version	v7.4.0-build2220 230510 (Interim)
System Configuration	Last Backup : N/A
Current Administrato...	Admin / 1 in total
Up Time	7 hours 21 minutes 51 seconds

License Information

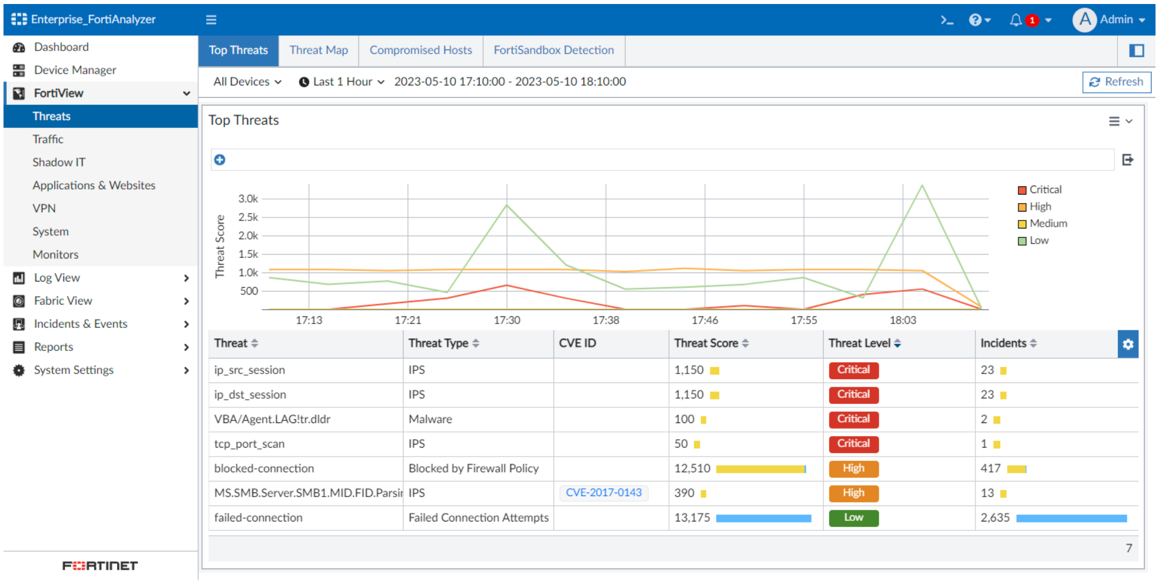
VMS License	✓ VMS License
ADOM License	☒ Not Licensed (0 Used / 5 Total)
FortiCloud	✓ Registered
	☒ Cloud Management
FortiGuard	
Indicators of Com...	✓ Expiring in 25 days
Outbreak Detectio...	✓ Licensed (Expires 2023-06-04)
Security Automation	✓ Expiring in 25 days
Industrial Security ...	⚠ Not Licensed (Trial)

You can access other pages, such as *Device Manager*, from the left-pane navigation.



□	Device Name	IP Address	Platform	HA Status	Description	Firmware Version
□	Enterprise_First_Floor	10.100.88.101	FortiGate-VM64-...			FortiGate 7.2.4,build139
□	Enterprise_FortiMail	10.100.88.4	FortiMail-VM			FortiMail 6.6
□	Enterprise_FortiSandbo:	10.100.88.13	FortiSandbox-VM			FortiSandbox 6.6
□	FGVM010000166969	10.100.55.25	FortiGate-VM64			FortiGate 5.2
□	fabric					
□	Branch_Office_01	10.1.0.1	FortiGate-VM64-...			FortiGate 7.2.4,build139
□	Branch_Office_02	10.2.0.1	FortiGate-VM64-...			FortiGate 7.2.4,build139
□	Enterprise_Core*	10.100.88.1	FortiGate-VM64-...			FortiGate 7.2.4,build139
□	Enterprise_Second_F	10.100.88.102	FortiGate-VM64-...			FortiGate 7.2.4,build139

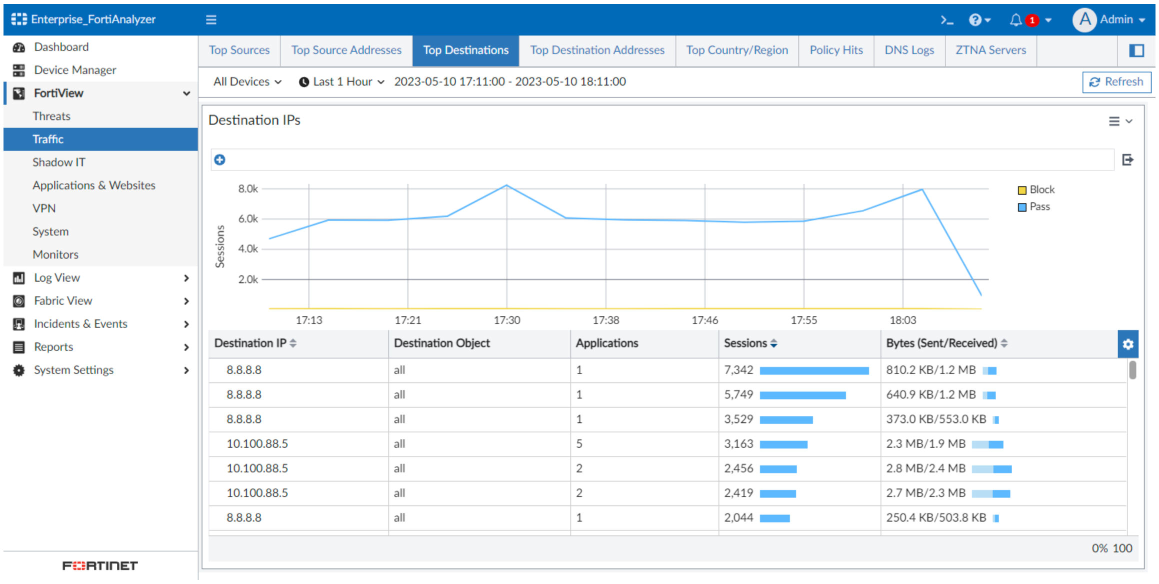
If there are sub-menus, as in *FortiView*, the left-pane navigation will expand to show other pages in that section.



Threat	Threat Type	CVE ID	Threat Score	Threat Level	Incidents
ip_src_session	IPS		1,150	Critical	23
ip_dst_session	IPS		1,150	Critical	23
VBA/Agent.LAG!tr.dldr	Malware		100	Critical	2
tcp_port_scan	IPS		50	Critical	1
blocked-connection	Blocked by Firewall Policy		12,510	High	417
MS.SMB.Server.SMB1.MID.FID.Parsir	IPS	CVE-2017-0143	390	High	13
failed-connection	Failed Connection Attempts		13,175	Low	2,635

7

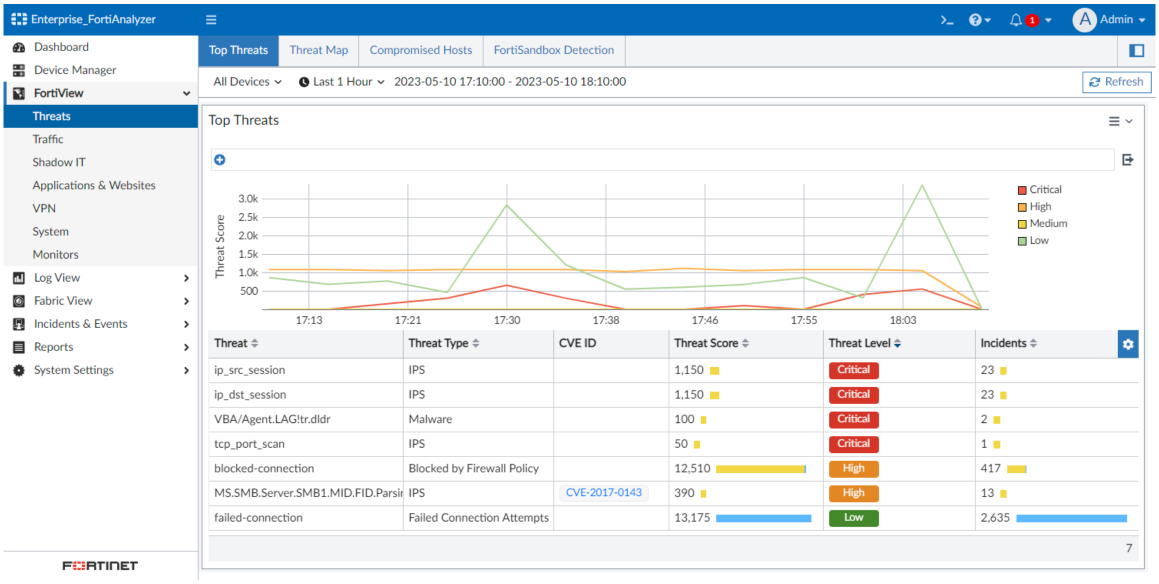
Further sub-menus may also be available along the top of the pane. For example, in the image below, the admin has navigated to *FortiView* > *Traffic* > *Top Destinations*.



Destination IP	Destination Object	Applications	Sessions	Bytes (Sent/Received)
8.8.8.8	all	1	7,342	810.2 KB/1.2 MB
8.8.8.8	all	1	5,749	640.9 KB/1.2 MB
8.8.8.8	all	1	3,529	373.0 KB/553.0 KB
10.100.88.5	all	5	3,163	2.3 MB/1.9 MB
10.100.88.5	all	2	2,456	2.8 MB/2.4 MB
10.100.88.5	all	2	2,419	2.7 MB/2.3 MB
8.8.8.8	all	1	2,044	250.4 KB/503.8 KB

0% 100

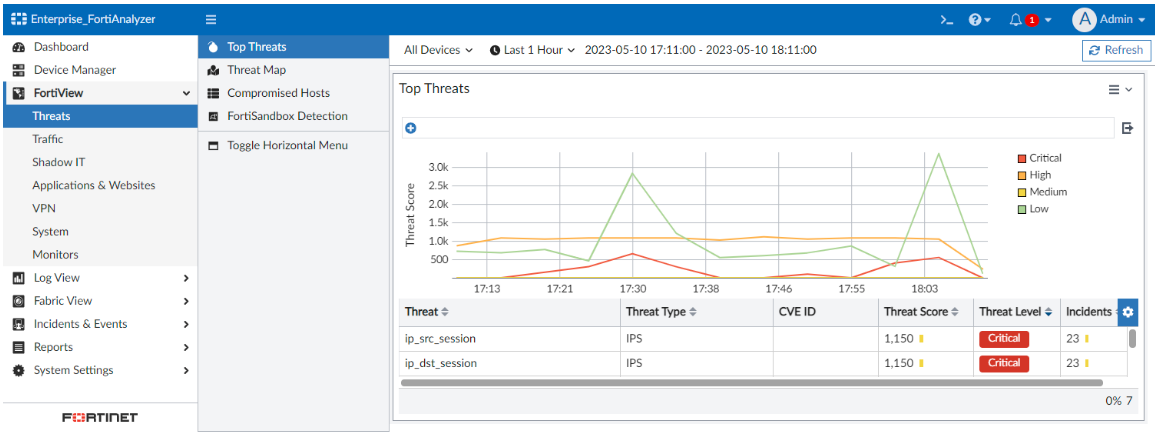
When available, you can click the horizontal view icon (◧) to switch to a vertical display of the sub-menu. The sub-menu will then display in a left-pane navigation instead.



Threat	Threat Type	CVE ID	Threat Score	Threat Level	Incidents
ip_src_session	IPS		1,150	Critical	23
ip_dst_session	IPS		1,150	Critical	23
VBA/Agent.LAG!tr.dldr	Malware		100	Critical	2
tcp_port_scan	IPS		50	Critical	1
blocked-connection	Blocked by Firewall Policy		12,510	High	417
MS.SMB.Server.SMB1.MID.FID.Parsir	IPS	CVE-2017-0143	390	High	13
failed-connection	Failed Connection Attempts		13,175	Low	2,635

7

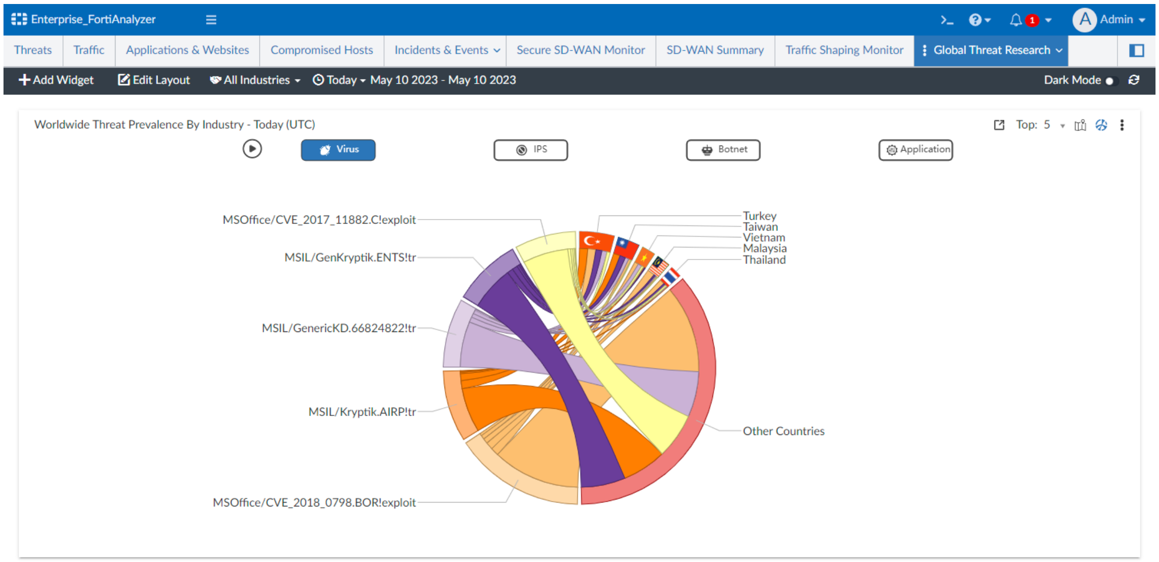
Click *Toggle Horizontal Menu* to return to the horizontal display at the top of the pane.



Threat	Threat Type	CVE ID	Threat Score	Threat Level	Incidents
ip_src_session	IPS		1,150	Critical	23
ip_dst_session	IPS		1,150	Critical	23

0% 7

On any page in the GUI, you can click the menu icon (▪) to hide the left-pane navigation. Click the menu icon (▪) again to re-open the left-pane navigation.



Fabric of FAZ topology chart

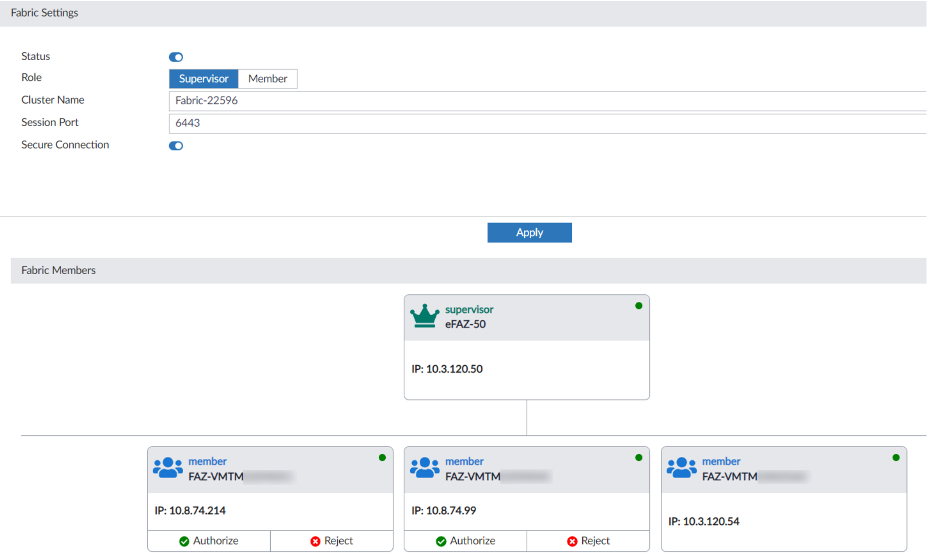
This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

- Configuring the FortiAnalyzer Fabric

A FortiAnalyzer Fabric topology chart is displayed on the supervisor to quickly identify connected members and their corresponding status.

FortiAnalyzer Fabric supervisor:

To view the topology on the supervisor, go to *System Settings* > *Fabric Management* > *Fabric Settings*. In the *Fabric Members* section, the topology displays all connected members.


Fabric Settings

Status	●
Role	Supervisor / Member
Cluster Name	Fabric-22596
Session Port	6443
Secure Connection	●

Apply

Fabric Members

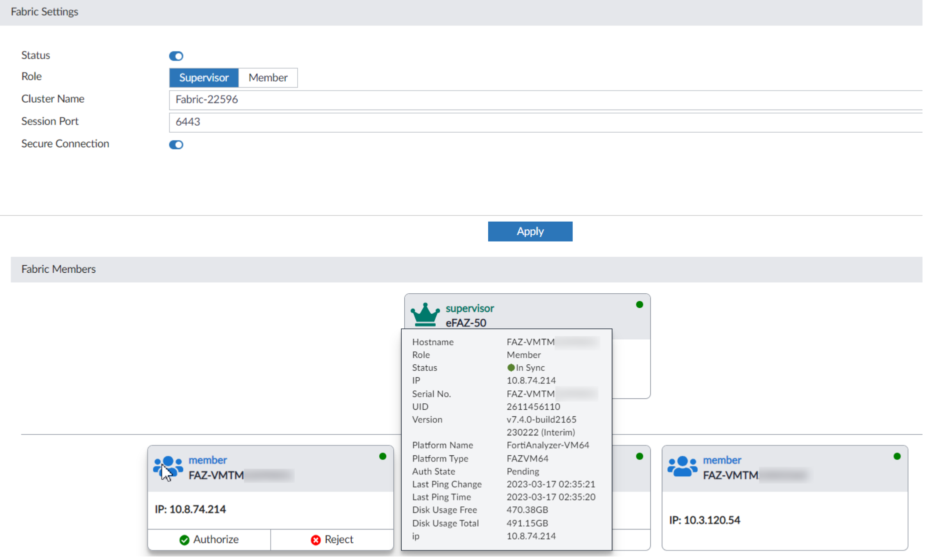
supervisor
eFAZ-50
IP: 10.3.120.50

member
FAZ-VMTM[redacted]
IP: 10.8.74.214
Authorize | Reject

member
FAZ-VMTM[redacted]
IP: 10.8.74.99
Authorize | Reject

member
FAZ-VMTM[redacted]
IP: 10.3.120.54

You can hover over the role for a FortiAnalyzer in the topology to display more information in a tooltip.



Fabric Settings

Status: ●
Role: Supervisor | Member
Cluster Name: Fabric-22596
Session Port: 6443
Secure Connection: ●

Apply

Fabric Members

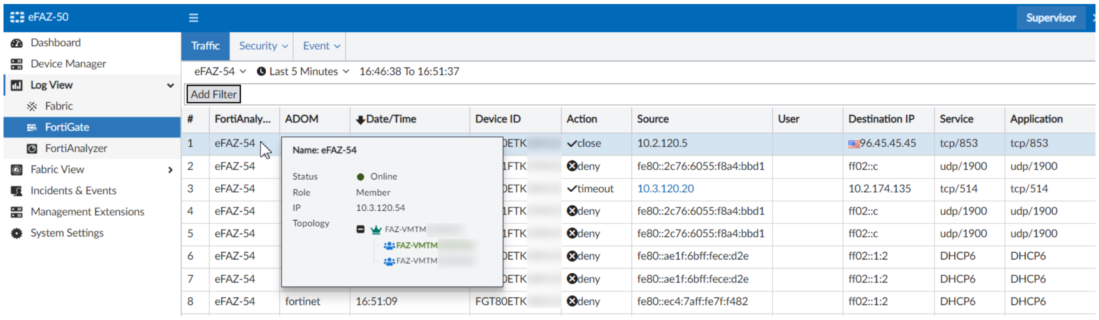
supervisor
eFAZ-50

Hostname	FAZ-VMTM[redacted]
Role	Member
Status	● In Sync
IP	10.8.74.214
Serial No.	FAZ-VMTM[redacted]
UID	2611456110
Version	v7.4.0-build2165 230222 (Interim)
Platform Name	FortiAnalyzer-VM64
Platform Type	FAZVM64
Auth State	Pending
Last Ping Change	2023-03-17 02:35:21
Last Ping Time	2023-03-17 02:35:20
Disk Usage Free	470.38GB
Disk Usage Total	491.15GB
ip	10.8.74.214

member
FAZ-VMTM[redacted]
IP: 10.8.74.214
Authorize | Reject

member
FAZ-VMTM[redacted]
IP: 10.3.120.54

You can also see the topology in the supervisor's *Log View*. Hover over a FortiAnalyzer in the *FortiAnalyzer Host Name* column to view the topology in a tooltip.



eFAZ-54 | Last 5 Minutes | 16:46:38 To 16:51:37

Add Filter

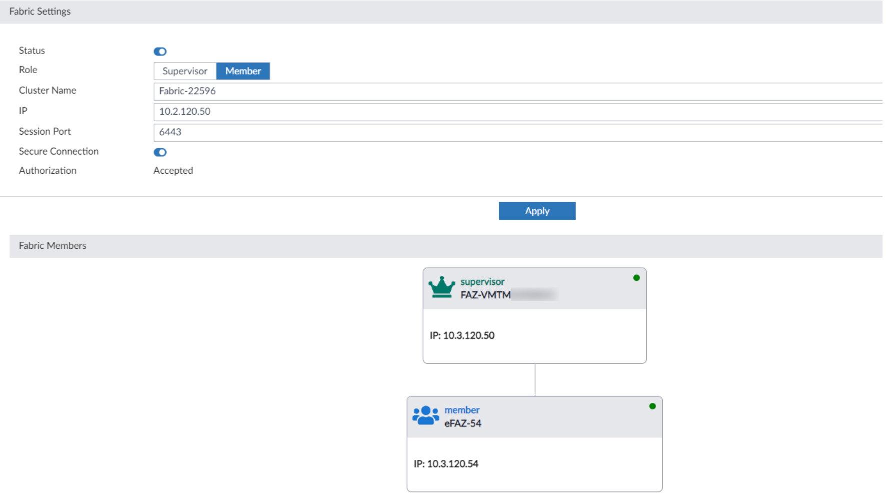
#	FortiAnaly...	ADOM	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application
1	eFAZ-54			ETK[redacted]	✓close	10.2.120.5		96.45.45.45	tcp/853	tcp/853
2	eFAZ-54			1FTK[redacted]	⊗deny	fe80::2c76:6055:f8a4:bbd1		ff02::c	udp/1900	udp/1900
3	eFAZ-54			ETK[redacted]	✓timeout	10.3.120.20		10.2.174.135	tcp/514	tcp/514
4	eFAZ-54			1FTK[redacted]	⊗deny	fe80::2c76:6055:f8a4:bbd1		ff02::c	udp/1900	udp/1900
5	eFAZ-54			1FTK[redacted]	⊗deny	fe80::2c76:6055:f8a4:bbd1		ff02::c	udp/1900	udp/1900
6	eFAZ-54			ETK[redacted]	⊗deny	fe80::ae1f:6bff:fece:d2e		ff02::1:2	DHCP6	DHCP6
7	eFAZ-54			ETK[redacted]	⊗deny	fe80::ae1f:6bff:fece:d2e		ff02::1:2	DHCP6	DHCP6
8	eFAZ-54	fortinet	16:51:09	FGT80ETK[redacted]	⊗deny	fe80::ec4:7aff:fe7f:f482		ff02::1:2	DHCP6	DHCP6

Name: eFAZ-54

Status	● Online
Role	Member
IP	10.3.120.54
Topology	FAZ-VMTM[redacted] FAZ-VMTM[redacted] FAZ-VMTM[redacted]

FortiAnalyzer Fabric member:

To view the topology on a member, go to *System Settings* > *Fabric Management* > *Fabric Settings*. In the *Fabric Members* section, the topology displays only the connection to the supervisor. It does not display the other members in the FortiAnalyzer Fabric.



