



# FortiAnalyzer - New Features Guide

Version 6.4.0

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<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 CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



June 1, 2023

FortiAnalyzer 6.4.0 New Features Guide

05-640-617437-20230601



# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Security-driven Networking</b>	<b>6</b>
SD-WAN	6
FortiAnalyzer SD-WAN Monitoring Dashboard	6
Enhanced SD-WAN Report	12
Secure SD-WAN assessment report 6.4.2	14
<b>Dynamic Cloud Security</b>	<b>17</b>
Public cloud	17
FortiCare license for AWS PAYG instances	17
Support for cloud-init service for KVM, Azure, and AWS 6.4.1	18
Application security	24
FortiWeb Pcap Support	24
<b>Zero Trust Network Access</b>	<b>27</b>
NAC	27
FortiNAC Report	27
IAM	28
SAML Fabric SSO	28
<b>AI-driven Security Operations</b>	<b>33</b>
SOC automation	34
Attach reports to incidents	34
Automation Playbooks	38
Add comments to incidents	45
Expanded incident analysis page	47
FortiSOC dashboards	51
FortiOS Connector	52
EMS Connector	56
Normalized Fabric logs	62
Incidents with multiple endpoints and users 6.4.2	66
Default playbook template improvements 6.4.1	67
Incident page improvement 6.4.1	70
Filters for local report action 6.4.2	76
SOC subscription license 6.4.1	77
Try it Out feature for FortiSoC 6.4.2	79
Vulnerabilities and software inventory data from EMS connector 6.4.2	81
FortiMail connector 6.4.2	85
Alerts on normalized logs 6.4.3	88
Normalized logs for reports 6.4.3	91
FortiGuard connector 6.4.3	93
Connector's health check 6.4.3	96
FortiGuard outbreak and alert service 6.4.6	97
Advanced threat protection	101
IoC re-scan events	101
FortiDeceptor logging	105
Unique count for event handler 6.4.2	107

FortiGate C&C Detection in SOC View 6.4.3 .....	108
FortiADC logging 6.4.3 .....	111
Dashboard/widgets/reports .....	113
FortiView custom widgets 6.4.1 .....	114
Extra caching for SOC reports 6.4.1 .....	117
Asset tags .....	118
Sankey Chart .....	120
FortiPortal user summary report 6.4.2 .....	121
FortiSandbox default report improvement 6.4.2 .....	123
Improved SOC incident report 6.4.2 .....	124
Add stackbar chart in FortiView 6.4.2 .....	126
Interface bandwidth widgets 6.4.2 .....	128
EMS classification tag 6.4.3 .....	130
Throughput utilization billing reporting 6.4.3 .....	133
Subnet list for reports 6.4.3 .....	135
Asset & Identity View Improvement 6.4.3 .....	138
Cyber-Physical Security .....	143
Facial Recognition 6.4.1 .....	143
Zoom function in FortiRecorder 6.4.1 .....	149
<b>Fabric Management Platform .....</b>	<b>152</b>
Single pane .....	152
Prompt admin to register FortiAnalyzer with FortiCloud .....	152
Online update and verification for third-party certificates (OCSP stapling) .....	158
FortiManager support for FortiAnalyzer HA .....	158
FortiAnalyzer firmware upgrade from FortiGuard servers .....	160
FortiAnalyzer GUI accessibility improvements 6.4.4 .....	161
<b>Other .....</b>	<b>165</b>
FortiAnalyzer Application logs .....	165

# Change Log

Date	Change Description
2023-06-01	Updated <a href="#">Throughput utilization billing reporting 6.4.3 on page 133</a> .
2022-07-05	Added <a href="#">Support for cloud-init service for KVM, Azure, and AWS 6.4.1 on page 18</a> .
2022-01-17	Added <a href="#">FortiGuard outbreak and alert service 6.4.6 on page 97</a> .
2021-06-01	Initial release of FortiAnalyzer 6.4.6.
2021-05-19	Updated information in <a href="#">Online update and verification for third-party certificates (OCSP stapling) on page 158</a> .
2021-01-28	Updated information in <a href="#">Throughput utilization billing reporting 6.4.3 on page 133</a> .
2020-12-16	Initial release of FortiAnalyzer 6.4.4.
2020-11-27	Added <a href="#">Connector's health check 6.4.3 on page 96</a> .
2020-10-22	Initial release of FortiAnalyzer 6.4.3.
2020-09-24	Added <a href="#">FortiMail connector 6.4.2 on page 85</a> .
2020-09-14	Added <a href="#">Asset tags on page 118</a> .
2020-08-31	Added <a href="#">Secure SD-WAN assessment report 6.4.2 on page 14</a> .
2020-08-20	Added: <ul style="list-style-type: none"><li>• <a href="#">Incidents with multiple endpoints and users 6.4.2 on page 66</a></li><li>• <a href="#">Vulnerabilities and software inventory data from EMS connector 6.4.2 on page 81</a></li></ul>
2020-08-13	Added: <ul style="list-style-type: none"><li>• <a href="#">SOC subscription license 6.4.1 on page 77</a></li><li>• <a href="#">Try it Out feature for FortiSoC 6.4.2 on page 79</a></li></ul>
2020-08-10	Added <a href="#">Unique count for event handler 6.4.2 on page 107</a> .
2020-08-06	Initial release of FortiAnalyzer 6.4.2.
2020-07-20	Added <a href="#">Zoom function in FortiRecorder 6.4.1 on page 149</a> .
2020-06-26	Added <a href="#">Facial Recognition 6.4.1 on page 143</a> .
2020-06-23	Added <a href="#">Sankey Chart on page 120</a> .
2020-06-15	Initial release of FortiAnalyzer 6.4.1.
2020-05-04	Added <a href="#">Normalized Fabric logs on page 62</a> .
2020-05-01	Added <a href="#">EMS Connector on page 56</a> Added <a href="#">FortiCare license for AWS PAYG instances on page 17</a>
2020-04-17	Added <a href="#">FortiDeceptor logging on page 105</a> .
2020-04-09	Initial release of FortiAnalyzer 6.4.0.

# Security-driven Networking

This section lists the new features added to FortiAnalyzer for Security-driven Networking. They are organized into the following sections:

- [SD-WAN on page 6](#)
  - [FortiAnalyzer SD-WAN Monitoring Dashboard on page 6](#)
  - [Enhanced SD-WAN Report on page 12](#)
  - [Secure SD-WAN assessment report 6.4.2 on page 14](#)

## SD-WAN

This section lists the new features added to FortiAnalyzer for SD-WAN.

List of new features:

- [FortiAnalyzer SD-WAN Monitoring Dashboard on page 6](#)
- [Enhanced SD-WAN Report on page 12](#)
- [Secure SD-WAN assessment report 6.4.2 on page 14](#)

## FortiAnalyzer SD-WAN Monitoring Dashboard

Charts similar to those available in the Secure SD-WAN Report can be found as widgets in the default SD-WAN dashboard of FortiView.

The *Monitors* window in *FortiView* has a predefined *Secure SD-WAN Monitor* pane with eight SD-WAN widgets.

A ninth widget, *SD-WAN Rules Utilization*, can be added to the dashboard.

### To view the SD-WAN widgets:

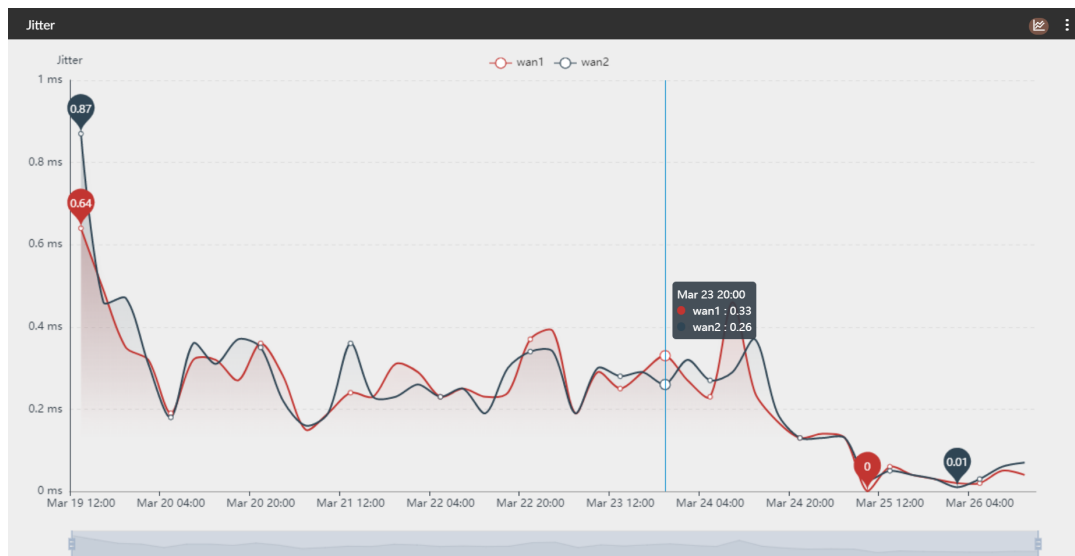
1. Go to *FortiView* > *Monitors*.
2. In the tree menu, select *Secure SD-WAN Monitor*.  
The *Secure SD-WAN Monitor* pane displays the SD-WAN widgets.

### Default SD-WAN Widgets:

1. *SD-WAN Performance Status*: It gives the status of individual links and the SD-WAN enhancements after the SD-WAN implementation.  
Hover over a bar to see its link status, date, and time in the tooltip.



2. **Jitter:** The *Jitter* widget shows a line chart of the jitter data for each SD-WAN link across the selected time period. Hover over the line chart to see date, time, and jitter data in the tooltip.

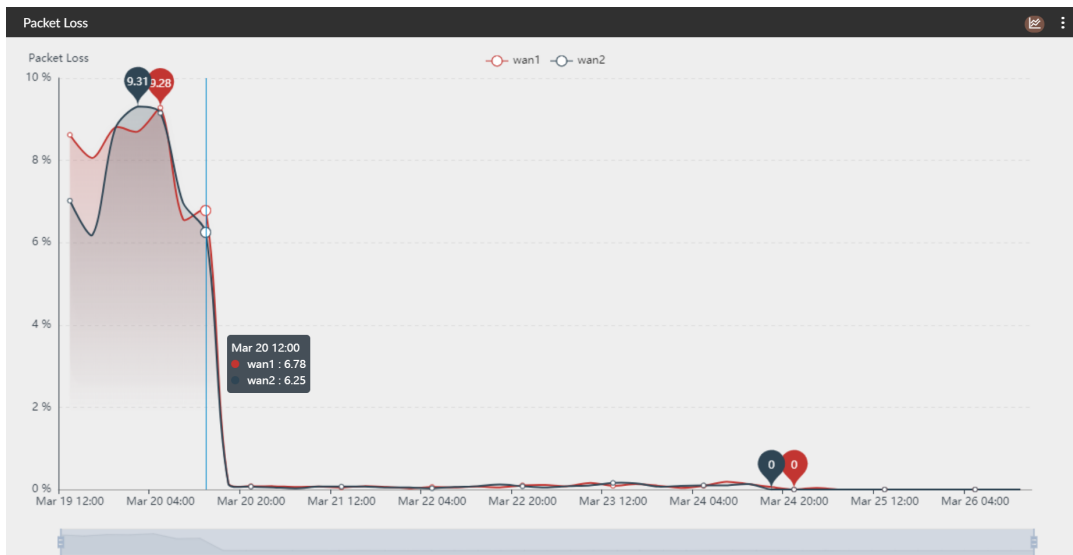


3. **Latency:** The *Latency* widget shows a line chart of the latency data for each SD-WAN link across the selected time period. Hover over the line chart to see date, time, and latency data in the tooltip.



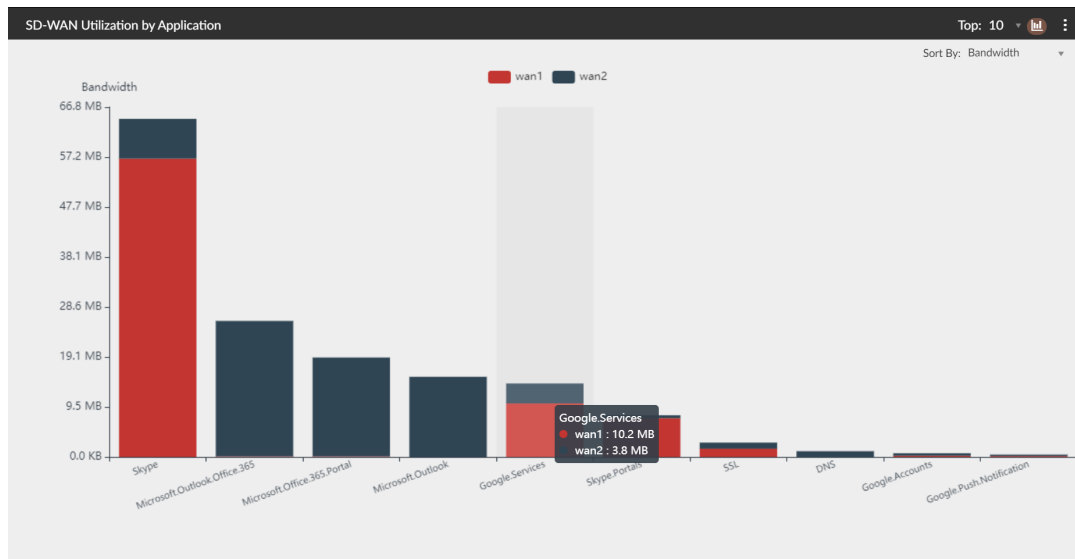
4. **Packet Loss:** The *Packet Loss* widget shows a line chart of the packet loss data for each SD-WAN link across the selected time period.

Hover over the line chart to see date, time, and packet loss data in the tooltip.



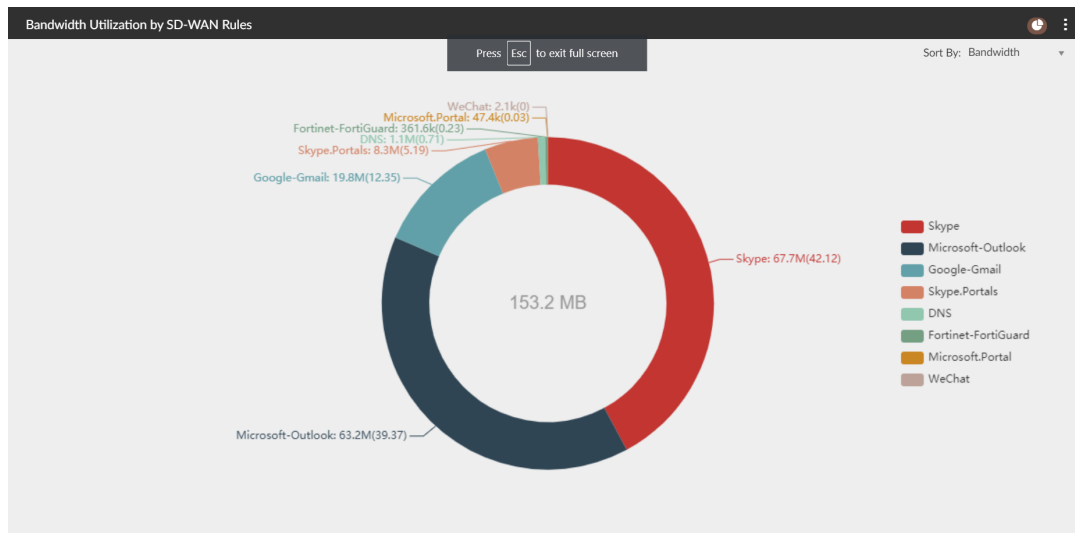
5. **SD-WAN Utilization by Application:** It shows a bar chart of the top 10, 20, or 30 applications on each SD-WAN link across the selected time period.

Hover over the bar chart to see application name and the utilization on each link in the tooltip.



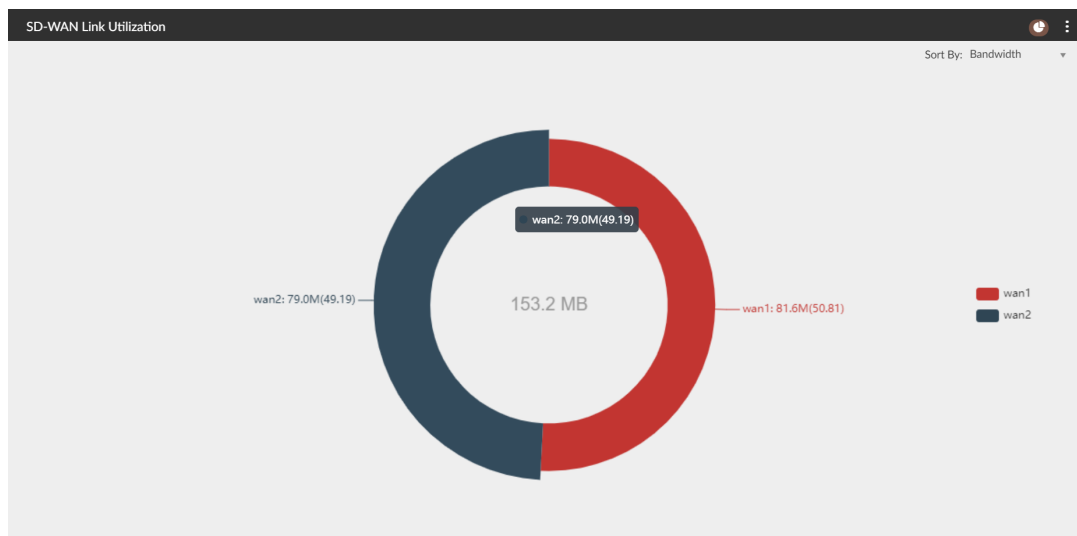
6. **Bandwidth Utilization by SD-WAN Rules:** It shows a donut chart of SD-WAN rules utilization across the selected time period.

Hover over the donut chart to see the rule name and utilization (percentage) in the tooltip.



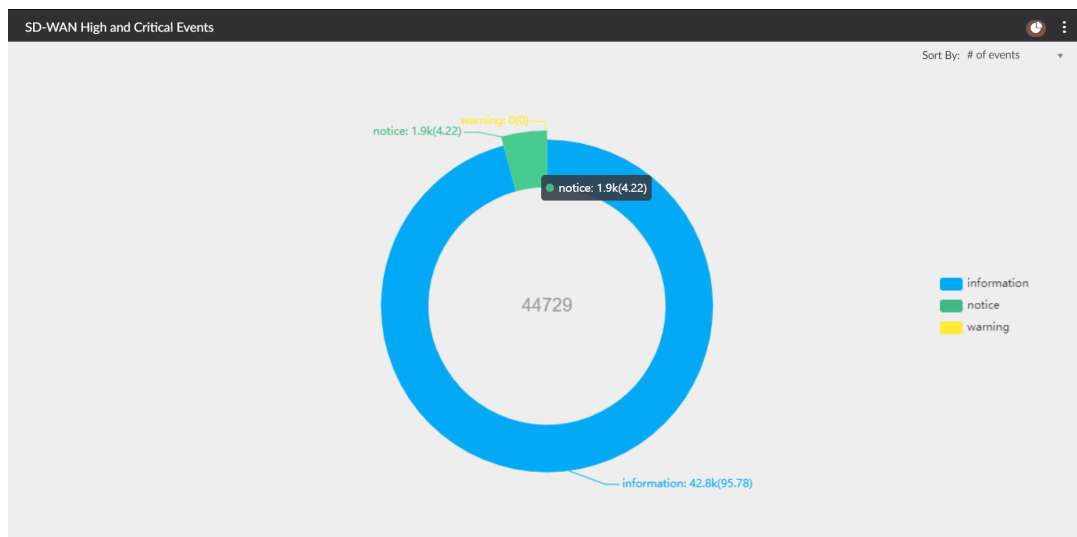
You can see the total utilization for all rules at the center of the donut chart.

7. **SD-WAN Link Utilization:** It shows a donut chart of utilization for each SD-WAN link across the selected time period. Hover over the donut chart to see link name and utilization (percentage) in the tooltip.



You can see the total utilization for all links at the center of the donut chart.

8. *SD-WAN High and Critical Events*: It shows a donut chart of events across the selected time period. Hover over the donut chart to see the event name and number (percentage) in the tooltip.

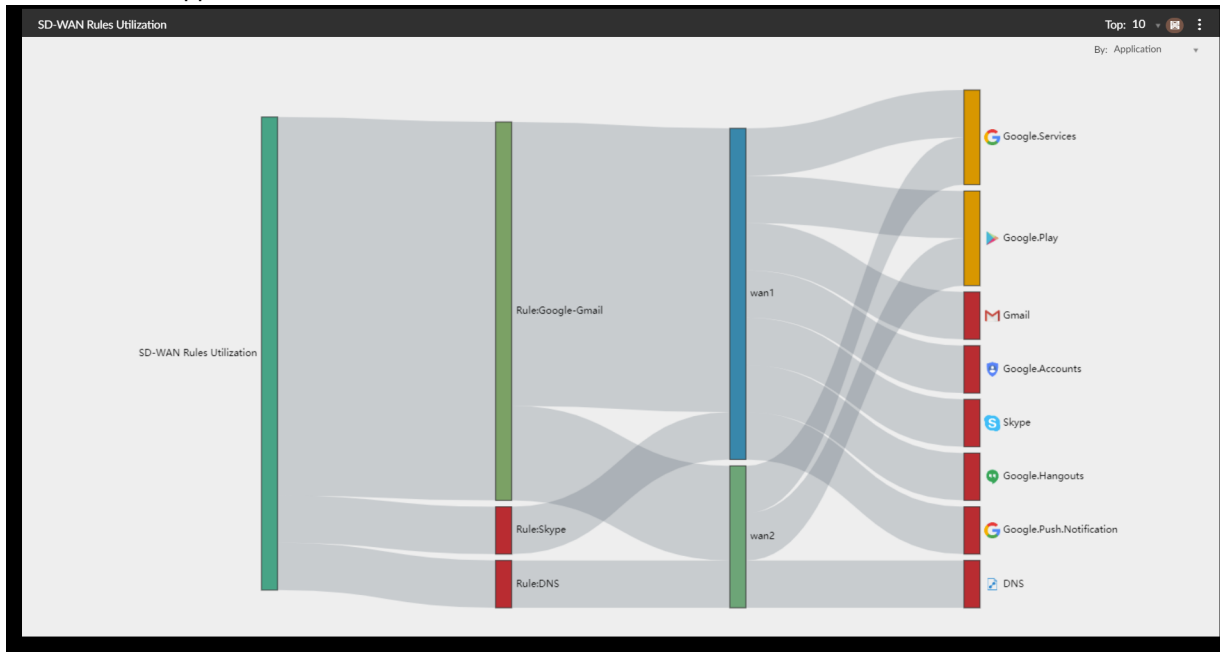


You can see the total number of events at the center of the donut chart.

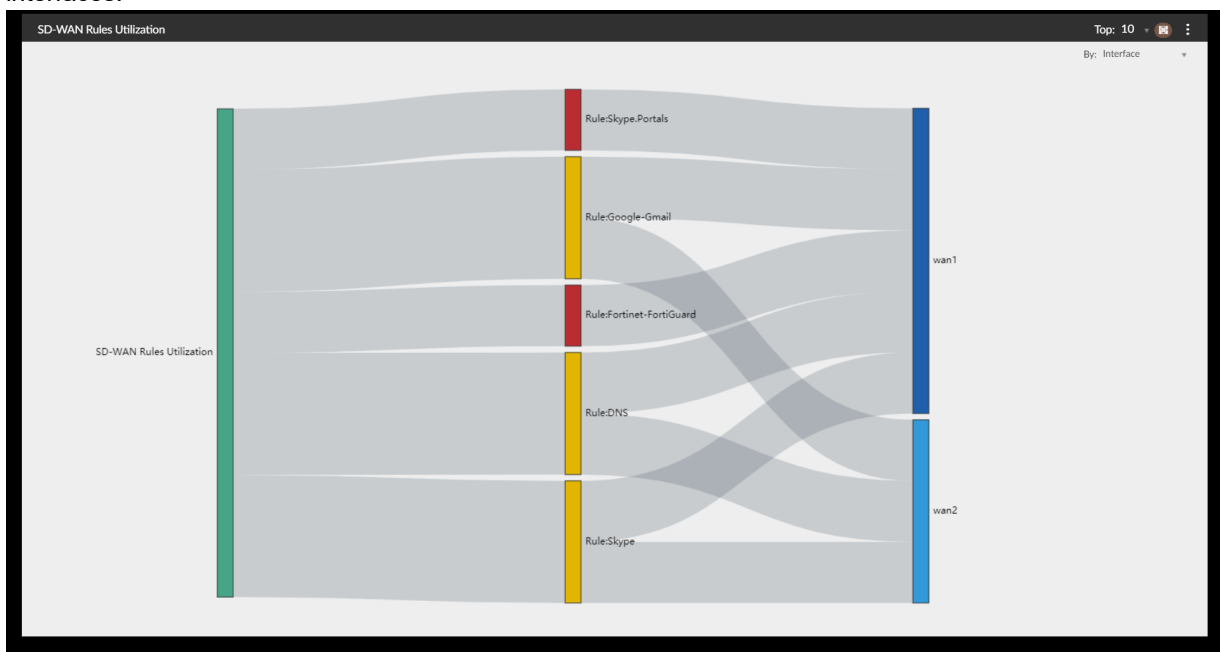


**To add the SD-WAN Rules Utilization widget:**

1. Go to *FortiView > Monitors > Secure SD-WAN Monitor*, and click *Edit Dashboard*.
2. Click the plus icon and select the *SD-WAN Rules Utilization* widget to add it to the dashboard, then click *Done*.  
The SD-WAN Rules Utilization widget includes two sankey diagrams. Toggle between the displayed diagrams by selecting a display type in the *By:* dropdown.
  - *SD-WAN Rules Utilization by Application:* SD-WAN rules are displayed connected to SD-WAN member interfaces and applications.



- *SD-WAN Rules Utilization by Interface:* SD-WAN rules are displayed connected to SD-WAN member interfaces.



## Enhanced SD-WAN Report

This report leverages enhanced FortiGate SD-Wan logs to display SD-Wan utilization by different rules, links, applications a users as well as link SLA, performance and quality KPIs such as Latency, Packet Loss and Jitter changes over time.

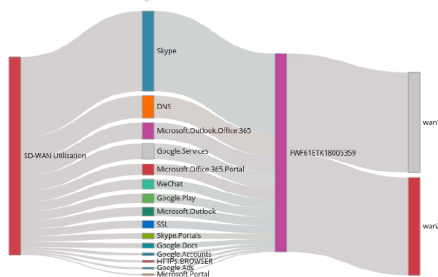
The enhanced report includes the following:

- Improved report cover page.



- Added Sankey chart type for better visualization.

Application usage should have a strong influence on your network architecture. Understanding which types of applications are used and specifically business application performance can improve user experience and productivity. Following chart illustrates a breakout of applications specific to your network as ranked by traffic volume. These applications can be prioritized by leveraging SD-WAN application steering strategies and Service Level Agreements (SLAs) in order to engineer their optimal path to the Internet.



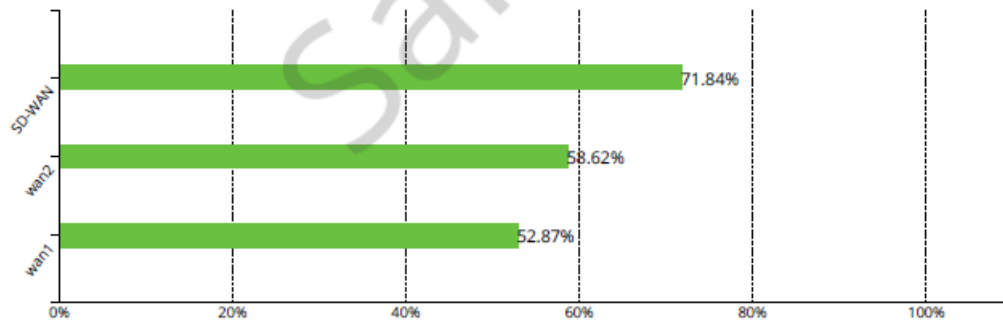
- Added horizontal bar chart: *SD-WAN Availability*.

## SD-WAN Performance

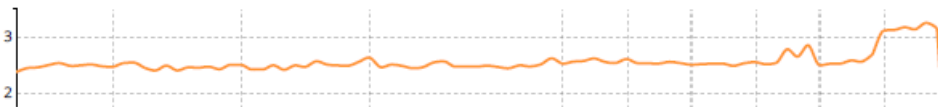
Multi-path technology can automatically fail over to the best available link when the primary WAN path degrades. This automation is built into the FortiGate, which reduces complexity for end-users while improving their experience and productivity.

### Overview of Device - FWF61ETK18005359

#### SD-WAN Availability



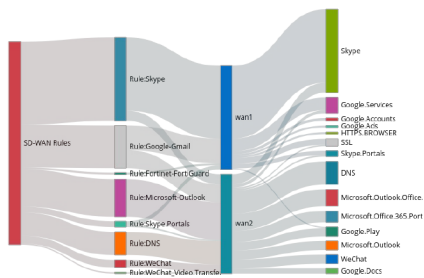
#### Latency After SD-WAN Implementation (ms)



- Added Sankey chart for device drilldown.

Device - FWF61ETK18005359

SD-WAN Device Traffic Distribution by Interface and Application

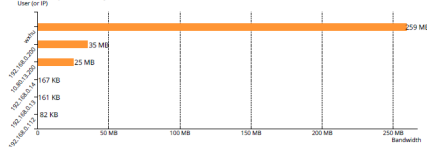


- Added horizontal bar chart: *SD-WAN Users*.

SD-WAN Users

By looking at source traffic, we can determine the originating source of any particular traffic. Certain botnets, command and control functions, and even remote access can be session heavy and indicative of targeted attacks or persistent threats. Following charts representative of source traffic activity that may need further investigation.