Fabric Settings

Status ●
Role: Supervisor | **Member**
Cluster Name: Fabric-22596
IP: 10.2.120.50
Session Port: 6443
Secure Connection ●
Authorization: Accepted

Apply

Fabric Members

supervisor
FAZ-VMTM[redacted]
IP: 10.3.120.50

member
eFAZ-54
IP: 10.3.120.54

Fabric of FAZ: member authorization with supervisor

This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

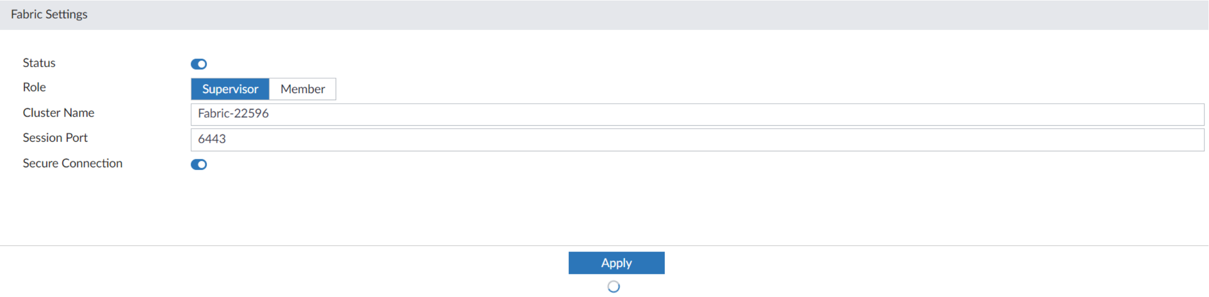
- Configuring the FortiAnalyzer Fabric

The FortiAnalyzer Fabric authentication process has been enhanced by implementing the following:

- Members can join the FortiAnalyzer Fabric by entering the cluster name and IP of the supervisor. No static password is required.
- The supervisor can authorize and reject members from joining the FortiAnalyzer Fabric.
- A `trusted-list` can be configured on the FortiAnalyzer Fabric supervisor to automatically authorize members if they match the configured serial number.
- A `trusted-list` can be configured on FortiAnalyzer Fabric members, so that they will join the FortiAnalyzer Fabric only if the supervisor matches the configured serial number.

FortiAnalyzer Fabric supervisor:

When configuring a FortiAnalyzer Fabric supervisor in *System Settings > Fabric Management*, there is no password configuration in the *Fabric Settings*.

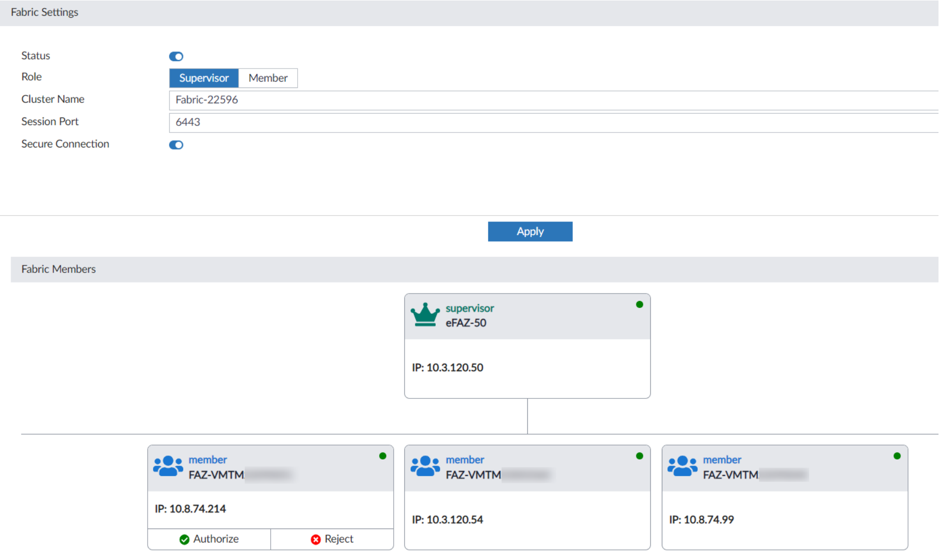


Fabric Settings

Status ●
Role: **Supervisor** | Member
Cluster Name: Fabric-22596
Session Port: 6443
Secure Connection ●

Apply

When members join the FortiAnalyzer Fabric, they will display in the topology for the supervisor. From this topology in the supervisor, you can authorize or reject the members.



Fabric Settings

Status: ●
Role: Supervisor | Member
Cluster Name: Fabric-22596
Session Port: 6443
Secure Connection: ●

Apply

Fabric Members

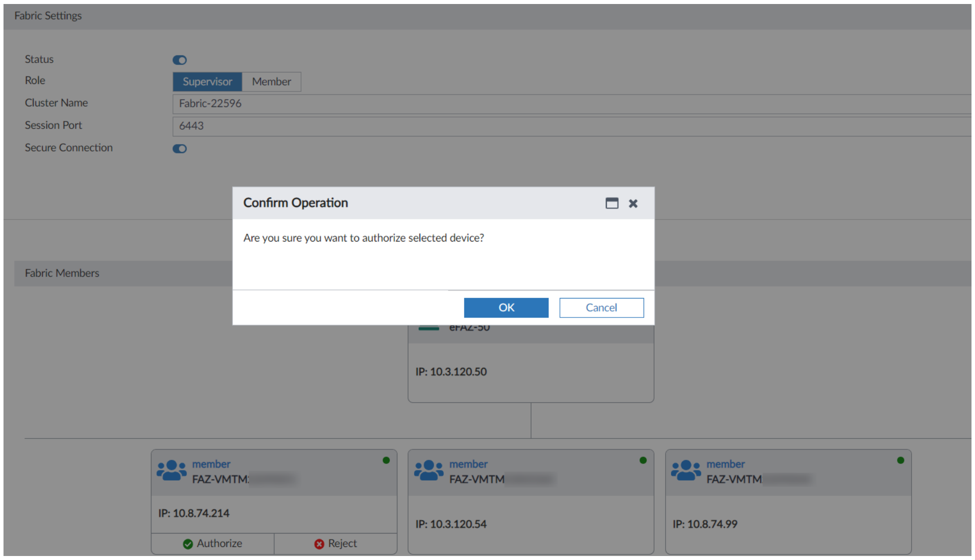
supervisor
eFAZ-50
IP: 10.3.120.50

member
FAZ-VMTM[redacted]
IP: 10.8.74.214
Authorize | Reject

member
FAZ-VMTM[redacted]
IP: 10.3.120.54

member
FAZ-VMTM[redacted]
IP: 10.8.74.99

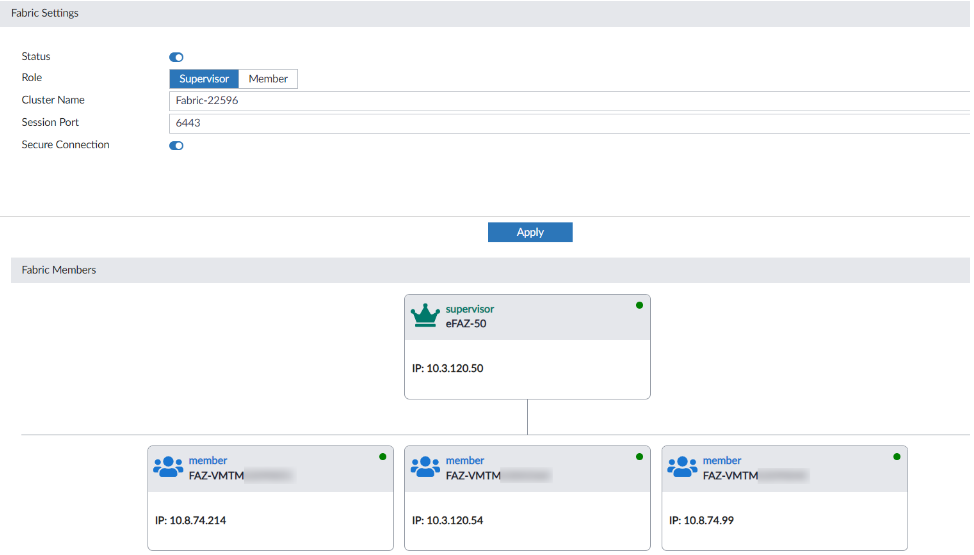
If authorized, the member will join the FortiAnalyzer Fabric and it will remain visible in the topology.



Confirm Operation

Are you sure you want to authorize selected device?

OK | Cancel



Fabric Settings

Status

Role: Supervisor | Member

Cluster Name: Fabric-22596

Session Port: 6443

Secure Connection

Fabric Members

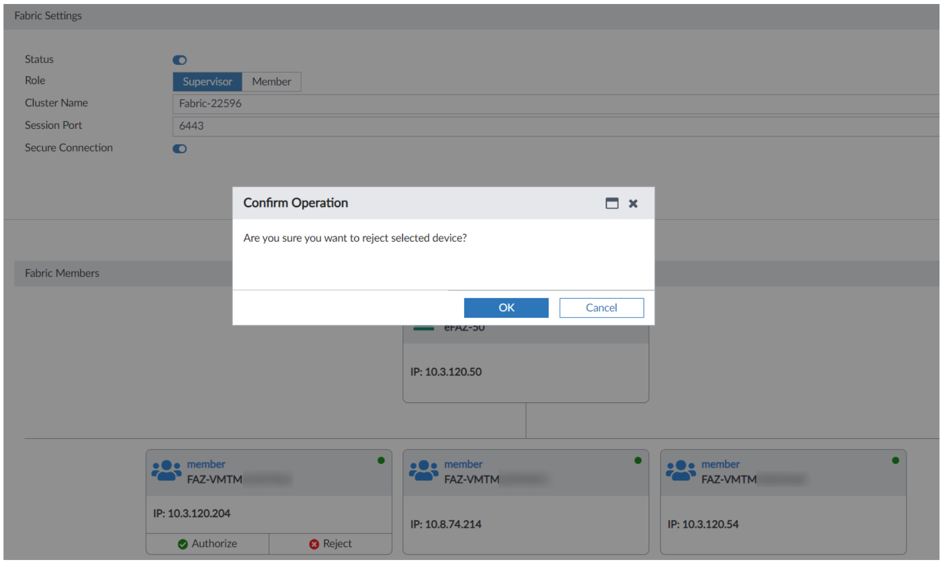
supervisor
eFAZ-50
IP: 10.3.120.50

member
FAZ-VMTM[redacted]
IP: 10.8.74.214

member
FAZ-VMTM[redacted]
IP: 10.3.120.54

member
FAZ-VMTM[redacted]
IP: 10.8.74.99

If rejected, the member will be removed from topology and it will be blocked from attempting to re-join the FortiAnalyzer Fabric for 10 minutes.



Fabric Settings

Status

Role: Supervisor | Member

Cluster Name: Fabric-22596

Session Port: 6443

Secure Connection

Confirm Operation

Are you sure you want to reject selected device?

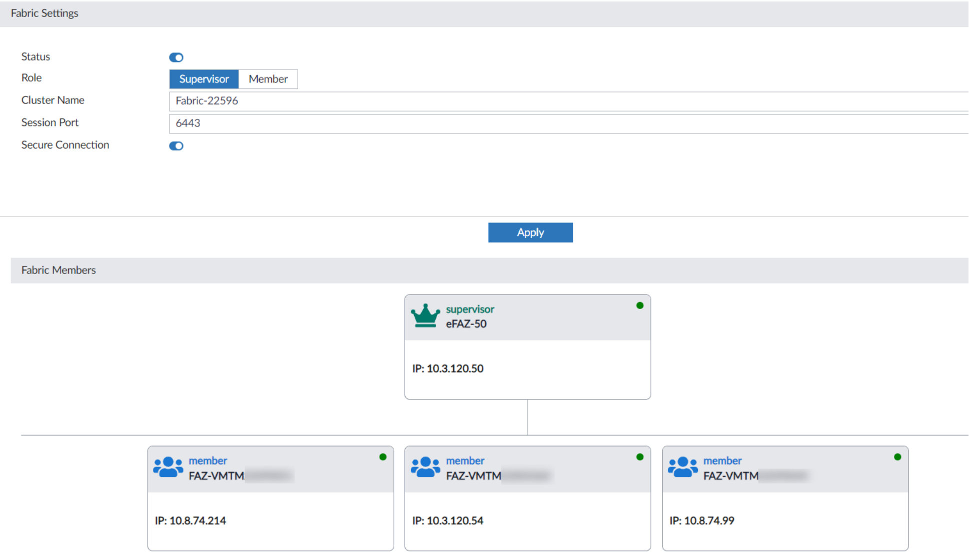
Fabric Members

eFAZ-50
IP: 10.3.120.50

member
FAZ-VMTM[redacted]
IP: 10.3.120.204

member
FAZ-VMTM[redacted]
IP: 10.8.74.214

member
FAZ-VMTM[redacted]
IP: 10.3.120.54



Fabric Settings

Status ●
Role Supervisor | Member
Cluster Name Fabric-22596
Session Port 6443
Secure Connection ●

Fabric Members

supervisor
eFAZ-50
IP: 10.3.120.50

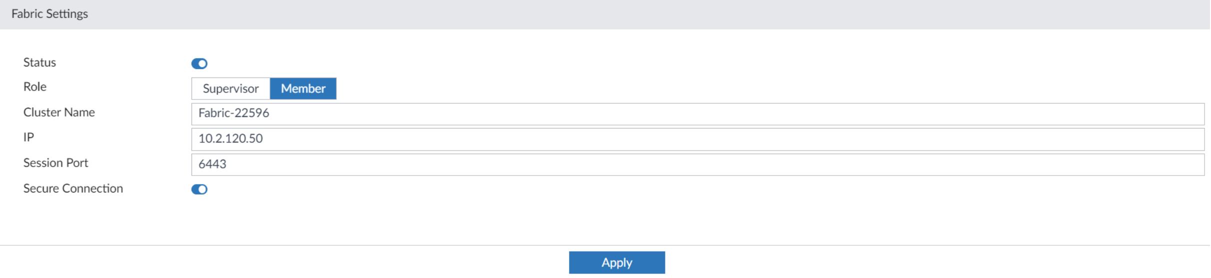
member
FAZ-VMTM[redacted]
IP: 10.8.74.214

member
FAZ-VMTM[redacted]
IP: 10.3.120.54

member
FAZ-VMTM[redacted]
IP: 10.8.74.99

FortiAnalyzer Fabric members:

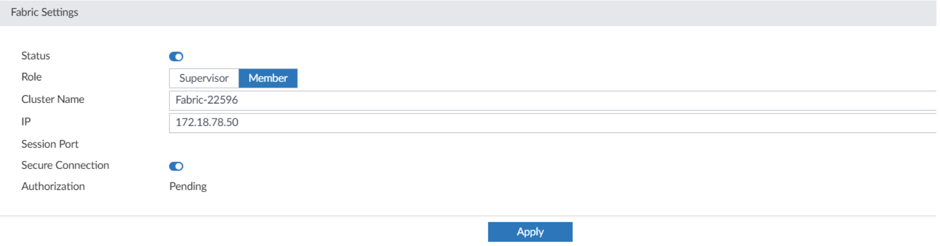
When joining a FortiAnalyzer Fabric as a member, go to *System Settings* > *Fabric Management*. You do not need to enter a password. Instead, enter the cluster name and IP of the supervisor.



Fabric Settings

Status ●
Role Supervisor | Member
Cluster Name Fabric-22596
IP 10.2.120.50
Session Port 6443
Secure Connection ●

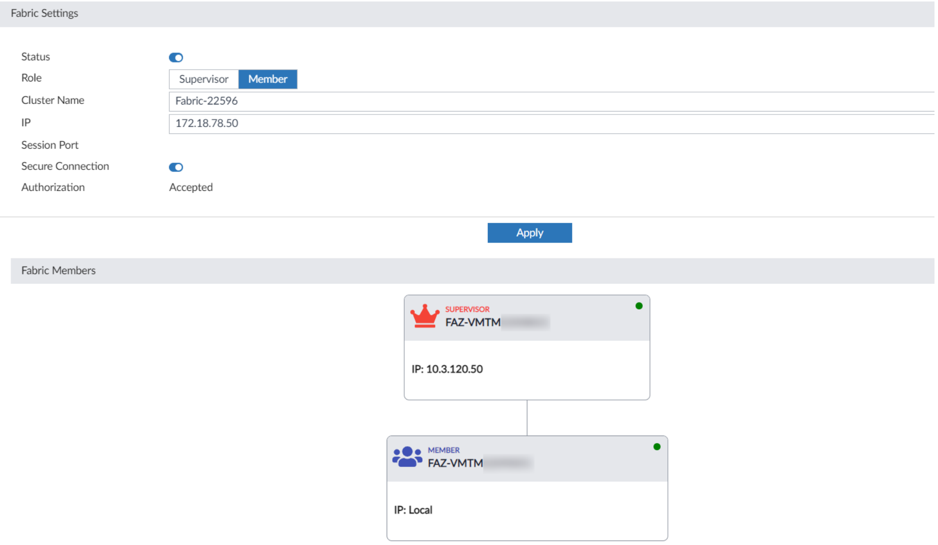
After configuring the FortiAnalyzer as a member, the *Authorization* field will display *Pending*.



Fabric Settings

Status ●
Role Supervisor | Member
Cluster Name Fabric-22596
IP 172.18.78.50
Session Port
Secure Connection ●
Authorization Pending

Once the member is authorized by the supervisor, the *Authorization* field will change to *Accepted*. The topology will display this member and the supervisor, but it will not display other members in the FortiAnalyzer Fabric.



Fabric Settings

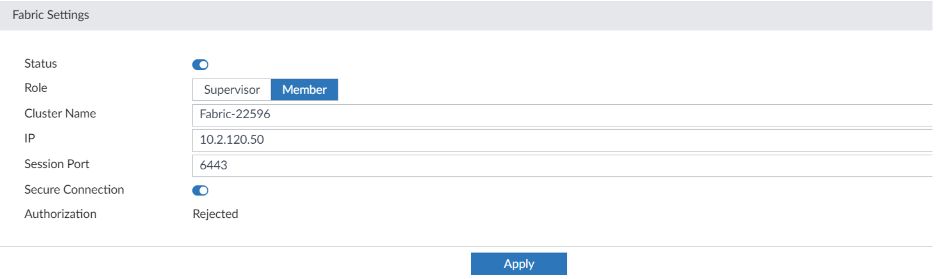
Status	●
Role	Supervisor [✓ Member]
Cluster Name	Fabric-22596
IP	172.18.78.50
Session Port	
Secure Connection	●
Authorization	Accepted

Fabric Members

SUPERVISOR
FAZ-VMTM[redacted]
IP: 10.3.120.50

MEMBER
FAZ-VMTM[redacted]
IP: Local

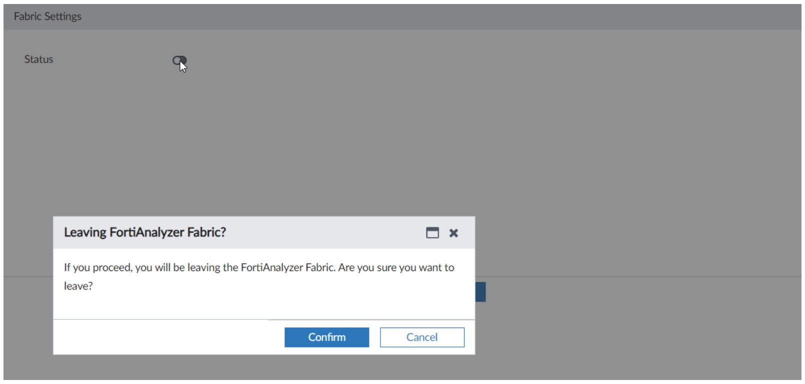
If the member is rejected by the supervisor, the *Authorization* field will change to *Rejected*. The member must wait 10 minutes before sending another request to join the FortiAnalyzer Fabric. To try again, click apply after the block-out time is complete.



Fabric Settings

Status	●
Role	Supervisor [✓ Member]
Cluster Name	Fabric-22596
IP	10.2.120.50
Session Port	6443
Secure Connection	●
Authorization	Rejected

To leave a FortiAnalyzer Fabric, go to *System Settings* > *Fabric Management* > *Fabric Settings* in the member and set the *Status* to disabled. A message will display to confirm the action.