SD-WAN Top Source by Traffic Volume



SD-WAN Top Source by Application and Traffic Volume

#	User (or IP)	Application	Bandwidth	% of Subtotal
1	10.10.10.10	Skype	123.51 MB	47.67%
		DNS	34.68 MB	13.39%
		Microsoft.Outlook	25.58 MB	9.87%
		Office365	75.32 MB	29.07%
		Others	75.32 MB	29.07%

To view the full sample report, go to *Reports > Templates* and select HTML or PDF for *Template - Secure SD-WAN Report*.

## Secure SD-WAN assessment report - 6.4.2

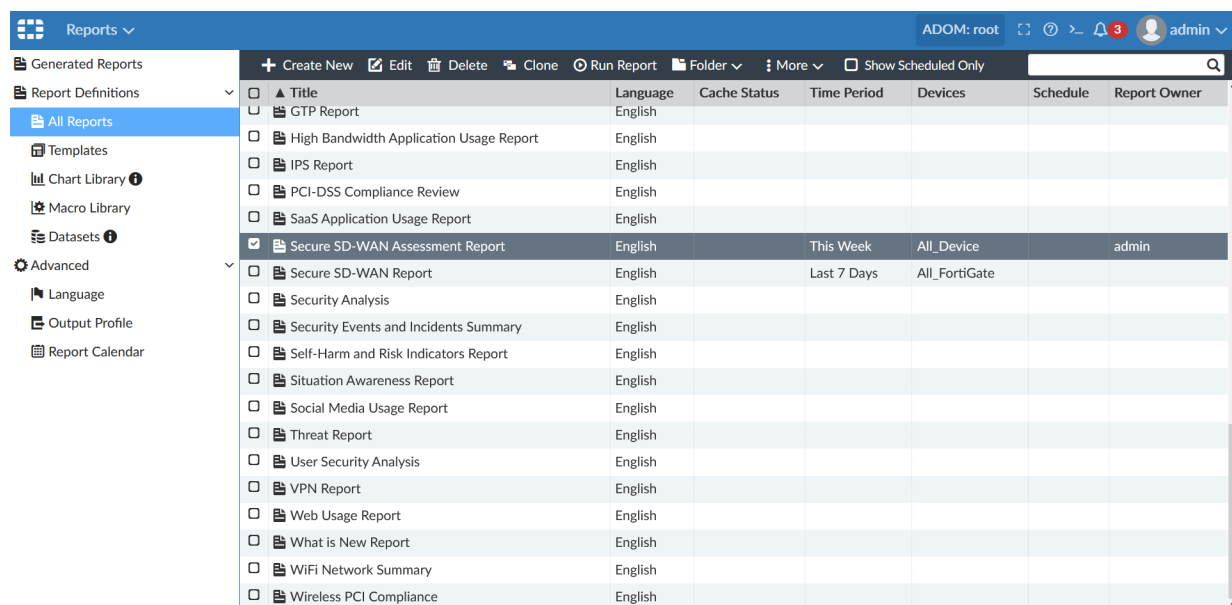
This new report on FortiAnalyzer will be consistent with CTAP Secure SD-WAN report that we already provide to prospective customers via the CTAP program.

### To view the Secure SD-WAN assessment report:

- In FortiAnalyzer, go to *Reports > Templates* and view *Template - Secure SD-WAN Assessment Report*.

Title	Language	Description	Category	Preview
Template - SaaS Application Usage Report	English	Summarizes the usage of SaaS apps compared to all applications, Sanctioned vs Unsancationed SaaS applications, and total bandwidth by SaaS Sanctioned and Unsancationed apps.	Application	HTML PDF
<b>Template - Secure SD-WAN Assessment Report</b>	English	Secure SD-WAN Assessment Report.	System	HTML PDF
Template - Secure SD-WAN Report	English	Secure SD-WAN Report.	System	HTML PDF
Template - Security Analysis	English	Security Analysis of traffic, application, user, destination, bandwidth and sessions. DHCP, Wifi, traffic history. Web usage by users, categories and sites. Top email by senders, recipients. Malware, botnet, intrusion detections, victims and sources. VPN usage. Admin Login and system events.	Security	HTML PDF
Template - Security Events and Incidents Summary	English	Present a brief summary of the events/Incidents collected.	Security	HTML PDF
Template - Self-Harm and Risk Indicators Report	English	Self-Harm and Risk Indicators Report.	Application	HTML PDF
Template - Situation Awareness Report	English	Provide awareness of your current security posture, and allow for a better understanding of the 'big picture' which will help anticipate what may happen to networks and systems enabling the	Security	HTML PDF

The report is also available in *All Reports*.



The screenshot shows the FortiAnalyzer Reports interface. On the left is a sidebar with navigation options: Reports (selected), Generated Reports, Report Definitions, All Reports, Templates, Chart Library, Macro Library, Datasets, Advanced, Language, Output Profile, and Report Calendar. The main area displays a table of report definitions. The table has columns for Title, Language, Cache Status, Time Period, Devices, Schedule, and Report Owner. The 'Secure SD-WAN Assessment Report' is selected and highlighted.

Title	Language	Cache Status	Time Period	Devices	Schedule	Report Owner
<input type="checkbox"/> ▲ Title	English					
<input type="checkbox"/> GTP Report	English					
<input type="checkbox"/> High Bandwidth Application Usage Report	English					
<input type="checkbox"/> IPS Report	English					
<input type="checkbox"/> PCI-DSS Compliance Review	English					
<input type="checkbox"/> SaaS Application Usage Report	English					
<input checked="" type="checkbox"/> Secure SD-WAN Assessment Report	English		This Week	All_Device		admin
<input type="checkbox"/> Secure SD-WAN Report	English		Last 7 Days	All_FortiGate		
<input type="checkbox"/> Security Analysis	English					
<input type="checkbox"/> Security Events and Incidents Summary	English					
<input type="checkbox"/> Self-Harm and Risk Indicators Report	English					
<input type="checkbox"/> Situation Awareness Report	English					
<input type="checkbox"/> Social Media Usage Report	English					
<input type="checkbox"/> Threat Report	English					
<input type="checkbox"/> User Security Analysis	English					
<input type="checkbox"/> VPN Report	English					
<input type="checkbox"/> Web Usage Report	English					
<input type="checkbox"/> What is New Report	English					
<input type="checkbox"/> WiFi Network Summary	English					
<input type="checkbox"/> Wireless PCI Compliance	English					

Below is a sample of the Secure SD-WAN assessment report.

## Executive Summary

We aggregated key findings from our Secure SD-WAN assessment within the Executive Summary below. While the highlights are listed below, a more detailed view of each section follows. Be sure to review the Recommended Actions page at the end of this report as well for actionable steps your organization can take to optimize your network for Direct Internet Access, protect your organization from external/branch office threats, and ultimately save money.

### Application

**261**External (Potential  
DIA) Applications**72.70 GB**Total Cloud IT  
Traffic**435.84 GB**Total VoIP/Audio/  
Video Traffic

Application usage should have a strong influence on your network architecture. Understanding which types of applications are used and specifically business application performance can improve user experience and productivity.

### Security

**74**Application  
Vulnerability  
Attacks Detected**359**Malware and/or  
Botnet Detected**69**High Risk  
Applications  
Detected

Maintaining a full security stack at the WAN edge is critical in any SD-WAN deployment where public Internet circuits are leveraged. Note that any threats observed within this report have effectively bypassed your existing network security gateway, so they should be considered active and may lead to increased risk (such as a data breach).

### Utilization

**55.69 TB**Total Bandwidth  
Used**1.11 TB**Total Non-  
Business Traffic**5.67 TB**Total SSL  
Encrypted Traffic

In addition to individual applications, understanding overall utilization can help with capacity planning, circuit selection, and streamlining network traffic over time. This awareness can also help reduce operational costs associated with backhauling traffic over more expensive WAN links (such as MPLS).

# Dynamic Cloud Security

This section lists the new features added to FortiAnalyzer for Dynamic Cloud Security. They are organized into the following sections

- [Public cloud on page 17](#)
  - [FortiCare license for AWS PAYG instances on page 17](#)
- [Application security on page 24](#)
  - [FortiWeb Pcap Support on page 24](#)

## Public cloud

This section lists the new features added to FortiAnalyzer for public cloud.

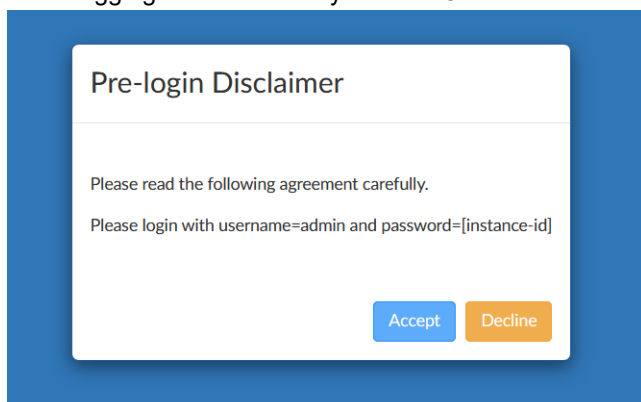
List of new features:

- [FortiCare license for AWS PAYG instances on page 17](#)
- [Support for cloud-init service for KVM, Azure, and AWS 6.4.1 on page 18](#)

## FortiCare license for AWS PAYG instances

FortiAnalyzer instances on AWS (PAYG) obtain FortiCare-generated licenses automatically.

When logging into a FortiAnalyzerAWS On Demand instance for the first time, a pre-login disclaimer page is displayed.



After successful login, the FAZ-AWS instance retrieves the license from the FortiCare server. This license includes a certificate that uses the serial number as the CN name.

The following is a comparison between the local certificate in a FortiAnalyzer 6.2.3 and 6.4.0 AWS On Demand instance.

### FortiAnalyzer-AWS On Demand 6.2.3

View Local Certificate	
Certificate Name	Fortinet_Local
Issuer	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-subca2001, emailAddress = support@fortinet.com
Subject	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiAnalyzer, CN = FAZ-VM000000001, emailAddress = support@fortinet.com
Valid From	2017-08-30 23:03:13 GMT
Valid To	2056-01-19 03:14:07 GMT
Version	3
Serial Number	38:f9
Extension	Name: X509v3 Subject Key Identifier Critical: no Content: EC:F5:B8:1A:C2:24:2C:2F:C1:25:8D:0F:5F:44:84:C9:66:A5:AC:94
	Name: X509v3 Authority Key Identifier Critical: no Content: keyid:98:2B:25:3C:30:CA:2C:2B:56:E7:DB:FC:59:33:B3:DC:3D:5B:6A:D7 DirName:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=fortinet-ca2/emailAddress=support@fortinet.com serial:20:01
	Name: X509v3 Basic Constraints Critical: yes Content: CA:FALSE
	Name: X509v3 Key Usage Critical: yes Content: Digital Signature

### FortiAnalyzer-AWS On Demand 6.4.0

View Local Certificate	
Certificate Name	Fortinet_Local
Issuer	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-subca2001, emailAddress = support@fortinet.com
Subject	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiAnalyzer, CN = FAZAWSTA200000050, emailAddress = support@fortinet.com
Valid From	2020-04-08 19:15:59 GMT
Valid To	2056-01-19 03:14:07 GMT
Version	3
Serial Number	0f:3d:10
Extension	Name: X509v3 Subject Key Identifier Critical: no Content: 12:CD:40:C8:D1:18:E8:8F:1F:FE:DD:C2:8E:0F:A8:3E:3F:0C:E3:BC
	Name: X509v3 Authority Key Identifier Critical: no Content: keyid:98:2B:25:3C:30:CA:2C:2B:56:E7:DB:FC:59:33:B3:DC:3D:5B:6A:D7 DirName:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=fortinet-ca2/emailAddress=support@fortinet.com serial:20:01
	Name: X509v3 Basic Constraints Critical: yes Content: CA:FALSE
	Name: X509v3 Key Usage Critical: yes Content: Digital Signature

## Support for cloud-init service for KVM, Azure, and AWS - 6.4.1

You can use the cloud-init service for customizing a prepared image of a virtual installation. The cloud-init service is built into the virtual instances of FortiAnalyzer-VM found on the support site so that you can use them on a VM platform that supports the use of the service. To customize the installation of a new FortiAnalyzer-VM instance, you must combine the seed image from the support site with user data information customized for each new installation.

Hypervisor platforms such as QEMU/KVM support the use of this service on most major Linux distributions, as well as BSD and Hyper-V. A number of cloud-based environments, such as VMware and AWS also support it.

You can use the cloud-init service to help install different instances based on a common seed image by assigning hostnames, adding SSH keys, and settings particular to the specific installation. You can add other more general customizations, such as the running of post install scripts.



While cloud-init is the service used to accomplish the customized installations of VMs, various other programs, depending on the platform, are used to create the customized ISOs used to create the images that will build the FortiAnalyzer-VM.



Although this feature supports FortiAnalyzer, this topic only includes examples for FortiManager.

---

This topic includes the following sections:

- [KVM on page 19](#)
- [AWS on page 21](#)
- [Microsoft Azure on page 22](#)

## KVM

### To configure on KVM:

1. On the host server (Ubuntu), start service `libvirtd`.
2. Prepare the FortiAnalyzer configuration and license file.

This license is named `0000`, without any extension.

The folder structure should be as follows:

```
<holding folder>
/openstack
/content
0000
/latest
user_data
```

For example:

```
config system global
    set hostname fmg-boot-strap
end
```

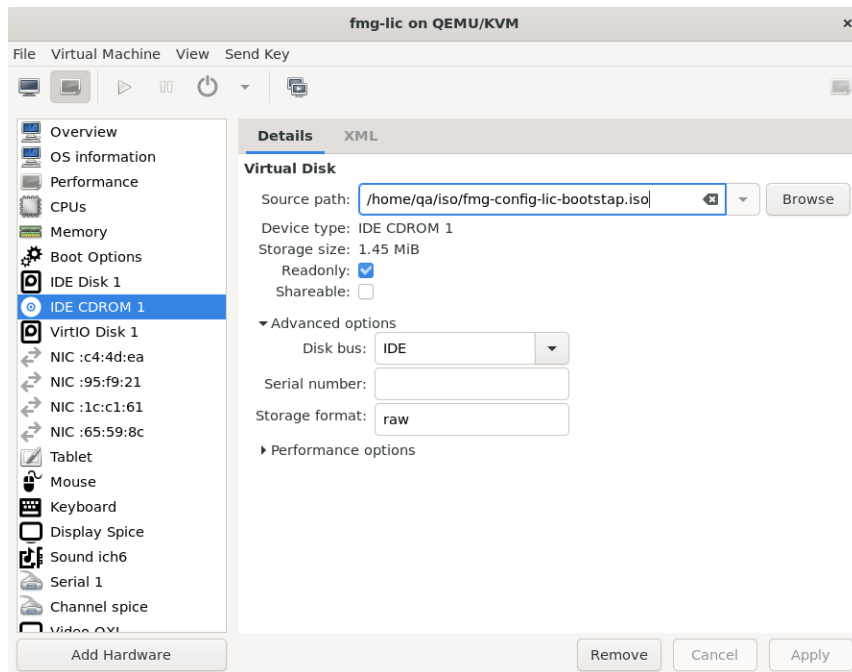
3. Convert the folder to an ISO image using the `mkisofs` utility.

Following is the syntax of the command:

```
mkisofs [options] [-o <filename of new ISO>] pathspec [pathspec...]
```

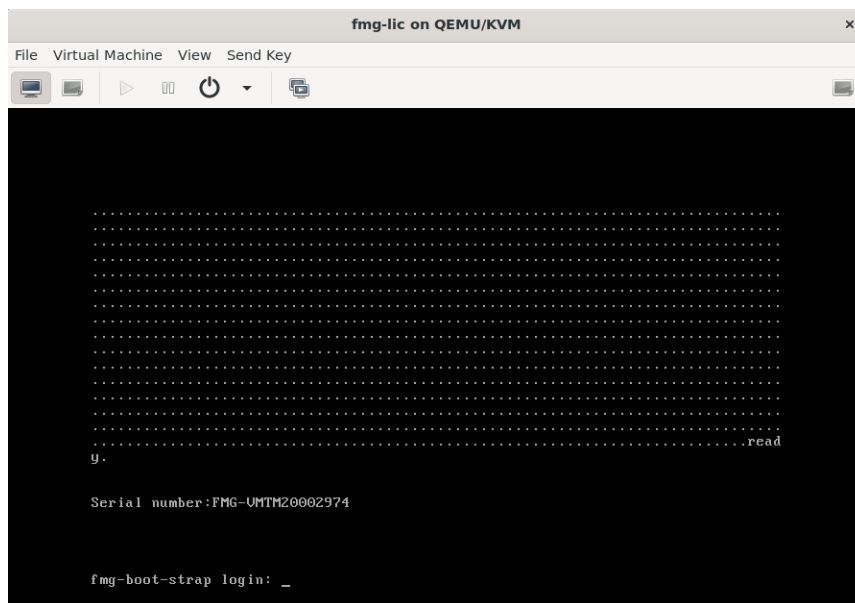
4. Create a FortiAnalyzer instance, attach a virtual CDROM, which is based on `fmg-config-lic-bootstap.iso`. The following command sets up a virtual CDROM drive as if it were on an IDE bus holding a virtual CD in it with no cache, and the data is in RAW format.

```
disk /home/username/test/fmg-config-lic-
bootstap.iso,device=cdrom,bus=ide,format=raw,cache=none -
```



5. Boot up the FortiAnalyzer KVM virtual machine.

In the following example for FortiManager, the configuration and license upload to the FortiManager KVM virtual machine.



```
bash# cat vmd.log.1
[186] cdrom mounted
[186] /cdrom/openstack/content/0000: size=9171:
-----BEGIN FMG VM LICENSE-----
QAAAAKgh6/7exA+Da/9ho2iypJYLjYKx+vFPBYd6cR6XlTq1WFz95Fz+b1n1sa2OPLldeC5h5sgh
CZMEcGUczbnSZMcQGgAAMC/mTe8EPRK/ARkMpi8Av3IIICm7Irgds8xk+cgeMpZTMBtq2FrXsAmr
yErFgUgYmouRu9VMtJnJl4nnFRXZzsBez/Xa7XeBBUeHuLuxAiHyI2rIUfXQOPeIgV06eLrFLdu
```

```
UpD1EqadFK3eDDoMX4wEFzLHJbbBrjErWKvu2Cf94sEDsaVQmI/Cv5nOzd9rQgR2TdxQ06YO25dr
cRuhoxA/nY4fvqwOcHbhUYpafF2NDeKiXzDVS1iRun5ZYFcCuIOTkGr2AQb5zx6MdlQgc+k8boIO
```

```
.....
```

```
JAYU8CgENbH++ClFTDAG6lznT68KcZDF7lcoAr56+p7OjXBEZrwUFVVIv4CWctfntG1v7uE9Po0P
9PZyNgupzf71stWtYDfgrSZO
-----END FMG VM LICENSE-----
```

```
[186] /cdrom/openstack/latest/user_data: size=438:
config system global
    set hostname fmg-boot-strap
end
```

## AWS

### To configure on AWS:

1. Go to the AWS marketplace, and follow the procedure to launch a FortiAnalyzer AZURE virtual machine.
2. On the 3. *Configure Instance* page, select the VPC subnet and the IAM role.

When selecting the VPC subnet, select the IAM role that was created, and specify information about the license file and configuration file from the AWS S3 bucket that was previously configured under *Advanced Settings*. In this example, the *IAM role name* is *fmgrole*.

**Step 3: Configure Instance Details**  
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

**Number of instances** ①  [Launch into Auto Scaling Group](#) ①

**Purchasing option** ① ☐ Request Spot instances

**Network** ①  [Create new VPC](#)

**Subnet** ①  [Create new subnet](#)  
218 IP Addresses available

**Auto-assign Public IP** ①

**Placement group** ① ☐ Add instance to placement group

**Capacity Reservation** ①  [Create new Capacity Reservation](#)

**IAM role** ①  [Create new IAM role](#)

**Shutdown behavior** ①

**Stop - Hibernate behavior** ① ☐ Enable hibernation as an additional stop behavior

**Enable termination protection** ① ☐ Protect against accidental termination

**Monitoring** ① ☐ Enable CloudWatch detailed monitoring

### 3. Expand *Advanced Details*, and set *User data* to *As text*, for example:

Step 3: Configure Instance Details

Additional charges will apply for dedicated tenancy.

Elastic Inference *i* ☐ Add an Elastic Inference accelerator  
Additional charges apply.

T2/T3 Unlimited *i* ☐ Enable  
Additional charges may apply

File systems *i*

▼ Network interfaces *i*

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-31b2c14f	Auto-assign	<input type="button" value="Add IP"/>	<input type="button" value="Add IP"/>

▼ Advanced Details

Metadata accessible *i* Enabled

Metadata version *i* V1 and V2 (token optional)

Metadata token response hop limit *i* 1

User data *i* ☒ As text ☐ As file ☐ Input is already base64 encoded

```
{
  "bucket": "fmg3",
  "region": "us-east-1",
  "license": "FMG-VM19003983 lic",
  "config": "fmg-hostname-config.txt"
}
```

### 4. Go to the FortiAnalyzer GUI, and log in.

### 5. In FortiAnalyzer, go to *System Settings > Dashboard*.

In the following example for FortiManager, the *System Information* widget displays the specified hostname, and the *License Information* widget displays the activated license.

System Settings

Dashboard

System Information

Host Name	bootstrap-hostname
Serial Number	FMG-VM19003983
Platform Type	FMG-VM64-AWS
HA Status	Standalone
System Time	Sun May 17 17:36:36 2020 PDT
Firmware Version	v6.4.0-build2002 200408 (GA)
System Configuration	Last Backup : N/A
Current Administrators	admin /1 in total
Up Time	3 minutes 17 seconds
Administrative Domain	<input type="checkbox"/> OFF
FortiAnalyzer Features	<input type="checkbox"/> OFF

System Resources

License Information

VM License	Type	Valid UUG
FortiCloud	VM Meter Service	Registered
FortiGuard	Server Location	No License
Management	Devices/VDOMs	Servers located in US only
Update Server	Antivirus and IPS	96.45.33.88 (United States)
	Web and Email Filter	209.222.147.36 (United States)
	FortiClient Update	96.45.33.106 (United States)

Unit Operation

FORTINET

## Microsoft Azure

### To configure on Microsoft Azure:

1. Use PowerShell to deploy the FortiAnalyzer Azure VM with user data.
2. Create a MIME text file named `azureinit.conf` in local PC `C:\Azure\misc` directory.  
You can change the directory path and file name using the `$customdataFile = C:\Azure\misc\azureinit.conf` parameter in the `ps1` file. The `azureinit.conf` is the text file in MIME format that includes both FortiGate CLI commands and license file content.

```
Content-Type: multipart/mixed; boundary="=====0740947994048919689=="
MIME-Version: 1.0
```

```
-----0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config"
```

```
config system admin setting
    set idle_timeout 480
    set shell-access enable
end
```

```
-----0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license"
```

```
-----BEGIN FMG VM LICENSE-----
QAAAAD1P27eiQC4JGGA1wDYnqMasNcDlXUtjg02/nt21seyucBTncObcRqPsXXFcRqkpoINA83PC
.....
IOb6sMYu8MnmDPAJLgygex1BdImccRJ3pe+E9ZgT5tAu7gBVhDa5Bo/kf3IdJOoRdxvFXcUGC0+k
4TgteYmIRK7E5C0ZGV0AGqn2zTmwaFxF9J22R68tkI3fGbHGbAfjcPN5IAdC7TWHWYJWEoOQy8o/
TJ9wReuzEIWC3SrWtgpqfMNM527h4RQrLXBJP0VOM+C4ZHkedrbBy7qFQWhHC+Lps8rsPh/Qj1PN
Ii6kVnHrAgf9dI7C4IAmEKlQ
-----END FMG VM LICENSE-----
```

```
-----0740947994048919689==--
```

After FortiAnalyzer Azure VM is created, the FortiAnalyzer license and configuration are uploaded.

3. Go to FortiAnalyzer GUI, and log in.
4. Go to *System Settings > Dashboard*. In the following example, the *System Information* widget displays the serial number.

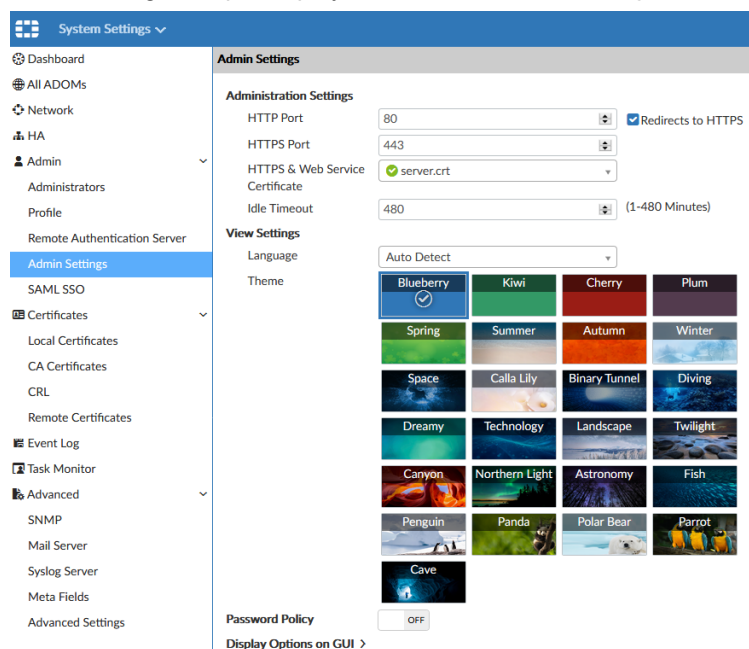
The screenshot displays the FortiAnalyzer GUI Dashboard. The left sidebar shows the navigation menu with 'System Settings' selected. The main content area is divided into several widgets:

- System Information:** A table displaying system details:
 

Host Name	fmg1307
Serial Number	FMG-VMTM19003983
Platform Type	FMG-VM64-AZURE
HA Status	Standalone
System Time	Sun May 17 22:29:17 2020 PDT
Firmware Version	v6.2.5-build1307 200515 (GA)
System Configuration	Last Backup: N/A
Current Administrators	fmgazure /1 in total
Up Time	26 minutes 13 seconds
Administrative Domain	<input type="checkbox"/> OFF
FortiAnalyzer Features	<input type="checkbox"/> OFF
- System Resources:** Three circular progress indicators showing usage levels:
  - Average CPU Usage: 0%
  - Memory Usage: 17%
  - Disk Usage: 27%
- Unit Operation:** A section for FortiManager-VM64-AZURE with buttons for Restart and Shutdown.
- Alert Message Console:** A table of recent alerts:
 

Time	Message
May 17, 22:18:38	Login from ssh: Failed for invalid user supervisor from 130.105.122.21 port 56777
May 17, 22:07:22	Login from ssh: Failed for invalid user root from 115.79.37.77 port 63928
- License Information:** A section at the bottom for license details.

5. Go to *System Settings > Admin > Admin Settings*.  
The following example displays the *Administration Settings*:



## Application security

This section lists the new features added to FortiAnalyzer for application security.

List of new features:

- [FortiWeb Pcap Support on page 24](#)

## FortiWeb Pcap Support

The FortiWeb attack log provides a deep analysis tool that allows customers to understand why a particular request was flagged as a violation. It gives detailed information in a 'Wireshark' like visual separating the HTTP requests into headers, cookies, parameters, and the HTTP body, highlighting the pattern that triggered the violation.

This enhancement in FortiAnalyzer allow users to view FortiWeb packet logs with additional HTTP request information included.

### To view FortiWeb packet logs:

1. Go to *Log View*.
2. In the tree menu, select *Application Attack Prevention*.  
The *Application Attack Prevention* pane opens.

#	Date/Time	Device ID	Source Name	Destination	Policy	Action	HTTP URL	HTTP Host	Message	Data
1	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
2	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
3	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
4	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
5	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
6	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
7	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
8	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
9	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
10	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	

In the *Application Attack Prevention* pane, FortiWeb packets appear in the far right-side under *Data*.



By default, *Data* is not visible in the log view. You can enable it from the settings on the far-right side.

FortiWeb packets also appear in the log detail panel.

#	Date/Time	Device ID	Source Name	Destination	Policy	Action	HTTP URL	HTTP Host	Message	Data
1	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
2	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
3	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
4	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
5	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
6	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
7	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
8	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
9	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	
10	01-10-14:59	FVVM020000194963	10.3.120.254	10.3.120.61	qa	Alert	/	172.18.78.239	Custom Access rule [bst_faz_cus_rule]	

3. Click on the packet icon to view the packet details.

The *View Attack Content* dialog appears. It shows packet details using the same design as IPS Archive.

### View Attack Content

Packet Header

```
GET / HTTP/1.1
User-Agent:python-requests/2.18.4
Accept-Encoding:gzip, deflate
Accept:/*/*
Connection:keep-alive
Host:172.18.78.239
Content-Length:48
Content-Type:application/x-www-form-urlencoded
```

Packet Body

```
para_limit7=select+user+from+sysibm.sysdummy1%3B
```

arguments

Name	Value
para_limit7	select user from sysibm.sysdummy1;

Cancel



# Zero Trust Network Access

This section lists the new features added to FortiAnalyzer for Zero Trust Network Access.

List of new features:

- [NAC on page 27](#)
  - [FortiNAC Report on page 27](#)
- [IAM on page 28](#)
  - [SAML Fabric SSO on page 28](#)

## NAC

This section lists the new features added to FortiAnalyzer for NAC.

List of new features:

- [FortiNAC Report on page 27](#)

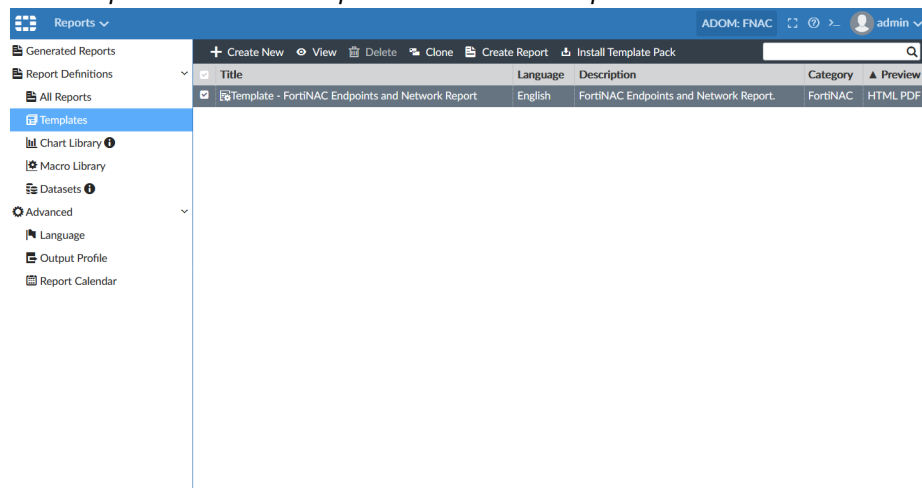
## FortiNAC Report

A default FortiAnalyzer report template has been added for endpoints and networks detected by FortiNAC.

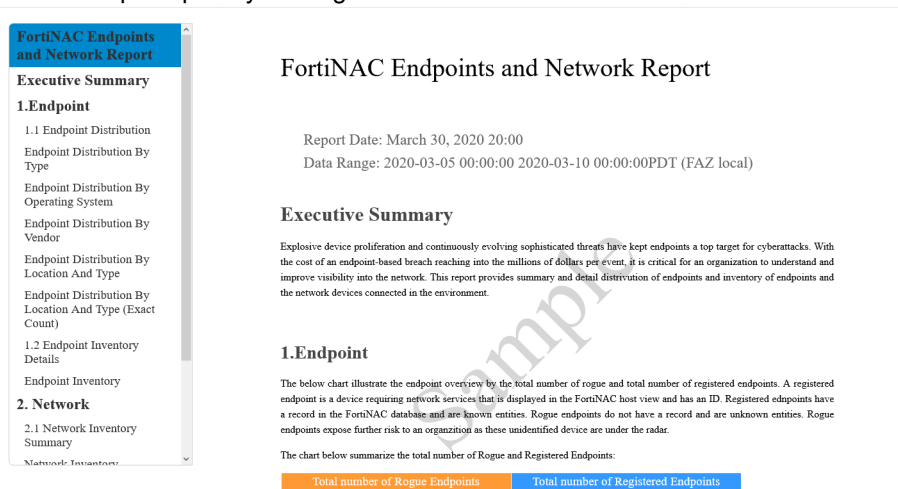
**To view the FortiNAC report template:**

1. Go to *Reports > Templates*.

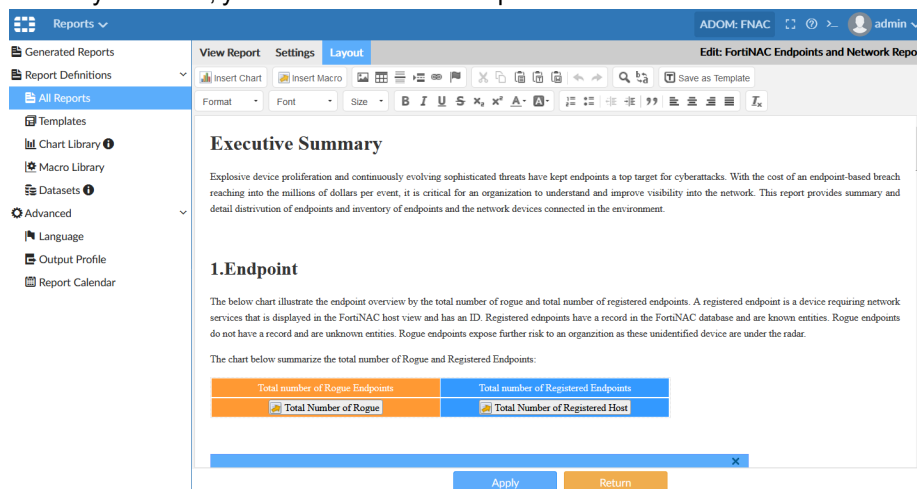
The *Template - FortiNAC Endpoints and Network Report* is available.



**2. View a sample report by clicking HTML or PDF.**



3. In the layout editor, you can customize the report.



## IAM

This section lists the new features added to FortiAnalyzer for IAM.

List of new features:

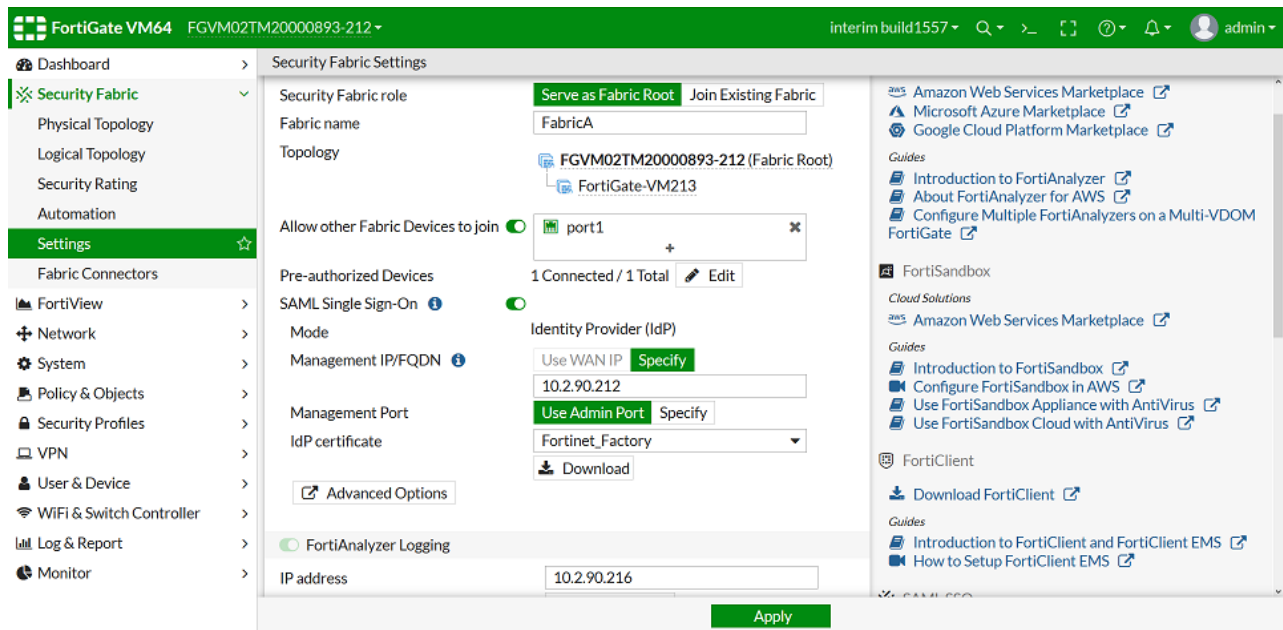
- SAML Fabric SSO on page 28

## SAML Fabric SSO

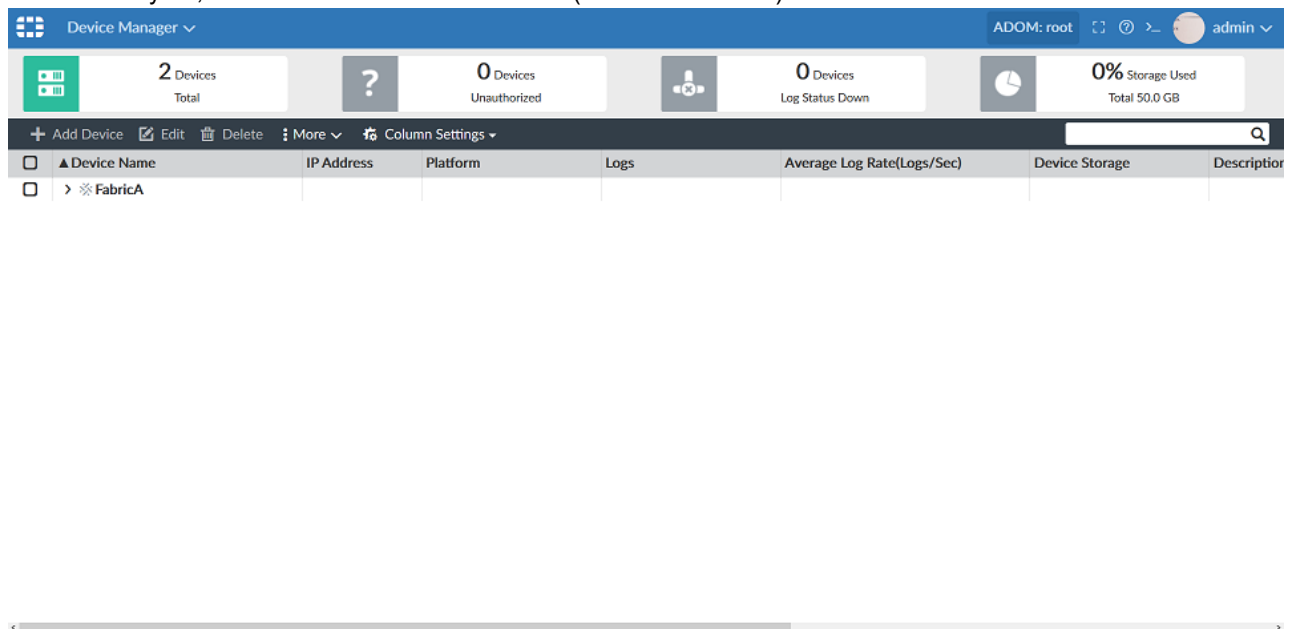
FortiAnalyzer supports SAML SSO as part of one or more Security Fabrics.

**To enable SAML Fabric SSO on FortiAnalyzer:**

1. On the root FortiGate of the Security Fabric, enable *SAML Single Sign-On*, and configure FortiAnalyzer logging by inputting the IP address of FortiAnalyzer.



2. On FortiAnalyzer, authorize FortiGate to an ADOM (or the root ADOM).



3. On FortiAnalyzer, go to *System Setting > SAML SSO > Fabric SP*. Input the FortiAnalyzer SP IP address, choose an existing admin profile as default profile for SSO admin users, and click *Apply*.

After a short wait (approximately 5 minutes), check the *Fabric IdPs* table on the Fabric SP page. Information about

Fabric IdPs is displayed.

**System Settings** | ADOM: root | admin

**Single Sign-On Settings**

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

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

SP Address: 10.2.90.216

Default Admin Profile: Restricted\_User

**Fabric IdPs**

	Root Device	ADOM Name	Status	IdP Settings
<input type="checkbox"/>	FGVM02TM20000893	root	Enabled	Entity ID: http://10.2.90.212/saml-idp/csf_j7mi9ojacy1g0wuzpe5pox Login URL: https://10.2.90.212/saml-idp/csf_j7mi9ojacy1g0wuzpe5p Logout URL: https://10.2.90.212/saml-idp/csf_j7mi9ojacy1g0wuzpe5
<input type="checkbox"/>	FGVM02TM20000899	fabricB	Enabled	Entity ID: http://10.2.90.215/saml-idp/csf_wl5j3jgxxvq70wtvhn503vb Login URL: https://10.2.90.215/saml-idp/csf_wl5j3jgxxvq70wtvhn503 Logout URL: https://10.2.90.215/saml-idp/csf_wl5j3jgxxvq70wtvhn50

Apply

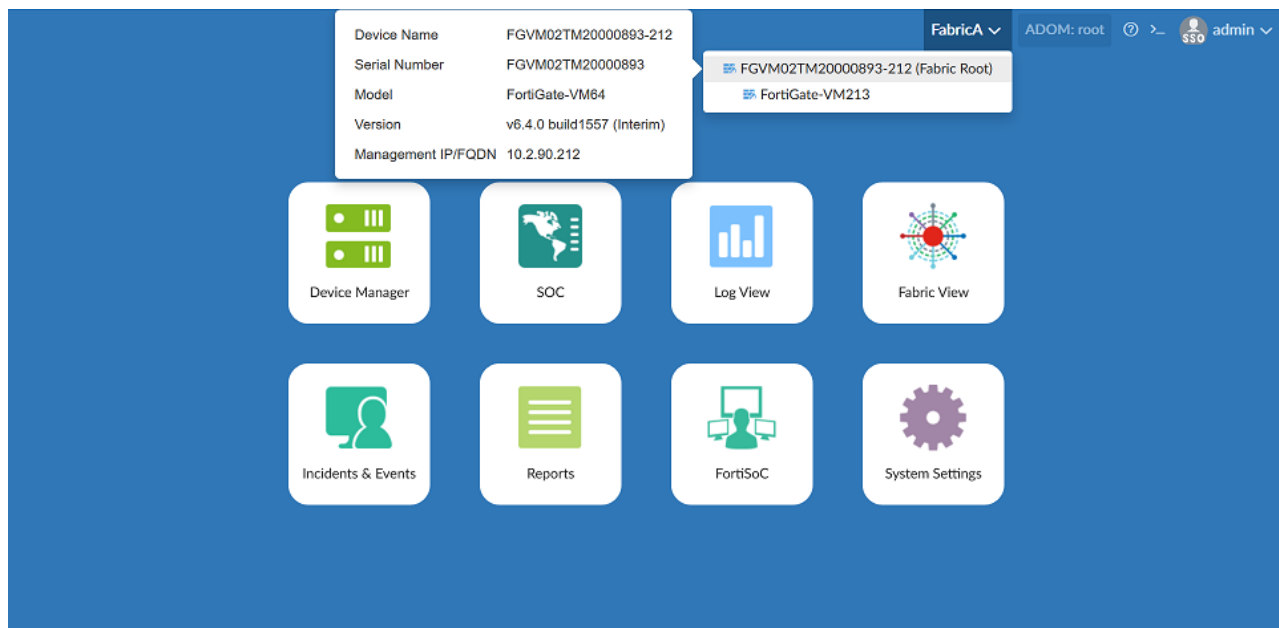
- Log in using Fabric SSO from the FortiAnalyzer login page.  
When logging in with Fabric SSO, each Fabric IdP registered on FortiAnalyzer is displayed. Choose an IdP to log in to using the SSO admin user account.  
Each SAML Fabric SSO is bound to the ADOM to which it was authorized, and the SSO admin only has access this specific ADOM on FortiAnalyzer.

**Select Fabric IdP**

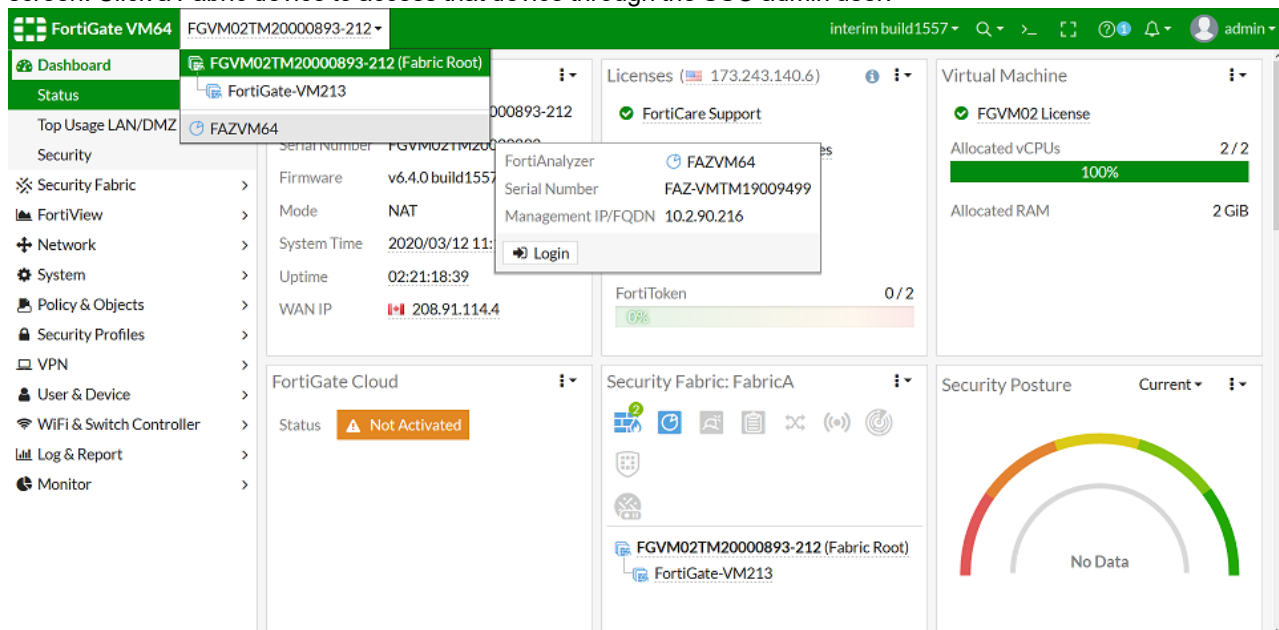
☒ FabricA root (2) ☒ FabricB fabricB (1)

Login via Fabric Single Sign-On

From the top-right corner menu on FortiAnalyzer, a Fabric tree including all FortiGates in the Fabric is displayed. Click a Fabric device to access that device through the SSO admin user.



From the root FortiGate of the Security Fabric, administrators can view the Fabric tree in the top-left corner of the screen. Click a Fabric device to access that device through the SSO admin user.



5. Additional Security Fabric IdPs can be registered by authorizing the root Fabric device onto a different FortiAnalyzer ADOM and repeating the steps above.

### To configure Fabric SAML SSO in the FortiAnalyzer CLI:

```
FAZVM64 # config sys saml
```

```
(saml)# show
config system saml
  set status enable
  set role FAB-SP
```

```
set server-address "10.2.90.216"
set default-profile "SSO_RW"
config fabric-idp
  edit "FGVM02TM20000893"
    set idp-cert "csf-FGVM02TM20000893"
    set idp-entity-id "http://10.2.90.212/saml-idp/csf_
j7mi9ojacylg0wuzpe5pox817zgq3cs/metadata/"
    set idp-single-logout-url "https://10.2.90.212/saml-idp/csf_
j7mi9ojacylg0wuzpe5pox817zgq3cs/logout/"
    set idp-single-sign-on-url "https://10.2.90.212/saml-idp/csf_
j7mi9ojacylg0wuzpe5pox817zgq3cs/login/"
    set idp-status enable
  next
  edit "FGVM02TM20000899"
    set idp-cert "csf-FGVM02TM20000899"
    set idp-entity-id "http://10.2.90.215/saml-idp/csf_
w15j3jgxvq70wtvhn503vbu7fetths5/metadata/"
    set idp-single-logout-url "https://10.2.90.215/saml-idp/csf_
w15j3jgxvq70wtvhn503vbu7fetths5/logout/"
    set idp-single-sign-on-url "https://10.2.90.215/saml-idp/csf_
w15j3jgxvq70wtvhn503vbu7fetths5/login/"
    set idp-status enable
  next
end
end
```

# AI-driven Security Operations

This section lists the new features added to FortiAnalyzer for AI-driven Security Operations.

List of new features:

- [SOC automation on page 34](#)
  - [Attach reports to incidents on page 34](#)
  - [Automation Playbooks on page 38](#)
  - [Add comments to incidents on page 45](#)
  - [Expanded incident analysis page on page 47](#)
  - [FortiSOC dashboards on page 51](#)
  - [FortiOS Connector on page 52](#)
  - [EMS Connector on page 56](#)
  - [Normalized Fabric logs on page 62](#)
  - [Incidents with multiple endpoints and users 6.4.2 on page 66](#)
  - [Default playbook template improvements 6.4.1 on page 67](#)
  - [Incident page improvement 6.4.1 on page 70](#)
  - [Filters for local report action 6.4.2 on page 76](#)
  - [SOC subscription license 6.4.1 on page 77](#)
  - [Try it Out feature for FortiSoC 6.4.2 on page 79](#)
  - [Vulnerabilities and software inventory data from EMS connector 6.4.2 on page 81](#)
  - [FortiMail connector 6.4.2 on page 85](#)
  - [Alerts on normalized logs 6.4.3 on page 88](#)
  - [Normalized logs for reports 6.4.3 on page 91](#)
  - [FortiGuard connector 6.4.3 on page 93](#)
  - [Connector's health check 6.4.3 on page 96](#)
- [Advanced threat protection on page 101](#)
  - [IoC re-scan events on page 101](#)
  - [FortiDeceptor logging on page 105](#)
  - [Unique count for event handler 6.4.2 on page 107](#)
  - [FortiGate C&C Detection in SOC View 6.4.3 on page 108](#)
  - [FortiADC logging 6.4.3 on page 111](#)
- [Dashboard/widgets/reports on page 113](#)
  - [FortiView custom widgets 6.4.1 on page 114](#)
  - [Extra caching for SOC reports 6.4.1 on page 117](#)
  - [Asset tags on page 118](#)
  - [Sankey Chart on page 120](#)
  - [FortiPortal user summary report 6.4.2 on page 121](#)
  - [FortiSandbox default report improvement 6.4.2 on page 123](#)
  - [Improved SOC incident report 6.4.2 on page 124](#)
  - [Add stackbar chart in FortiView 6.4.2 on page 126](#)
  - [Interface bandwidth widgets 6.4.2 on page 128](#)
  - [EMS classification tag 6.4.3 on page 130](#)

- [Throughput utilization billing reporting 6.4.3 on page 133](#)
- [Subnet list for reports 6.4.3 on page 135](#)
- [Cyber-Physical Security on page 143](#)
  - [Facial Recognition 6.4.1 on page 143](#)
  - [Zoom function in FortiRecorder 6.4.1 on page 149](#)

## SOC automation

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

List of new features:

- [Attach reports to incidents on page 34](#)
- [Automation Playbooks on page 38](#)
- [Add comments to incidents on page 45](#)
- [Expanded incident analysis page on page 47](#)
- [FortiSOC dashboards on page 51](#)
- [FortiOS Connector on page 52](#)
- [EMS Connector on page 56](#)
- [Normalized Fabric logs on page 62](#)
- [Incidents with multiple endpoints and users 6.4.2 on page 66](#)
- [Default playbook template improvements 6.4.1 on page 67](#)
- [Incident page improvement 6.4.1 on page 70](#)
- [Filters for local report action 6.4.2 on page 76](#)
- [SOC subscription license 6.4.1 on page 77](#)
- [Try it Out feature for FortiSoC 6.4.2 on page 79](#)
- [Vulnerabilities and software inventory data from EMS connector 6.4.2 on page 81](#)
- [FortiMail connector 6.4.2 on page 85](#)
- [Alerts on normalized logs 6.4.3 on page 88](#)
- [Normalized logs for reports 6.4.3 on page 91](#)
- [FortiGuard connector 6.4.3 on page 93](#)
- [Connector's health check 6.4.3 on page 96](#)
- [FortiGuard outbreak and alert service 6.4.6 on page 97](#)

## Attach reports to incidents

You can attach reports to incidents to add historical data in addition to real-time events through one of the following methods:

- Manually added by an admin after incident creation.
- Automatically added by SOC automation playbooks. SOC automation is a licensed feature.

Two views are available in the *Incident Analysis* page:

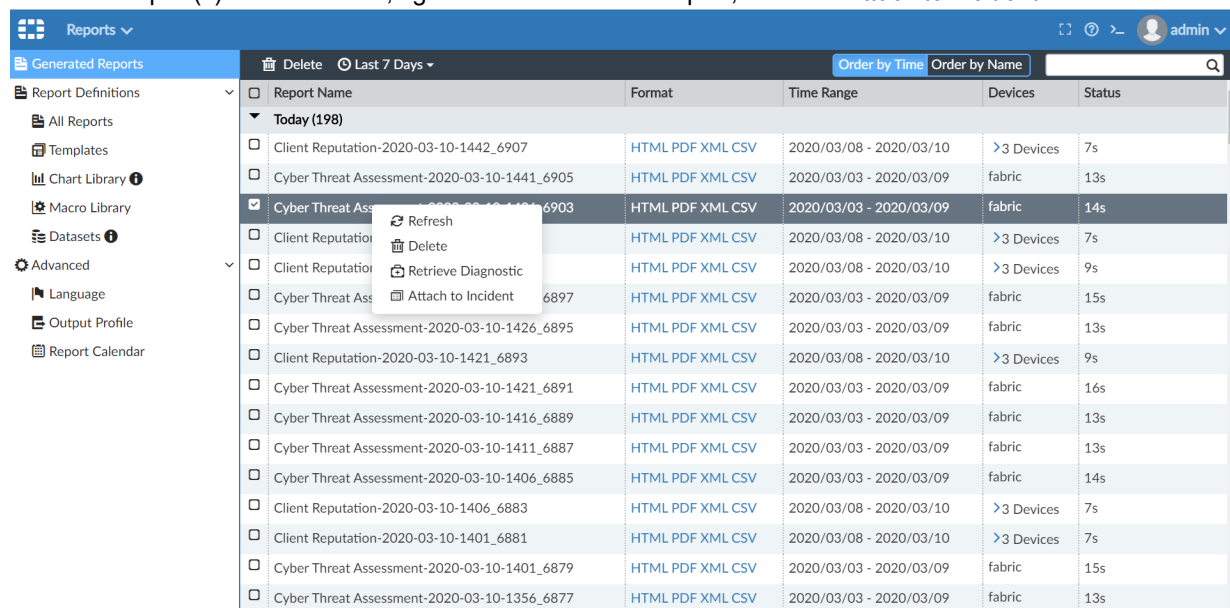
- Closed view showing attached reports.
- Open view showing the content of the report.



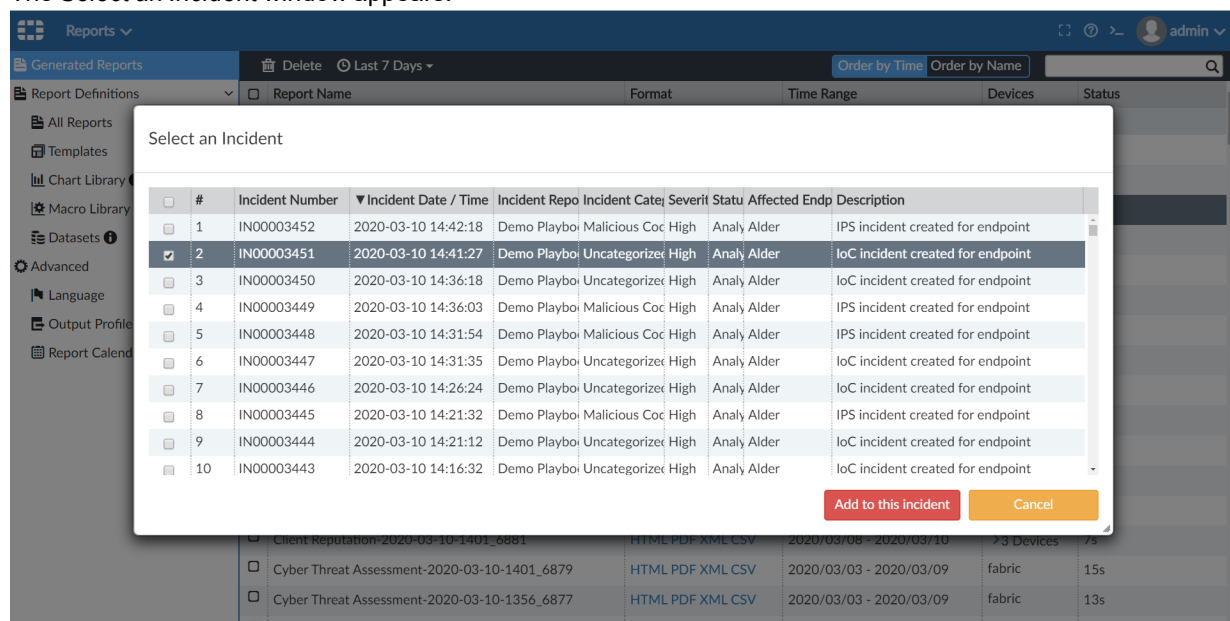
## To attach reports from Generated Reports:

### 1. Go to *Reports > Generated Reports*.

Select the report(s) to be attached, right-click on a selected report, and click *Attach to Incident*.



The *Select an Incident* window appears.



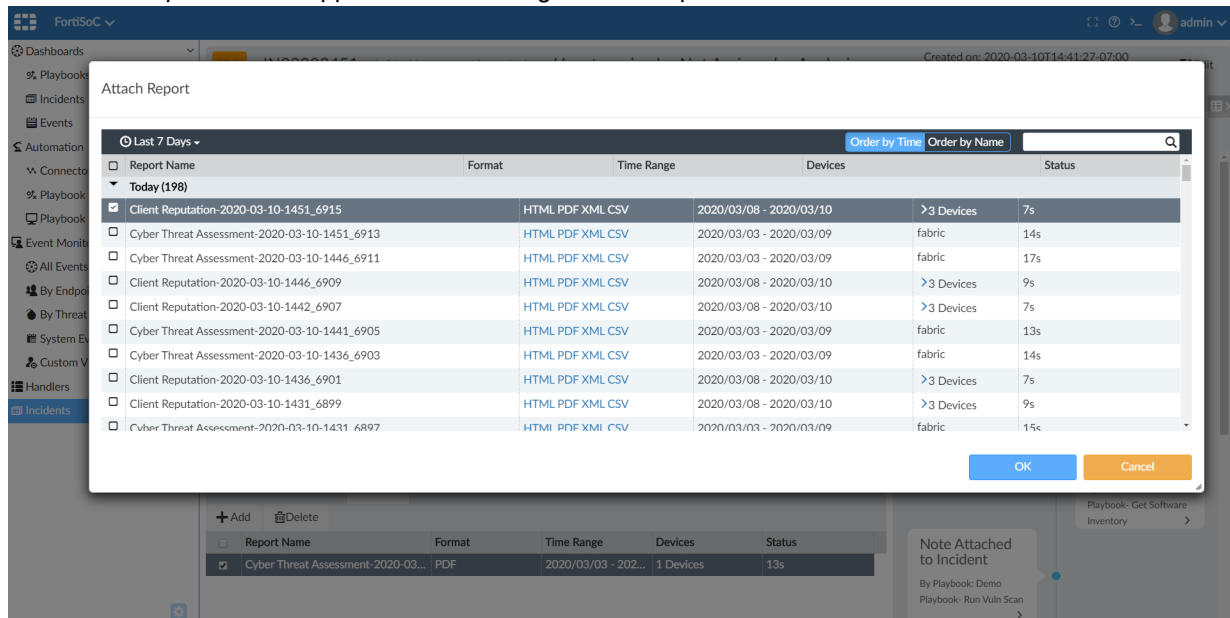
### 2. Select an incident and click *Add to this incident*.