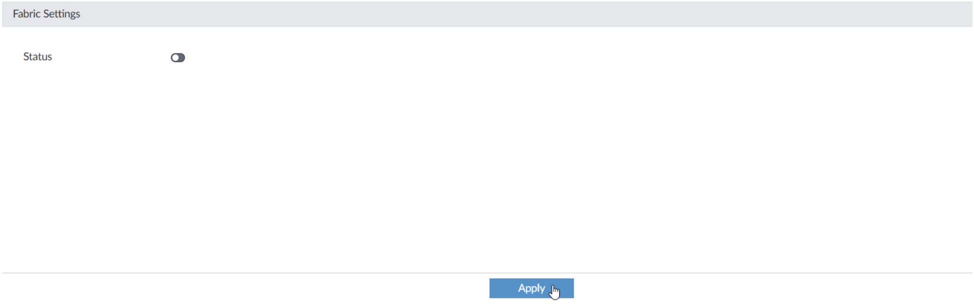
Fabric Settings

Status

Leaving FortiAnalyzer Fabric?

If you proceed, you will be leaving the FortiAnalyzer Fabric. Are you sure you want to leave?

After confirming the message, click *Apply* to save the configuration.



If needed, the member can re-join the FortiAnalyzer Fabric, but it will need to be authorized by the supervisor again.

Trusted-list for a FortiAnalyzer Fabric:

The `trusted-list` configuration is completed on the CLI for both the supervisor and the members.

In the supervisor's CLI, you can add members' serial numbers to a `trusted-list`. This supports wildcard; for example, FAZ-VMTM120033*. Once a member's serial number is added to the `trusted-list`, that FortiAnalyzer can automatically join the FortiAnalyzer Fabric as a member without the supervisor's authorization.

To add a member to the `trusted-list`, enter the following command in the supervisor's CLI:

```
config system soc-fabric
   config trusted-list
      edit 1
      set serial <member's serial number, which can include wildcards (*)>
   end
end
```

In the member's CLI, you can configure a `trusted-list` with the supervisor's serial number to verify the legitimacy of the supervisor. This prevents data leakage to a falsified supervisor. Members will only join the FortiAnalyzer Fabric when the supervisor's serial number matches the members `trusted-list`.

To configure a `trusted-list` on a member, enter the following command in the member's CLI:

```
config system soc-fabric
   config trusted-list
      edit 1
      set serial <Supervisor's serial number>
   end
end
```

For members without a `trusted-list` configured, they will treat all supervisors as legitimate.

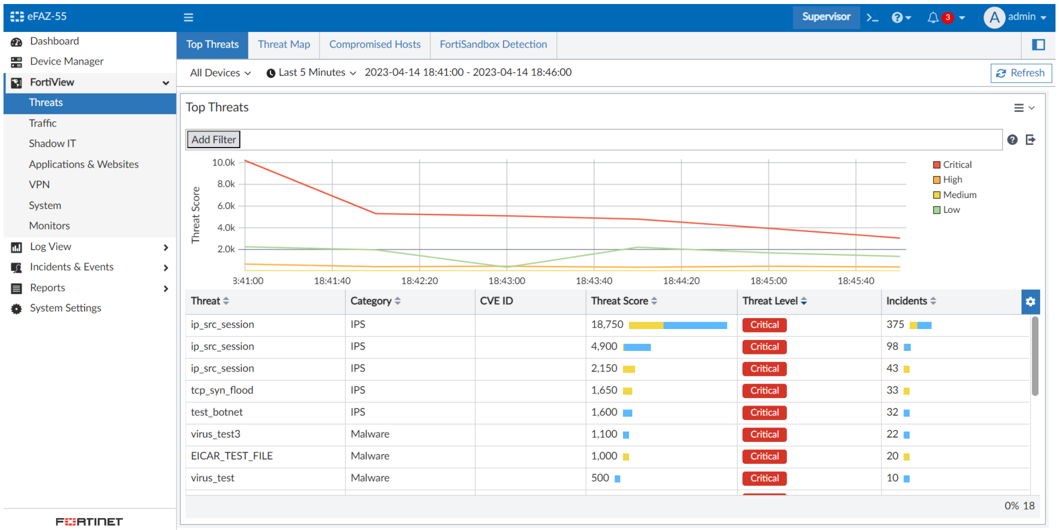
Fabric of FAZ global FortiView support

This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

- FortiView

The FortiAnalyzer supervisor allows you to see FortiView analytics across the entire FortiAnalyzer Fabric. For more granular analysis, you can filter by the FortiAnalyzer members or ADOMs.

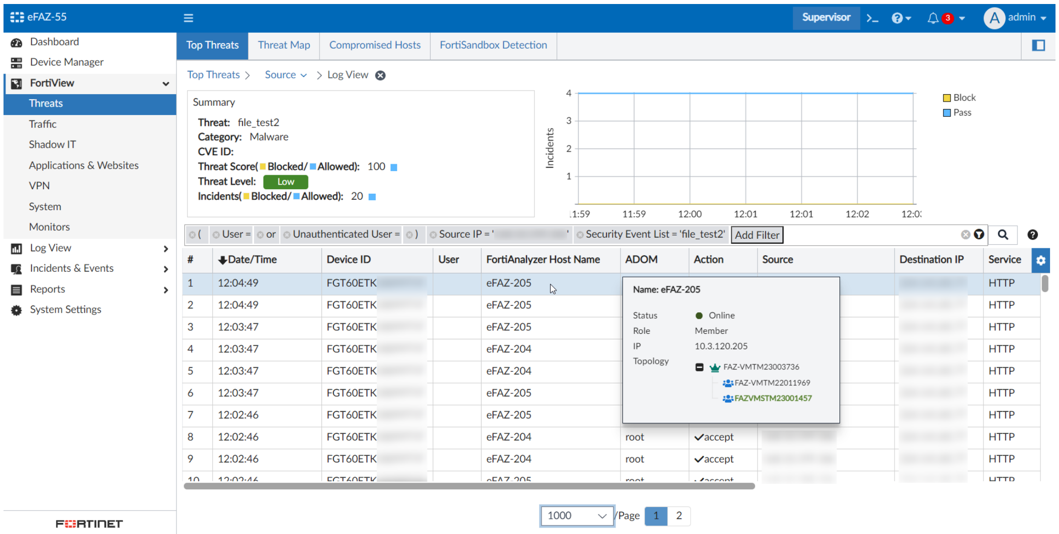
In the FortiAnalyzer Fabric supervisor, go to the *FortiView* panes. The information in these panes are generated from all members in the Fabric cluster. See the below example of *FortiView > Threats > Top Threats*.



Threat	Category	CVE ID	Threat Score	Threat Level	Incidents
ip_src_session	IPS		18,750	Critical	375
ip_src_session	IPS		4,900	Critical	98
ip_src_session	IPS		2,150	Critical	43
tcp_syn_flood	IPS		1,650	Critical	33
test_botnet	IPS		1,600	Critical	32
virus_test3	Malware		1,100	Critical	22
EICAR_TEST_FILE	Malware		1,000	Critical	20
virus_test	Malware		500	Critical	10

0% 18

Double-click an entry to drill down to a *Log View* of the information. In this view, you can determine the member using the *FortiAnalyzer Host Name* column.



Summary

Threat: file_test2
Category: Malware
CVE ID:
Threat Score(Blocked/Allowed): 100
Threat Level: Low
Incidents(Blocked/Allowed): 20

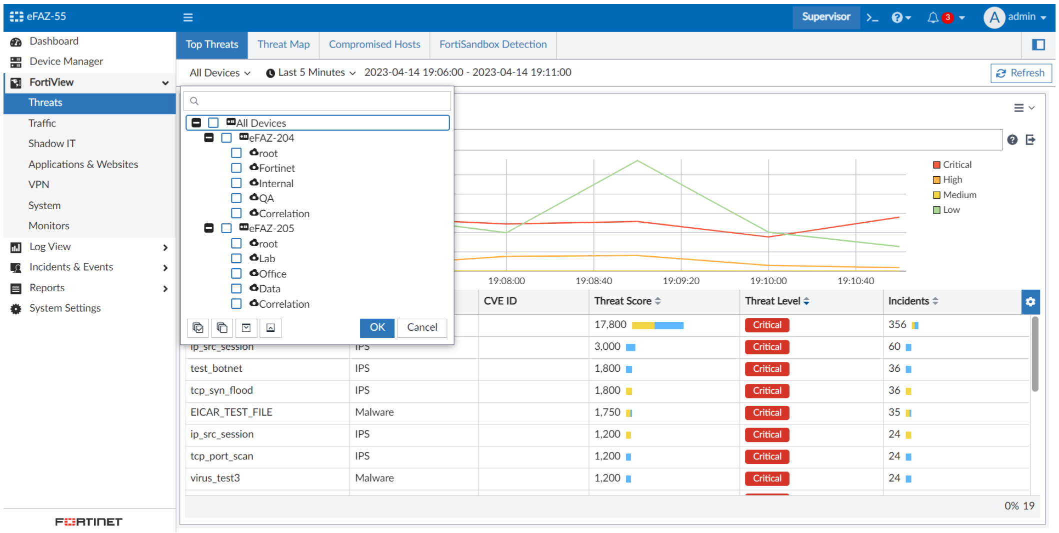
(User = or Unauthenticated User =) Source IP = '[redacted]' Security Event List = 'file_test2'

#	Date/Time	Device ID	User	FortiAnalyzer Host Name	ADOM	Action	Source	Destination IP	Service
1	12:04:49	FGT60ETK[redacted]		eFAZ-205				[redacted]	HTTP
2	12:04:49	FGT60ETK[redacted]		eFAZ-205				[redacted]	HTTP
3	12:03:47	FGT60ETK[redacted]		eFAZ-205				[redacted]	HTTP
4	12:03:47	FGT60ETK[redacted]		eFAZ-204				[redacted]	HTTP
5	12:03:47	FGT60ETK[redacted]		eFAZ-204				[redacted]	HTTP
6	12:03:47	FGT60ETK[redacted]		eFAZ-205				[redacted]	HTTP
7	12:02:46	FGT60ETK[redacted]		eFAZ-205				[redacted]	HTTP
8	12:02:46	FGT60ETK[redacted]		eFAZ-204	root	✓accept	[redacted]	[redacted]	HTTP
9	12:02:46	FGT60ETK[redacted]		eFAZ-204	root	✓accept	[redacted]	[redacted]	HTTP
10	12:02:46	FGT60ETK[redacted]		eFAZ-205	root	✓accept	[redacted]	[redacted]	HTTP

Name: eFAZ-205
Status: ● Online
Role: Member
IP: 10.3.120.205
Topology: FAZ-VMTM23003736
FAZ-VMTM22011969
FAZVMSTM23001457

1000 /Page 1 2

You can also filter the *FortiView* panes by the Fabric members or ADOMs in the device list.



		CVE ID	Threat Score	Threat Level	Incidents
			17,800	Critical	356
ip_src_session	IPS		3,000	Critical	60
test_botnet	IPS		1,800	Critical	36
tcp_syn_flood	IPS		1,800	Critical	36
EICAR_TEST_FILE	Malware		1,750	Critical	35
ip_src_session	IPS		1,200	Critical	24
tcp_port_scan	IPS		1,200	Critical	24
virus_test3	Malware		1,200	Critical	24

Fabric of FAZ: Central report support and creating Fabric groups

This information is also available in the FortiAnalyzer 7.4 Fabric Deployment Guide:

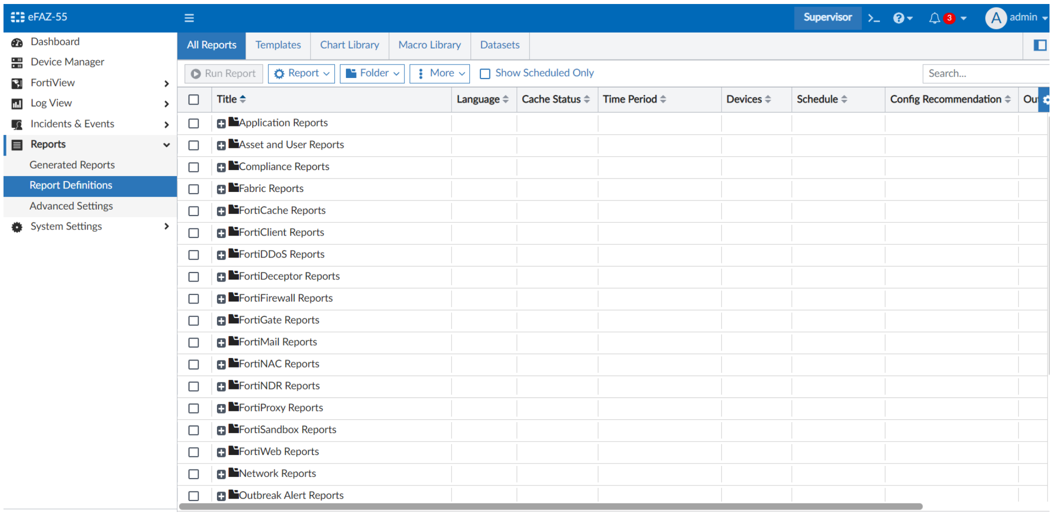
- Reports
- Fabric Groups

Reports can now be executed from the Fabric supervisor that fetches and aggregates data from multiple FortiAnalyzer Fabric members. Reports are centrally visible on the supervisor.

Additionally, FortiAnalyzer Fabric members or ADOMs can be grouped in a Fabric Group, which can be used in the *Log View*, *FortiView* and *Reports* device filter.

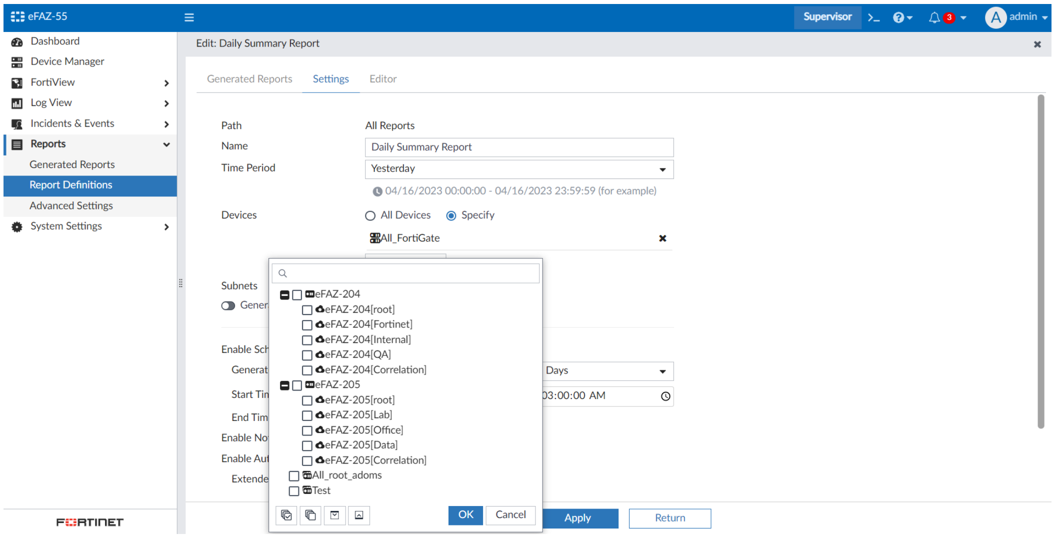
Reports:

The *Reports* panes are available in the FortiAnalyzer Fabric supervisor.



□	Title	Language	Cache Status	Time Period	Devices	Schedule	Config Recommendation	Ou
□	Application Reports							
□	Asset and User Reports							
□	Compliance Reports							
□	Fabric Reports							
□	FortiCache Reports							
□	FortiClient Reports							
□	FortiDDoS Reports							
□	FortiDeceptor Reports							
□	FortiFirewall Reports							
□	FortiGate Reports							
□	FortiMail Reports							
□	FortiNAC Reports							
□	FortiNDR Reports							
□	FortiProxy Reports							
□	FortiSandbox Reports							
□	FortiWeb Reports							
□	Network Reports							
□	Outbreak Alert Reports							

In the supervisor, you can edit a report to specify which devices (Fabric members, ADOMs, and Fabric Groups) to include when running the report.



Path: All Reports

Name: Daily Summary Report

Time Period: Yesterday

04/16/2023 00:00:00 - 04/16/2023 23:59:59 (for example)

Devices: ○ All Devices ● Specify

All_FortiGate

Subnets

Gener

Enable Sch

Generat — Days

Start Tin — 03:00:00 AM

End Tim

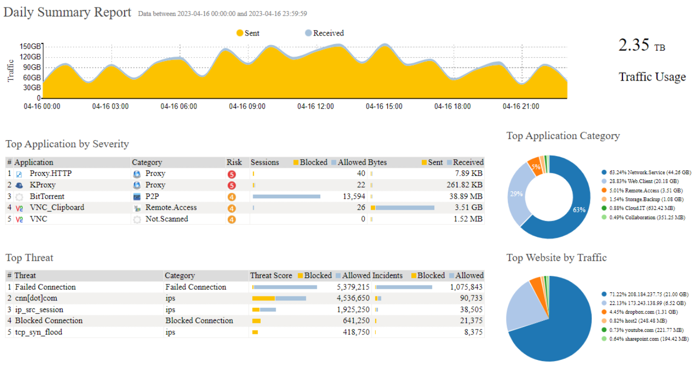
Enable No

Enable Aut

Extende

- □ eFAZ-204
  - □ eFAZ-204[root]
  - □ eFAZ-204[Fortinet]
  - □ eFAZ-204[Internal]
  - □ eFAZ-204[QA]
  - □ eFAZ-204[Correlation]
- □ eFAZ-205
  - □ eFAZ-205[root]
  - □ eFAZ-205[Lab]
  - □ eFAZ-205[Office]
  - □ eFAZ-205[Data]
  - □ eFAZ-205[Correlation]
- □ All_root_adoms
- □ Test

The reports' formats, charts, and tables are the same as a regular FortiAnalyzer's, but they include aggregated results from all the selected members.


Daily Summary Report
Data between 2023-04-16 00:00:00 and 2023-04-16 23:59:59
Sent
Received
Traffic
150GB
120GB
90GB
60GB
30GB
0
04-16 00:00
04-16 03:00
04-16 06:00
04-16 09:00
04-16 12:00
04-16 15:00
04-16 18:00
04-16 21:00
2.35 TB
Traffic Usage
Top Application Category
5%
29%
63%
63.24% Network.Service (44.26 GB)
28.83% Web.Client (20.18 GB)
5.01% Remote.Access (3.51 GB)
1.54% Storage.Backup (1.08 GB)
0.88% Cloud.IT (632.42 MB)
0.49% Collaboration (351.25 MB)
Top Website by Traffic
71.22% 208.184.237.75 (21.00 GB)
22.13% 173.243.138.99 (6.52 GB)
4.45% dropbox.com (1.31 GB)
0.82% host2 (248.48 MB)
0.73% youtube.com (221.77 MB)
0.64% sharepoint.com (194.42 MB)

Top Application by Severity

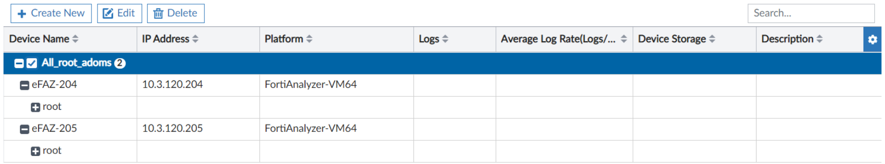
#	Application	Category	Risk	Sessions ■ Blocked ■ Allowed	Bytes ■ Sent ■ Received
1	Proxy.HTTP	Proxy	5	40	7.89 KB
2	KProxy	Proxy	5	22	261.82 KB
3	BitTorrent	P2P	4	13,594	38.89 MB
4	VNC_Clipboard	Remote.Access	4	26	3.51 GB
5	VNC	Not.Scanned	4	0	1.52 MB

Top Threat

#	Threat	Category	Threat Score ■ Blocked ■ Allowed	Incidents ■ Blocked ■ Allowed
1	Failed Connection	Failed Connection	5,379,215	1,075,843
2	cnn[dot]com	ips	4,536,650	90,733
3	ip_src_session	ips	1,925,250	38,505
4	Blocked Connection	Blocked Connection	641,250	21,375
5	tcp_syn_flood	ips	418,750	8,375

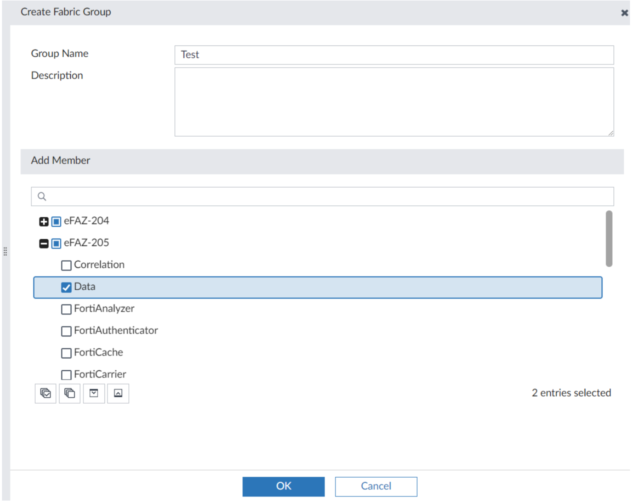
To create a Fabric Group in a FortiAnalyzer Fabric:

1. In the FortiAnalyzer Fabric supervisor, go to *System Settings > Fabric Management > Fabric Groups*.



Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/...	Device Storage	Description
☑ All_root_adoms 2						
eFAZ-204	10.3.120.204	FortiAnalyzer-VM64				
root						
eFAZ-205	10.3.120.205	FortiAnalyzer-VM64				
root						

2. Click *Create New*.
3. In the *Group Name* field, enter a name for the Fabric Group.
4. In the *Add Member* section, select the FortiAnalyzer Fabric members to include.
   To add only specific ADOMs from the member, expand the member in the list and select the ADOMs to include.