## To attach reports from the Incident Analysis page:

- Go to *Incidents & Events/FortiSoC > Incidents* and double-click on an incident to view the Incident Analysis page.
- On the bottom of the page, click the *Report* tab.

3. Click **Add**.

The **Attach Report** window appears with a list of generated reports available for selection.

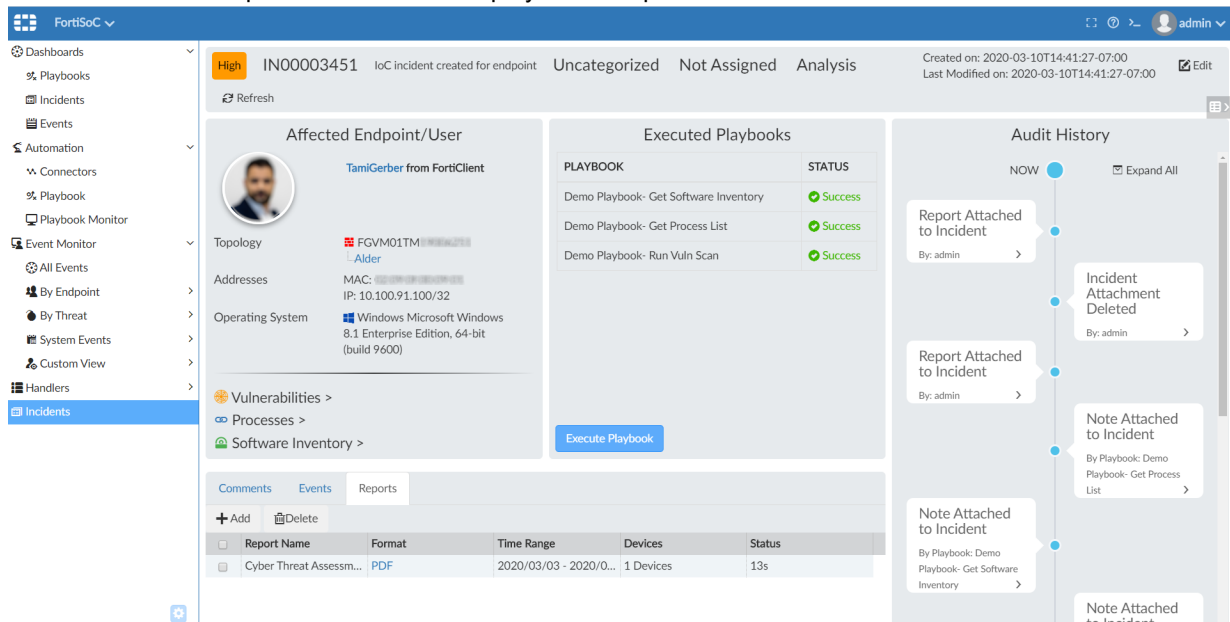
4. Select one or more reports and click **OK**.

The reports are added to incident as an attachment.

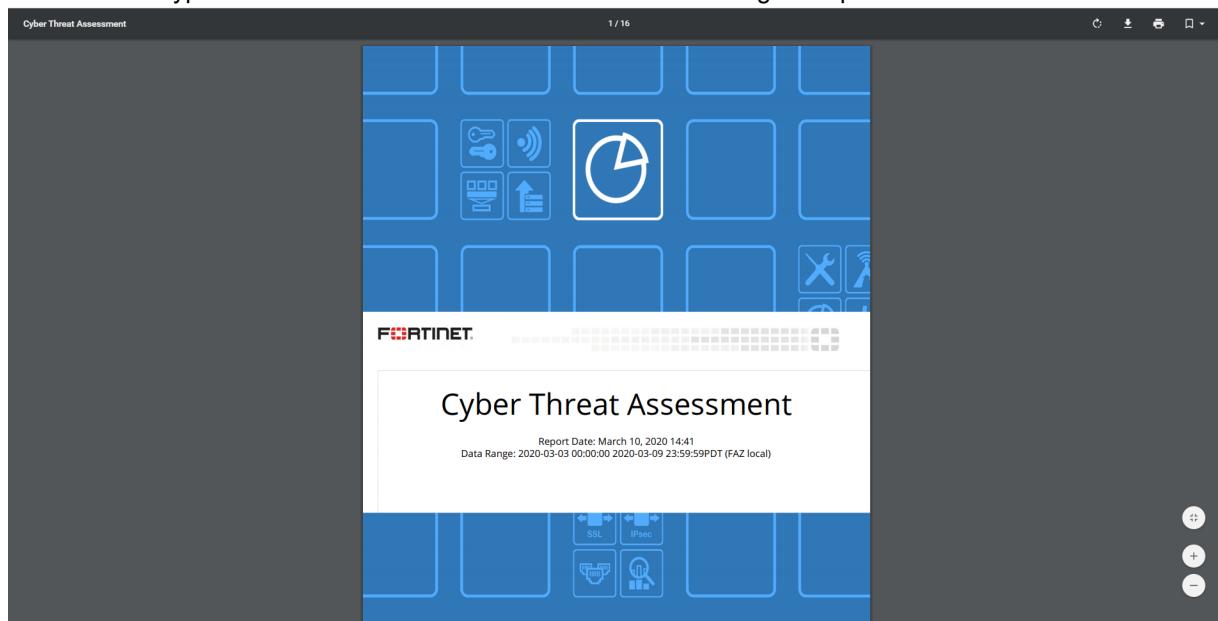
### To view reports in the Incident Analysis page:

1. In the Incident Analysis page, click the **Reports** tab.

The list of attached reports is shown and displays basic report information.

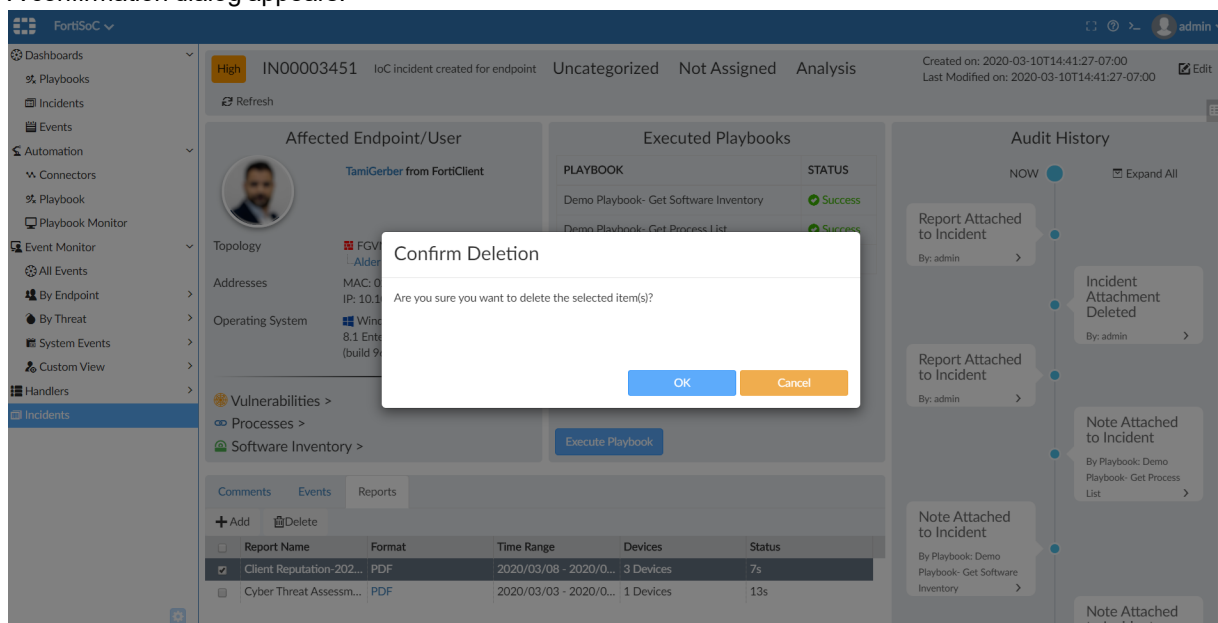


- Click a format type in the *Format* column to launch a new tab showing the report's content.



#### To delete reports from the Incident Analysis page:

- In the Incident Analysis page, click the *Reports* tab.
- Select the report(s) to be deleted, and click *Delete*.  
A confirmation dialog appears.



- Click OK.  
The selected reports are deleted from incident.

## Automation Playbooks

A sequence of one or more actions offered by SOC connectors can be defined in playbooks and executed manually or automatically.

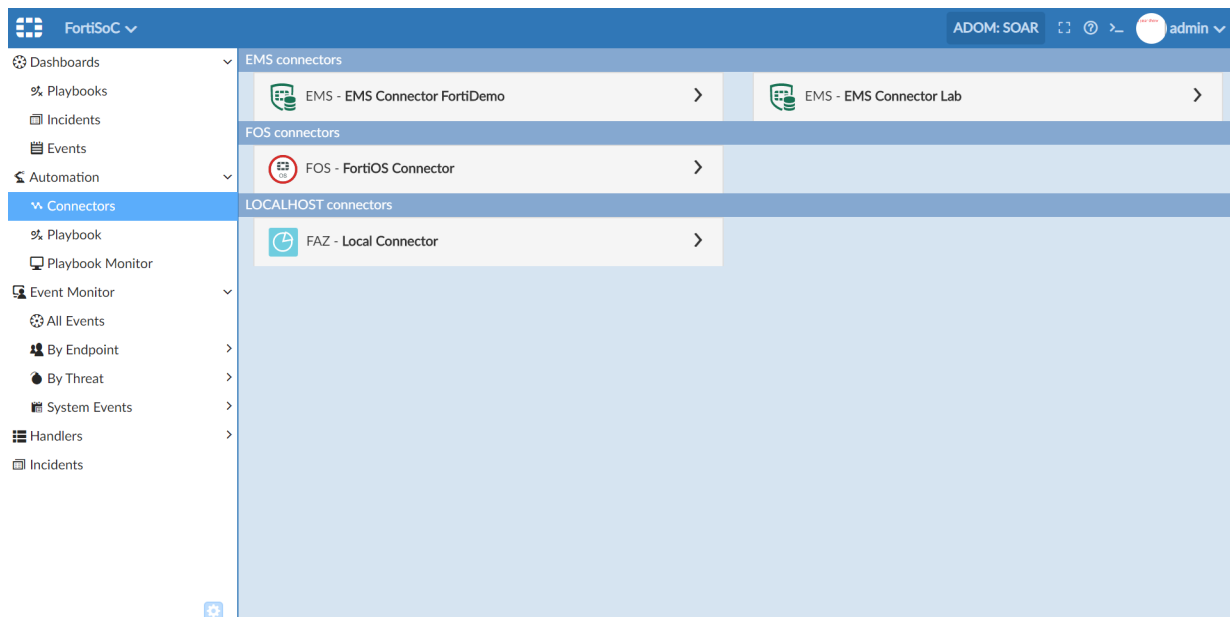
Playbooks consist of a trigger and multiple actions from configured connectors.

- Playbook triggers include:
  - Incident
  - Event
  - On Schedule
  - On Demand
- Playbook actions:
  - This is the automated action taken by the playbook at any step.
  - Actions can be configured with default input values or take inputs from the trigger or preceding actions.
  - Actions be selected from the local FortiAnalyzer or a configured connector's list of actions.

## Connectors

To view FortiSoC connectors:

1. View the connector list from *FortiSoC > Automation > Connectors*.



2. Click on a connector to view its details.  
The actions available with each connector are displayed, including the action name, and the action's parameters used in the playbook.

- EMS connectors:

The screenshot shows the FortiSoC interface with the 'Connectors' menu item selected. The main panel displays the 'EMS connectors' section. A table lists the following connectors:

Name	Description	Parameter	Status
AV Full Scan	run full av scan on endpoints	epid* or fctuid*	Enabled
AV Quick Scan	run quick av scan on endpoints	epid* or fctuid*	Enabled
Get Endpoints	retrieve list of endpoints and all of the related information to enrich fortianalyzer asset and identity views	epid fctuid	Enabled
Get Process List	retrieve list of running process on endpoints os	epid* or fctuid* start_timestamp limit offset	Enabled
Get Software Inventory	retrieve list of software and apps installed on endpoint to enrich fortianalyzer asset	epid* or fctuid*	Enabled

The right sidebar shows the 'EMS - EMS Connector Lab' section.

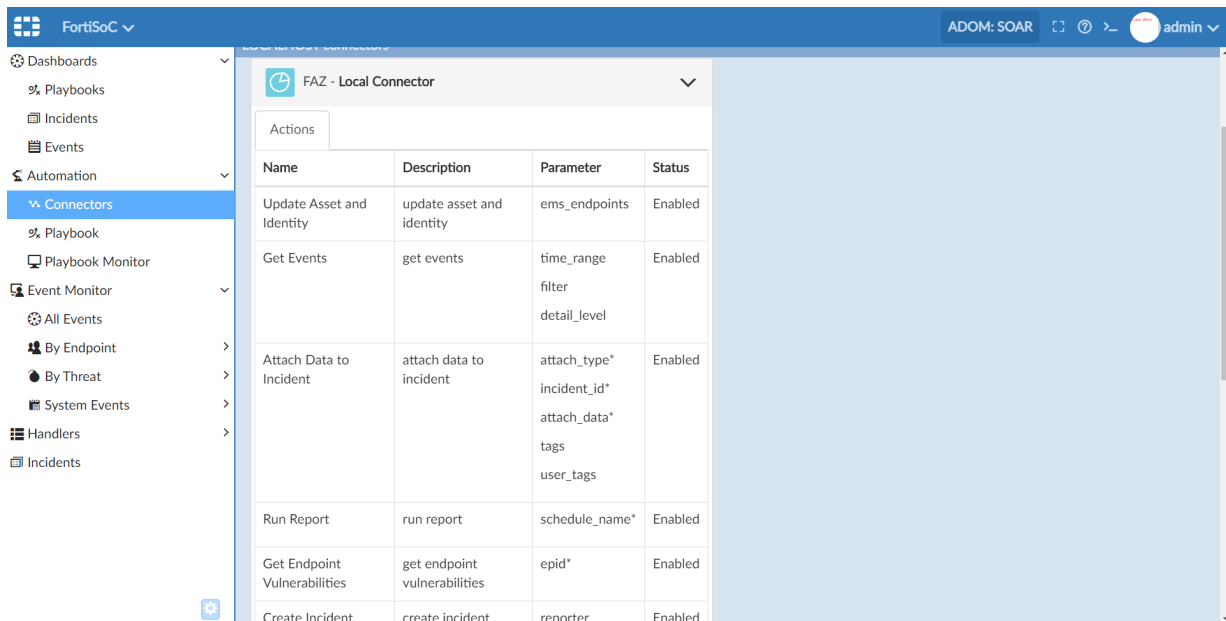
- FOS connectors:

The screenshot shows the FortiSoC interface with the 'Connectors' menu item selected. The main panel displays the 'FOS connectors' section. A table lists the following connectors:

Automation Rule	Automation Action(s)	Parameters
activate_strict_ips	activate_strict_ips	policyid
add_cnc_to_blacklist	add_cnc_to_blacklist	cncip

The right sidebar shows the 'FOS - FortiOS Connector' section. Below the table, there are two sections for 'FGVM04TM19002537' and 'FGVM02TM19002716', each containing the same table structure as above. The bottom section shows 'LOCALHOST connectors' with 'FAZ - Local Connector' listed.

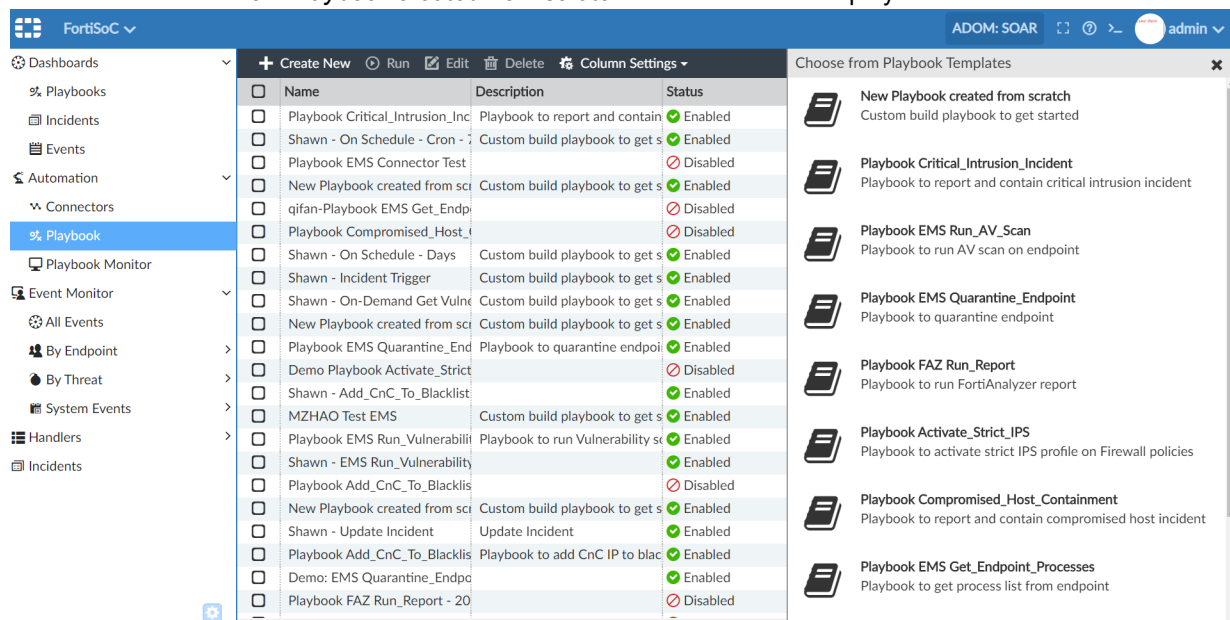
- Local connectors:



## Playbooks

### To create a playbook:

- Click **Create New** from the Playbook list, and select a template. You can also select **New Playbook created from scratch** to start with a blank playbook.



2. Provide a name and description for the playbook, and set it to *Enabled* if you want to use it immediately after saving the playbook.

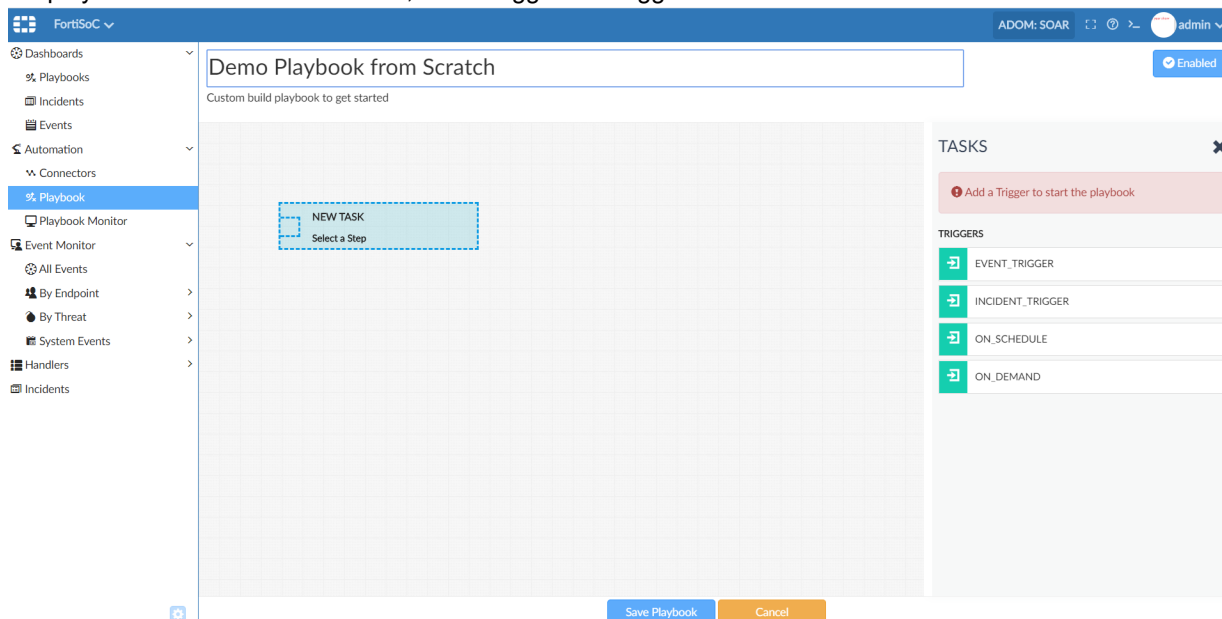
The screenshot shows the FortiSoC interface with the 'Automation' menu open and 'Playbook' selected. A new playbook is being created with the title 'Demo Critical\_Intrusion\_Incident' and the description 'Playbook to report and contain critical intrusion incident'. The status is set to 'Enabled'. The workflow diagram shows three tasks: 'EVENT\_TRIGGER STARTER', 'CREATE\_INCIDENT Create Incident', and 'VULN\_SCAN'. The 'EVENT\_TRIGGER STARTER' task is connected to both 'CREATE\_INCIDENT' and 'VULN\_SCAN'. The 'CREATE\_INCIDENT' task is also connected to 'VULN\_SCAN'. The 'VULN\_SCAN' task is connected to the 'EVENT\_TRIGGER STARTER' task. The interface includes a sidebar with navigation options like Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, Handlers, and Incidents. The top bar shows 'FortiSoC' and 'ADOM: SOAR'.

3. If a predefined template is selected, check each trigger and task configuration, and update them as need by clicking the edit icon.

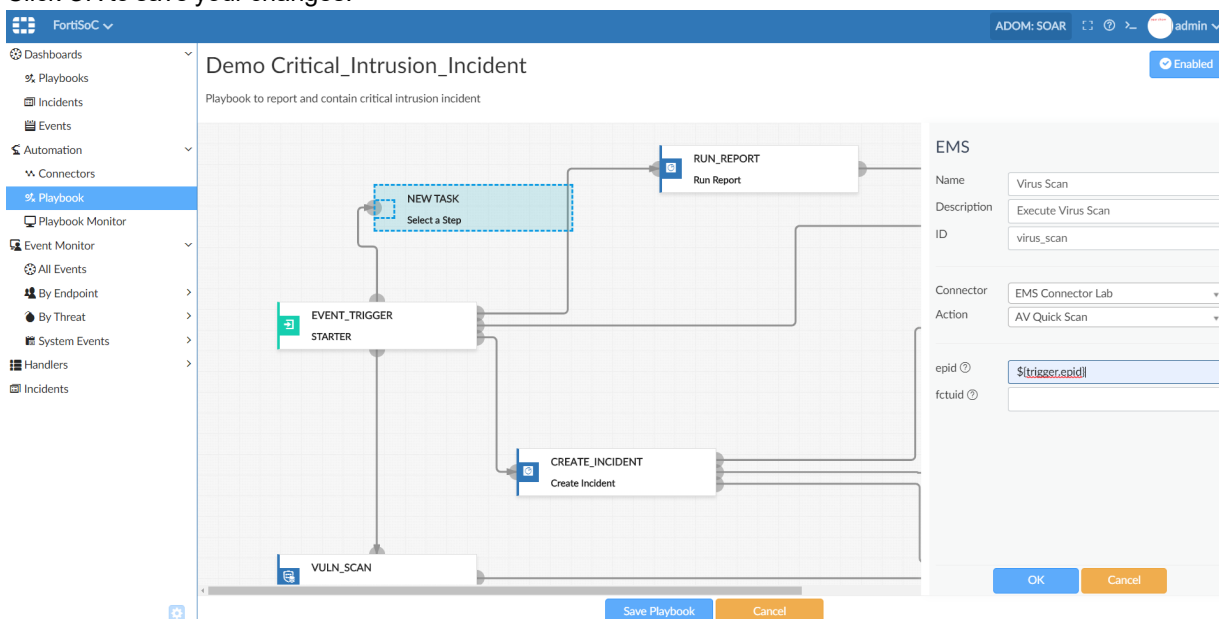
The screenshot shows the FortiSoC interface with the 'Automation' menu open and 'Playbook' selected. The 'Demo Critical\_Intrusion\_Incident' playbook is selected, and the 'EVENT\_TRIGGER STARTER' task is highlighted. The configuration panel on the right shows the task configuration. The task is named 'EVENT\_TRIGGER STARTER' and has two triggers: 'threat\_type' and 'severity'. The 'threat\_type' trigger is configured with 'Match Criteria' set to 'Equal To' and 'Value' set to 'ips'. The 'severity' trigger is configured with 'Match Criteria' set to 'Equal To' and 'Value' set to 'Critical'. The task is connected to the 'CREATE\_INCIDENT Create Incident' task and the 'VULN\_SCAN Run Vulnerability Scan on Endpoint' task. The interface includes a sidebar with navigation options like Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, Handlers, and Incidents. The top bar shows 'FortiSoC' and 'ADOM: SOAR'.

Field	Match Criteria	Value
threat_type	Equal To	ips
severity	Equal To	Critical

4. If a playbook is created from scratch, select trigger and trigger filter conditions.



5. Add a task by clicking the connector point of a parent task or trigger and dragging-and-dropping a new task onto the playbook.
- Select the *Connector* type.
  - Enter a name, description, and the ID for the task.
  - Select a connector and action, and enter the action's required parameters. The parameter may come from any parent task/trigger output or be a fixed value.
  - Click OK to save your changes.





## 6. Save the playbook once finished and the playbook will appear in the playbook list.

<input type="checkbox"/>	Name	Description	Status	Created Time	Modified Time
<input checked="" type="checkbox"/>	Demo Critical_Intrusion_Incident	Playbook to report and contain critical i	Enabled	Today at 3:27 PM	Today at 3:43 PM
<input type="checkbox"/>	New Playbook created from scratch - 2	Custom build playbook to get started	Enabled	Today at 3:01 PM	Today at 3:01 PM
<input type="checkbox"/>	New Playbook created from scratch - 2	Custom build playbook to get started	Enabled	Today at 2:03 PM	Today at 2:16 PM
<input type="checkbox"/>	Playbook Critical_Intrusion_Incident - 2	Playbook to report and contain critical i	Enabled	Today at 2:03 PM	Today at 2:03 PM
<input type="checkbox"/>	New Playbook created from scratch - 2	Custom build playbook to get started	Enabled	Today at 1:49 PM	Today at 1:49 PM
<input type="checkbox"/>	Playbook Critical_Intrusion_Incident - 2	Playbook to report and contain critical i	Enabled	Today at 12:14 PM	Today at 12:14 PM
<input type="checkbox"/>	MZHAAO Test EMS	Custom build playbook to get started	Enabled	Yesterday at 9:07 AM	Yesterday at 9:09 AM
<input type="checkbox"/>	Playbook Compromised_Host_Containment	Playbook to report and contain compro	Enabled	Last Wednesday at 12:42 PM	Last Wednesday at 12:42 PM
<input type="checkbox"/>	Playbook Compromised_Host_Containment	Playbook to report and contain compro	Enabled	Last Wednesday at 12:42 PM	Last Wednesday at 12:42 PM
<input type="checkbox"/>	Shawn - On schedule - Cron - evry Frid	Custom build playbook to get started	Enabled	Last Tuesday at 5:01 PM	Last Wednesday at 12:00 PM
<input type="checkbox"/>	Shawn - On Schedule - Cron - 7:00.11.1	Custom build playbook to get started	Enabled	Last Tuesday at 4:58 PM	Last Wednesday at 10:34 AM
<input type="checkbox"/>	Shawn - On Schedule - Days	Custom build playbook to get started	Enabled	Last Tuesday at 4:57 PM	Last Wednesday at 10:01 AM
<input type="checkbox"/>	Shawn - On Schedule - Hours	Custom build playbook to get started	Enabled	Last Tuesday at 4:47 PM	Last Wednesday at 10:01 AM
<input type="checkbox"/>	Shawn - On Schedule - minutes	Custom build playbook to get started	Enabled	Last Tuesday at 4:45 PM	Last Wednesday at 9:39 AM
<input type="checkbox"/>	Shawn - On Schedule - Seconds	Custom build playbook to get started	Enabled	Last Tuesday at 4:44 PM	Last Wednesday at 10:04 AM
<input type="checkbox"/>	New Playbook created from scratch - 2	Custom build playbook to get started	Enabled	Last Tuesday at 4:40 PM	Last Tuesday at 4:41 PM
<input type="checkbox"/>	Playbook EMS Run_Vulnerability_Scan	Playbook to run Vulnerability scan on e	Enabled	Last Tuesday at 4:25 PM	Last Tuesday at 4:25 PM
<input type="checkbox"/>	Mar-3 New Playbook created from scratch	Custom build playbook to get started	Enabled	Last Tuesday at 11:24 AM	Last Tuesday at 11:42 AM
<input type="checkbox"/>	Playbook EMS Run_Vulnerability_Scan	Playbook to run Vulnerability scan on e	Enabled	Last Monday at 10:44 AM	Last Monday at 10:44 AM
<input type="checkbox"/>	Playbook Add_CnC_To_Blacklist - 2020	Playbook to add CnC IP to blacklist on	Enabled	Last Monday at 10:44 AM	Last Monday at 10:44 AM
<input type="checkbox"/>	Playbook EMS Get_Endpoint_Processes	Playbook to get process list from endpc	Enabled	Last Monday at 10:43 AM	Last Monday at 10:43 AM
<input type="checkbox"/>	Playbook Compromised_Host_Containment	Playbook to report and contain compro	Enabled	Last Monday at 10:42 AM	Last Wednesday at 9:32 AM
<input type="checkbox"/>	Playbook Activate_Strict_IPS - 2020-03	Playbook to activate strict IPS profile or	Enabled	Last Monday at 10:42 AM	Last Monday at 10:42 AM
<input type="checkbox"/>	Playbook FAZ Run_Report - 2020-03-03	Playbook to run FortiAnalyzer report	Enabled	Last Monday at 10:41 AM	Last Monday at 10:41 AM
<input type="checkbox"/>	Playbook EMS Run_AV_Scan - 2020-03	Playbook to run AV scan on endpoint	Enabled	Last Monday at 10:40 AM	Last Monday at 10:40 AM
<input type="checkbox"/>	Playbook EMS Quarantine_Endpoint - 2	Playbook to quarantine endpoint	Enabled	Last Monday at 10:40 AM	Last Monday at 10:40 AM
<input type="checkbox"/>	Playbook EMS Quarantine_Endpoint - 2	Playbook to quarantine endpoint	Enabled	02/28/2020	02/28/2020
<input type="checkbox"/>	Shawn - Update Incident	Update Incident	Enabled	02/26/2020	02/26/2020

### To run an on-demand playbook:

1. Go to *FortiSoC > Automation > Playbooks*.
2. Select a playbook configured with an *On\_Demand* trigger.
3. Click *Run* in the toolbar or through the context menu of the selected playbook.