Group Name: Test

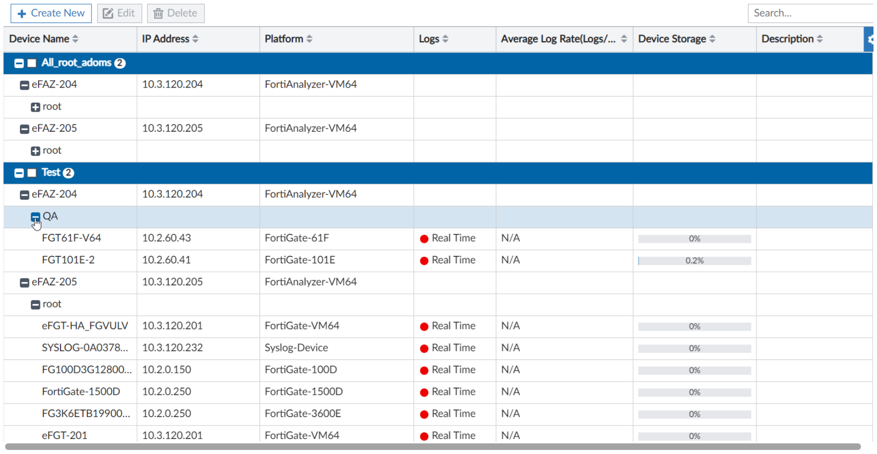
Description:

- ⊞ ■ eFAZ-204
- ⊟ ■ eFAZ-205
  - ☐ Correlation
  - ☑ Data
  - ☐ FortiAnalyzer
  - ☐ FortiAuthenticator
  - ☐ FortiCache
  - ☐ FortiCarrier

2 entries selected

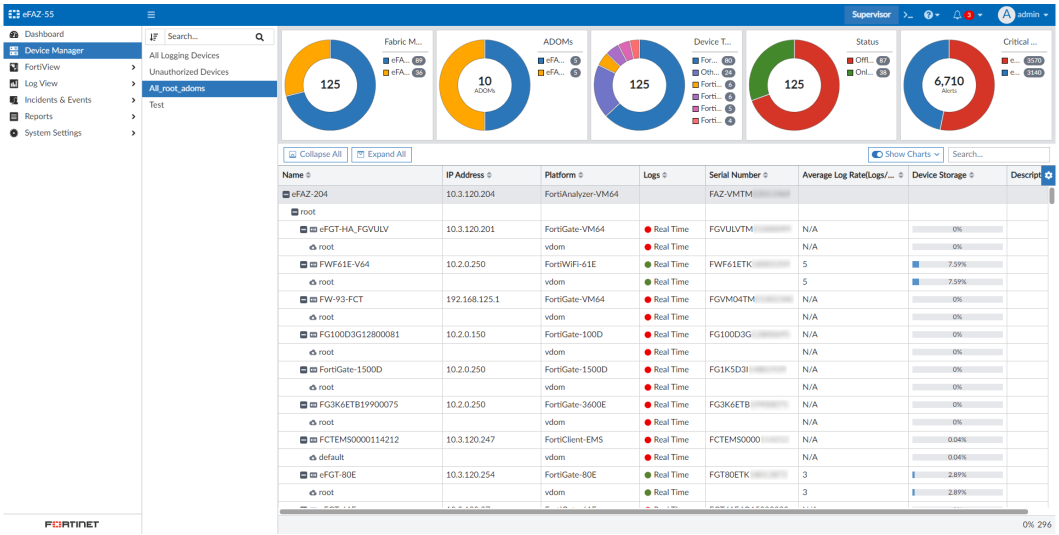
5. Click *OK*.

The Fabric Group can now be edited or deleted from the table.



Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/...	Device Storage	Description
⊟ ■ All_root_adoms 2						
⊟ eFAZ-204	10.3.120.204	FortiAnalyzer-VM64				
⊞ root						
⊟ eFAZ-205	10.3.120.205	FortiAnalyzer-VM64				
⊞ root						
⊟ ■ Test 2						
⊟ eFAZ-204	10.3.120.204	FortiAnalyzer-VM64				
⊟ QA						
FGT61F-V64	10.2.60.43	FortiGate-61F	● Real Time	N/A	0%	
FGT101E-2	10.2.60.41	FortiGate-101E	● Real Time	N/A	0.2%	
⊟ eFAZ-205	10.3.120.205	FortiAnalyzer-VM64				
⊟ root						
eFGT-HA_FGVULV	10.3.120.201	FortiGate-VM64	● Real Time	N/A	0%	
SYSLOG-0A0378...	10.3.120.232	Syslog-Device	● Real Time	N/A	0%	
FG100D3G12800...	10.2.0.150	FortiGate-100D	● Real Time	N/A	0%	
FortiGate-1500D	10.2.0.250	FortiGate-1500D	● Real Time	N/A	0%	
FG3K6ETB19900...	10.2.0.250	FortiGate-3600E	● Real Time	N/A	0%	
eFGT-201	10.3.120.201	FortiGate-VM64	● Real Time	N/A	0%	

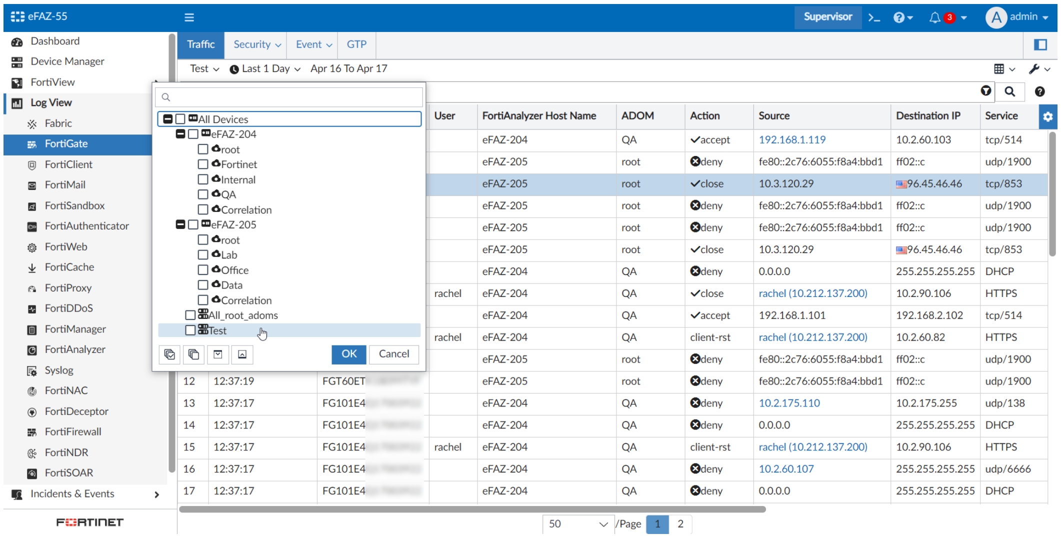
The Fabric Group is also visible in *Device Manager*.



Name	IP Address	Platform	Logs	Serial Number	Average Log Rate(Logs/...	Device Storage	Descript
⊟ eFAZ-204	10.3.120.204	FortiAnalyzer-VM64		FAZ-VMTM[redacted]			
⊟ root							
⊟ eFGT-HA_FGVULV	10.3.120.201	FortiGate-VM64	● Real Time	FGVULVTM[redacted]	N/A	0%	
root		vdom	● Real Time		N/A	0%	
⊟ FWF61E-V64	10.2.0.250	FortiWiFi-61E	● Real Time	FWF61ETK[redacted]	5	7.59%	
root		vdom	● Real Time		5	7.59%	
⊟ FW-93-FCT	192.168.125.1	FortiGate-VM64	● Real Time	FGVM04TM[redacted]	N/A	0%	
root		vdom	● Real Time		N/A	0%	
⊟ FG100D3G12800081	10.2.0.150	FortiGate-100D	● Real Time	FG100D3G[redacted]	N/A	0%	
root		vdom	● Real Time		N/A	0%	
⊟ FortiGate-1500D	10.2.0.250	FortiGate-1500D	● Real Time	FG1K5D3I[redacted]	N/A	0%	
root		vdom	● Real Time		N/A	0%	
⊟ FG3K6ETB19900075	10.2.0.250	FortiGate-3600E	● Real Time	FG3K6ETB[redacted]	N/A	0%	
root		vdom	● Real Time		N/A	0%	
⊟ FCTEMS0000114212	10.3.120.247	FortiClient-EMS	● Real Time	FCTEMS0000[redacted]	N/A	0.04%	
default		vdom	● Real Time		N/A	0.04%	
⊟ eFGT-80E	10.3.120.254	FortiGate-80E	● Real Time	FGT80ETK[redacted]	3	2.89%	
root		vdom	● Real Time		3	2.89%	

0% 296

It can be selected in the device filter for *FortiView*, *Log View*, and *Reports*. See an example in *Log View* below.



			User	FortiAnalyzer Host Name	ADOM	Action	Source	Destination IP	Service
				eFAZ-204	QA	✓accept	192.168.1.119	10.2.60.103	tcp/514
				eFAZ-205	root	⊗deny	fe80::2c76:6055:f8a4:bbd1	ff02::c	udp/1900
				eFAZ-205	root	✓close	10.3.120.29	96.45.46.46	tcp/853
				eFAZ-205	root	⊗deny	fe80::2c76:6055:f8a4:bbd1	ff02::c	udp/1900
				eFAZ-205	root	⊗deny	fe80::2c76:6055:f8a4:bbd1	ff02::c	udp/1900
				eFAZ-205	root	✓close	10.3.120.29	96.45.46.46	tcp/853
				eFAZ-204	QA	⊗deny	0.0.0.0	255.255.255.255	DHCP
			rachel	eFAZ-204	QA	✓close	rachel (10.212.137.200)	10.2.90.106	HTTPS
				eFAZ-204	QA	✓accept	192.168.1.101	192.168.2.102	tcp/514
			rachel	eFAZ-204	QA	client-rst	rachel (10.212.137.200)	10.2.60.82	HTTPS
				eFAZ-205	root	⊗deny	fe80::2c76:6055:f8a4:bbd1	ff02::c	udp/1900
12	12:37:19	FGT60ET[redacted]		eFAZ-205	root	⊗deny	fe80::2c76:6055:f8a4:bbd1	ff02::c	udp/1900
13	12:37:17	FG101E4[redacted]		eFAZ-204	QA	⊗deny	10.2.175.110	10.2.175.255	udp/138
14	12:37:17	FG101E4[redacted]		eFAZ-204	QA	⊗deny	0.0.0.0	255.255.255.255	DHCP
15	12:37:17	FG101E4[redacted]	rachel	eFAZ-204	QA	client-rst	rachel (10.212.137.200)	10.2.90.106	HTTPS
16	12:37:17	FG101E4[redacted]		eFAZ-204	QA	⊗deny	10.2.60.107	255.255.255.255	udp/6666
17	12:37:17	FG101E4[redacted]		eFAZ-204	QA	⊗deny	0.0.0.0	255.255.255.255	DHCP

Block out contract device from upgrading to next or major or minor release

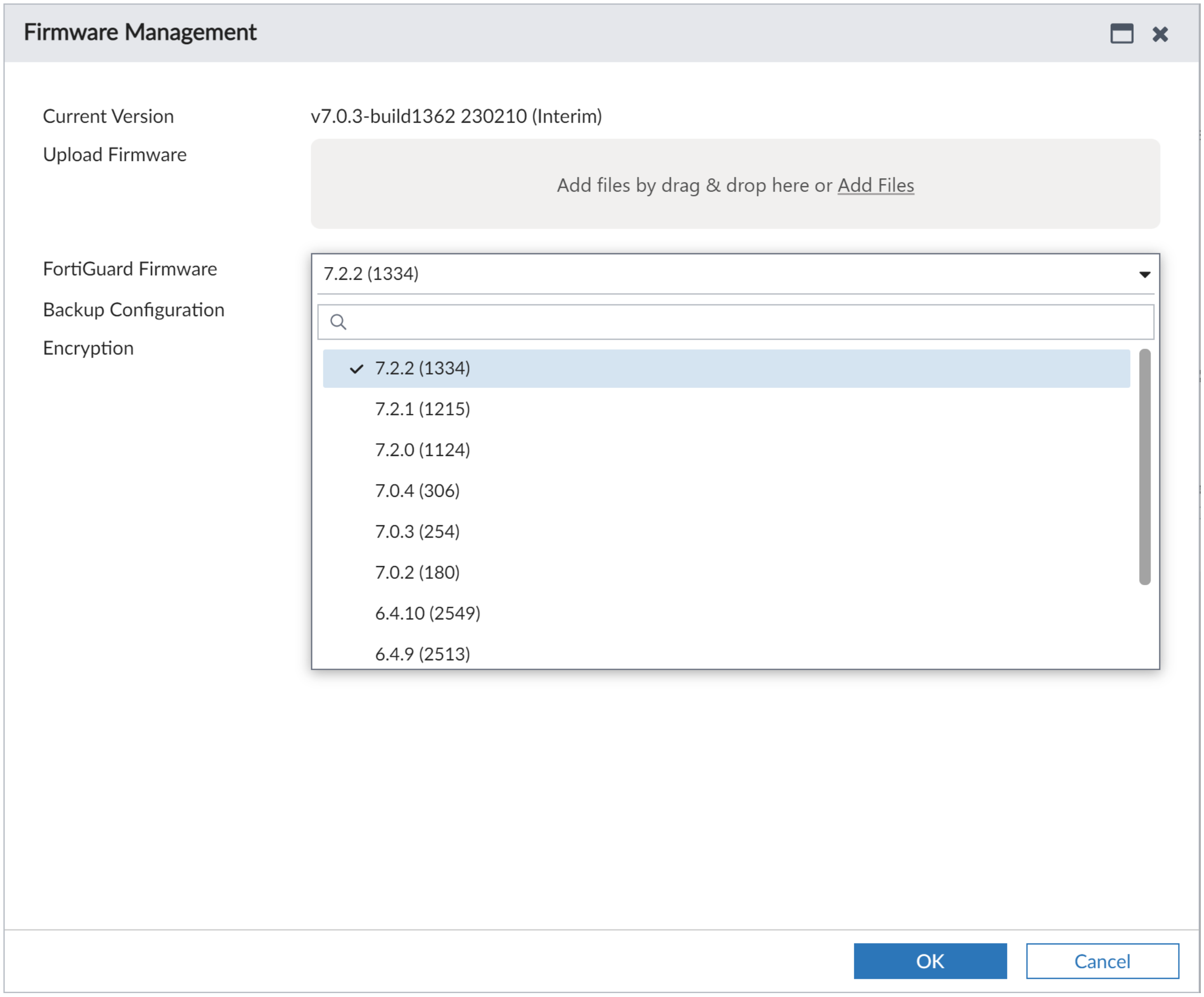
This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- Updating the system firmware

To view available FortiGuard images:

1. A FortiAnalyzer with a valid contract will display all available FortiGuard images and allow upgrading or downgrading to any version.

- System Settings:



Firmware Management

Current Version v7.0.3-build1362 230210 (Interim)

Upload Firmware

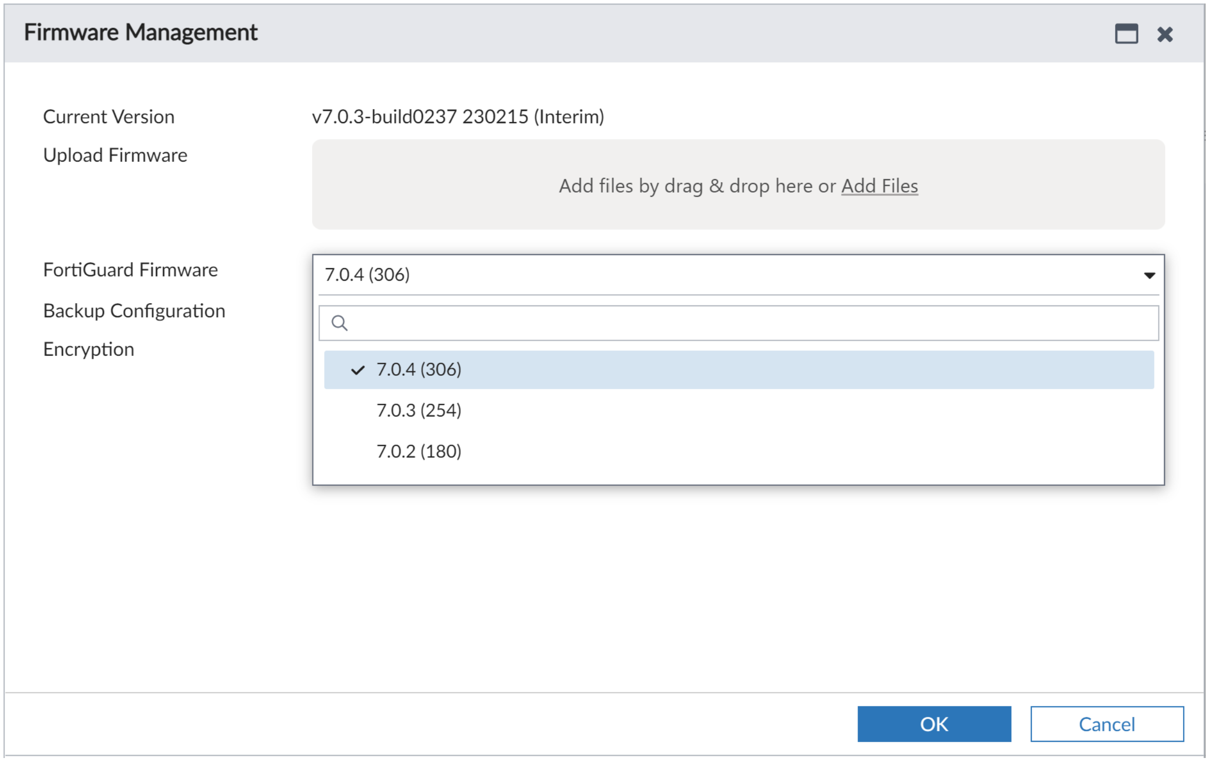
FortiGuard Firmware 7.2.2 (1334)

Backup Configuration

Encryption

2. A FortiAnalyzer without a valid contract or with an expired contract will only display available patch images and support patch upgrades.

- System Settings:



Firmware Management

Current Version v7.0.3-build0237 230215 (Interim)

Upload Firmware: Add files by drag & drop here or Add Files

FortiGuard Firmware: 7.0.4 (306)

Backup Configuration

Encryption

✓ 7.0.4 (306)

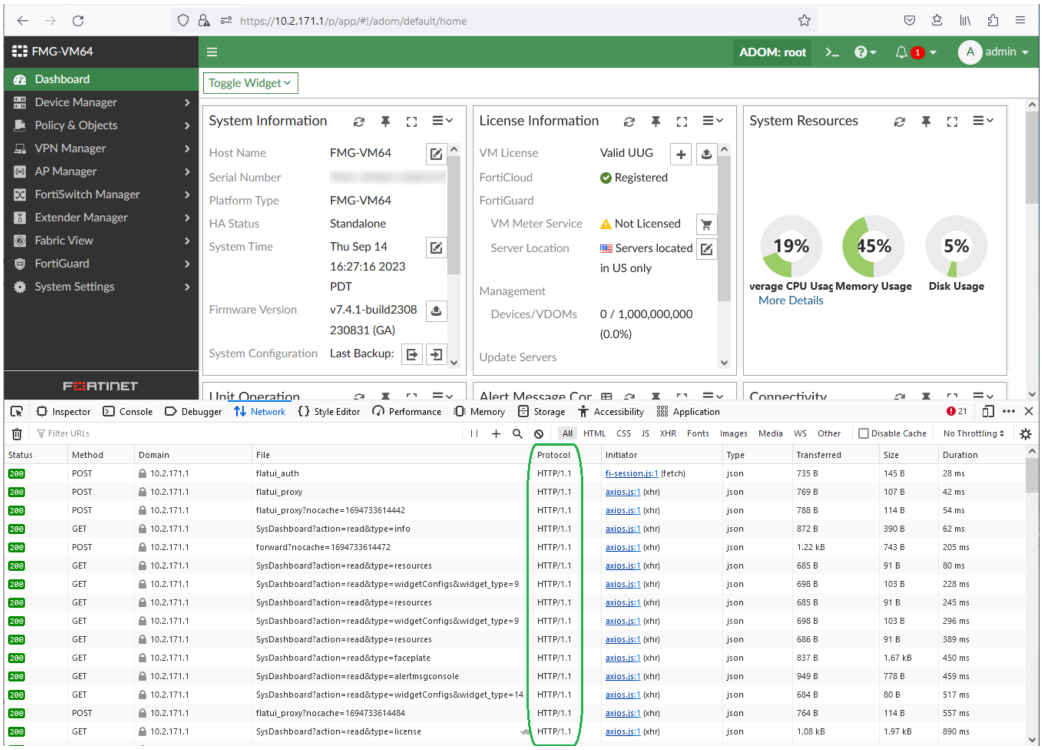
7.0.3 (254)

7.0.2 (180)

FortiManager and FortiAnalyzer support HTTP/2 for improved security, multiplexing, and reduced network latency - 7.4.1

FortiManager and FortiAnalyzer support HTTP/2 for improved security, multiplexing, and reduced network latency.