## 4. Input the desired parameters if prompted.

The top screenshot shows the FortiSoC interface with the Playbook list. A context menu is open over the 'Demo - EMS Quarantine\_Endpoint' row, showing options: Create New, Run, Edit, and Delete.

The bottom screenshot shows the FortiSoC interface with the 'Manually Run Playbook' dialog box open. The dialog displays the selected playbook 'Demo: EMS Quarantine\_Endpoint' and a list of endpoints to choose from. The selected endpoint is 'WIN7-SP1-USGCB (17173)'.

Name	Description	Status	Created Time	Modified Time
Demo Critical_Intrusion_Incident	Playbook to report and contain critical i	Enabled	Today at 3:27 PM	Today at 3:43 PM
Demo Playbook Activate_Strict_IPS		Disabled	02/13/2020	Today at 4:35 PM
Demo - EMS Quarantine_Endpoint		Enabled	02/13/2020	02/19/2020
Demo - FAZ Run_Report		Disabled	02/13/2020	02/13/2020
Demo - On Demand - EMS connector	Custom build playbook to get started	Enabled	02/14/2020	Today at 4:19 PM

Playbooks with an *Incident*, *Event*, or *On\_Schedule* trigger run automatically once the trigger's filter is matched.

## Playbook Monitor

### To view the Playbook Monitor:

1. Go to *FortiSoC > Automation > Playbook Monitor*.  
All playbook jobs that are running or have been run are displayed.

Job ID	Playbook	Started By	Started On	Ended On	Status
2020-03-06 16:34:01-08	Demo: EMS Quarantine_Endpoint		2020-03-06 16:34:01 -0800		Running
2020-03-06 16:31:01.402591-08	Shawn - Event - Critical_Intrusion_I		2020-03-06 16:31:01 -0800		Running
2020-03-06 16:31:01.369082-08	Demo Critical_Intrusion_Incident		2020-03-06 16:31:01 -0800		Running
2020-03-06 16:31:01.351865-08	Shawn - Event - Critical_Intrusion_I		2020-03-06 16:31:01 -0800		Running
2020-03-06 16:31:01.336097-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:31:01 -0800	2020-03-06 16:33:32 -0800	Failed
2020-03-06 16:31:01.317748-08	Demo Critical_Intrusion_Incident		2020-03-06 16:31:01 -0800		Running
2020-03-06 16:31:01.299048-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:31:01 -0800		Running
2020-03-06 16:31:01.277038-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:31:01 -0800	2020-03-06 16:33:32 -0800	Failed
2020-03-06 16:31:01.258213-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:31:01 -0800		Running
2020-03-06 16:31:01.237178-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:31:01 -0800		Running
2020-03-06 16:31:01.196981-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:31:01 -0800		Running
2020-03-06 16:20:33.527576-08	Shawn - On Schedule - Seconds		2020-03-06 16:30:57 -0800	2020-03-06 16:34:05 -0800	Success
2020-03-06 16:30:17.784103-08	Shawn - Event - Critical_Intrusion_I		2020-03-06 16:30:17 -0800		Running
2020-03-06 16:30:17.751177-08	Demo Critical_Intrusion_Incident		2020-03-06 16:30:17 -0800		Running
2020-03-06 16:30:17.751016-08	Shawn - Event - Critical_Intrusion_I		2020-03-06 16:30:17 -0800		Running
2020-03-06 16:30:17.717608-08	Demo Critical_Intrusion_Incident		2020-03-06 16:30:17 -0800		Running
2020-03-06 16:30:17.717697-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:30:17 -0800	2020-03-06 16:34:03 -0800	Failed
2020-03-06 16:30:17.685005-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:30:17 -0800	2020-03-06 16:34:03 -0800	Failed
2020-03-06 16:30:17.680101-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:30:17 -0800		Running
2020-03-06 16:30:17.652048-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:30:17 -0800		Running
2020-03-06 16:30:17.644339-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:30:17 -0800		Running
2020-03-06 16:30:17.62037-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:30:17 -0800		Running
2020-03-06 16:25:36.511726-08	Shawn - Event - Critical_Intrusion_I		2020-03-06 16:25:36 -0800	2020-03-06 16:29:39 -0800	Failed
2020-03-06 16:25:36.480822-08	Demo Critical_Intrusion_Incident		2020-03-06 16:25:36 -0800	2020-03-06 16:28:29 -0800	Failed
2020-03-06 16:25:36.45478-08	Shawn - Event - Critical_Intrusion_I		2020-03-06 16:25:36 -0800	2020-03-06 16:29:08 -0800	Failed
2020-03-06 16:25:36.449897-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:25:36 -0800	2020-03-06 16:27:48 -0800	Failed
2020-03-06 16:25:36.422202-08	Demo Critical_Intrusion_Incident		2020-03-06 16:25:36 -0800	2020-03-06 16:28:29 -0800	Failed
2020-03-06 16:25:36.419556-08	Playbook Critical_Intrusion_Incident		2020-03-06 16:25:36 -0800		Running

2. Double-click a job or click the details icon in the status column to view the playbook status details.

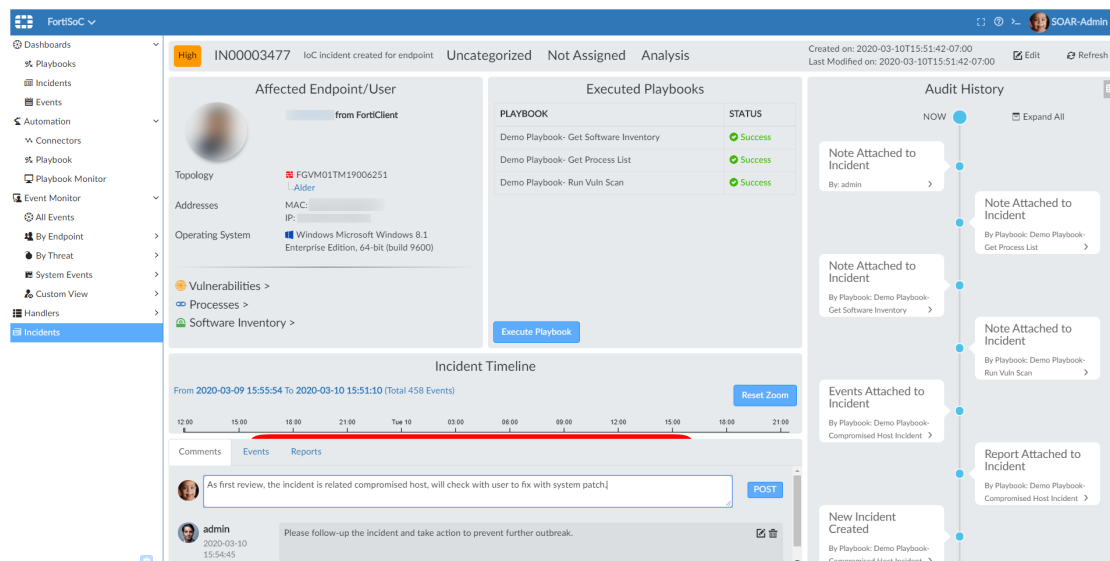
Task ID	Task	Started On	Ended On	Status
faz_attach_action_status_to_incident	Attach action status to incident			Scheduled
ems_quarantine_endpoint	Quarantine Endpoint			Scheduled

## Add comments to incidents

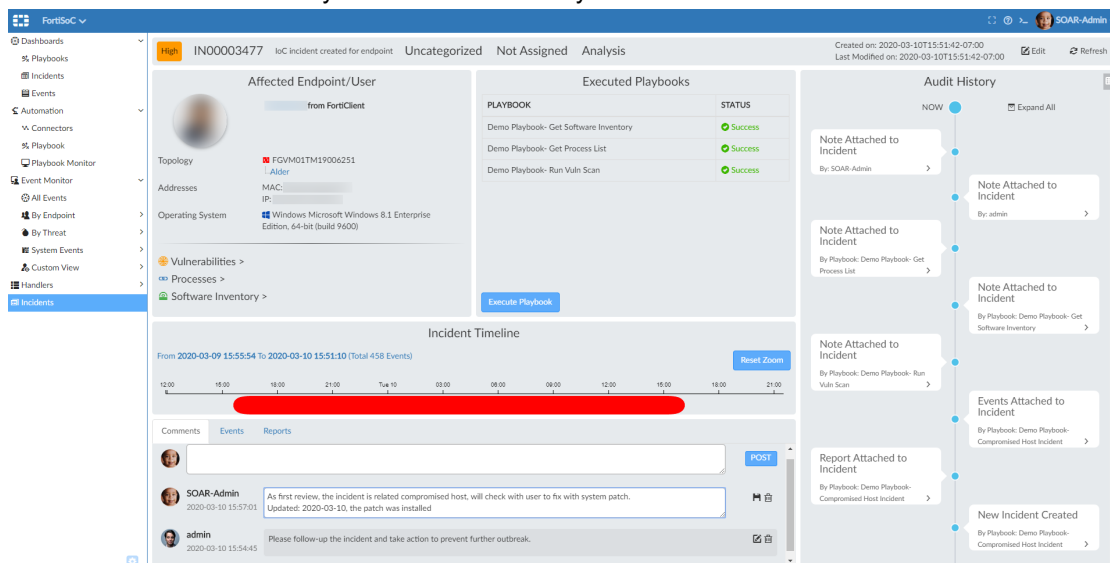
This feature introduces *Comments* to the *Incident Analysis* pane. It allows comments by admins with their names and timestamps displayed.

**To post a comment:**

1. Go to *FortiSoC*.
2. In the tree menu, select *Incidents*.  
The *Incidents* pane opens.

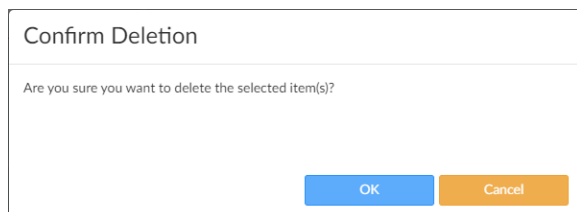


3. In the *Incidents* pane, enter your comment in the comment box under *Incident Timeline* and select *Post*. Comments show up next to admins who posted them, with the latest at the top.
4. Click on the *edit* icon next to your comment to modify it when needed.



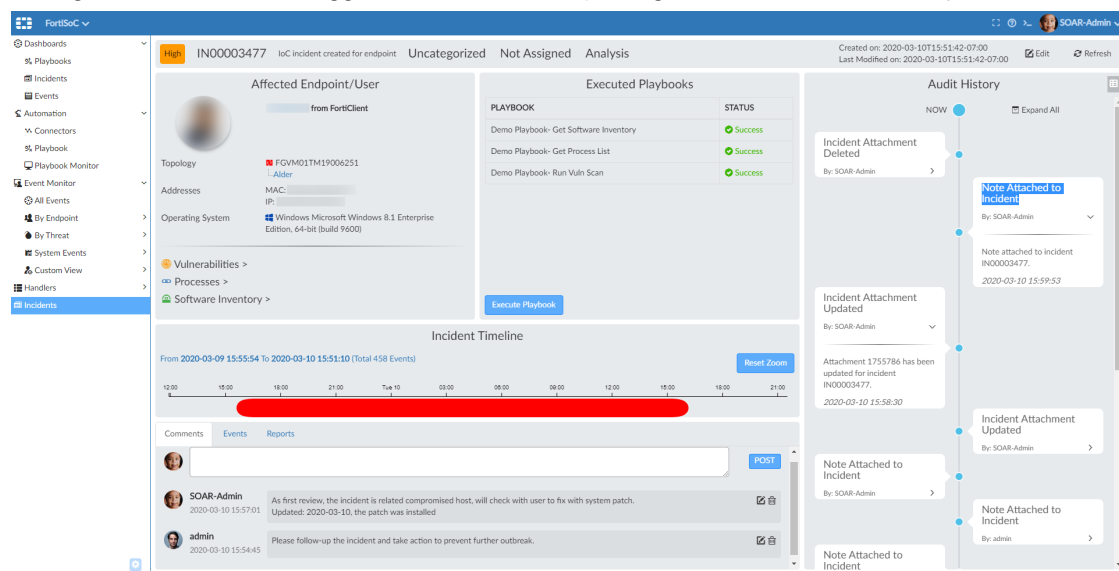
### To delete a comment:

1. Click on *delete* next to your comment to delete the comment. The *Confirmation Deletion* dialog opens.



From the *Confirmation Deletion* dialog box, click *OK* to delete your comment.

Changes in comments are logged in the *Audit History* on right, with the latest at the top.

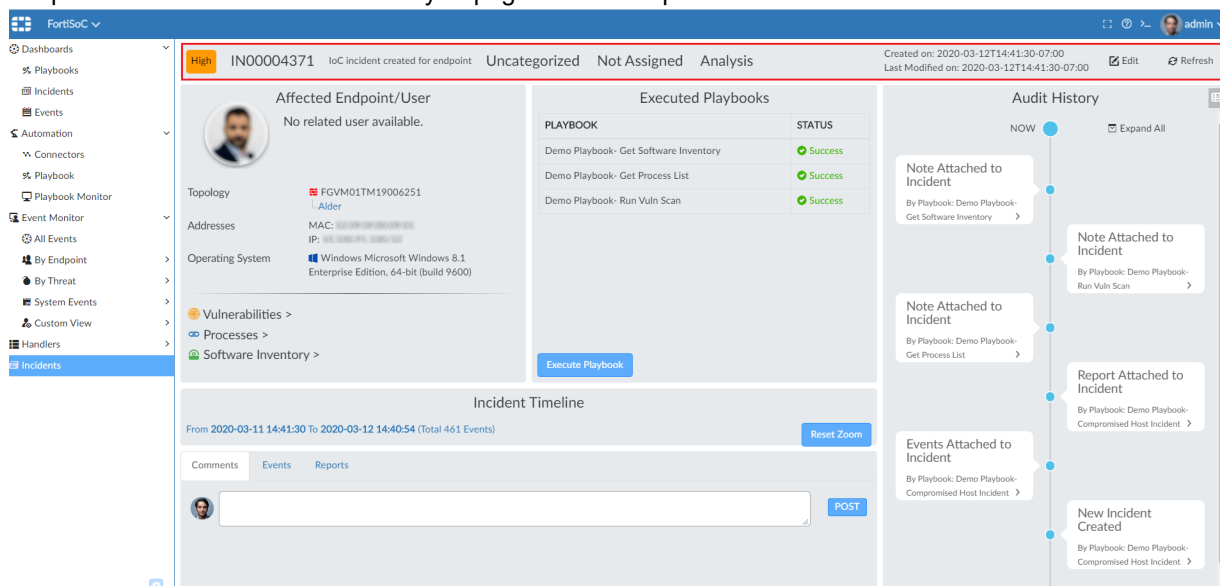


## Expanded incident analysis page

The incident analysis page has been expanded and redesigned to integrate with SOC playbooks and accommodate more evidence and notes for SOC analysis.

The expanded incident analysis page includes the following new and enhanced features:

- The incident headline bar provides basic information about the incident.
  - Basic information includes severity, incident number, incident description, category, assigned to, and incident create/modify time.
  - Click *Edit* to edit the incident information.
  - Click *Refresh* to update all incident information, including executed playbooks, audit history, and retrieved endpoint information. All incident analysis page content is updated.



- The incident analysis page provides more information about affected endpoints.

**FortiSoC** | High | IN00004371 | IoC incident created for endpoint | Uncategorized | Not Assigned | Analysis | Created on: 2020-03-12T14:41:30-07:00 | Last Modified on: 2020-03-12T14:41:30-07:00 | Edit | Refresh

**Affected Endpoint/User**  
No related user available.

Topology: FGVM01TM19006251 - Alder

Addresses: MAC: 00:0C:29:00:00:00, IP: 10.10.10.10

Operating System: Windows Microsoft Windows 8.1 Enterprise Edition, 64-bit (build 9600)

Vulnerabilities > | Processes > | Software Inventory >

**Executed Playbooks**

PLAYBOOK	STATUS
Demo Playbook- Get Software Inventory	Success
Demo Playbook- Get Process List	Success
Demo Playbook- Run Vuln Scan	Success

Execute Playbook

**Incident Timeline**  
From 2020-03-11 14:41:30 To 2020-03-12 14:40:54 (Total 461 Events) | Reset Zoom

Comments | Events | Reports

**Audit History**  
NOW | Expand All

- Note Attached to Incident (By Playbook: Demo Playbook- Get Software Inventory)
- Note Attached to Incident (By Playbook: Demo Playbook- Run Vuln Scan)
- Note Attached to Incident (By Playbook: Demo Playbook- Get Process List)
- Report Attached to Incident (By Playbook: Demo Playbook- Compromised Host Incident)
- Events Attached to Incident (By Playbook: Demo Playbook- Compromised Host Incident)
- New Incident Created (By Playbook: Demo Playbook- Compromised Host Incident)

- The incident analysis page provides automation (playbook) execution from within incidents.

**FortiSoC** | High | IN00004371 | IoC incident created for endpoint | Uncategorized | Not Assigned | Analysis | Created on: 2020-03-12T14:41:30-07:00 | Last Modified on: 2020-03-12T14:41:30-07:00 | Edit | Refresh

**Affected Endpoint/User**  
No related user available.

Topology: FGVM01TM19006251 - Alder

Addresses: MAC: 00:0C:29:00:00:00, IP: 10.10.10.10

Operating System: Windows Microsoft Windows 8.1 Enterprise Edition, 64-bit (build 9600)

Vulnerabilities > | Processes > | Software Inventory >

**Executed Playbooks**

PLAYBOOK	STATUS
Demo Playbook- Get Software Inventory	Success
Demo Playbook- Get Process List	Success
Demo Playbook- Run Vuln Scan	Success

Execute Playbook

**Incident Timeline**  
From 2020-03-11 14:41:30 To 2020-03-12 14:40:54 (Total 461 Events) | Reset Zoom

Comments | Events | Reports

**Audit History**  
NOW | Expand All

- Note Attached to Incident (By Playbook: Demo Playbook- Get Software Inventory)
- Note Attached to Incident (By Playbook: Demo Playbook- Run Vuln Scan)
- Note Attached to Incident (By Playbook: Demo Playbook- Get Process List)
- Report Attached to Incident (By Playbook: Demo Playbook- Compromised Host Incident)
- Events Attached to Incident (By Playbook: Demo Playbook- Compromised Host Incident)
- New Incident Created (By Playbook: Demo Playbook- Compromised Host Incident)

- Incident timelines show the timeline of events added to the incident.

The screenshot shows the FortiSoC interface for incident IN00004371. The incident is categorized as 'High' and 'Uncategorized'. The affected endpoint is FGVM01TM19006251, an Alder device running Windows Microsoft Windows 8.1 Enterprise Edition. The incident timeline shows a duration from 2020-03-11 14:41:30 to 2020-03-12 14:40:54. The audit history on the right shows a sequence of events: 'Note Attached to Incident', 'Note Attached to Incident', 'Note Attached to Incident', 'Report Attached to Incident', 'Events Attached to Incident', and 'New Incident Created'.

- Multiple incident attachments are supported and can be viewed from the attachment area.

- Comments

The screenshot shows the FortiSoC interface with the incident details for IN00004371. The comments section is highlighted with a red box, showing a comment from 'admin' dated 2020-03-12 14:57:23. The comment text is 'hi, please investigate the incident and follow-up for fix action.' The interface also shows the incident details and audit history.

## Events

**Incident Details:** IN00004371, IoC Incident created for endpoint, Uncategorized, Not Assigned, Analysis. Created on: 2020-03-12T14:41:30-07:00. Last Modified on: 2020-03-12T14:41:30-07:00.

**Affected Endpoint/User:** No related user available.

**Executed Playbooks:**

PLAYBOOK	STATUS
Demo Playbook- Get Software Inventory	Success
Demo Playbook- Get Process List	Success
Demo Playbook- Run Vuln Scan	Success

**Incident Timeline:** From 2020-03-11 14:41:30 To 2020-03-12 14:40:54 (Total 461 Events)

**Events Table:**

#	Event	Event Status	Event Type	Cou	Severity	First Occurrence	Last Update	Additional In Handler	Tags	Device Name
1	endpoint...	undefined	1	critical	2020-03-11 14:41:30	2020-03-11 14:41:30	[ "type": "...	Intrusion ...	Enterprise_FI...	Enterprise_FI...
2	Compromi...	undefined	2	critical	2020-03-11 14:45:56	2020-03-11 14:45:57	infected-d...	Compromi...	C&C ...	Enterprise_FI...
3	Compromi...	undefined	2	critical	2020-03-11 14:50:54	2020-03-11 14:50:56	infected-d...	Compromi...	C&C ...	Enterprise_C...
4	endpoint...	undefined	1	critical	2020-03-11 14:55:52	2020-03-11 14:55:52	[ "type": "...	Intrusion ...	Enterprise_FI...	Enterprise_FI...
5	Compromi...	undefined	2	critical	2020-03-11 14:55:53	2020-03-11 14:55:53	infected-d...	Compromi...	C&C ...	Enterprise_FI...

**Audit History:** Note Attached to Incident, Report Attached to Incident, Events Attached to Incident, New Incident Created.

## Reports

**Incident Details:** IN00004371, IoC Incident created for endpoint, Uncategorized, Not Assigned, Analysis. Created on: 2020-03-12T14:41:30-07:00. Last Modified on: 2020-03-12T14:41:30-07:00.

**Affected Endpoint/User:** No related user available.

**Executed Playbooks:**

PLAYBOOK	STATUS
Demo Playbook- Get Software Inventory	Success
Demo Playbook- Get Process List	Success
Demo Playbook- Run Vuln Scan	Success

**Incident Timeline:** From 2020-03-11 14:41:30 To 2020-03-12 14:40:54 (Total 461 Events)

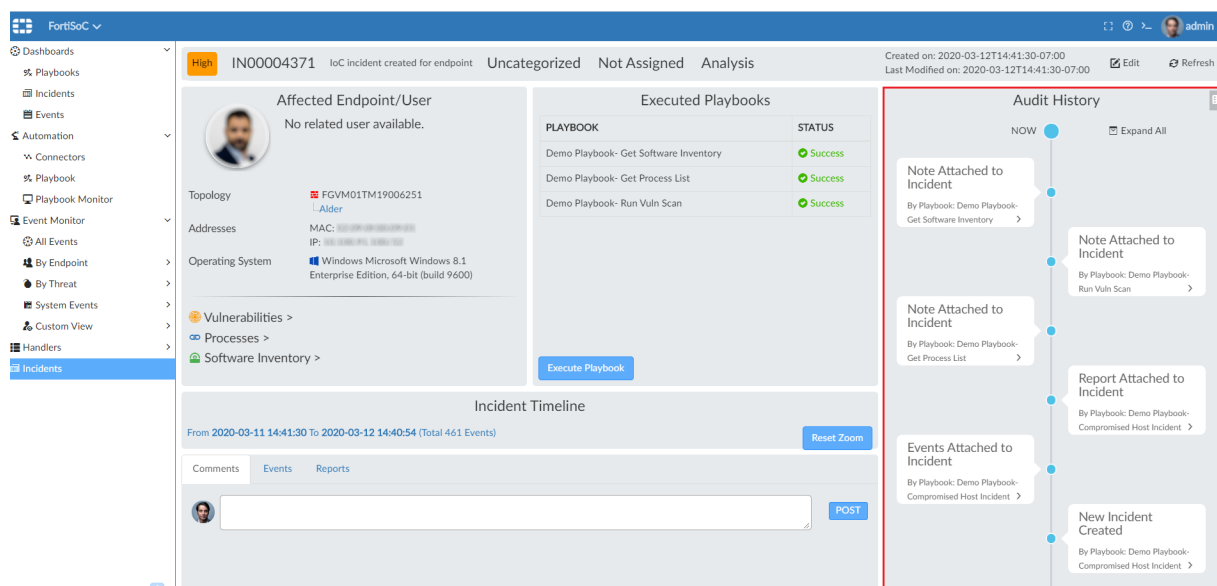
**Reports Table:**

Report Name	Format	Time Range	Devices	Status
Cyber Threat Assessment-2020-03-12-1441_8747	PDF	2020/03/05 - 2020/03/11	1 Devices	16s

**Audit History:** Note Attached to Incident, Report Attached to Incident, Events Attached to Incident, New Incident Created.

- Incident audit history shows the history of changes to the incident. Click the toggle icon in the top-right corner to hide/display the audit history panel.



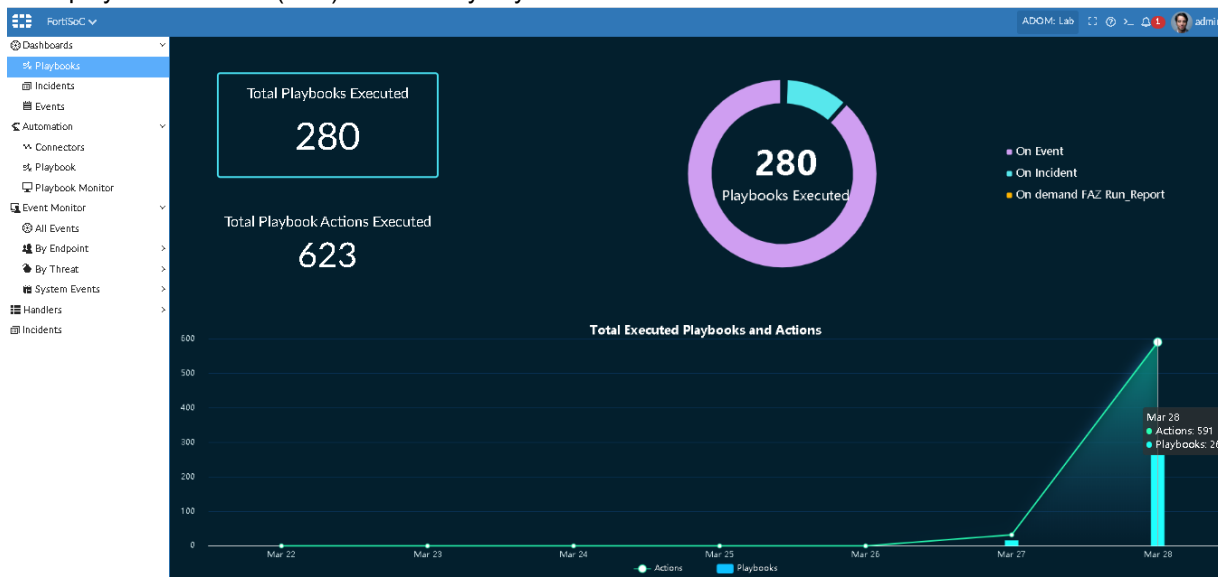


## FortiSOC dashboards

FortiSOC dashboards display events, incidents, and SOC playbook trends and breakdowns.

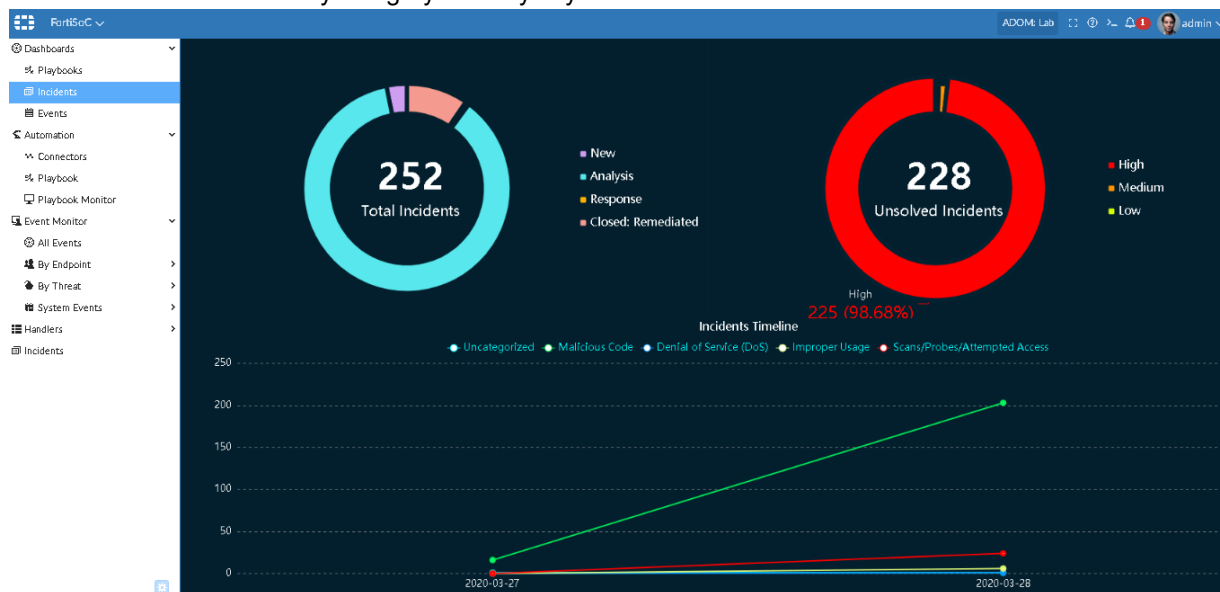
FortiSOC dashboards include the following:

- Playbook dashboard displays:
  - Total playbooks/actions (task) executed.
  - Total playbook executed by playbook.
  - Total playbooks/actions (task) executed by day trend.