- Before this feature was implemented, HTTP/1.1 is used and can be viewed in the browser's Web Developer Tools:



https://10.2.171.1/p/app/#!/adom/default/home

FMG-VM64 · ADOM: root · admin

System Information

Host Name: FMG-VM64
Serial Number: [redacted]
Platform Type: FMG-VM64
HA Status: Standalone
System Time: Thu Sep 14 16:27:16 2023 PDT
Firmware Version: v7.4.1-build2308 230831 (GA)
System Configuration: Last Backup:

License Information

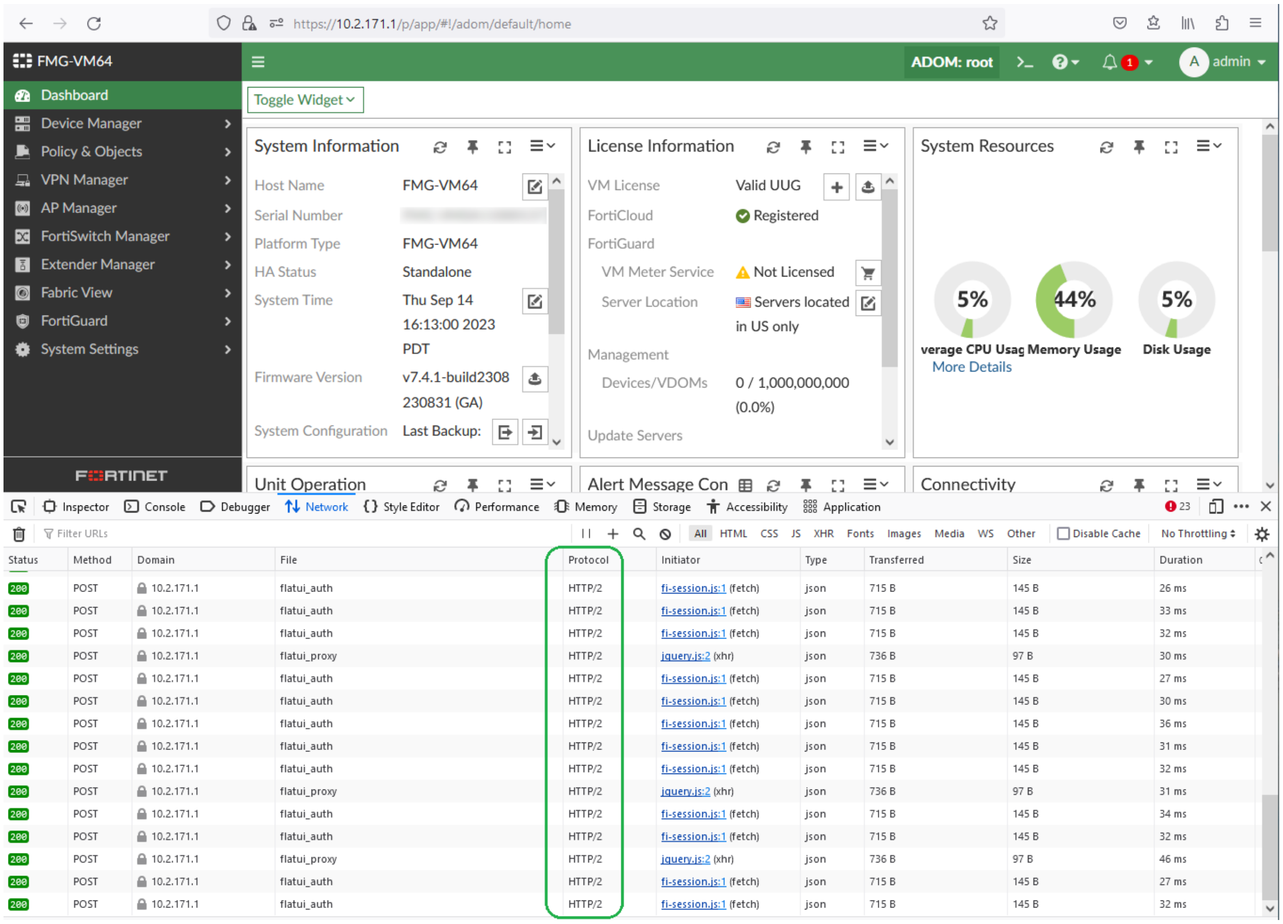
VM License: Valid UUG
FortiCloud: Registered
FortiGuard
VM Meter Service: Not Licensed
Server Location: Servers located in US only
Management
Devices/VDOMs: 0 / 1,000,000,000 (0.0%)
Update Servers

System Resources

19% verage CPU Usag · 45% Memory Usage · 5% Disk Usage
More Details

Status	Method	Domain	File	Protocol	Initiator	Type	Transferred	Size	Duration
200	POST	10.2.171.1	flatui_auth	HTTP/1.1	fi-session.js:1 (fetch)	json	735 B	145 B	28 ms
200	POST	10.2.171.1	flatui_proxy	HTTP/1.1	axios.js:1 (xhr)	json	769 B	107 B	42 ms
200	POST	10.2.171.1	flatui_proxy?nocache=1694733614442	HTTP/1.1	axios.js:1 (xhr)	json	788 B	114 B	54 ms
200	GET	10.2.171.1	SysDashboard?action=read&type=info	HTTP/1.1	axios.js:1 (xhr)	json	872 B	390 B	62 ms
200	POST	10.2.171.1	forward?nocache=1694733614472	HTTP/1.1	axios.js:1 (xhr)	json	1.22 kB	743 B	205 ms
200	GET	10.2.171.1	SysDashboard?action=read&type=resources	HTTP/1.1	axios.js:1 (xhr)	json	685 B	91 B	80 ms
200	GET	10.2.171.1	SysDashboard?action=read&type=widgetConfigs&widget_type=9	HTTP/1.1	axios.js:1 (xhr)	json	698 B	103 B	228 ms
200	GET	10.2.171.1	SysDashboard?action=read&type=resources	HTTP/1.1	axios.js:1 (xhr)	json	685 B	91 B	245 ms
200	GET	10.2.171.1	SysDashboard?action=read&type=widgetConfigs&widget_type=9	HTTP/1.1	axios.js:1 (xhr)	json	698 B	103 B	296 ms
200	GET	10.2.171.1	SysDashboard?action=read&type=resources	HTTP/1.1	axios.js:1 (xhr)	json	686 B	91 B	389 ms
200	GET	10.2.171.1	SysDashboard?action=read&type=faceplate	HTTP/1.1	axios.js:1 (xhr)	json	837 B	1.67 kB	450 ms
200	GET	10.2.171.1	SysDashboard?action=read&type=alertmsgconsole	HTTP/1.1	axios.js:1 (xhr)	json	949 B	778 B	459 ms
200	GET	10.2.171.1	SysDashboard?action=read&type=widgetConfigs&widget_type=14	HTTP/1.1	axios.js:1 (xhr)	json	684 B	80 B	517 ms
200	POST	10.2.171.1	flatui_proxy?nocache=1694733614484	HTTP/1.1	axios.js:1 (xhr)	json	764 B	114 B	557 ms
200	GET	10.2.171.1	SysDashboard?action=read&type=license	HTTP/1.1	axios.js:1 (xhr)	json	1.08 kB	1.97 kB	890 ms

- After apache-mode is set to "event", HTTP/2 is used and can be viewed in the browser's Web Developer Tools:



https://10.2.171.1/p/app/#!/adom/default/home

FMG-VM64 · ADOM: root · admin

System Information

Host Name: FMG-VM64
Serial Number: [redacted]
Platform Type: FMG-VM64
HA Status: Standalone
System Time: Thu Sep 14 16:13:00 2023 PDT
Firmware Version: v7.4.1-build2308 230831 (GA)
System Configuration: Last Backup:

License Information

VM License: Valid UUG
FortiCloud: Registered
FortiGuard
VM Meter Service: Not Licensed
Server Location: Servers located in US only
Management
Devices/VDOMs: 0 / 1,000,000,000 (0.0%)
Update Servers

System Resources

5% verage CPU Usag · 44% Memory Usage · 5% Disk Usage
More Details

Status	Method	Domain	File	Protocol	Initiator	Type	Transferred	Size	Duration
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	26 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	33 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	32 ms
200	POST	10.2.171.1	flatui_proxy	HTTP/2	jquery.js:2 (xhr)	json	736 B	97 B	30 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	27 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	30 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	36 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	31 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	32 ms
200	POST	10.2.171.1	flatui_proxy	HTTP/2	jquery.js:2 (xhr)	json	736 B	97 B	31 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	34 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	32 ms
200	POST	10.2.171.1	flatui_proxy	HTTP/2	jquery.js:2 (xhr)	json	736 B	97 B	46 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	27 ms
200	POST	10.2.171.1	flatui_auth	HTTP/2	fi-session.js:1 (fetch)	json	715 B	145 B	32 ms

To configure the apache-mode in the FortiAnalyzer CLI:

Enter the following command in the FortiAnalyzer CLI:

```
config system global
   set apache-mode {event| prefork}
      event Apache event mode.
      prefork Apache prefork mode.
   set apache-mode event
end
```

Backup strategy and configuration setup added to the FortiAnalyzer setup wizard - 7.4.2

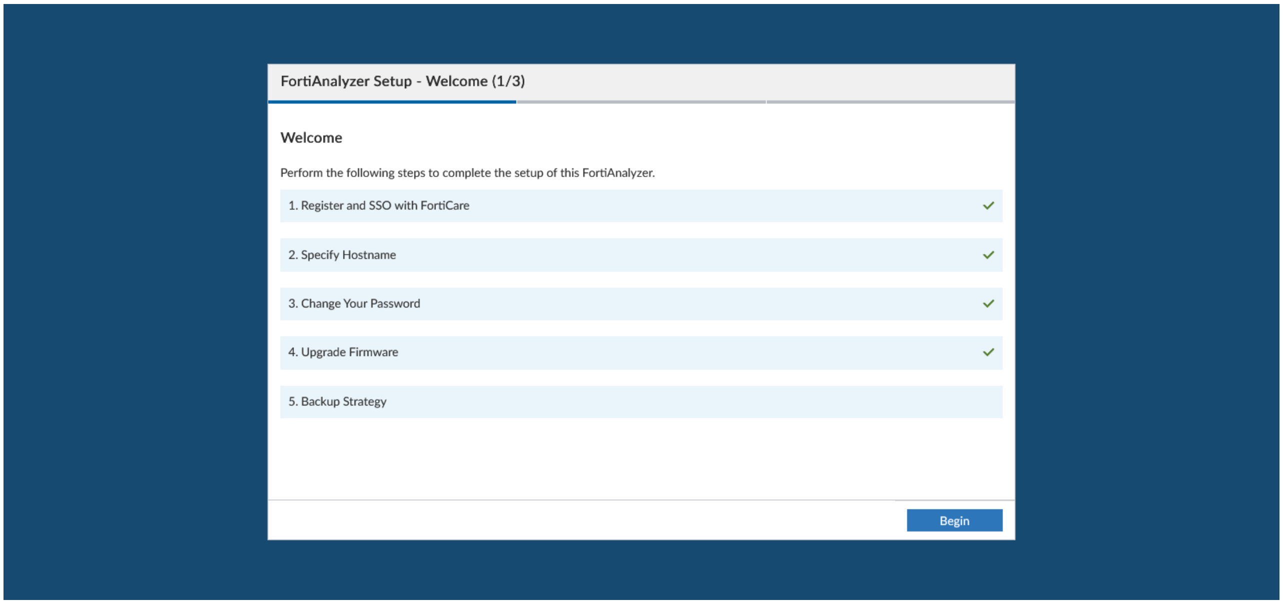
Backup strategy and configuration setup has been added to the FortiAnalyzer setup wizard.

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

- FortiAnalyzer Setup Wizard

To set a backup strategy using the onboarding wizard:

1. When logging into FortiAnalyzer, the new *Backup Strategy* option will be displayed as part of the setup wizard if it has not already been completed.



FortiAnalyzer Setup - Welcome (1/3)

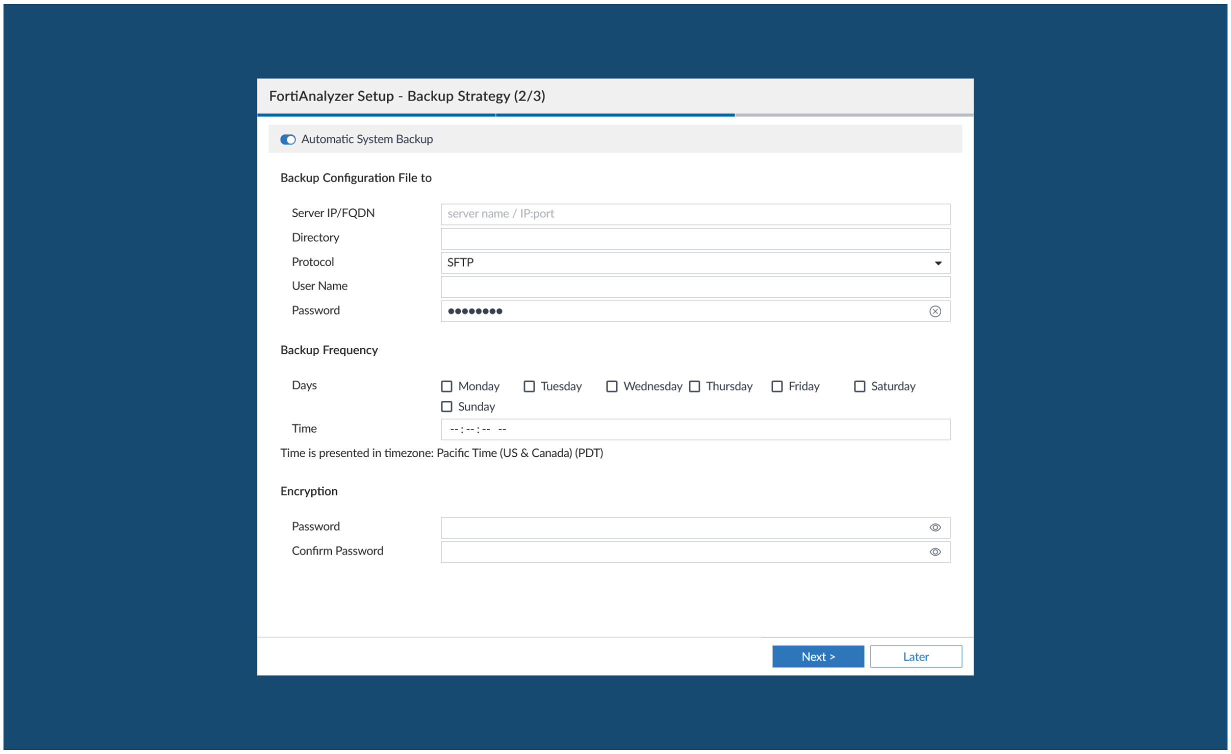
Welcome

Perform the following steps to complete the setup of this FortiAnalyzer.

1. Register and SSO with FortiCare ✓
2. Specify Hostname ✓
3. Change Your Password ✓
4. Upgrade Firmware ✓
5. Backup Strategy

2. After the *Register and SSO with FortiCare*, *Specify Hostname*, *Change Your Password*, and *Upgrade Firmware* steps are completed, you can proceed to configure your *Backup Strategy*.
   - If you do not wish to set a backup strategy at this time, you can click Later to postpone the task. Next time you log in to FortiAnalyzer, you will see that the *Backup Strategy* task is not completed and you will be prompted to complete the configuration.
3. To configure the backup strategy, enter the following configuration:

a. *Backup Configuration File to*: Settings that determine where the backup file will be saved.
b. *Backup Frequency*: Settings that determines how often the backup will be performed.
c. *Encryption*: Set a password for encryption of the backup configuration.
d. Click *Next* to complete the configuration.



FortiAnalyzer Setup - Backup Strategy (2/3)

Automatic System Backup

Backup Configuration File to

Server IP/FQDN	server name / IP:port
Directory	
Protocol	SFTP
User Name	
Password	••••••••

Backup Frequency

Days: □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

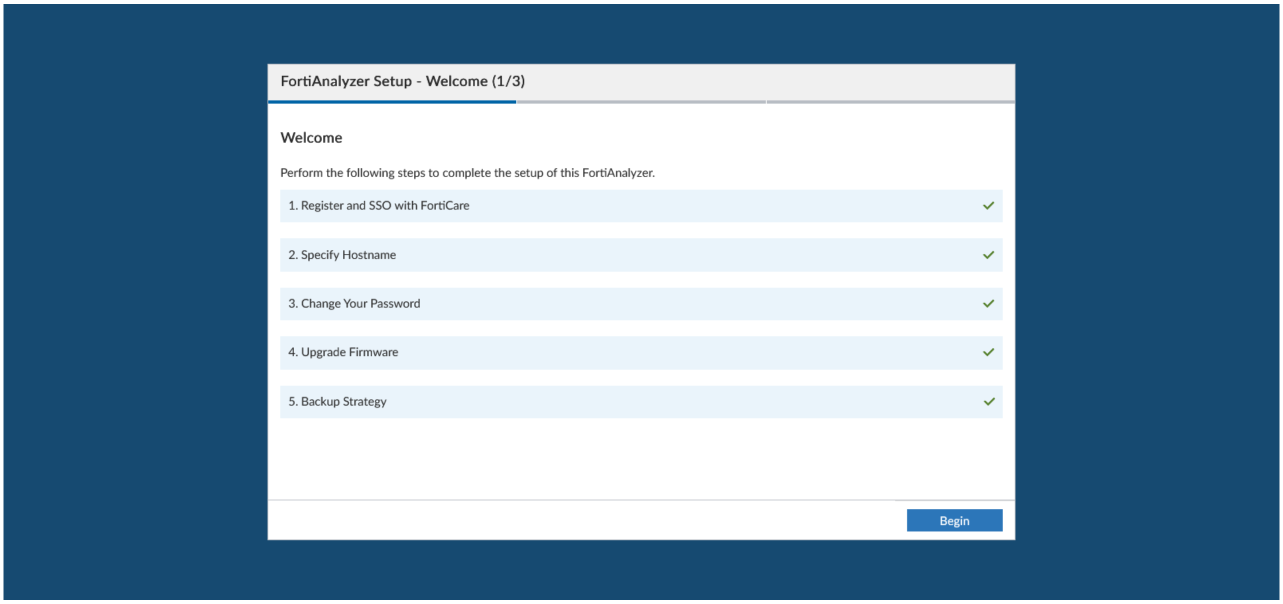
Time: -- : -- : -- --

Time is presented in timezone: Pacific Time (US & Canada) (PDT)

Encryption

Password	
Confirm Password	

The next time you log in to FortiAnalyzer, the Backup Strategy task will be displayed with a check mark indicating completion.



FortiAnalyzer Setup - Welcome (1/3)

Welcome

Perform the following steps to complete the setup of this FortiAnalyzer.

1. Register and SSO with FortiCare ✓
2. Specify Hostname ✓
3. Change Your Password ✓
4. Upgrade Firmware ✓
5. Backup Strategy ✓

You can go to *Dashboard* to view the *Next Backup* date and time in the *System Information* widget.

Cloud Services

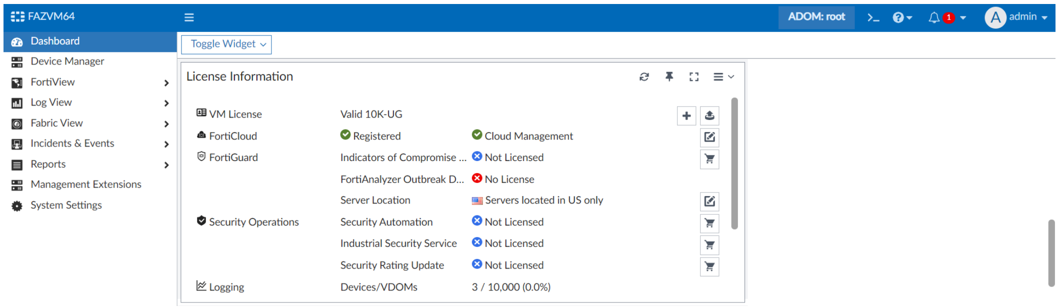
This section lists the new features added to FortiAnalyzer for cloud services:

- FortiAnalyzer supports FortiCare Elite Service on page 152

FortiAnalyzer supports FortiCare Elite Service

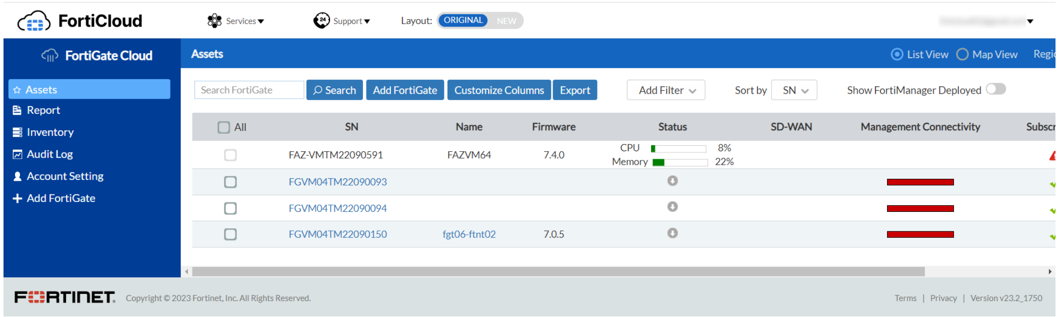
FortiAnalyzer and FortiAnalyzer Cloud now supports FortiCare Elite Service.

To use this service, cloud management must be enabled on the FortiAnalyzer and the FortiGate Cloud portal.



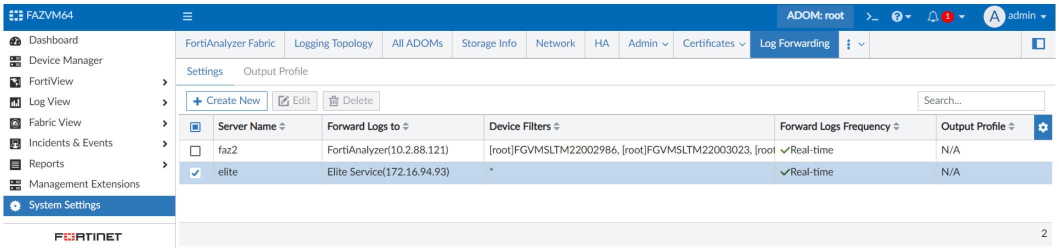
License Information

VM License	Valid 10K-UG	
FortiCloud	✓ Registered	✓ Cloud Management
FortiGuard	Indicators of Compromise ...	☒ Not Licensed
	FortiAnalyzer Outbreak D...	☒ No License
	Server Location	Servers located in US only
Security Operations	Security Automation	☒ Not Licensed
	Industrial Security Service	☒ Not Licensed
	Security Rating Update	☒ Not Licensed
Logging	Devices/VDOMs	3 / 10,000 (0.0%)



□ All	SN	Name	Firmware	Status	SD-WAN	Management Connectivity	Subscr
□	FAZ-VMTM22090591	FAZVM64	7.4.0	CPU 8% Memory 22%			
□	FGVM04TM22090093					🟥	
□	FGVM04TM22090094					🟥	
□	FGVM04TM22090150	fgt06-ftnt02	7.0.5			🟥	

Log forwarding configuration to the Elite Service can be viewed in the FortiAnalyzer GUI. This log forwarding configuration cannot be edited or deleted.



■	Server Name	Forward Logs to	Device Filters	Forward Logs Frequency	Output Profile
□	faz2	FortiAnalyzer(10.2.88.121)	[root]FGVMSLTM22002986, [root]FGVMSLTM22003023, [root	✓Real-time	N/A
☑	elite	Elite Service(172.16.94.93)	*	✓Real-time	N/A

The log forward configuration to Elite Service is also visible in the FortiAnalyzer CLI. For example:

```
config system log-forward
   edit 40000
      set mode forwarding
         set fwd-max-delay realtime
         set server-name "elite"
         set server-addr "172.16.94.93"
         set fwd-server-type elite-service
         set fwd-reliable enable
         set fwd-compression enable
         set fwd-archives disable
         set proxy-service disable
            config device-filter
               edit 1
                  set action include-like
                  set device "*"
               next
            end
         set log-filter-status enable
            config log-filter
               edit 1
                  set field level
                  set oper >=
                  set value "critical"
               next
               edit 2
                  set field logid
                  set value "0110052000"
               next
            end
         set signature 1449934396
      next
```

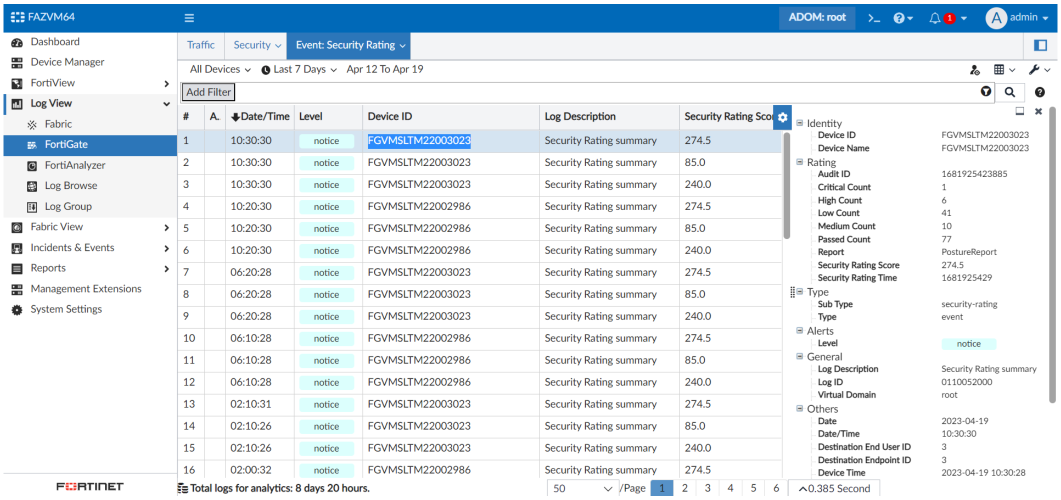
You can disable the Elite Service in the FortiAnalyzer CLI, if needed. It can also be re-enabled using the same command. In the FortiAnalyzer CLI, enter:

```
config system central-management
   set elite-service {enable | disable}
end
```

If `elite-service` is disabled, the log forwarding to Elite Service will automatically be removed. FGC will push the configuration back if the `elite-service` is later set to `enable`.

```
FAZVM64 # config system central-management
   (central-management)# get
   type  : cloud-management
   elite-service  : enable
```

Logs that meet the filter within the log forward configuration will be forwarded to Elite log server. See a sample log in the FortiAnalyzer GUI below:



#	A.	Date/Time	Level	Device ID	Log Description	Security Rating Sco
1		10:30:30	notice	FGVMSLTM22003023	Security Rating summary	274.5
2		10:30:30	notice	FGVMSLTM22003023	Security Rating summary	85.0
3		10:30:30	notice	FGVMSLTM22003023	Security Rating summary	240.0
4		10:20:30	notice	FGVMSLTM22002986	Security Rating summary	274.5
5		10:20:30	notice	FGVMSLTM22002986	Security Rating summary	85.0
6		10:20:30	notice	FGVMSLTM22002986	Security Rating summary	240.0
7		06:20:28	notice	FGVMSLTM22003023	Security Rating summary	274.5
8		06:20:28	notice	FGVMSLTM22003023	Security Rating summary	85.0
9		06:20:28	notice	FGVMSLTM22003023	Security Rating summary	240.0
10		06:10:28	notice	FGVMSLTM22002986	Security Rating summary	274.5
11		06:10:28	notice	FGVMSLTM22002986	Security Rating summary	85.0
12		06:10:28	notice	FGVMSLTM22002986	Security Rating summary	240.0
13		02:10:31	notice	FGVMSLTM22003023	Security Rating summary	274.5
14		02:10:26	notice	FGVMSLTM22003023	Security Rating summary	85.0
15		02:10:26	notice	FGVMSLTM22003023	Security Rating summary	240.0
16		02:00:32	notice	FGVMSLTM22002986	Security Rating summary	274.5

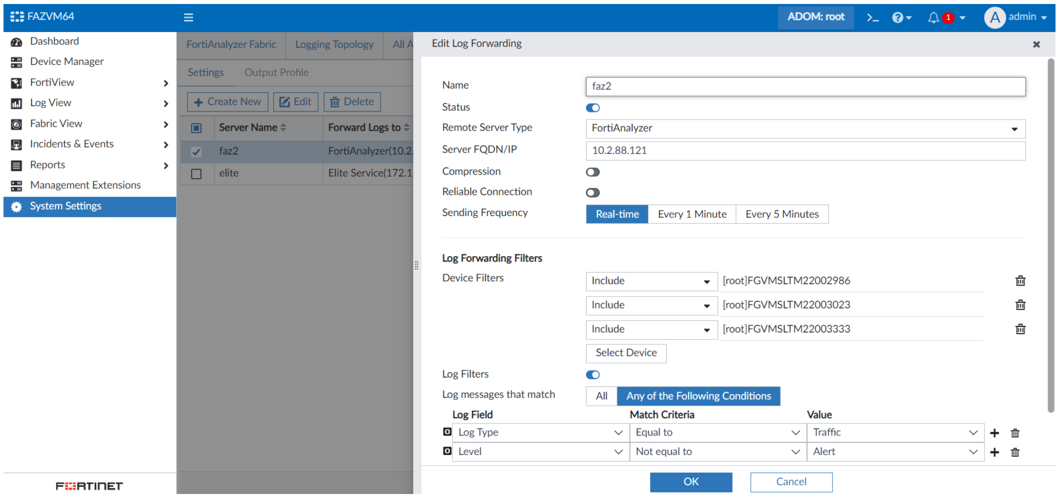
Total logs for analytics: 8 days 20 hours.   50 /Page 1 2 3 4 5 6 0.385 Second

Identity	
Device ID	FGVMSLTM22003023
Device Name	FGVMSLTM22003023
Rating	
Audit ID	1681925423885
Critical Count	1
High Count	6
Low Count	41
Medium Count	10
Passed Count	77
Report	PostureReport
Security Rating Score	274.5
Security Rating Time	1681925429
Type	
Sub Type	security-rating
Type	event
Alerts	
Level	notice
General	
Log Description	Security Rating summary
Log ID	0110052000
Virtual Domain	root
Others	
Date	2023-04-19
Date/Time	10:30:30
Destination End User ID	3
Destination Endpoint ID	3
Device Time	2023-04-19 10:30:28

Sample logs from Elite log server:

```
2023-04-14 13:50:42,136 DEBUG Processing /dev/shm/fams/log_upload/proc/FAZ-
     VMTM22090591.1264692.nrt.e.1681505055.562204.34406
2023-04-14 13:50:42,137 DEBUG Create new raw log file: elog_20230414_135042 for (*****,
     elog)
2023-04-14 13:50:47,083 DEBUG ---sending elite kafka msg---,
     elitelogserver.remoteaccessmgr.faz.fsbp, {"action":"downloadFsbpFile","data":
     {"fazSn":"FAZ-
     VMTM22090591","fgtSn":"FGVMSLTM22002986","auditId":*****,"accountId":*****,"auditTime"
     :1681490426}}
```

Note that this log forward configuration does NOT impact other types of log forwarding.



	Server Name	Forward Logs to
☑	faz2	FortiAnalyzer(10.2
□	elite	Elite Service(172.1

Edit Log Forwarding

Name	faz2
Status	● (on)
Remote Server Type	FortiAnalyzer
Server FQDN/IP	10.2.88.121
Compression	○
Reliable Connection	○
Sending Frequency	[✓ Real-time] Every 1 Minute Every 5 Minutes

Log Forwarding Filters

Device Filters	Include	[root]FGVMSLTM22002986
	Include	[root]FGVMSLTM22003023
	Include	[root]FGVMSLTM22003333
	Select Device	
Log Filters	●	
Log messages that match	All [✓ Any of the Following Conditions]	

Log Field	Match Criteria	Value
Log Type	Equal to	Traffic
Level	Not equal to	Alert

OK Cancel

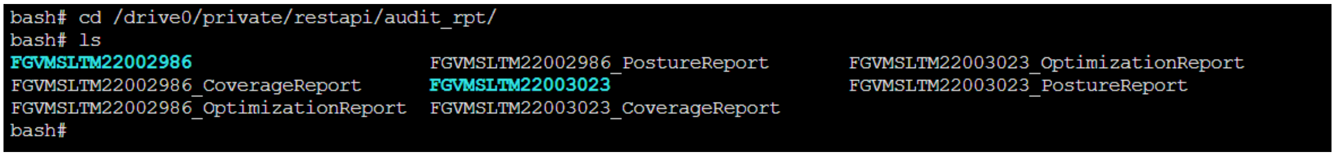
The Elite log server can call API to get the Fortinet Security Best Practices (FSBP) reports.

API:

```
{
   "apiver": 3,
   "url": "/fazsys/auditrpt/fgt-orig-rpt",
   "data":
      {
         "devid": "FGVMSLTM22002986",
         "auditID": "1681505424727"
```

```
            }
    }
```

The reports are updated in FortiAnalyzer:



```
bash# cd /drive0/private/restapi/audit_rpt/
bash# ls
FGVMSLTM22002986                      FGVMSLTM22002986_PostureReport       FGVMSLTM22003023_OptimizationReport
FGVMSLTM22002986_CoverageReport       FGVMSLTM22003023                     FGVMSLTM22003023_PostureReport
FGVMSLTM22002986_OptimizationReport  FGVMSLTM22003023_CoverageReport
bash#
```

This log forward config does not impact other types of log forward in FortiAnalyzer.

Operational Technology

This section lists the new features added to FortiAnalyzer for Operational Technology:

- Operational Technology (OT) Security Service on page 156
- OT Purdue Model in a consolidated Asset & Identity Center Dashboard on page 158
- OT Security Risk Report on page 161

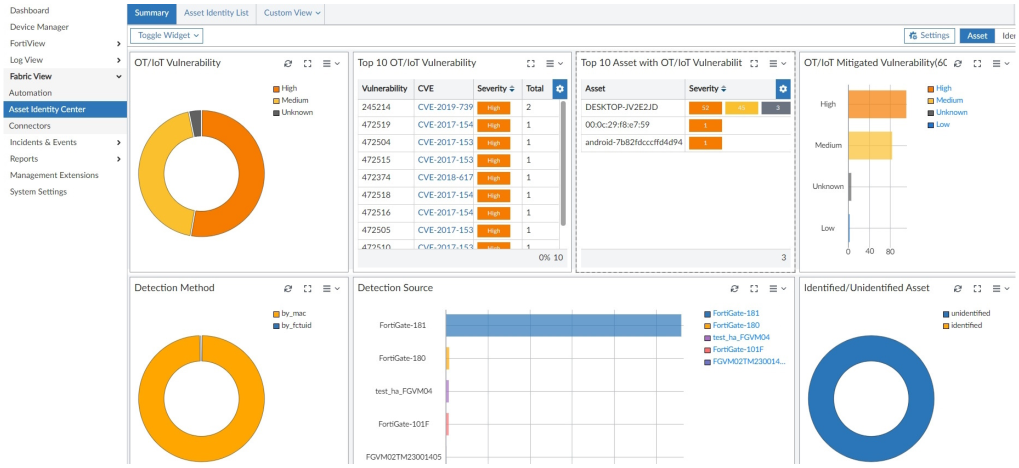
Operational Technology (OT) Security Service

Upon purchasing the OT Security Service Entitlement, the *Asset Identity Center* in FortiAnalyzer will include valuable information regarding the detected OT/IoT vulnerabilities. This includes information such as:

- A breakdown of OT/IoT vulnerabilities with corresponding severity
- Top 10 OT/IoT vulnerabilities by number of occurrences
- Top 10 assets with OT/IoT vulnerabilities
- Details of the vulnerabilities per endpoints

With this service, you can access the following features:

- Go to *Asset Identity Center* > *Summary* for OT/IoT Vulnerability widgets.



Top 10 OT/IoT Vulnerability

Vulnerability	CVE	Severity	Total
245214	CVE-2019-739	High	2
472519	CVE-2017-154	High	1
472504	CVE-2017-153	High	1
472515	CVE-2017-153	High	1
472374	CVE-2018-617	High	1
472518	CVE-2017-154	High	1
472516	CVE-2017-154	High	1
472505	CVE-2017-153	High	1
472510	CVE-2017-153	High	1

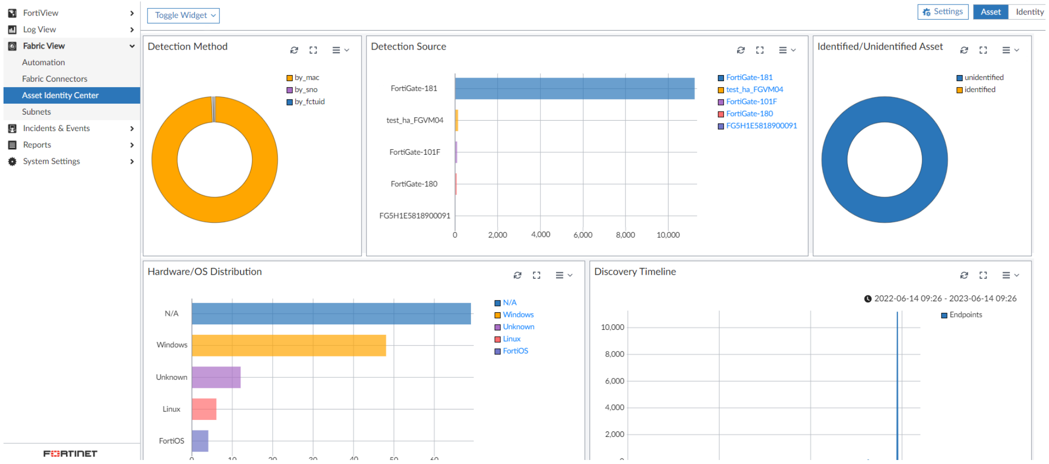
0% 10

Top 10 Asset with OT/IoT Vulnerabilit

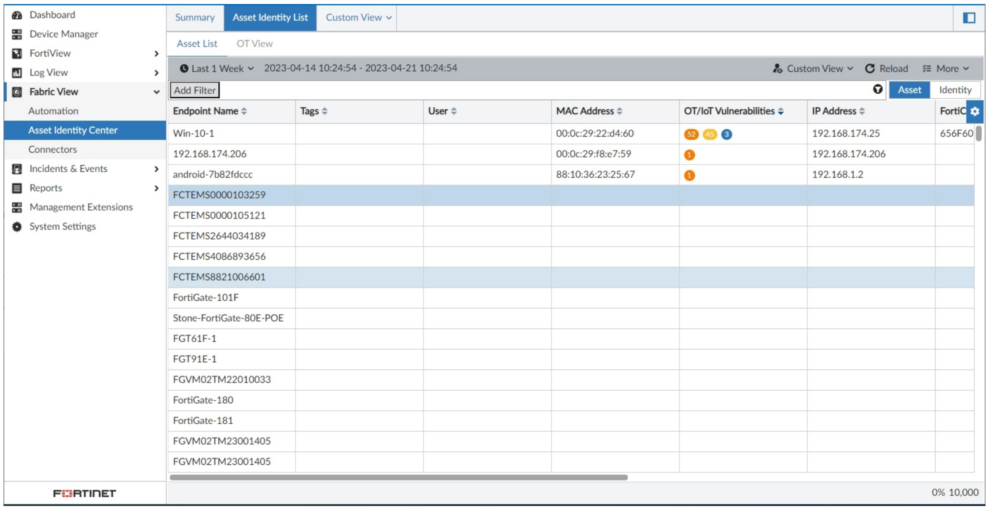
Asset	Severity		
DESKTOP-JV2E2JD	52	45	3
00:0c:29:f8:e7:59	1		
android-7b82fdcccffd4d94	1		

3

If you do not have a license for the service, the widgets will not be visible.



- Go to *Asset Identity Center > Asset Identity List > Asset List* to view *OT/IoT Vulnerabilities* in the table.

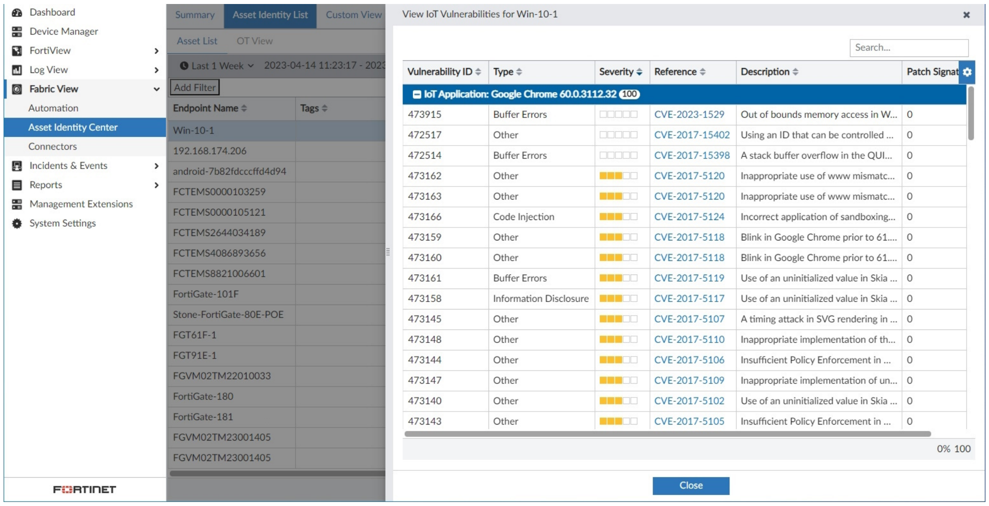


2023-04-14 10:24:54 - 2023-04-21 10:24:54

Endpoint Name	Tags	User	MAC Address	OT/IoT Vulnerabilities	IP Address	FortiC
Win-10-1			00:0c:29:22:d4:60	52 45 3	192.168.174.25	656F60
192.168.174.206			00:0c:29:f8:e7:59	1	192.168.174.206	
android-7b82fdccc			88:10:36:23:25:67	1	192.168.1.2	
FCTEMS0000103259						
FCTEMS0000105121						
FCTEMS2644034189						
FCTEMS4086893656						
FCTEMS8821006601						
FortiGate-101F						
Stone-FortiGate-80E-POE						
FGT61F-1						
FGT91E-1						
FGVM02TM22010033						
FortiGate-180						
FortiGate-181						
FGVM02TM23001405						
FGVM02TM23001405						

0% 10,000

- Click the numbers in the *OT/IoT Vulnerabilities* column to display the vulnerabilities in more detail, including *Type*, *Severity*, *Reference*, and *Description*.

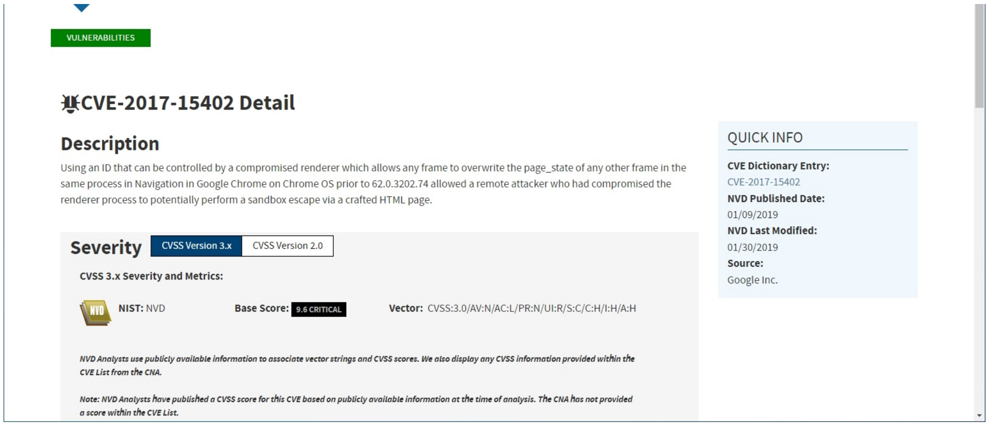


View IoT Vulnerabilities for Win-10-1

Vulnerability ID	Type	Severity	Reference	Description	Patch Signat
IoT Application: Google Chrome 60.0.3112.32 100					
473915	Buffer Errors	□□□□□	CVE-2023-1529	Out of bounds memory access in W...	0
472517	Other	□□□□□	CVE-2017-15402	Using an ID that can be controlled ...	0
472514	Buffer Errors	□□□□□	CVE-2017-15398	A stack buffer overflow in the QUI...	0
473162	Other	■■■□□	CVE-2017-5120	Inappropriate use of www mismatc...	0
473163	Other	■■■□□	CVE-2017-5120	Inappropriate use of www mismatc...	0
473166	Code Injection	■■■□□	CVE-2017-5124	Incorrect application of sandboxing...	0
473159	Other	■■■□□	CVE-2017-5118	Blink in Google Chrome prior to 61....	0
473160	Other	■■■□□	CVE-2017-5118	Blink in Google Chrome prior to 61....	0
473161	Buffer Errors	■■■□□	CVE-2017-5119	Use of an uninitialized value in Skia ...	0
473158	Information Disclosure	■■■□□	CVE-2017-5117	Use of an uninitialized value in Skia ...	0
473145	Other	■■■□□	CVE-2017-5107	A timing attack in SVG rendering in ...	0
473148	Other	■■■□□	CVE-2017-5110	Inappropriate implementation of th...	0
473144	Other	■■■□□	CVE-2017-5106	Insufficient Policy Enforcement in ...	0
473147	Other	■■■□□	CVE-2017-5109	Inappropriate implementation of un...	0
473140	Other	■■■□□	CVE-2017-5102	Use of an uninitialized value in Skia ...	0
473143	Other	■■■□□	CVE-2017-5105	Insufficient Policy Enforcement in ...	0

0% 100

- Click the CVE reference in the *Reference* column to view the details.