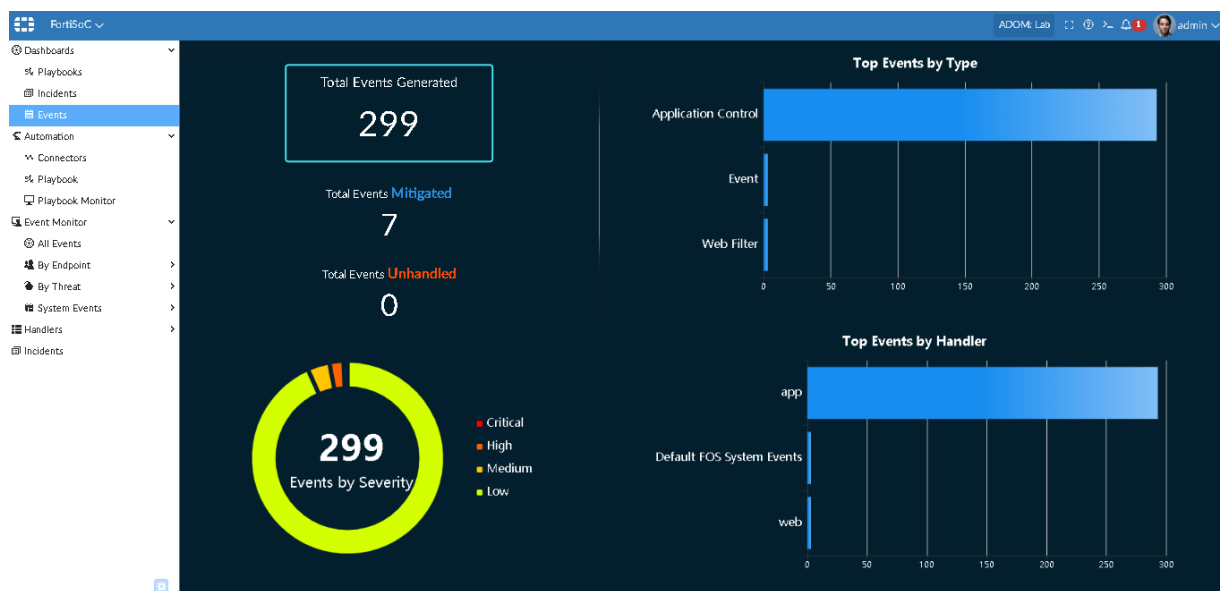


- Incident dashboard displays:
  - Total incidents by status.
  - Total unresolved (not closed) incidents by severity.

- Total incidents breakdown by category trend by day.



- Events dashboard displays:
  - Total events by *Generated/Mitigated/Unhandled*.
  - Total events by severity.
  - Total events breakdown by type.
  - Total events breakdown by event handler



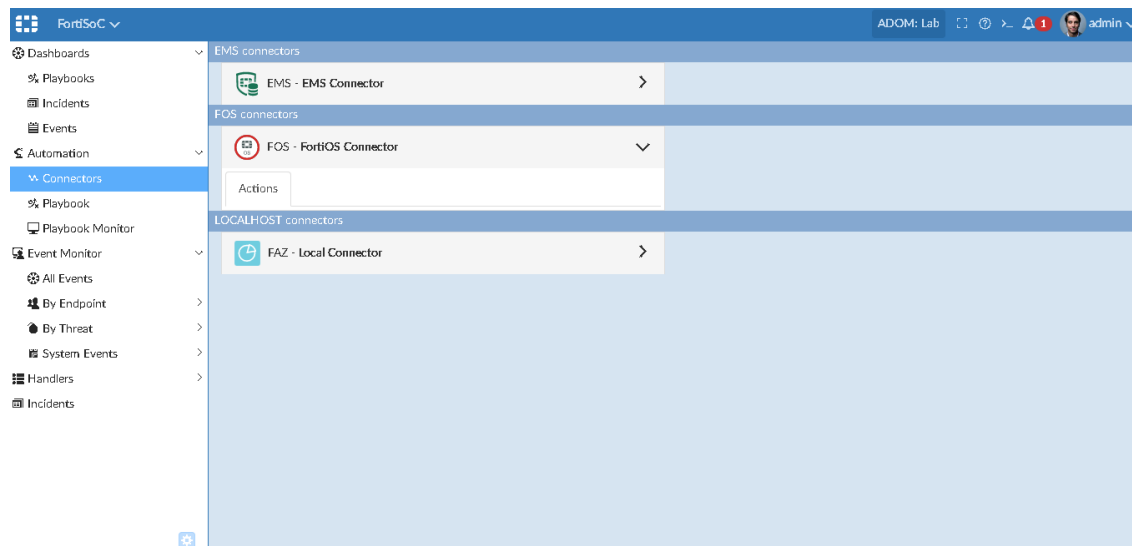
## FortiOS Connector

The FortiOS connector on FortiAnalyzer now allows SOC playbooks to use FortiOS automation rules as actions.

## To create a FortiSoC connector:

1. Go to *FortiSoC > Automation > Connectors*.

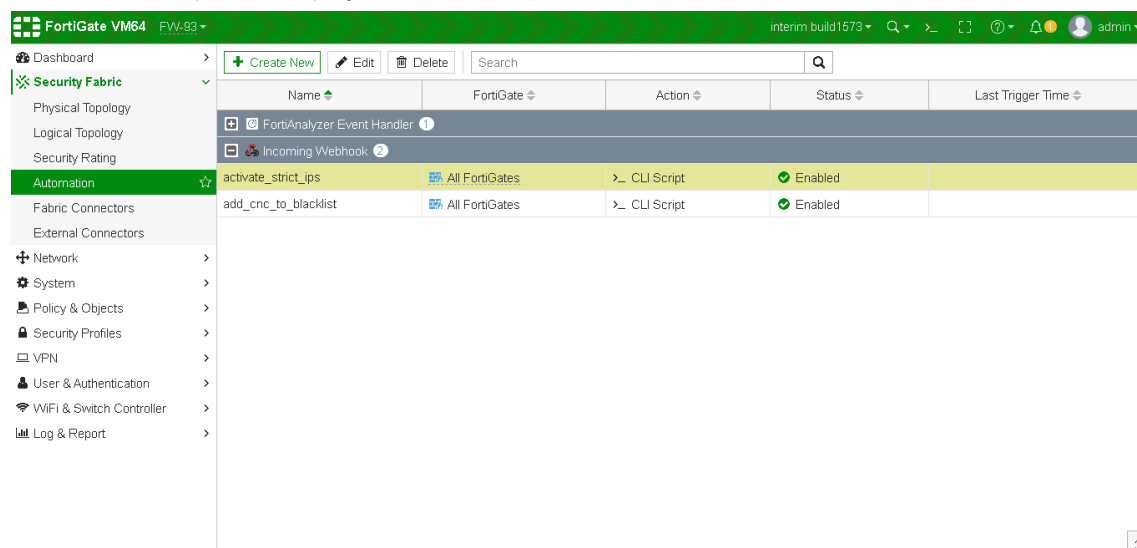
The *Connectors* pane opens.



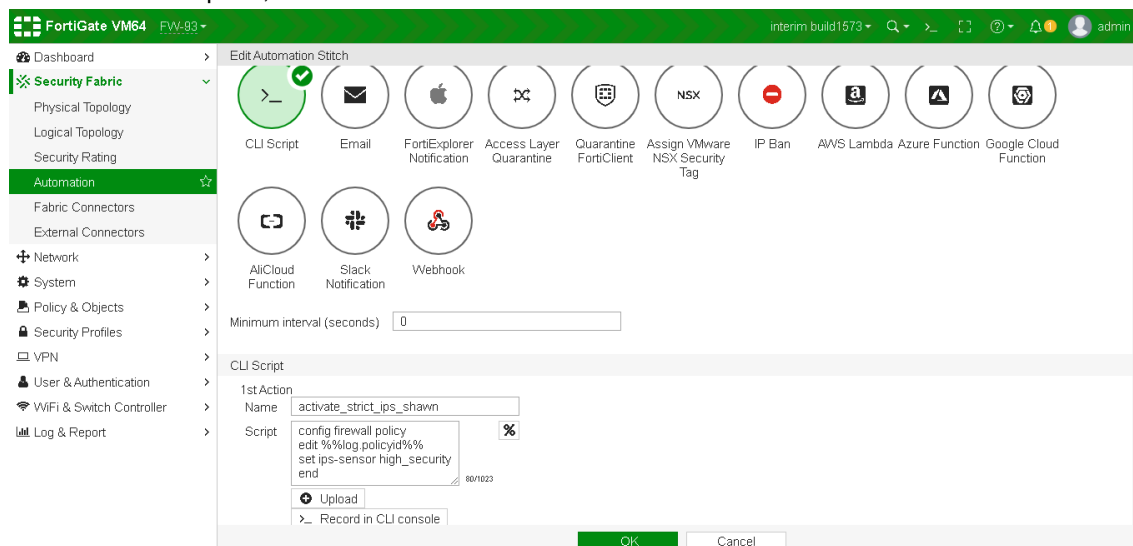
There are no FortiOS connectors available at this time. FortiOS connector is created once FortiAnalyzer has the first FortiGate prompted.

2. Go to *Security Fabric > Automation* to create an incoming webhook stitch on FortiGate.

The *Automation* pane is displayed.

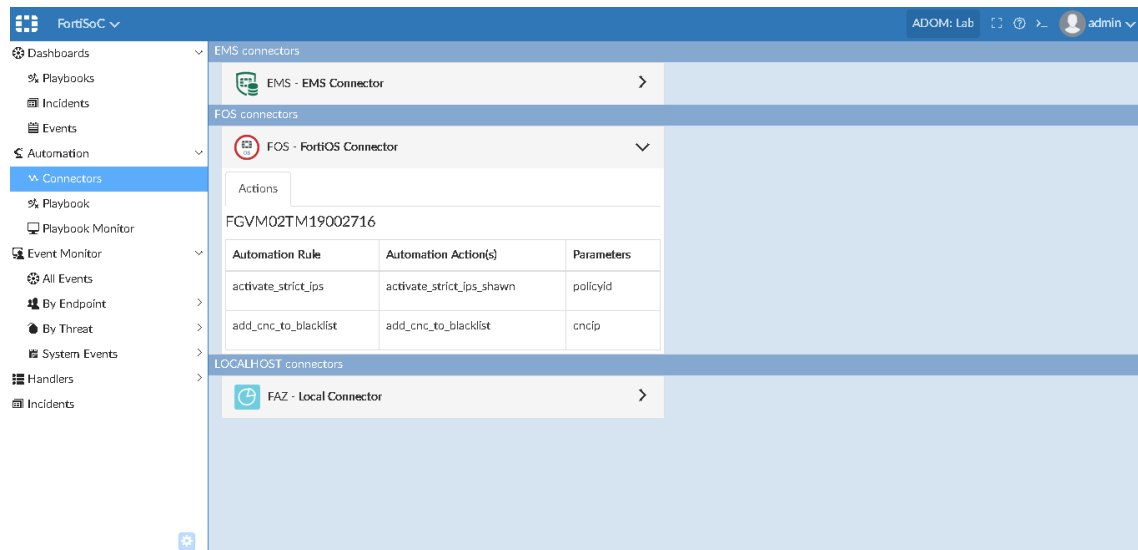


3. In the *Automation* pane, select *Edit* to edit automation stitch.



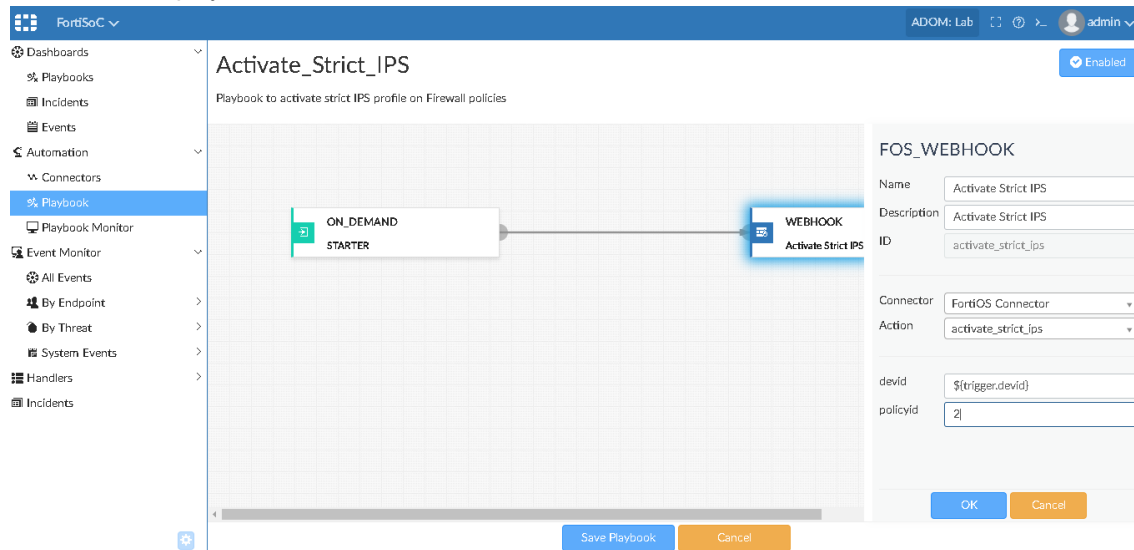
Click OK.

4. Now, go to *FortiSoC > Automation > Connectors*.  
You will see that the connector shows up in *FortiOS Connector*.



**To deploy FortiOS connector action:**

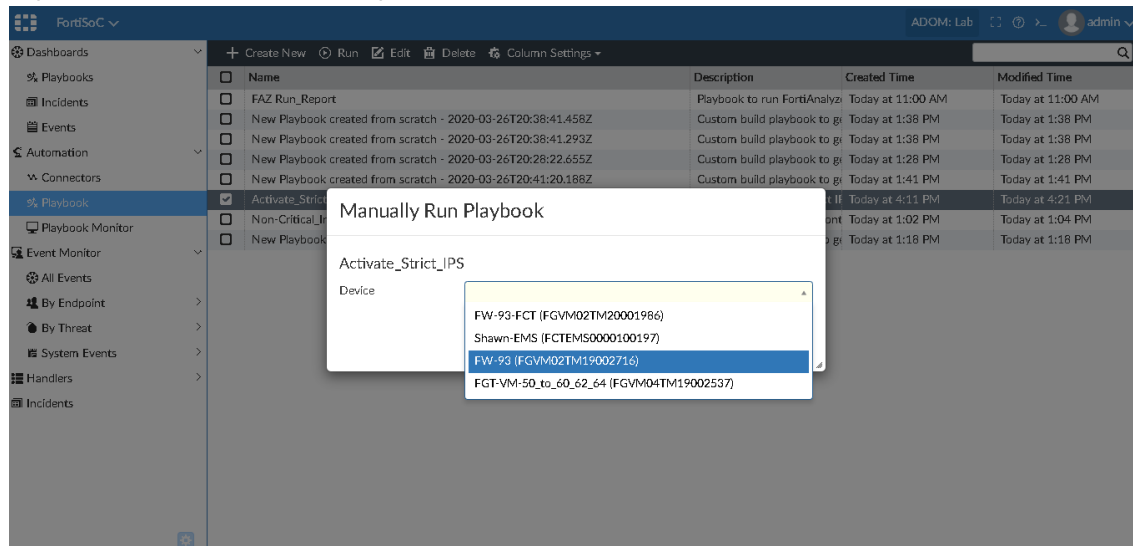
1. Go to *FortiSoC > Automation > Playbooks*.
2. Customize the playbook task to use FortiOS connector action.



Click *Save Playbook*.

**To run a playbook:**

1. Go to *FortiSoC > Automation > Playbooks*.
2. Select a playbook and click *Run* from the toolbar or right click on the playbook and select *Run* to automatically direct request to the FortiGate with the specified device.



CSF device request is handled by the CSF root and dispatched to the specified device.

FortiGate VM64 FW-93

interim build1573

admin

Dashboard

Security Fabric

Network

System

Policy & Objects

Firewall Policy

Authentication Rules

Create New

Edit

Delete

Policy Lookup

Search

Interface Pair View

By Sequence

To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
lab (tunnel-184)	all	all	always	ALL	ACCEPT	Disabled	ssl no-inspection	All	0 B
93-Rack (port2)	all	all	always	ALL	ACCEPT	Disabled	ssl no-inspection	All	191.32 GB
rt1	all	all	always	ALL	ACCEPT	Disabled	ssl no-inspection	All	63.72 GB
rt1	all	93-lab	always	ALL	ACCEPT	Disabled	ssl no-inspection	All	0 B

FortiGate VM64 FW-93

interim build1573

admin

Dashboard

Security Fabric

Network

System

Policy & Objects

Firewall Policy

Authentication Rules

IPv4 DoS Policy

Create New

Edit

Delete

Policy Lookup

Search

Interface Pair View

By Sequence

To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
toLab (tunnel-184)	all	all	always	ALL	ACCEPT	Disabled	ssl no-inspection	All	0 B
Lab-Rack (port2)	all	all	always	ALL	ACCEPT	Disabled	IPS strict ssl certificate-inspection	All	191.33 GB
2)	port1	all	always	ALL	ACCEPT	Disabled	ssl no-inspection	All	63.72 GB
84)	port1	all	always	ALL	ACCEPT	Disabled	ssl no-inspection	All	0 B

## EMS Connector

EMS connector on FortiAnalyzer allows automation playbooks to reach out to endpoints and collect information or take containment actions.

### To configure an EMS connector for use in FortiSoC playbooks:

- Configure a FortiClient EMS 6.4.0 server which supports the FortiAnalyzer EMS connector feature.

FortiClient Endpoint Management Server

Dashboard

FortiClient Status

Vulnerability Scan

Endpoints

Quarantine Management

Software Inventory

Endpoint Policy

Endpoint Profiles

Manage Installers

Policy Components

Telemetry Server Lists

Compliance Verification

Administration

System Settings

0

Vulnerable Endpoints

1

Infected Endpoints

2

Web Filter Detections

0

Sandbox Detections

0

Quarantine

System Information

License Information

Endpoint Connection

Endpoint Management

Hostname

Version

Database

System Time

Uptime

DESKTOP-21354PH

6.4.0 build 8247 (Interim)

Backup Restore

2020-04-14 02:52:14 PM

11:22:21:57

Serial Number

FortiCloud Account

Fabric Agent with Endpoint Protection

Sandbox Cloud

FortiClient Licenses Used

Chromebook

Chromebook Licenses Used

FCTEMS1975003231

Add

Expiring 2020-05-22

Expiring 2020-05-26

2 out of 300

Expiring 2020-05-28

0 out of 400

2

Total

2

Online

2

Total

2

Managed

2. Register FortiClient to the EMS server. In the example below, two FortiClients have been registered.

The screenshot shows the FortiClient Endpoint Management Server dashboard. The top bar indicates the status of endpoints: 0 Not Installed, 0 Not Registered, 0 Out-Of-Sync, and 1 Security Risk. The main table lists two endpoints:

Endpoint Name	User	IP Address	Policy	Status
DESKTOP-6FPNHJ7	jyang	172.18.32.73	Policy Default	EMS
DESKTOP-IE1AT7U	jyang	172.18.32.72	Policy Default	EMS

3. In FortiClient EMS *System Settings*, configure FortiClient EMS to send logs to FortiAnalyzer.

The screenshot shows the FortiClient EMS System Settings page. The 'Log' section is expanded, showing the following configuration:

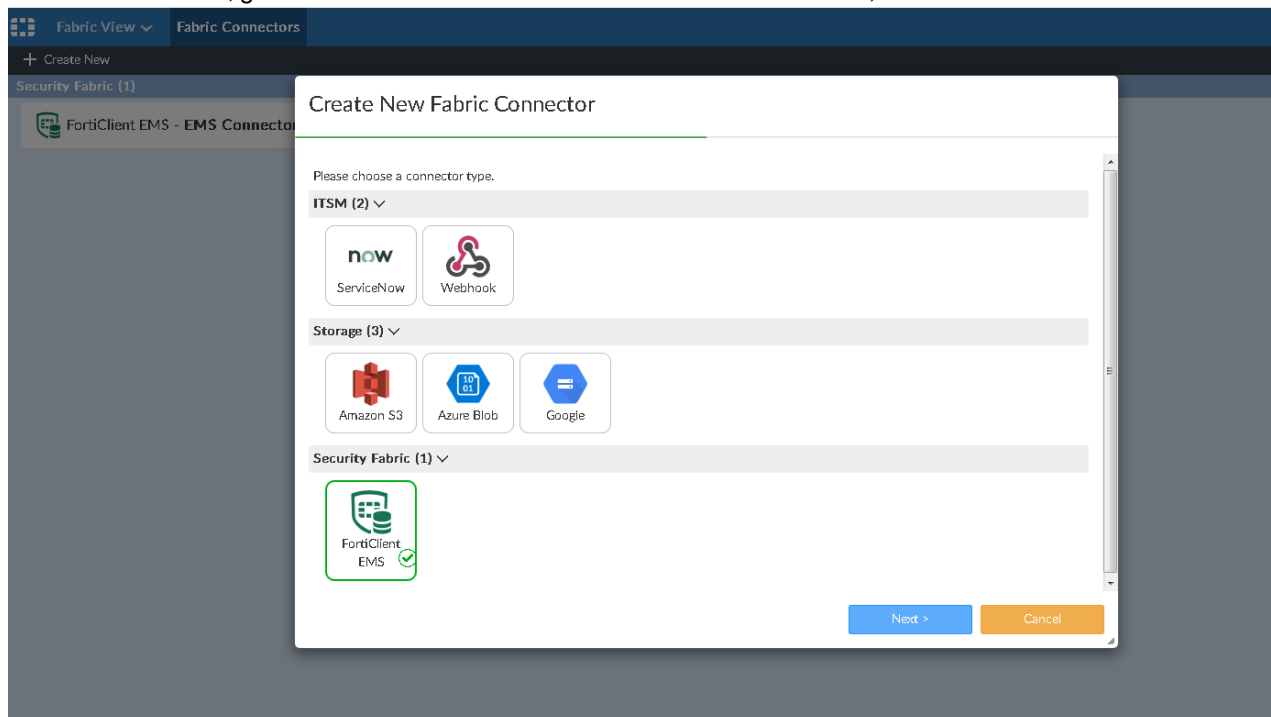
- ☒ Client-Based Logging When On-Net
- ☒ Upload Logs to FortiAnalyzer/FortiManager
- ☒ Upload UTM Logs
- ☒ Upload Vulnerability Logs
- ☒ Upload Event Logs
- IP Address/Hostname: 172.18.32.27
- Upload Schedule: 6 minutes
- Log Generation Timeout: 60 seconds

4. In FortiAnalyzer, register the EMS device to a Fabric ADOM.

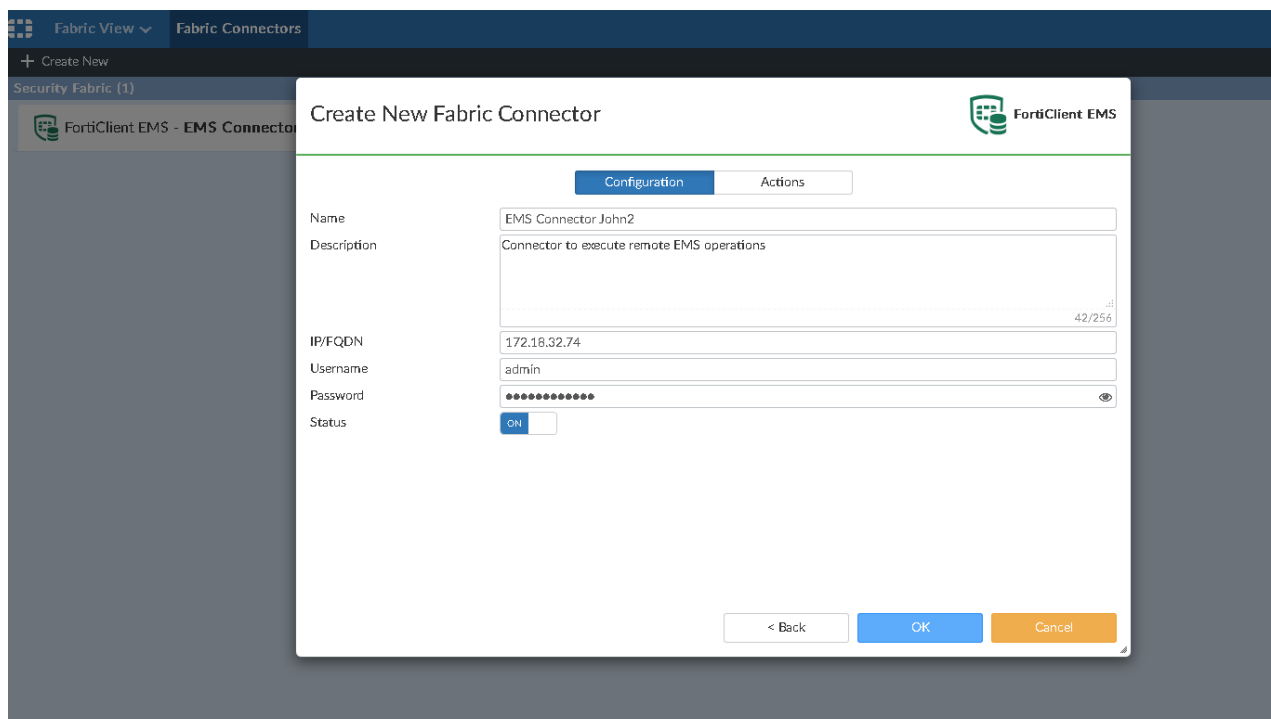
The screenshot shows the FortiAnalyzer Device Manager. The top bar indicates 1 Devices Total and 0 Devices Log Status Down. The table below lists the registered device:

Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	HA Status
FCTEMS1975003231	0.0.0.0	FortiClient-EMS	Real Time	N/A	(0.01%)	N/A

5. In the Fabric ADOM, go to *Fabric View > Fabric Connectors*. Click *Create New*, and select *FortiClient EMS*.



Configure the EMS connector, and click **OK**.



6. Go to *FortiSoC > Automation > Connectors*. Here you can view the actions FortiAnalyzer can take on endpoints using the EMS connector.



FortiSoC

Dashboards

Playbooks

Incidents

Events

Automation

Connectors

Playbook

Playbook Monitor

Event Monitor

All Events

By Endpoint

By Threat

System Events

Handlers

Incidents

EMS connectors

EMS - EMS Connector John

Actions

Name	Description	Parameter	Output
AV Full Scan	run full av scan on endpoints	Endpoint ID (epid)* or FortiClient ID (ctuid)*	N/A
AV Quick Scan	run quick av scan on endpoints	Endpoint ID (epid)* or FortiClient ID (ctuid)*	N/A
Get Endpoints	retrieve list of endpoints and all of the related information to enrich fortianalyzer asset and identity views	Endpoint ID (epid) FortiClient ID (ctuid)	ems_endpoints
Get Process List	retrieve list of running process on endpoints os	Endpoint ID (epid)* or FortiClient ID (ctuid)*	processes
Get Software Inventory	retrieve list of software and apps installed on endpoint to enrich fortianalyzer asset view	Endpoint ID (epid)* or FortiClient ID (ctuid)*	softwares
Quarantine	quarantines endpoints	Endpoint ID (epid)* or FortiClient ID (ctuid)*	N/A
Unquarantine	unquarantines endpoints	Endpoint ID (epid)* or FortiClient ID (ctuid)*	N/A
Vulnerability Scan	run vulnerability scan on endpoints	Endpoint ID (epid)* or FortiClient ID (ctuid)*	N/A

FOS connectors

FOS - FortiOS Connector

LOCALHOST connectors

FAZ - Local Connector

Playbook EMS connector examples

Below are two examples of how the FortiClient EMS connector enables actions in FortiSoC playbooks:

## To create a playbook from a template:

1. Go to *FortiSoC > Automation > Playbook*, and click *Create New*.

FortiSoC v

ADOM: Fab\_FCT\_only

+ Create New Run Edit Delete Column Settings

Name	Description	Status
No record found.		

Choose from Playbook Templates

- New Playbook created from scratch  
Custom build playbook to get started
- Playbook Critical\_Intrusion\_Incident  
Playbook to report and contain critical intrusion incident
- Playbook EMS Run\_AV\_Scan  
Playbook to run AV scan on endpoint
- Playbook EMS Quarantine\_Endpoint  
Playbook to quarantine endpoint
- Playbook FAZ Run\_Report  
Playbook to run FortiAnalyzer report
- Playbook Activate\_Strict\_IPS  
Playbook to activate strict IPS profile on Firewall policies
- Playbook Compromised\_Host\_Containment  
Playbook to report and contain compromised host incident
- Playbook EMS Get\_Endpoint\_Proc...  
Playbook to get process list from endpoint
- Playbook Add\_CnC\_To\_Blacklist  
Playbook to add CnC IP to blacklist on edge Firewalls
- Playbook EMS Run\_Vulnerability\_Scan  
Playbook to run Vulnerability scan on endpoint

2. From the list of templates, select *Playbook EMS Run\_Vulnerability\_Scan*.  
This template will run a vulnerability scan on an endpoint. Save the playbook.