CVE-2017-15402 Detail

Description

Using an ID that can be controlled by a compromised renderer which allows any frame to overwrite the page_state of any other frame in the same process in Navigation in Google Chrome on Chrome OS prior to 62.0.3202.74 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.6 CRITICAL **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:
CVE-2017-15402
NVD Published Date:
01/09/2019
NVD Last Modified:
01/30/2019
Source:
Google Inc.

- In the FortiAnalyzer CLI, you can enter the following command to check the status of the endpoint data link between FortiAnalyzer and FortiGate:

```
diagnose test application oftpd 20 fgt-stat
```

OT Purdue Model in a consolidated Asset & Identity Center Dashboard

This information is also available in the FortiAnalyzer 7.4 Administration Guide:

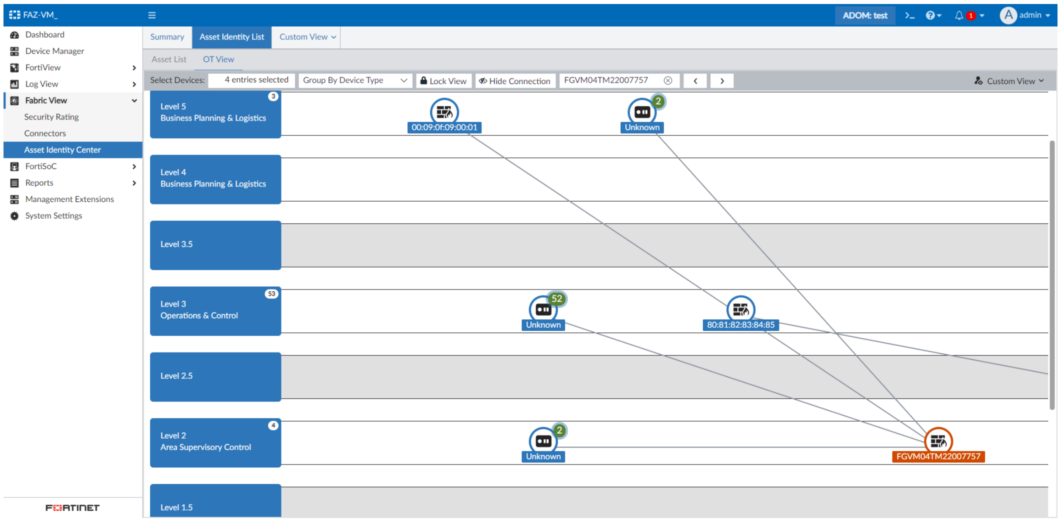
- OT View

An OT Purdue model has been added to a new and consolidated *Asset & Identity Center*.

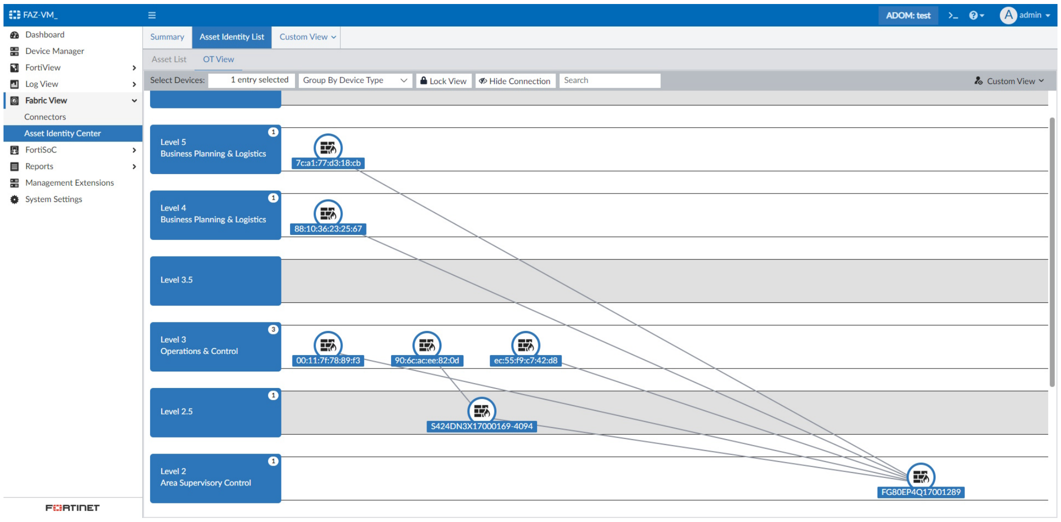
This spec introduces a consolidated dashboard for both Assets and Identities: *Fabric View > Asset Identity Center*. In previous versions, Asset and Identity each had a separate dashboard.

In the new *OT View*, each asset is represented in its corresponding Purdue Layer. All associated endpoints are visible with clear, linear relationships.

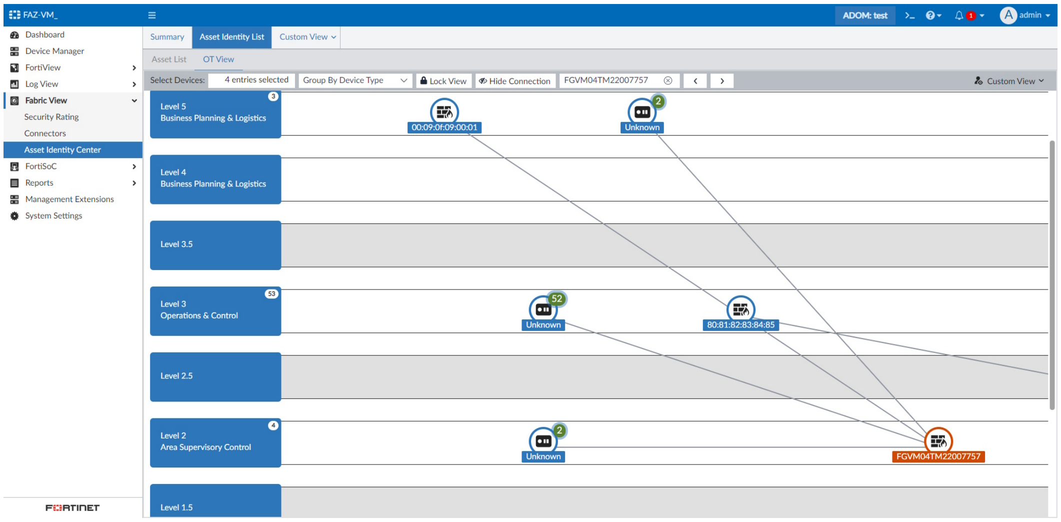
To view the new *OT View*, go to *Fabric View > Asset Identity Center > OT View*.



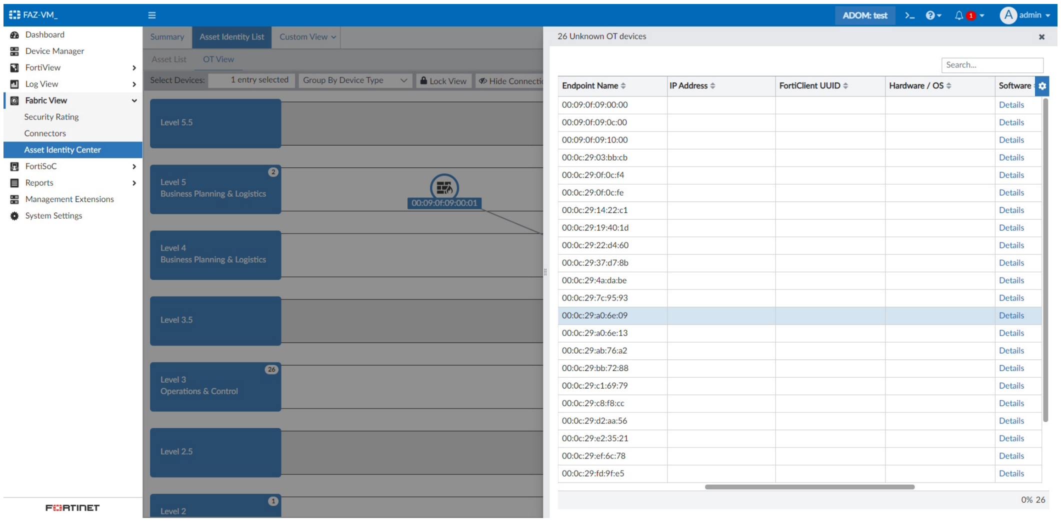
Use the *Select Devices* fields to display all endpoints associated with specified devices.



Use the *Search* field to find a specific endpoint, as needed.



Click an endpoint to review the details of the endpoint or the endpoint's group.

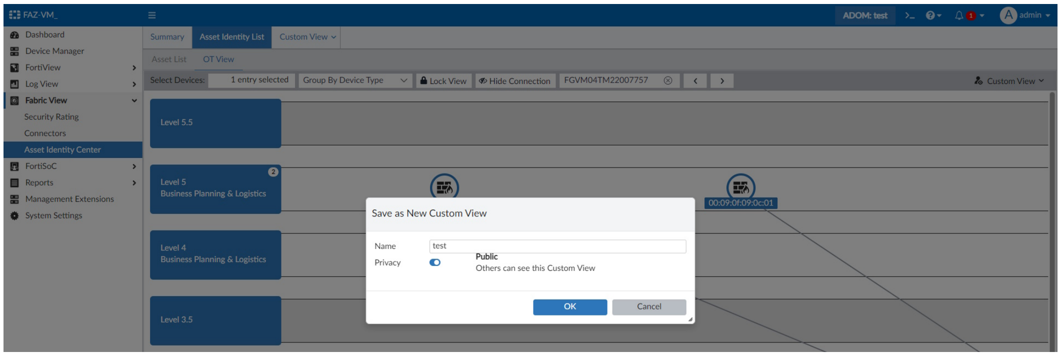


26 Unknown OT devices

Endpoint Name	IP Address	FortiClient UUID	Hardware / OS	Software
00:09:0f:09:00:00				Details
00:09:0f:09:0c:00				Details
00:09:0f:09:10:00				Details
00:0c:29:03:bb:cb				Details
00:0c:29:0f:0c:f4				Details
00:0c:29:0f:0c:fe				Details
00:0c:29:14:22:c1				Details
00:0c:29:19:40:1d				Details
00:0c:29:22:d4:60				Details
00:0c:29:37:d7:8b				Details
00:0c:29:4a:da:be				Details
00:0c:29:7c:95:93				Details
00:0c:29:a0:6e:09				Details
00:0c:29:a0:6e:13				Details
00:0c:29:ab:76:a2				Details
00:0c:29:bb:72:88				Details
00:0c:29:c1:69:79				Details
00:0c:29:c8:f8:cc				Details
00:0c:29:d2:aa:56				Details
00:0c:29:e2:35:21				Details
00:0c:29:ef:6c:78				Details
00:0c:29:fd:9f:e5				Details

0% 26

Within the *OT View* pane, click *Custom View > Save As Custom View* to create a custom view.



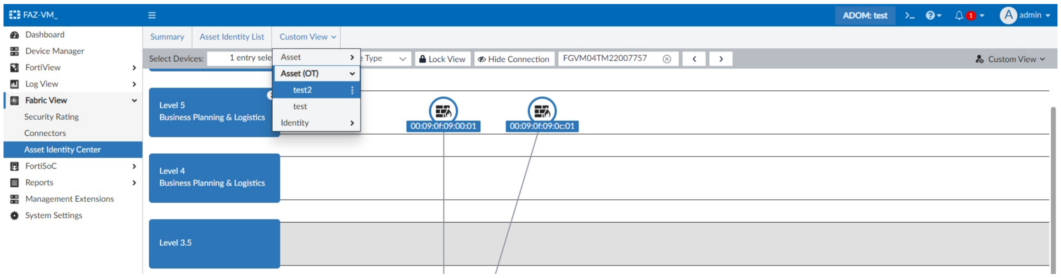
Save as New Custom View

Name: test

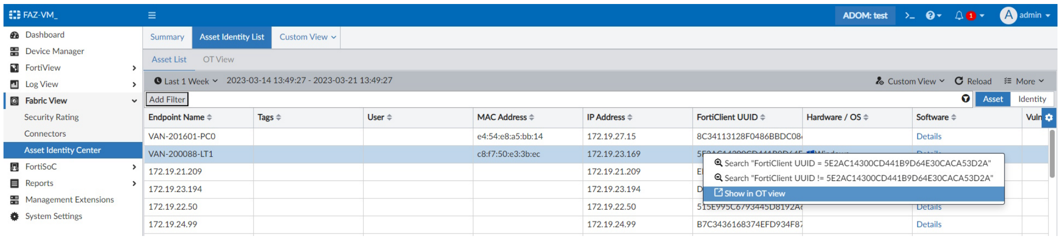
Privacy: Public
Others can see this Custom View

OK | Cancel

The saved custom views are available in *Fabric View > Asset Identity Center > Custom View*.



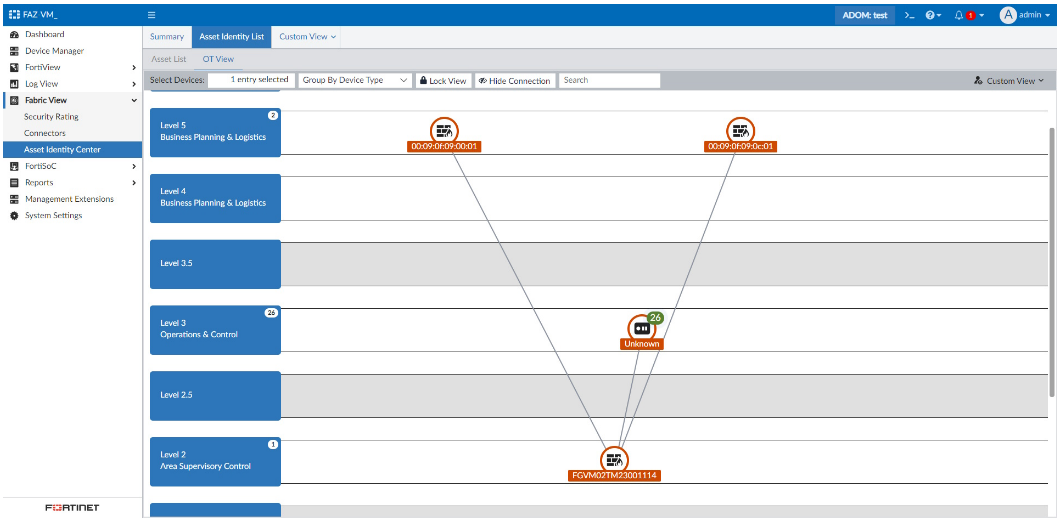
When using *Fabric View > Asset Identity Center > Asset List*, you can right-click an endpoint and click *Show in OT view* to display it in the OT view instead of the asset list.



2023-03-14 13:49:27 - 2023-03-21 13:49:27

Endpoint Name	Tags	User	MAC Address	IP Address	FortiClient UUID	Hardware / OS	Software	Vuln
VAN-201601-PC0			e4:54:e8:a5:bb:14	172.19.27.15	8C34113128F0486BBDC08		Details	
VAN-200088-LT1			c8:f7:50:e3:3b:ec	172.19.23.169	5E[illegible]	[illegible]	[illegible]	
172.19.21.209				172.19.21.209	E[illegible]			
172.19.23.194				172.19.23.194	D[illegible]			
172.19.22.50				172.19.22.50	515E995C6793445D8192A		Details	
172.19.24.99				172.19.24.99	B7C3436168374EFD934F87		Details	

After clicking *Show in OT* view, the *Fabric View* > *Asset Identity Center* > *OT View* opens to display the selected endpoint.

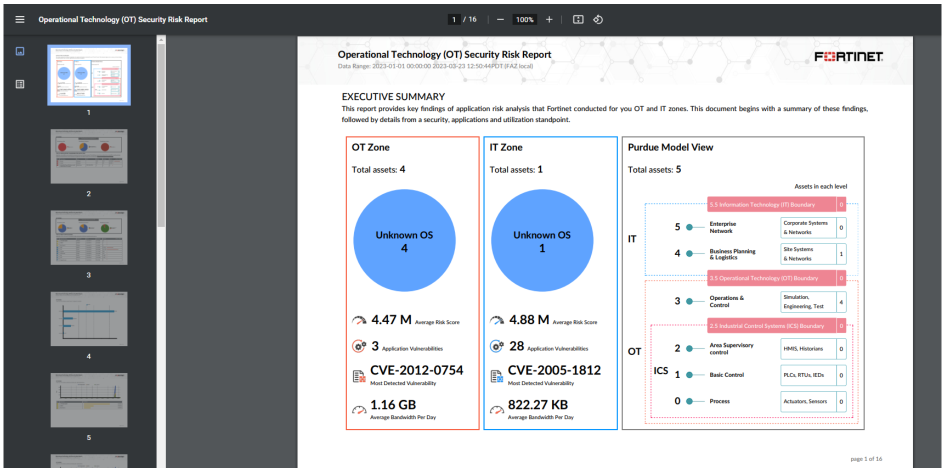


OT Security Risk Report

An *Operational Technology (OT) Security Risk Report* has been added to provide:

- Application risk analysis for OT and IT zones
- Blind-spot and hidden risks detection
- Purdue Model asset mapping

For example, see a sample of the report in PDF format below:



Operational Technology (OT) Security Risk Report

Data Range: 2023-01-01 00:00:00 2023-03-23 12:50:44PDT (FAZ local)

EXECUTIVE SUMMARY

This report provides key findings of application risk analysis that Fortinet conducted for you OT and IT zones. This document begins with a summary of these findings, followed by details from a security, applications and utilization standpoint.

OT Zone

Total assets: 4

Unknown OS 4

4.47 M Average Risk Score

3 Application Vulnerabilities

CVE-2012-0754 Most Detected Vulnerability

1.16 GB Average Bandwidth Per Day

IT Zone

Total assets: 1

Unknown OS 1

4.88 M Average Risk Score

28 Application Vulnerabilities

CVE-2005-1812 Most Detected Vulnerability

822.27 KB Average Bandwidth Per Day

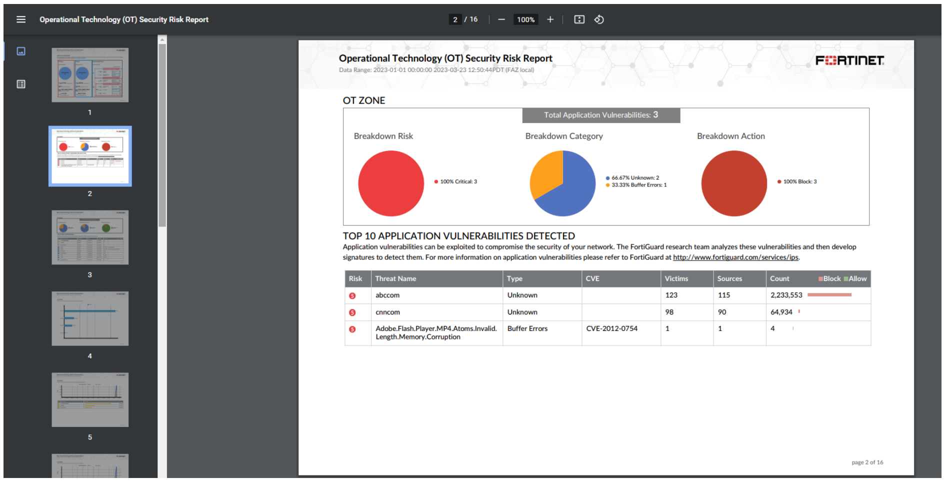
Purdue Model View

Total assets: 5

Assets in each level

		Level			Assets in each level
IT			5.5 Information Technology (IT) Boundary		0
		5	Enterprise Network	Corporate Systems & Networks	0
		4	Business Planning & Logistics	Site Systems & Networks	1
			3.5 Operational Technology (OT) Boundary		0
OT		3	Operations & Control	Simulation, Engineering, Test	4
			2.5 Industrial Control Systems (ICS) Boundary		0
	ICS	2	Area Supervisory control	HMIS, Historians	0
		1	Basic Control	PLCs, RTUs, IEDs	0
		0	Process	Actuators, Sensors	0

page 1 of 16



Operational Technology (OT) Security Risk Report
Data Range: 2023-01-01 00:00:00 2023-03-23 12:50:44PDT (FAZ local)

OT ZONE

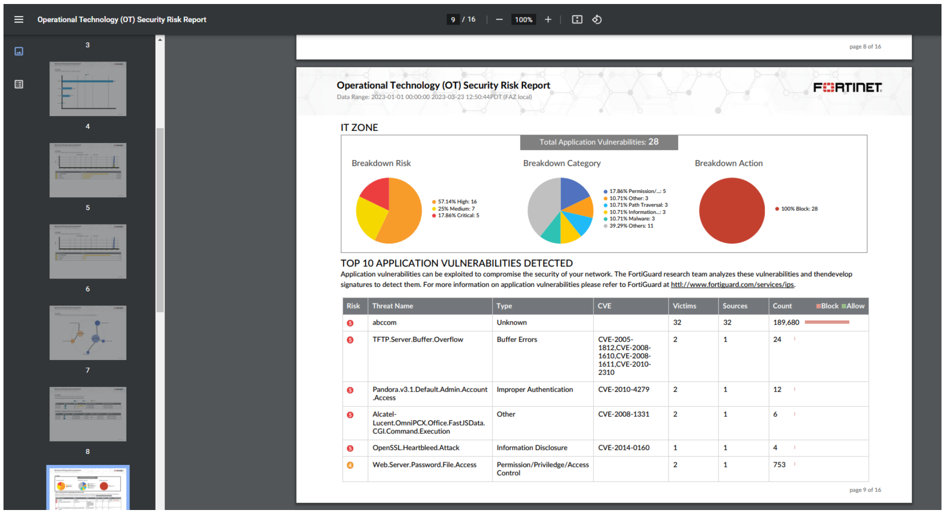
Total Application Vulnerabilities: 3

Breakdown Risk | Breakdown Category | Breakdown Action

TOP 10 APPLICATION VULNERABILITIES DETECTED

Application vulnerabilities can be exploited to compromise the security of your network. The FortiGuard research team analyzes these vulnerabilities and then develop signatures to detect them. For more information on application vulnerabilities please refer to FortiGuard at http://www.fortiguard.com/services/ips.