FortiSoC v

ADOM: Fab

Playbook EMS Run\_Vulnerability\_Scan - 2020-04-14T22:10:50.011Z

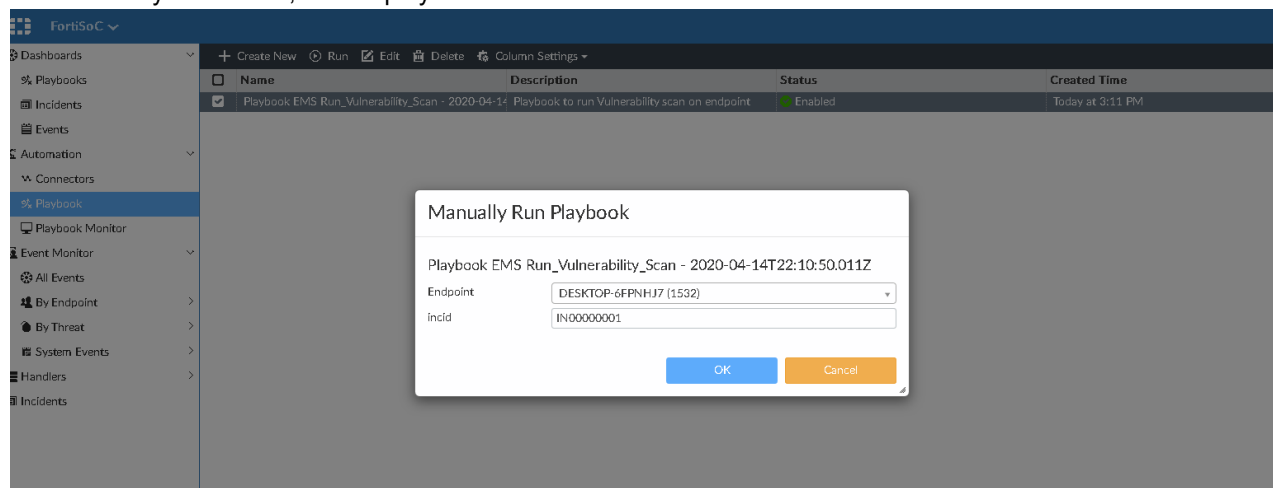
Playbook to run Vulnerability scan on endpoint

ON\_DEMAND STARTER

VULN\_SCAN  
Run Vulnerability Scan on E...

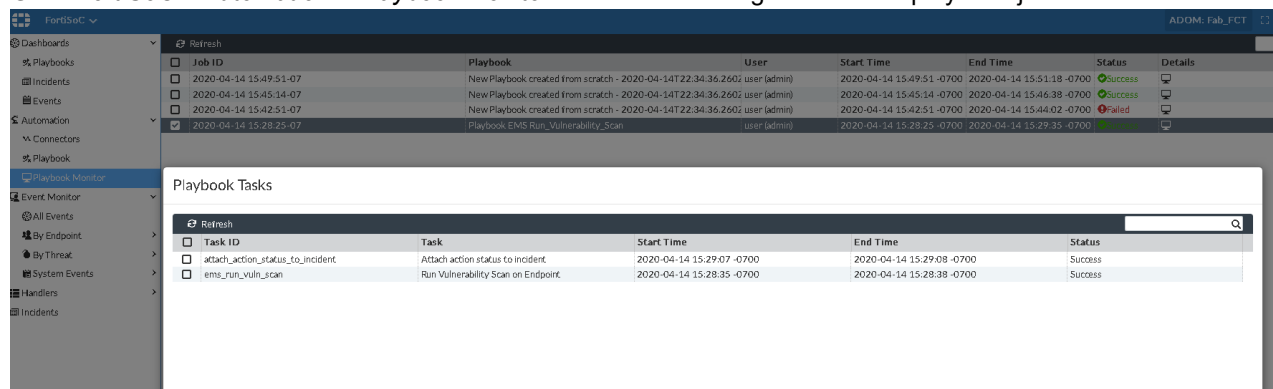
ATTACH\_DATA\_TO\_INCIDENT  
Attach action status to incid...

### 3. From the Playbook menu, run the playbook.



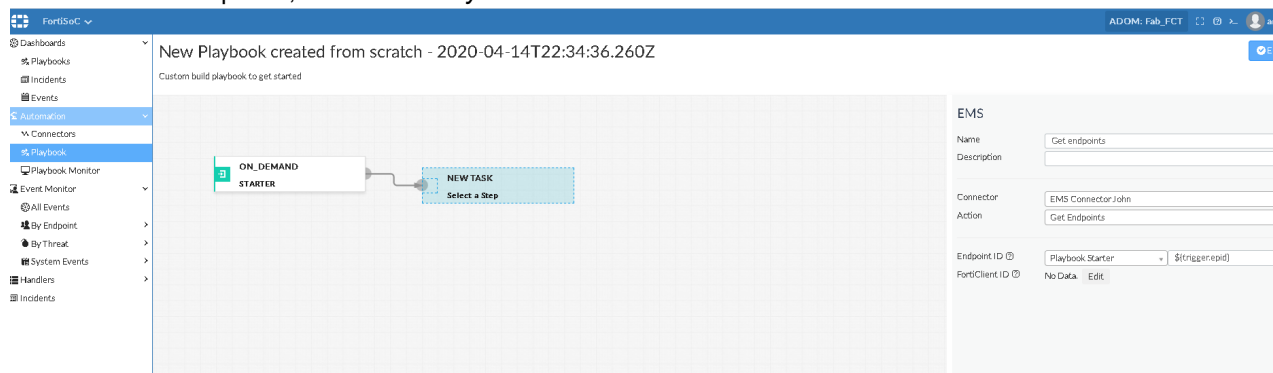
A prompt appears to select the endpoint on which to perform the vulnerability scan.

### 4. Go to *FortiSoC > Automation > Playbook Monitor* to view the running status of the playbook job.



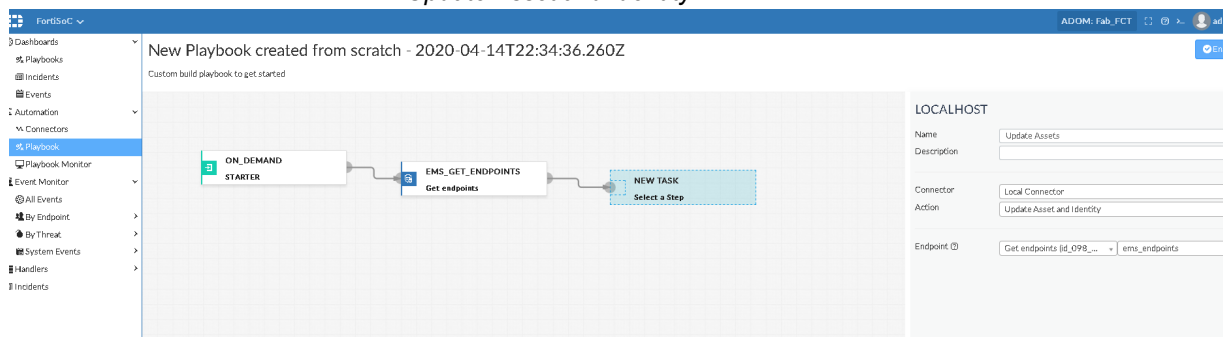
## To create a playbook from scratch

- Go to *FortiSoC > Automation > Playbook*, and click *Create New*.  
From the list of templates, select *New Playbook created from scratch*.



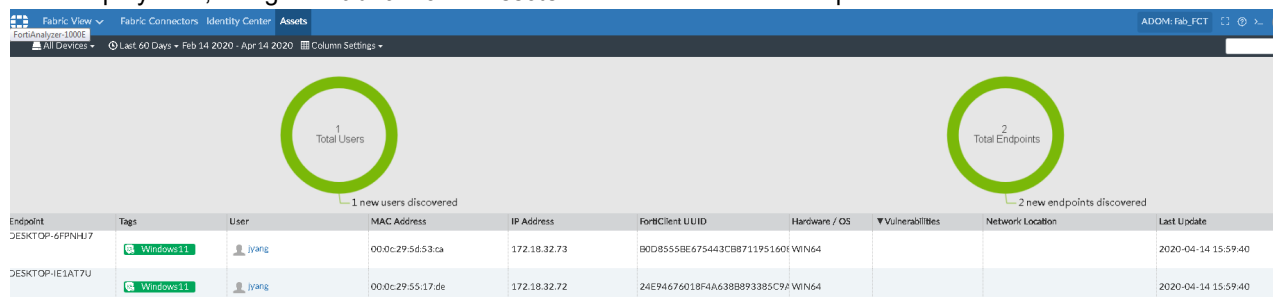
- Configure the playbook:
  - Select the *On Demand* trigger.
  - Add a task with the EMS connector *Get Endpoints* action.

- c. Add a task with the Local connector *Update Asset and Identity* action.



3. Click *Save Playbook*.

4. Run the playbook, and go to *Fabric View > Assets* to view the collected endpoint information.



## Normalized Fabric logs

All logs from different Fabric devices are normalized and available for search in *Log View* under the *Fabric* section.

- In FortiAnalyzer 6.4.0, SIEM features are available with all VM models and most hardware models (FortiAnalyzer 400E and above).
- When one or more devices are added or promoted to a Fabric ADOM and logs are being sent to FortiAnalyzer, a SIEM database (siemdb) is automatically created for the ADOM. All logs are inserted into the siemdb and displayed in *Log View > Fabric > All*.
- SIEM databases are created based on ADOMs. If there are multiple Fabric ADOMs with logs, the same number of SIEM databases are automatically created.

## To create a Fabric ADOM and view normalized Fabric logs:

1. Go to *System Settings > All ADOMs* and create a Fabric ADOM. For example, *Fabric\_ADOM1*.

2. Configure a FortiGate to send logs to FortiAnalyzer, and promote the FortiGate device to the Fabric ADOM.

3. From the CLI, confirm the siemdb has been created properly for the *Fabric\_ADOM1* ADOM.

```
FAZVM64 # diagnose test application siemdbd 6
ADOM Fabric_ADOM1[150] : part-days=1 rows=33 bytes=21.4KB time=[2020-04-27
15:40:17, 2020-04-27 15:40:17] duration=1s
*** Total tracked ADOMs: 1, Time to refresh: 27(sec)
```

#### 4. Go to **Log View > Fabric > All**. Normalized logs from FortiGate are automatically displayed in the siemdb format.

Log View <span>ADOM: Fabric_ADOM1</span>										
* Fabric	Last 1 Hour 14:43:15 To 15:43:14									
* All	Add Filter									
FortiGate	#	▼ Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name	User ID
▼ Traffic	1	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.143	192.168.10.92		
▼ Security	2	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.51	192.168.10.92		
Application Control	3	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.58	192.168.10.92		
Web Filter	4	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.110	192.168.10.92		
Custom View	5	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.182	192.168.10.92		
Log Browse	6	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.92	192.168.10.92		
Log Group	7	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.207	192.168.10.92		
	8	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.133	192.168.10.92		
	9	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.202	192.168.10.92		
	10	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.55	192.168.10.92		
	11	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.134	192.168.10.92		
	12	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.181	192.168.10.92		
	13	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.129	192.168.10.92		
	14	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.60	192.168.10.92		
	15	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.159	192.168.10.92		
	16	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.12	192.168.10.92		
	17	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.40	192.168.10.92		
	18	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.14	192.168.10.92		
	19	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.93	192.168.10.92		
	20	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.204	192.168.10.92		
	21	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.14	192.168.10.92		
	22	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.13	192.168.10.92		

When other types of devices such as FortiMail and FortiWeb are added to the Fabric ADOM, their logs are also displayed.

Log View <span>ADOM: Fabric_ADOM1</span>										
* Fabric	Last 1 Hour 14:52:45 To 15:52:44									
* All	Add Filter									
FortiGate	#	▼ Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name	User ID
FortiMail	1	15:50:44	FE-2KB3R09600010	Newsletter: score = 0	spam	information		13.13.13.13		
FortiWeb	2	15:50:43	FE-2KB3R09600010	Newsletter: score = 0	spam	information		13.13.13.13		
Custom View	3	15:50:42	FE-2KB3R09600010	URI lookup: http://b...	spam	information		13.13.13.13		
Log Browse	4	15:50:41	FE-2KB3R09600010	DKIM Check Failed. ...	spam	information		13.13.13.13		
Log Group	5	15:50:40	FE-2KB3R09600010	FortiGuard spam ou...	spam	information		12.12.12.12		
	6	15:50:39	FE-2KB3R09600010	SPF=SOFTFAIL: (he...	spam	information		13.13.13.13		
	7	15:50:38	FE-2KB3R09600010	Newsletter: score = 2	spam	information		13.13.13.13		
	8	15:50:37	FE-2KB3R09600010	SPF=SOFTFAIL: (he...	spam	information		13.13.13.13		
	9	15:47:28	FV400C3M12000023	[Signatures name: a]...	attack	Medium	61.149.143.226	116.213.69.32		
	10	15:47:27	FV400C3M12000023	[Signatures name: a]...	attack	High	61.149.143.226	116.213.69.32		
	11	15:47:26	FV400C3M12000023	[Signatures name: a]...	attack	Medium	61.149.143.226	116.213.69.32		
	12	15:47:25	FV400C3M12000023	[Signatures name: a]...	attack	High	61.149.143.226	116.213.69.32		
	13	15:47:24	FV400C3M12000023	[Signatures name: a]...	attack	Medium	61.149.143.226	116.213.69.32		
	14	15:47:23	FV400C3M12000023	[Signatures name: a]...	attack	Medium	61.149.143.226	116.213.69.32		
	15	15:47:22	FV400C3M12000023	[Signatures name: a]...	attack	Medium	61.149.143.226	116.213.69.32		
	16	15:47:21	FV400C3M12000023	[Signatures name: a]...	attack	High	61.149.143.226	116.213.69.32		
	17	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.143	192.168.10.92		
	18	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.51	192.168.10.92		
	19	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.58	192.168.10.92		
	20	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.110	192.168.10.92		
	21	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.182	192.168.10.92		
	22	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.92	192.168.10.92		
	23	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.207	192.168.10.92		
	24	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.133	192.168.10.92		
	25	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.202	192.168.10.92		

Click **Column Settings** to change the columns that are displayed.

The screenshot shows the FortiAnalyzer Log View interface. On the left, there is a sidebar with a tree view containing 'Fabric', 'FortiGate', 'FortiMail', 'FortiWeb', 'Custom View', 'Log Browse', and 'Log Group'. The main area displays a table of logs with columns: #, Date/Time, Source IP, and Destination IP. A 'Column Settings' dialog box is open in the center, allowing users to select which columns to display. The dialog has a search bar and a list of checkboxes for various fields: Net Direction, Net Name, Net Payload ID, Net Protocol, Net Received Bytes, Net Received Packets, Net SSID, Net Sent Bytes, Net Sent Packets, Net Session Duration, and Net Session ID. At the bottom of the dialog are buttons for 'Save as Default', 'OK', and 'Cancel'.

Double click on an individual log to view its details. Details are displayed according to groups.

The screenshot shows the FortiAnalyzer Log View interface with a detailed view of a log entry. The main table lists logs with columns: #, Date/Time, Data Source ID, Event Message, Event Type, Event Severity, Source IP, Destination IP, and Host ID. A log entry is selected, and its details are shown on the right side of the interface. The details are organized into groups: ADOM, Data, Event, Host, Application, and Network. Each group contains a list of fields and their values. For example, the 'Data' group includes fields like ADOM OID, Data Parser Name, Data Source ID, Data Source Name, Data Source Type, Data Timestamp, Date/Time, End User ID, Endpoint ID, Log User ID, and Time Stamp. The 'Event' group includes Event Action, Event ID, Event Severity, Event Sub Type, and Event Type. The 'Host' group includes Host IP and Host Location. The 'Application' group includes Application Name and Application Service. The 'Network' group includes Destination Geo, Destination IP, Destination Interface, Destination Port, Net Protocol, Net Received Bytes, Net Received Packets, Net Sent Bytes, Net Sent Packets, Net Session Duration, Source Geo, Source IP, and Source Interface.

SIEM log display can be filtered based on SIEM fields.

Log View									
Fabric									
Last 4 Hours 12:47:37 To 16:47:36									
Event Type = "traffic" Add Filter									
#	Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name	User ID
1	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.143	192.168.10.92		
2	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.51	192.168.10.92		
3	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.58	192.168.10.92		
4	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.110	192.168.10.92		
5	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.182	192.168.10.92		
6	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.92	192.168.10.92		
7	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.207	192.168.10.92		
8	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.133	192.168.10.92		
9	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.202	192.168.10.92		
10	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.55	192.168.10.92		
11	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.134	192.168.10.92		
12	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.181	192.168.10.92		
13	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.129	192.168.10.92		
14	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.60	192.168.10.92		
15	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.159	192.168.10.92		
16	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.12	192.168.10.92		
17	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.40	192.168.10.92		
18	15:40:17	FG1K5D3I14803379		traffic	notice	10.62.1.14	192.168.10.92		

## Incidents with multiple endpoints and users - 6.4.2

This is an enhancement to the FortiSoc module supporting multiple endpoints and users for incidents.

To view incidents with multiple endpoints/users:

1. In the Event Monitor, you can raise or add events with multiple endpoints and users to an incident.

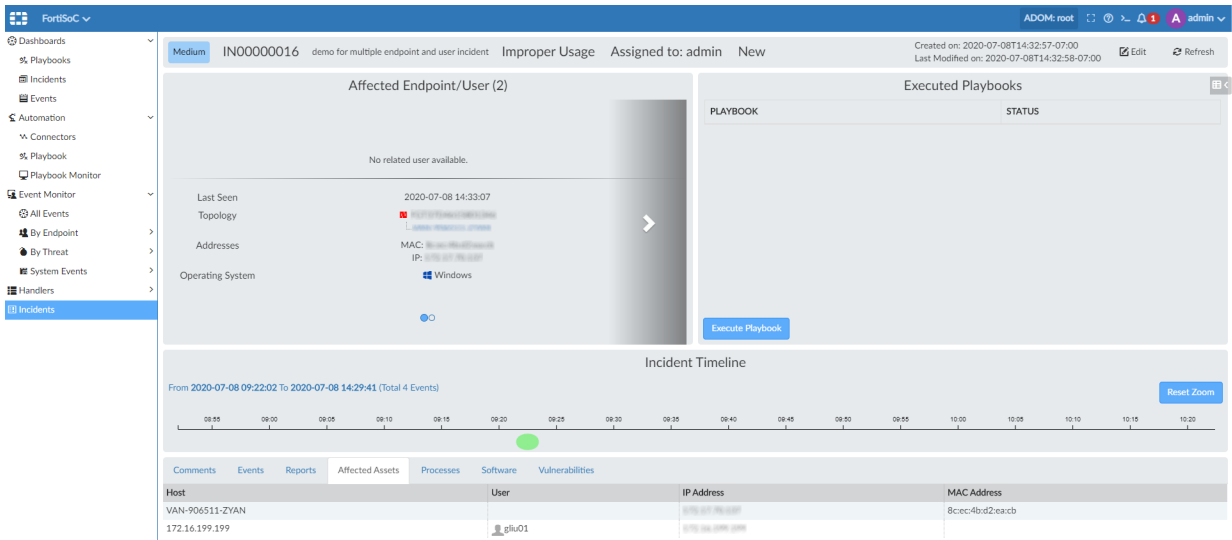


When endpoint/users are manually raised/added to an incident, only the first endpoint will be displayed when the incident is raised and there is an approximate five second delay to show multiple endpoint/user information on the incident analysis page. When a playbook runs a task using the local connector to create an incident, there is an approximate 20 second delay to display all information.

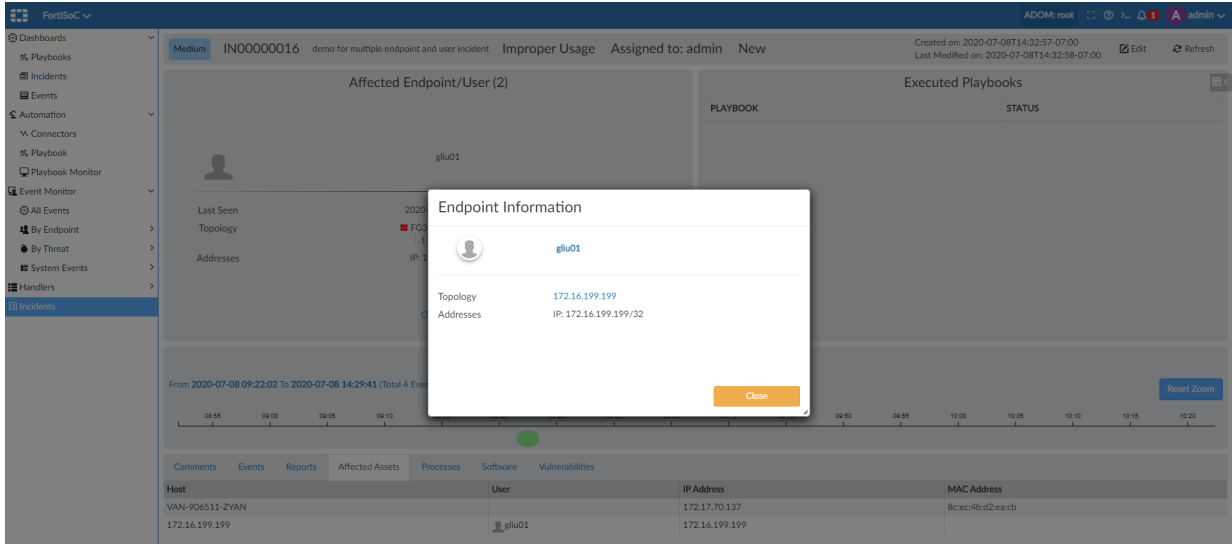
FortiSoc									
ADOM: root									
Refresh Custom View									
#	Event	Event ID	Event Stat	Event Ty	Count	Severity	First Occurrence	Last Update	Additional Info
10	System time modified (2)	...		EV...		medium	13 days ago	12 days ago	
11	> 172.16.198.6 (1)	2020070...	Mitigated	SSL	90	Low	5 hours ago	10 minutes ago	Server certifi...
12	> 23.23.200.42 (1)	2020070...	Mitigated	SSL	1	Low	5 hours ago	5 hours ago	Server certifi...
13	> ET002187D74755 (1)	2020070...	Mitigated	SSL	3	Low	5 hours ago	5 minutes ago	Server certifi...
14	> 52.205.56.5 (1)	2020070...	Mitigated	SSL	1	Low	5 hours ago	5 hours ago	Server certifi...
15	> 40.69.216.129 (8)	...	Mitigated	SSL	22	Low	5 hours ago	An hour ago	Server certifi...
16	> 40.70.229.150 (30)	...	Mitigated	SSL	70	Low	5 hours ago	7 minutes ago	Server certifi...
17	> debian (1)	2020070...	Mitigated	SSL	3	Low	5 hours ago	2 hours ago	Server certifi...
18	> 52.201.183.155 (1)	2020070...	Mitigated	SSL	3	Low	5 hours ago	2 hours ago	Server certifi...
19	> 4THFLOORLAB-JAM (1)	...	Mitigated	SSL	3	Low	5 hours ago	2 hours ago	Server certifi...
20	> VAN-906511-ZYAN (1)	...	Mitigated	SSL	4	Low	2020-07-08 09:21:47	2020-07-08 13:21:45	Server certifi...
21	> 213.155.156.180 (1)	...	Mitigated	SSL	1	Low	5 hours ago	5 hours ago	Server certifi...
22	> 172.30.1.239 (13)	...	Mitigated	SSL	1333	Low	5 hours ago	2 minutes ago	Server certifi...
23	> VAN-201657-PC2 (1)	...	Mitigated	SSL	14	Low	5 hours ago	16 minutes ago	Server certifi...
24	> 213.136.67.12 (1)	...	Mitigated	SSL	2	Low	5 hours ago	5 hours ago	Server certifi...
25	> 68.70.200.128 (1)	...	Mitigated	SSL	6	Low	5 hours ago	5 hours ago	Server certifi...
26	> 172.16.199.199 (1)	...	Mitigated	SSL	26	Low	2020-07-08 09:22:59	2020-07-08 14:29:41	Server certifi...
27	> Teamviewer (74)	...	Mitigated	Ap...	14318	Medium	5 hours ago	2 minutes ago	...
28	> VAN-200557-PC2 (1)	2020070...	Mitigated	Ap...	6	Low	5 hours ago	9 minutes ago	AppID:1479...

2. On the incident analysis page, information about multiple endpoint/users is available in the *Affected Assets* tab. You can also click the navigation arrows in the *Affected Endpoint/User* widget to show additional users and endpoints.





Click a user in the Affected Assets list to see additional endpoint information in a dialog window.



## Default playbook template improvements - 6.4.1

The list of default Playbook templates has been updated.

<b>FAZ Localhost</b>	Compromised Host Incident
	Critical Intrusion Incident
	Attach Endpoint Vulnerability list to Incident
<b>FortiOS</b>	Quarantine Endpoint by FortiOS

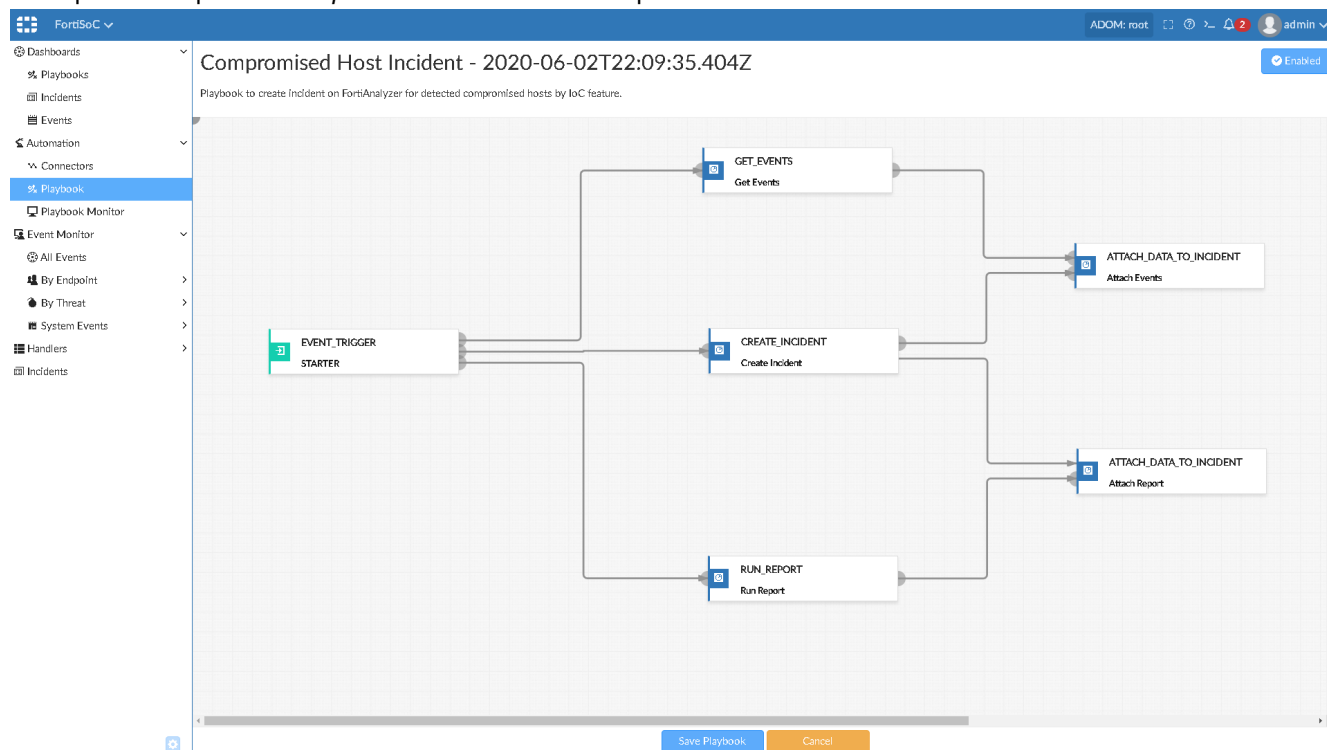
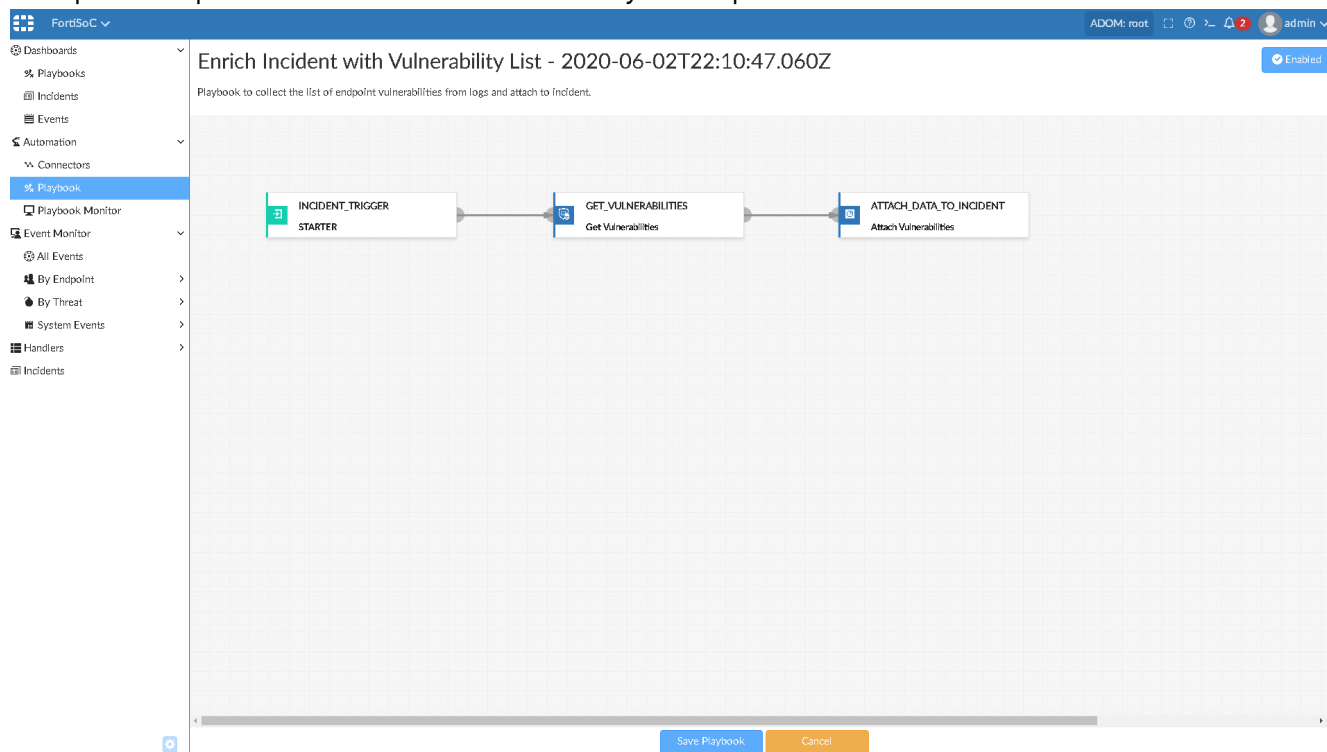
<b>EMS</b>	Update Asset and Identity Database
	Run AV Scan on Endpoint
	Run Vulnerability Scan on Endpoint
	Quarantine Endpoint by EMS
	Unquarantine Endpoint by EMS
	Enrich Incident with Process List
	Enrich Incident with Vulnerability List
	Enrich Incident with Software Inventory

The screenshot shows the FortiAnalyzer 6.4.0 Playbook Templates interface. The left sidebar contains the navigation menu with the following items: Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbooks (selected), Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, Handlers, and Incidents. The main area displays a table of playbook templates. The table has columns for Name, Description, and Status. The status column shows 'No record found.' for the first row. The right sidebar shows a list of playbook templates with their names and descriptions.