Risk	Threat Name	Type	CVE	Victims	Sources	Count ■Block ■Allow
5	abccom	Unknown		123	115	2,233,553
5	cnncom	Unknown		98	90	64,934
5	Adobe.Flash.Player.MP4.Atoms.Invalid.Length.Memory.Corruption	Buffer Errors	CVE-2012-0754	1	1	4



Operational Technology (OT) Security Risk Report
Data Range: 2023-01-01 00:00:00 2023-03-23 12:50:44PDT (FAZ local)

IT ZONE

Total Application Vulnerabilities: 28

Breakdown Risk | Breakdown Category | Breakdown Action

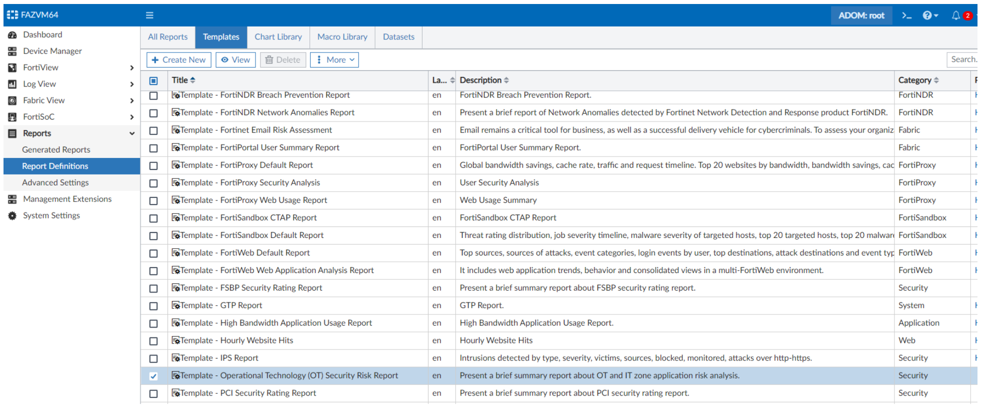
TOP 10 APPLICATION VULNERABILITIES DETECTED

Application vulnerabilities can be exploited to compromise the security of your network. The FortiGuard research team analyzes these vulnerabilities and thendevelop signatures to detect them. For more information on application vulnerabilities please refer to FortiGuard at httl://www.fortiguard.com/services/ips.

Risk	Threat Name	Type	CVE	Victims	Sources	Count ■Block ■Allow
5	abccom	Unknown		32	32	189,680
5	TFTP.Server.Buffer.Overflow	Buffer Errors	CVE-2005-1812,CVE-2008-1610,CVE-2008-1611,CVE-2010-2310	2	1	24
5	Pandora.v3.1.Default.Admin.Account.Access	Improper Authentication	CVE-2010-4279	2	1	12
5	Alcatel-Lucent.OmniPCX.Office.FastJSData.CGI.Command.Execution	Other	CVE-2008-1331	2	1	6
5	OpenSSL.Heartbleed.Attack	Information Disclosure	CVE-2014-0160	1	1	4
4	Web.Server.Password.File.Access	Permission/Priviledge/Access Control		2	1	753

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Operational Technology (OT) Security Risk Report*.



☐	Title	La...	Description	Category
☐	Template - FortiNDR Breach Prevention Report	en	FortiNDR Breach Prevention Report.	FortiNDR
☐	Template - FortiNDR Network Anomalies Report	en	Present a brief report of Network Anomalies detected by Fortinet Network Detection and Response product FortiNDR.	FortiNDR
☐	Template - Fortinet Email Risk Assessment	en	Email remains a critical tool for business, as well as a successful delivery vehicle for cybercriminals. To assess your organiz	Fabric
☐	Template - FortiPortal User Summary Report	en	FortiPortal User Summary Report.	Fabric
☐	Template - FortiProxy Default Report	en	Global bandwidth savings, cache rate, traffic and request timeline. Top 20 websites by bandwidth, bandwidth savings, cac	FortiProxy
☐	Template - FortiProxy Security Analysis	en	User Security Analysis	FortiProxy
☐	Template - FortiProxy Web Usage Report	en	Web Usage Summary	FortiProxy
☐	Template - FortiSandbox CTAP Report	en	FortiSandbox CTAP Report	FortiSandbox
☐	Template - FortiSandbox Default Report	en	Threat rating distribution, job severity timeline, malware severity of targeted hosts, top 20 targeted hosts, top 20 malware	FortiSandbox
☐	Template - FortiWeb Default Report	en	Top sources, sources of attacks, event categories, login events by user, top destinations, attack destinations and event typ	FortiWeb
☐	Template - FortiWeb Web Application Analysis Report	en	It includes web application trends, behavior and consolidated views in a multi-FortiWeb environment.	FortiWeb
☐	Template - FSBP Security Rating Report	en	Present a brief summary report about FSBP security rating report.	Security
☐	Template - GTP Report	en	GTP Report.	System
☐	Template - High Bandwidth Application Usage Report	en	High Bandwidth Application Usage Report.	Application
☐	Template - Hourly Website Hits	en	Hourly Website Hits	Web
☐	Template - IPS Report	en	Intrusions detected by type, severity, victims, sources, blocked, monitored, attacks over http-https.	Security
☑	Template - Operational Technology (OT) Security Risk Report	en	Present a brief summary report about OT and IT zone application risk analysis.	Security
☐	Template - PCI Security Rating Report	en	Present a brief summary report about PCI security rating report.	Security

3. From the *More* dropdown, click *Create Report* to create a report using the template.
   You can also click *Clone* to clone the template and make adjustments.

To run the Operational Technology (OT) Security Risk Report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *Operational Technology (OT) Security Risk Report*.
   The *Edit: Operational Technology (OT) Security Risk Report* pane opens.
2. Click *Run Report*.
   Once the report is available, click the format to view the report in.

Other

This section lists the other new features added to FortiAnalyzer:

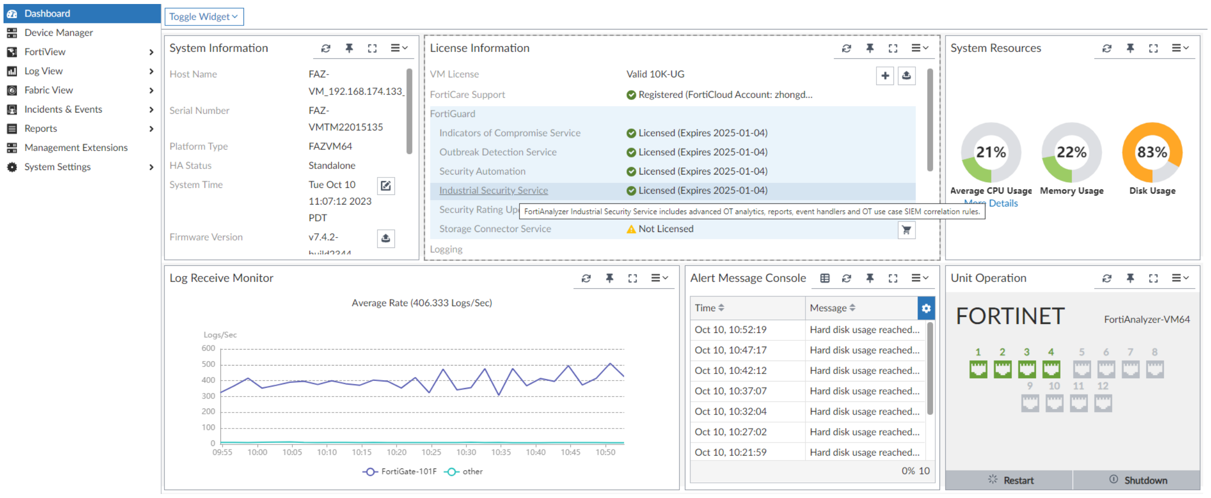
- Licensing adjustment on page 164

Licensing adjustment

Version 7.4.0 introduces multiple adjustments to the FortiAnalyzer licensing model to accommodate extra licenses:

- *Security Operations* > *Security Automation* has been renamed to *FortiGuard* > *Security Automation*
- A new subscription has been introduced for OT Security Service, enabling access to OT-related features like the OT Dashboard and report. This can be found on the FortiAnalyzer GUI under the name *Industrial Security Service*.
- A new subscription has been introduced for Security Rating and Compliance, allowing access to additional compliance reports such as PCI, FSBP, and CIS. This can be found on the FortiAnalyzer GUI under the name *Security Rating Update*.

These licenses are visible in the *License Information* widget.



System Information

Host Name	FAZ-VM_192.168.174.133_
Serial Number	FAZ-VMTM22015135
Platform Type	FAZVM64
HA Status	Standalone
System Time	Tue Oct 10 11:07:12 2023 PDT
Firmware Version	v7.4.2-build2344

License Information

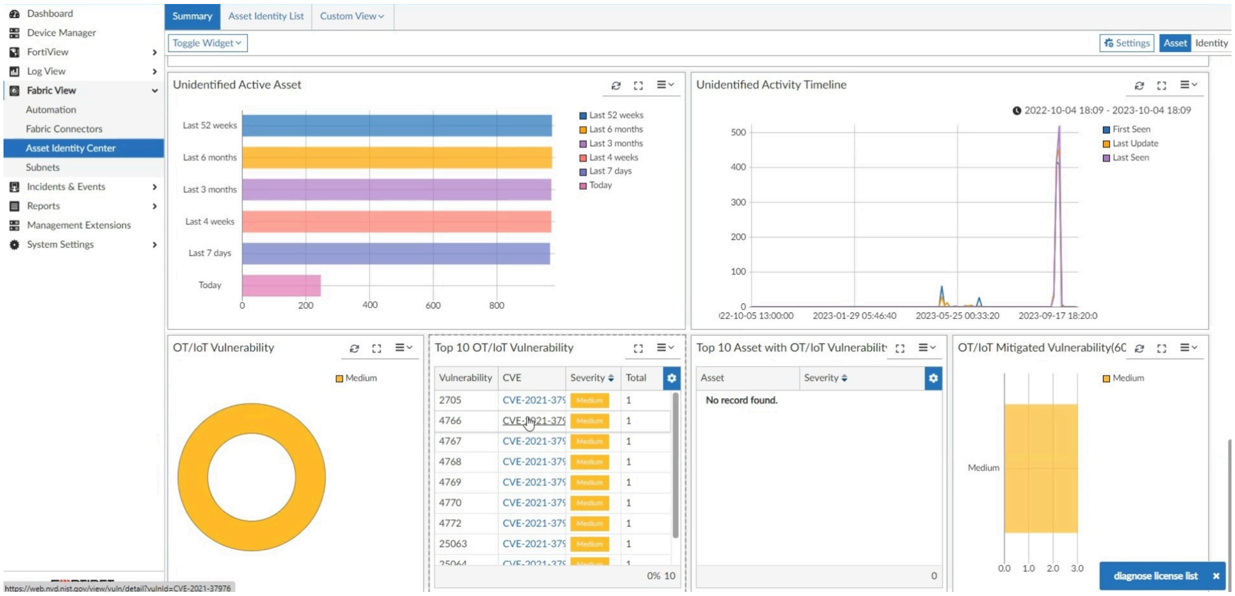
VM License	Valid 10K-UG
FortiCare Support	✓ Registered (FortiCloud Account: zhongd...
FortiGuard	
Indicators of Compromise Service	✓ Licensed (Expires 2025-01-04)
Outbreak Detection Service	✓ Licensed (Expires 2025-01-04)
Security Automation	✓ Licensed (Expires 2025-01-04)
Industrial Security Service	✓ Licensed (Expires 2025-01-04)
Security Rating Up	
Storage Connector Service	⚠ Not Licensed
Logging	

FortiAnalyzer Industrial Security Service includes advanced OT analytics, reports, event handlers and OT use case SIEM correlation rules.

Time	Message
Oct 10, 10:52:19	Hard disk usage reached...
Oct 10, 10:47:17	Hard disk usage reached...
Oct 10, 10:42:12	Hard disk usage reached...
Oct 10, 10:37:07	Hard disk usage reached...
Oct 10, 10:32:04	Hard disk usage reached...
Oct 10, 10:27:02	Hard disk usage reached...
Oct 10, 10:21:59	Hard disk usage reached...

0% 10

If licensed for the *Industrial Security Service*, the *OT/IoT Vulnerability* widgets will be visible in *Fabric View* > *Asset Identity Center* > *Summary*.



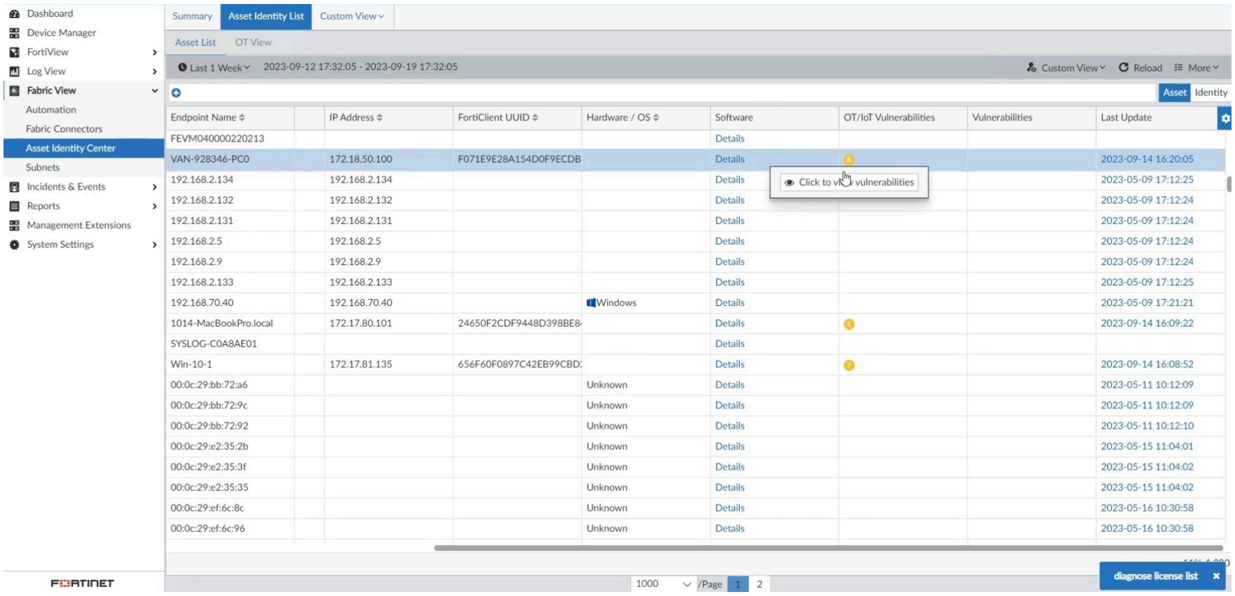
Vulnerability	CVE	Severity	Total
2705	CVE-2021-379	Medium	1
4766	CVE-2021-379	Medium	1
4767	CVE-2021-379	Medium	1
4768	CVE-2021-379	Medium	1
4769	CVE-2021-379	Medium	1
4770	CVE-2021-379	Medium	1
4772	CVE-2021-379	Medium	1
25063	CVE-2021-379	Medium	1
25064	CVE-2021-379	Medium	1

0% 10

Asset	Severity
No record found.	

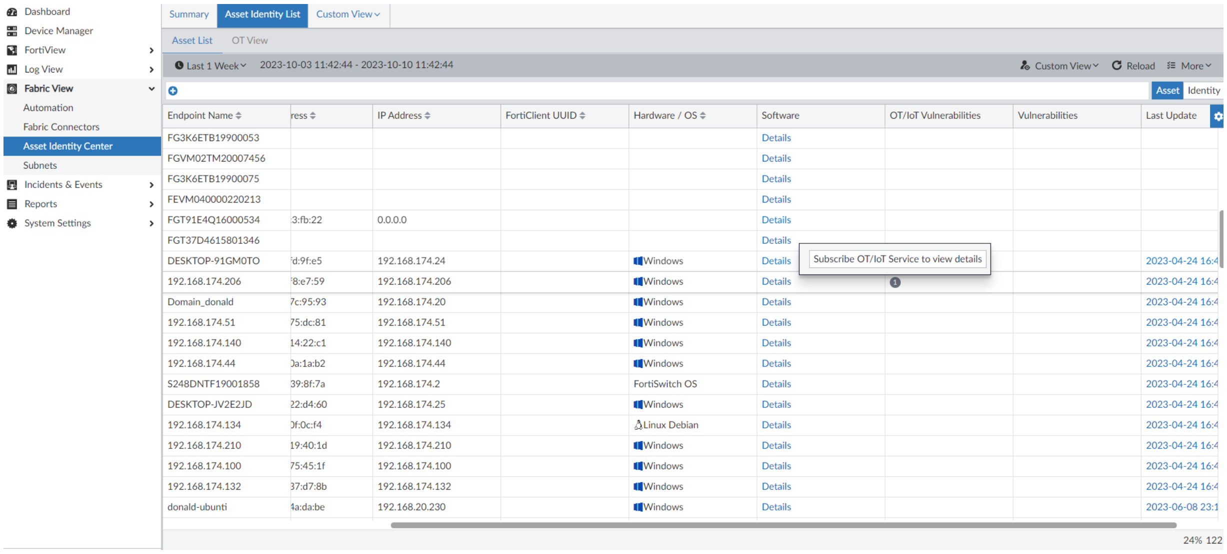
0

The *OT/IoT Vulnerabilities* will also be available in *Fabric View > Asset Identity Center > Asset Identity List*.



Endpoint Name		IP Address	FortiClient UUID	Hardware / OS	Software	OT/IoT Vulnerabilities	Vulnerabilities	Last Update
FEVM040000220213					Details			
VAN-928346-PC0		172.18.50.100	F071E9E28A154D0F9ECDB		Details	●		2023-09-14 16:20:05
192.168.2.134		192.168.2.134			Details			2023-05-09 17:12:25
192.168.2.132		192.168.2.132			Details			2023-05-09 17:12:24
192.168.2.131		192.168.2.131			Details			2023-05-09 17:12:24
192.168.2.5		192.168.2.5			Details			2023-05-09 17:12:24
192.168.2.9		192.168.2.9			Details			2023-05-09 17:12:24
192.168.2.133		192.168.2.133			Details			2023-05-09 17:12:25
192.168.70.40		192.168.70.40		Windows	Details			2023-05-09 17:21:21
1014-MacBookPro.local		172.17.80.101	24650F2CDF9448D398BE8		Details	●		2023-09-14 16:09:22
SYSLOG-C0A8AE01					Details			
Win-10-1		172.17.81.135	656F60F0897C42EB99CBD		Details	●		2023-09-14 16:08:52
00:0c:29:bb:72:a6				Unknown	Details			2023-05-11 10:12:09
00:0c:29:bb:72:9c				Unknown	Details			2023-05-11 10:12:09
00:0c:29:bb:72:92				Unknown	Details			2023-05-11 10:12:10
00:0c:29:e2:35:2b				Unknown	Details			2023-05-15 11:04:01
00:0c:29:e2:35:3f				Unknown	Details			2023-05-15 11:04:02
00:0c:29:e2:35:35				Unknown	Details			2023-05-15 11:04:02
00:0c:29:ef:6c:8c				Unknown	Details			2023-05-16 10:30:58
00:0c:29:ef:6c:96				Unknown	Details			2023-05-16 10:30:58

If unlicensed for the *Industrial Security Service*, these features will not be available.



Last 1 Week 2023-10-03 11:42:44 - 2023-10-10 11:42:44

Endpoint Name	ress	IP Address	FortiClient UUID	Hardware / OS	Software	OT/IoT Vulnerabilities	Vulnerabilities	Last Update
FG3K6ETB19900053					Details			
FGVM02TM20007456					Details			
FG3K6ETB19900075					Details			
FEVM040000220213					Details			
FGT91E4Q16000534	:3:fb:22	0.0.0.0			Details			
FGT37D4615801346					Details			
DESKTOP-91GM0TO	'd:9f:e5	192.168.174.24		Windows	Details			2023-04-24 16:4
192.168.174.206	'8:e7:59	192.168.174.206		Windows	Details	1		2023-04-24 16:4
Domain_donald	7c:95:93	192.168.174.20		Windows	Details			2023-04-24 16:4
192.168.174.51	75:dc:81	192.168.174.51		Windows	Details			2023-04-24 16:4
192.168.174.140	14:22:c1	192.168.174.140		Windows	Details			2023-04-24 16:4
192.168.174.44	Da:1a:b2	192.168.174.44		Windows	Details			2023-04-24 16:4
S248DNTF19001858	39:8f:7a	192.168.174.2		FortiSwitch OS	Details			2023-04-24 16:4
DESKTOP-JV2E2JD	22:d4:60	192.168.174.25		Windows	Details			2023-04-24 16:4
192.168.174.134	Df:0c:f4	192.168.174.134		Linux Debian	Details			2023-04-24 16:4
192.168.174.210	19:40:1d	192.168.174.210		Windows	Details			2023-04-24 16:4
192.168.174.100	75:45:1f	192.168.174.100		Windows	Details			2023-04-24 16:4
192.168.174.132	37:d7:8b	192.168.174.132		Windows	Details			2023-04-24 16:4
donald-ubunti	4a:da:be	192.168.20.230		Windows	Details			2023-06-08 23:1

Subscribe OT/IoT Service to view details

For more information about OT features in FortiAnalyzer, see Operational Technology on page 156.

Index

The following index provides a list of all new features added to FortiAnalyzer 7.4. The index allows you to quickly identify the version where the feature first became available in FortiAnalyzer.

Select a version number to navigate in the index to the new features available for that release:

7.4.0

Fabric View

Security Operations

Log and Report

System

Cloud Services

Operational Technology

Other

7.4.1

Security Fabric

Security Operations

Log and Report

System

7.4.2

Security Operations

Log and Report

System

www.fortinet.com