Name	Description	Status
No record found.		

Choose from Playbook Templates

- New Playbook created from scratch**  
Custom build playbook to get started
- Enrich Incident with Vulnerability List**  
Playbook to collect the list of endpoint vulnerabilities from logs and attach to Incident.
- Compromised Host Incident**  
Playbook to create Incident on FortiAnalyzer for detected compromised hosts by IoC feature.
- Run Vulnerability Scan on Endpoint**  
Playbook to run vulnerability scan on endpoint.
- Update Asset and Identity Database**  
Playbook to automatically update FortiAnalyzer Asset and Identity database with endpoint and user information from EMS
- Quarantine Endpoint by EMS**  
Playbook to quarantine endpoint by EMS connector
- Enrich Incident with Software Inventory**  
Playbook to get software inventory from endpoint by EMS Connector and attach to Incident.
- Quarantine Endpoint by FortiOS**  
Playbook to quarantine endpoint by FOS connector providing MAC address or FortiClient UID
- Enrich Incident with Process List**  
Playbook to get running processes on endpoint by EMS connector and attach to Incident.
- Run AV Scan on Endpoint**  
Playbook to run AV scan on Endpoint by EMS Connector
- Unquarantine Endpoint by EMS**  
Playbook to unquarantine endpoint by EMS connector
- Critical Intrusion Incident**  
Playbook to create Incident on FortiAnalyzer for detected critical intrusions by IPS
- Attach Endpoint Vulnerability list to Incident**  
Playbook to collect the list of endpoint vulnerabilities from logs and attach to Incident.

Example of the updated *Compromised Host Incident* template:Example of the updated *Enrich Incident with Vulnerability List* template:

## Incident page improvement - 6.4.1

This is an enhancement to the incident analysis page that offers a more useful view for users by introducing *Processes*, *Software* and *Vulnerabilities* tabs. These tabs include endpoint information that attaches to incidents.

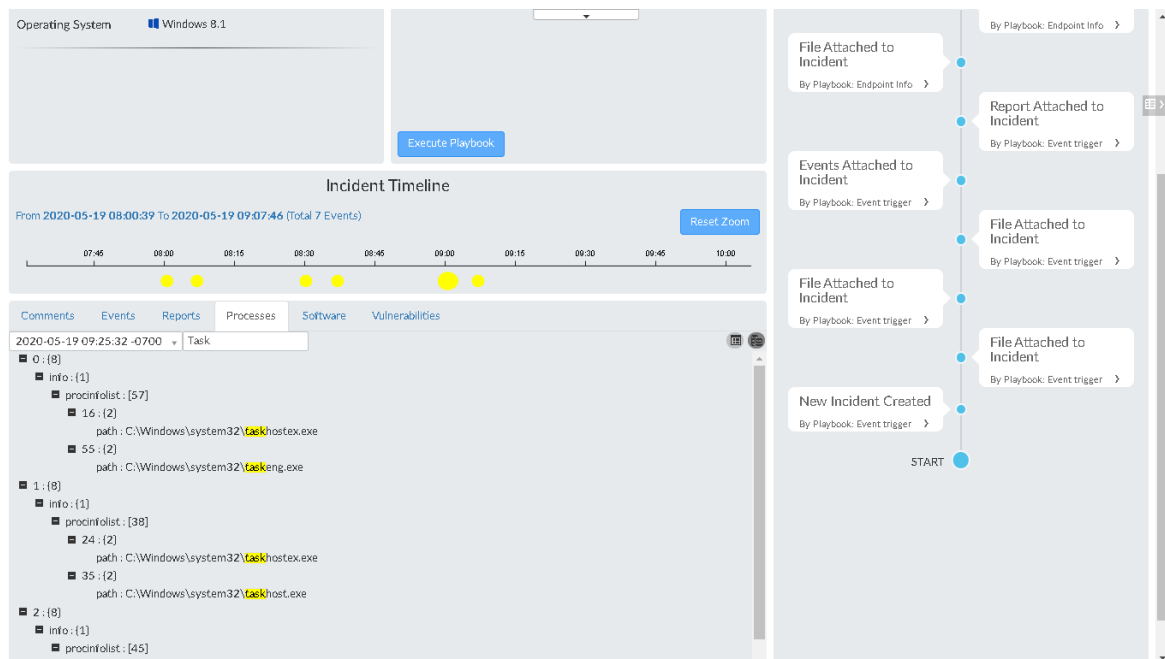
### To view the incident page improvements:

- Go to *FortiSOC > Incidents*, and select an incident to view the *Incident Analysis* page.
  - Incident attachment for endpoint processes:
    - Click the table view icon in the top-right corner in the attachment section to view endpoint processes in a table format.

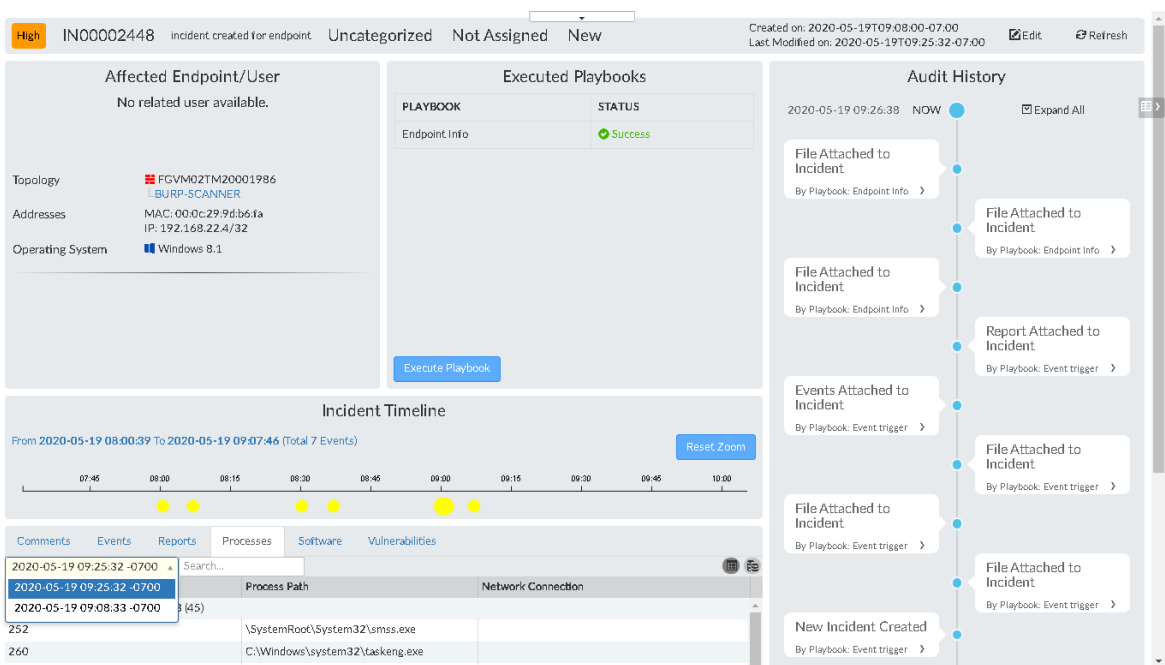
The screenshot shows the FortiSOC interface for incident IN00002710. The left sidebar contains navigation options like Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, and Handlers. The main content area is divided into several sections:

- Incident Header:** Shows incident ID IN00002710, status (Uncategorized, Not Assigned, New), and creation/modification timestamps.
- Affected Endpoint/User:** Displays a profile icon, topology (FGVM02TM20001986), addresses (MAC: 00:0c:29:23:9c:8b, IP: 192.168.22.6/32), and operating system (WIN64 Microsoft Windows Server 2012 Datacenter Edition, 64-bit (build 9200)).
- Executed Playbooks:** A table with columns for Playbook and Status.
- Incident Timeline:** A horizontal timeline showing events from 2020-05-14 01:50:04 to 2020-05-14 15:11:28 (Total 62 Events).
- Process List:** A table with columns for Process ID, Process Path, and Network Connection. The table lists several processes, including svchost.exe and csrss.exe.

- Click the raw data icon in the top-right corner in the attachment section to view endpoint process information as raw data.



- Select a time from the snapshots dropdown to view different snapshots.



- Enter search keywords in the search field to view filtered records which match the keyword. Matching keywords are highlighted in the results.

Operating System: Windows 8.1

Execute Playbook

Incident Timeline

From 2020-05-19 08:00:39 To 2020-05-19 09:07:46 (Total 7 Events)

Reset Zoom

Comments Events Reports Processes Software Vulnerabilities

2020-05-19 09:25:32 -0700 Task

Process ID	Process Path	Network Connection
FortiClient.FCT8004234043193 (3)		
260	C:\Windows\system32\Taskeng.exe	
1184	C:\Windows\system32\Taskhost.exe	
3400	C:\Windows\system32\Taskeng.exe	
FortiClient.FCT8002380964133 (2)		
FortiClient.FCT8002828241805 (2)		

File Attached to Incident  
By Playbook: Endpoint Info

Report Attached to Incident  
By Playbook: Event trigger

Events Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

New Incident Created  
By Playbook: Event trigger

START

- Incident attachment for installed software.
  - Click the table view in the top-right corner in the attachment section to view installed software in a table format.

Operating System: Windows 8.1

Execute Playbook

Incident Timeline

From 2020-05-19 08:00:39 To 2020-05-19 09:07:46 (Total 7 Events)

Reset Zoom

Comments Events Reports Processes Software Vulnerabilities

2020-05-19 09:25:32 -0700 Search...

Software	Installation Path	Installation Time
FortiClient	C:\Program Files\Fortinet\FortiClient\	2020-05-07
Google Chrome	C:\Program Files (x86)\Google\Chrome\Application	2020-03-20
Google Update Helper		2020-03-20
Java 8 Update 45 (64-bit)		2015-06-17
Java Auto Updater		2015-06-17
Mozilla Firefox 51.0.1 (x86 en-US)	C:\Program Files (x86)\Mozilla Firefox	2017-01-25
Mozilla Maintenance Service		2017-02-08
NUit 2.6.3		2015-08-12

File Attached to Incident  
By Playbook: Endpoint Info

Report Attached to Incident  
By Playbook: Event trigger

Events Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

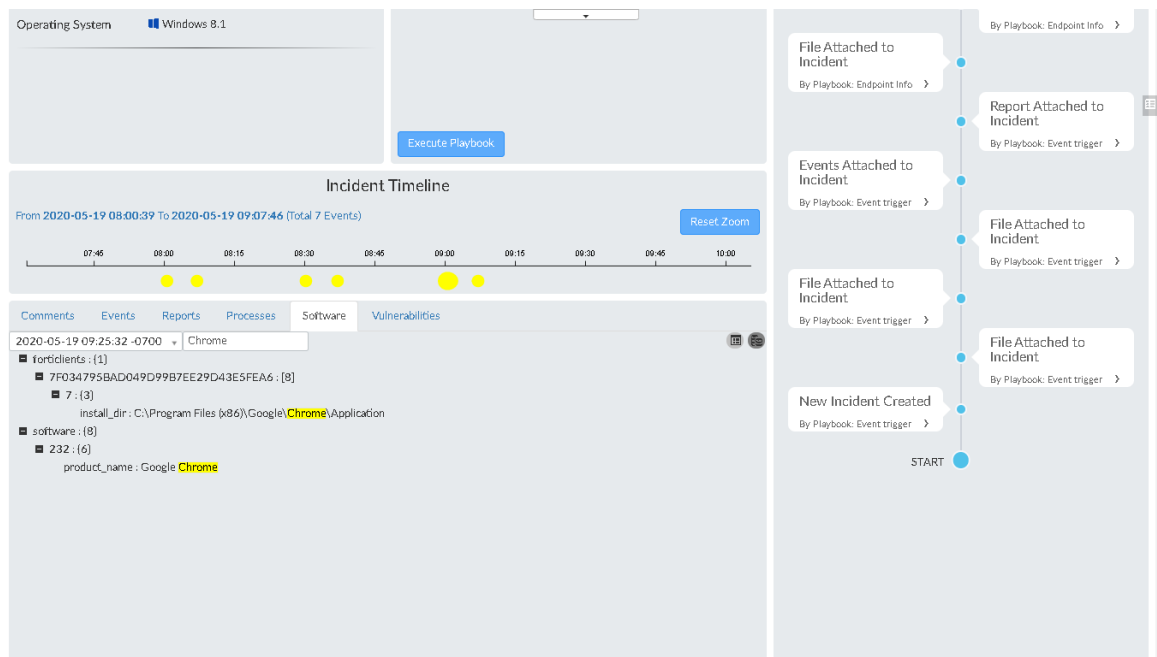
File Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

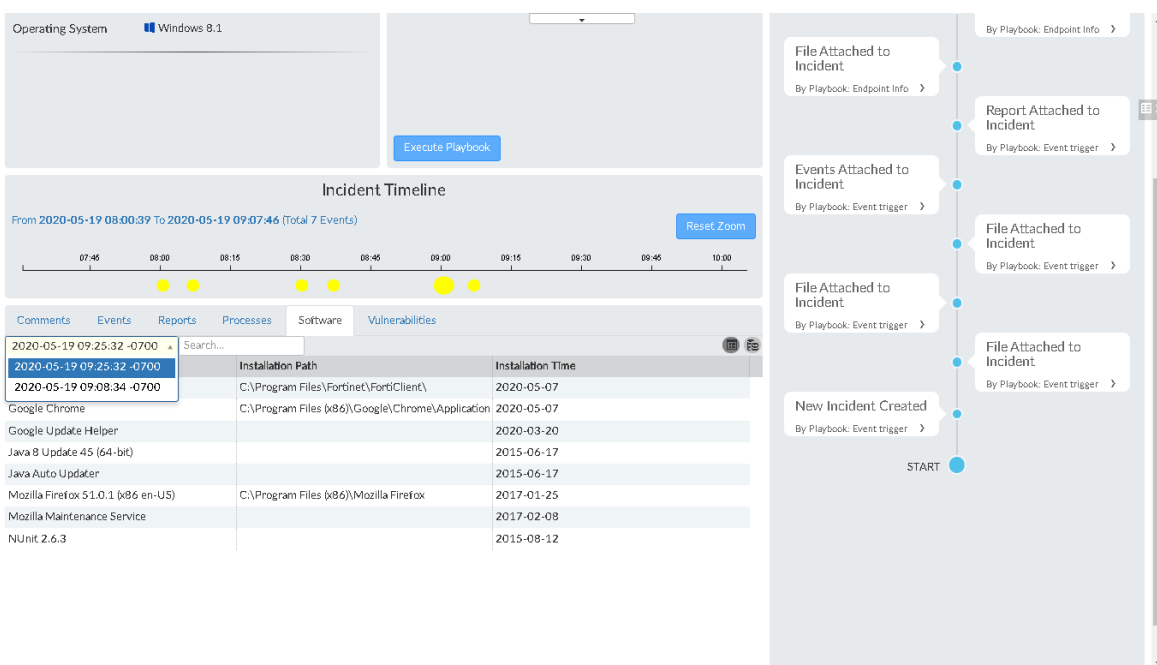
New Incident Created  
By Playbook: Event trigger

START

- Click the raw data icon in the top-right corner in the attachment section to view installed software information as raw data.



- Select a time from the snapshots dropdown to view different snapshots.



- Enter search keywords in the search field to view filtered records which match the keyword. Matching keywords are highlighted in the results.

Operating System: Windows 8.1

Execute Playbook

Incident Timeline

From 2020-05-19 08:00:39 To 2020-05-19 09:07:46 (Total 7 Events)

Reset Zoom

Comments Events Reports Processes Software Vulnerabilities

2020-05-19 09:25:32 -0700 Chrome

Software	Installation Path	Installation Time
Google Chrome	C:\Program Files (x86)\Google\Chrome\Application	2020-05-07

File Attached to Incident  
By Playbook: Endpoint Info

Report Attached to Incident  
By Playbook: Event trigger

Events Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

New Incident Created  
By Playbook: Event trigger

START

- Incident attachment for endpoint vulnerabilities.
  - Click the table view icon in the top-right corner in the attachment section to view endpoint vulnerabilities in a table format.

Operating System: Windows 8.1

Execute Playbook

Incident Timeline

From 2020-05-19 08:00:39 To 2020-05-19 09:07:46 (Total 7 Events)

Reset Zoom

Comments Events Reports Processes Software Vulnerabilities

2020-05-19 09:25:32 -0700 Search...

Vulnerability ID	Vulnerability Name	Severity	Category
24087	Vulnerability in .NET Framework Could Allow	Low	Operating System
25918	Security Update for Volume Manager Drive	Medium	Operating System
35449	Security vulnerabilities fixed in Firefox 52	Critical	Web Client
35604	Integer overflow in createImageBitmap()	Critical	Web Client
35808	Security vulnerabilities fixed in Firefox 53	Critical	Web Client
35918	Use after free in ANGLE	High	Web Client
36288	Security vulnerabilities fixed in Firefox 54	Critical	Web Client
36587	Security vulnerabilities fixed in Firefox 55	Critical	Web Client
36713	Security vulnerabilities fixed in Firefox 56	Critical	Web Client
41048	Security vulnerabilities fixed in Firefox 57	Critical	Web Client
41110	Security vulnerabilities fixed in Firefox 57.0	High	Web Client
41157	Security vulnerabilities fixed in Firefox 57.0	High	Web Client
41158	Microsoft Windows RRAS Service Remote	Medium	Operating System
javascript:void(0)	Microsoft Springline Engine Mammov Cmmv High		Web Client

File Attached to Incident  
By Playbook: Endpoint Info

Report Attached to Incident  
By Playbook: Event trigger

Events Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

File Attached to Incident  
By Playbook: Event trigger

New Incident Created  
By Playbook: Event trigger

START

- Click the raw data icon in the top-right corner in the attachment section to view endpoint process information as raw data.



Operating System: Windows 8.1

Execute Playbook

Incident Timeline

From 2020-05-19 08:00:39 To 2020-05-19 09:07:46 (Total 7 Events)

Reset Zoom

Comments Events Reports Processes Software Vulnerabilities

2020-05-19 09:25:32 -0700 Directx

vulns : {101}

- 55618 : (5)
  - vuln\_name : Microsoft: DirectX Elevation of Privilege Vulnerability
- 55627 : (5)
  - vuln\_name : Microsoft: DirectX Elevation of Privilege Vulnerability
- 55629 : (5)
  - vuln\_name : Microsoft: DirectX Information Disclosure Vulnerability

File Attached to Incident

Report Attached to Incident

Events Attached to Incident

File Attached to Incident

File Attached to Incident

File Attached to Incident

New Incident Created

START

- Select a time from the snapshots dropdown to view different snapshots.

Operating System: Windows 8.1

Execute Playbook

Incident Timeline

From 2020-05-19 08:00:39 To 2020-05-19 09:07:46 (Total 7 Events)

Reset Zoom

Comments Events Reports Processes Software Vulnerabilities

2020-05-19 09:25:32 -0700

2020-05-19 09:08:34 -0700

Vulnerability ID	Vulnerability Name	Severity	Category
61720	Arbitrary code execution through unsanitization	Critical	Web Client
61856	Firefox Vulnerability CVE-2017-5397	Critical	Web Client
61856	Firefox Vulnerability CVE-2017-5452	Medium	Web Client
61866	Firefox Vulnerability CVE-2017-7771	High	Web Client
61867	Firefox Vulnerability CVE-2017-7772	High	Web Client
61868	Firefox Vulnerability CVE-2017-7773	High	Web Client
61721	Firefox Vulnerability CVE-2017-7774	Critical	Web Client
61869	Firefox Vulnerability CVE-2017-7776	High	Web Client
61870	Firefox Vulnerability CVE-2017-7777	High	Web Client
61861	Firefox Vulnerability CVE-2018-18499	Medium	Web Client
61862	Firefox Vulnerability CVE-2018-18510	Medium	Web Client
61863	Firefox Vulnerability CVE-2018-5124	Medium	Web Client
61871	Firefox Vulnerability CVE-2018-5179	High	Web Client
41750	Internet Explorer Information Disclosure V	Medium	Web Client

File Attached to Incident

Report Attached to Incident

Events Attached to Incident

File Attached to Incident

File Attached to Incident

File Attached to Incident

New Incident Created

START

- Enter search keywords in the search field to view filtered records which match the keyword. Matching keywords are highlighted in the results.

The screenshot displays the FortiAnalyzer interface. At the top, there's a search bar with 'Critical' entered. Below it, a table lists vulnerabilities with columns for Vulnerability ID, Name, Severity, and Category. The 'Severity' column is filtered to show only 'Critical' items. To the right, a timeline shows events from 2020-05-19 08:00:39 to 2020-05-19 09:07:46. On the far right, a vertical timeline shows a sequence of events: 'File Attached to Incident', 'Report Attached to Incident', 'Events Attached to Incident', 'File Attached to Incident', 'File Attached to Incident', and 'New Incident Created'.

Vulnerability ID	Vulnerability Name	Severity	Category
41752	Arbitrary code execution through unsanitiz	Critical	Web Client
61720	Firefox Vulnerability CVE-2017-5397	Critical	Web Client
61721	Firefox Vulnerability CVE-2017-7774	Critical	Web Client
55617	Microsoft Windows Deployment Services	Critical	Operating System
48963	Out of bounds memory write while process	Critical	Web Client
62143	Security Vulnerabilities fixed in Firefox 72.0	Critical	Web Client
35449	Security vulnerabilities fixed in Firefox 52	Critical	Web Client
35808	Security vulnerabilities fixed in Firefox 53	Critical	Web Client
36288	Security vulnerabilities fixed in Firefox 54	Critical	Web Client
36587	Security vulnerabilities fixed in Firefox 55	Critical	Web Client
36713	Security vulnerabilities fixed in Firefox 56	Critical	Web Client
41048	Security vulnerabilities fixed in Firefox 57	Critical	Web Client
41634	Security vulnerabilities fixed in Firefox 58	Critical	Web Client
48652	Security vulnerabilities fixed in Firefox 59	Critical	Web Client

## Filters for local report action - 6.4.2

This is an enhancement to the existing feature to address limitations on resources and timeline by offering filter, time range and log field selection for the local report playbook action.

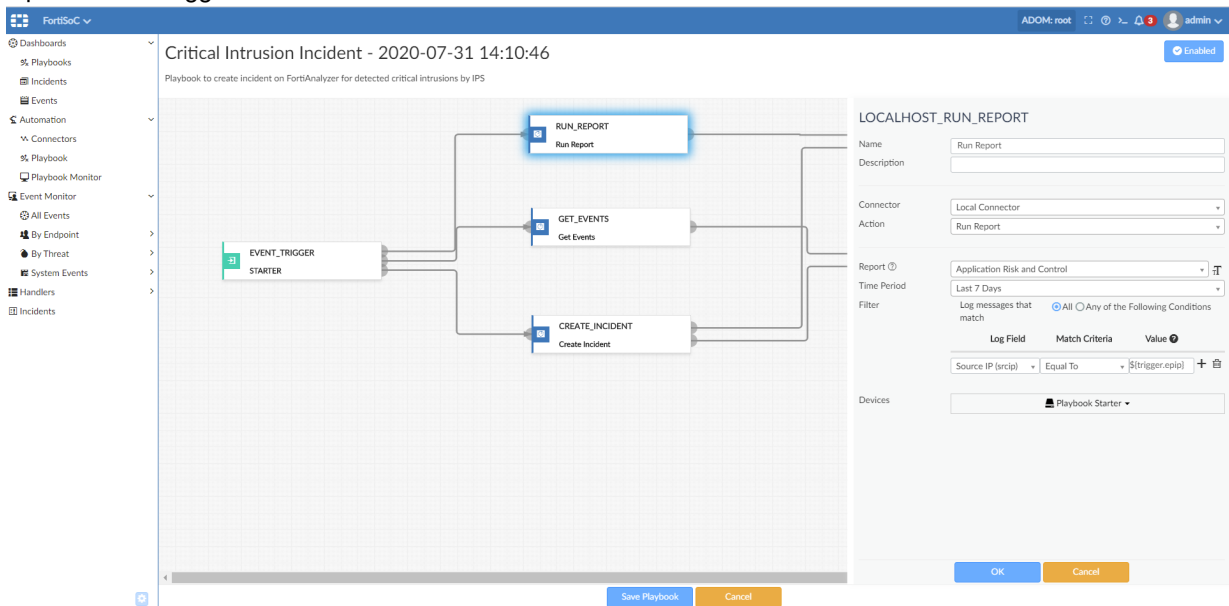
To view report options for local report actions in playbooks:

1. Reports with the *Extended Log Filtering* option enabled are supported in the local connector's Run Report action.

The screenshot shows the FortiAnalyzer interface with a playbook configuration for 'LOCALHOST\_RUN\_REPORT'. The playbook is titled 'Critical Intrusion Incident - 2020-07-31 14:10:46'. It includes a 'STARTER' event trigger, followed by 'GET\_EVENTS' and 'CREATE\_INCIDENT' actions. The 'LOCALHOST\_RUN\_REPORT' configuration panel on the right shows the following settings:

- Name: Run Report
- Description: (empty)
- Connector: Local Connector
- Action: Run Report
- Report: (dropdown menu)
- Time Period: (dropdown menu)
- Start Time: YYYY/MM/DD HH:MM:SS
- End Time: YYYY/MM/DD HH:MM:SS
- Filter: No Data
- Devices: All Devices

2. Reports support custom time ranges, device filters, and log filters in the playbook task.
  - a. **Time range** - Select a time range from the dropdown list or enter a custom time range.
  - b. **Filter** - Select the filters to apply to the report.
  - c. **Devices** - Select the devices to be included in the report, or choose *Playbook Starter* to use a dynamic device input from the trigger.



## SOC subscription license - 6.4.1

FortiSOC features in FortiAnalyzer are enabled through a SOC subscription license. The SOC subscription license includes features such as playbooks, connecting to third-party feeds, and incident investigation.

## To view the SOC subscription license in FortiAnalyzer:

1. The SOC subscription license can be viewed in *System Settings > Dashboard* in the *License Information* widget. You can also check the license through the CLI using the `diagnose license list` command.

The screenshot displays the FortiAnalyzer System Settings Dashboard. The left sidebar shows the navigation menu with 'System Settings' selected. The main content area is divided into two sections: 'License Information' and 'System Information'.

**License Information:**

VM License	Type	Valid 10K-UG
FortiCloud	Not Registered	
FortiGuard	Indicators of Compromise Service	Licensed (Expires 2030-01-04)
Security Operations	SOC Service	Licensed (Expires 2030-01-04)
Logging	Devices/VDOMs	66 of 10,000 (0.7%)
	GB/Day	0.1 of 100 (0.1%)
	VM Storage	Unlimited
Storage Connector	Cloud	No License
Service	Antivirus and IPS	192.168.100.105
Update Server	FortiClient Update	192.168.100.207

**System Information:**

Host Name	FAZVM64
Serial Number	FAZ-VMTM20007144
Platform Type	FAZVM64
HA Status	Standalone
System Time	Fri Jul 10 16:52:39 2020 PDT
Firmware Version	v6.4.0-build2097 200709 (Interim)
System Configuration	Last Backup : N/A
Current Administrators	admin / 3 in total
Up Time	7 hours 4 minutes 4 seconds

The CLI Console on the right shows the output of the `diagnose license list` command:

```

FAZVM64 # diagnose license list
List FortiAnalyzer license.
update FortiAnalyzer license.
FAZVM64 # diagnose license list
Name      Status      Expiry      Description
-----
VDBE      Valid       2030-01-04  post breach detection
SCPC      No license  0000-00-00  cloud storage service
SOAR      Valid       2030-01-04  SOAR and SIEM bundle service
  
```

2. With a valid license, FortiSoC features are fully available.

The screenshot displays the FortiSoC dashboard. The left sidebar shows the navigation menu with 'FortiSoC' selected. The main content area shows a grid of security modules: Device Manager, FortiView, Log View, Fabric View, FortiSoC, Reports, and System Settings.

Below the grid, there is a table showing the status of endpoints:

Endpoint	Status	Created Time	Modified Time
Quarantine endpoint	Disabled	05/26/2020	05/26/2020

3. When the license is expired or there is no valid license, FortiSoC includes a try-it-out mode with a maximum of five playbooks run per day.

**License Information**

- FortiCloud: Not Registered
- Indicators of Compromise: Licensed (Expires 2030-01-04)
- Service Server Location: Servers located in US only
- Security Operations: SOC Service (Expired)
- Logging: Devices/VDOMs: 181 of 4,000 (4.5%)
- Storage Connector Service: Cloud: No License
- Update Server: AntiVirus and IPS: 192.168.100.105
- FortiClient Update: 96.45.33.106 Sunnyvale, California, United States

**System Information**

- Host Name: FAZ3000F
- Serial Number: FL-3KF3R16000119
- HA Status: Standalone
- System Time: Fri Jul 10 16:53:19 2020 PDT
- Firmware Version: v6.4.0-build2097 200710 (Interim)
- System Configuration: Last Backup: N/A
- Current Administrators: admin / 5 in total
- Up Time: 1 hour 2 minutes 40 seconds
- Administrative Domain: ON
- Operation Mode: Analyzer Collector

**System Resources**

- 8%
- 6%
- 4%

**CLI Console**

```
Connected FAZ3000F # diagnose license list
Name      Status      Expiry      Description
-----
YBDS      Valid       2030-01-04  post breach detection
SCPC      No License  0000-00-00  cloud storage service
SCAR      Expired     2020-07-04  SOAR and SIEM bundle service
FAZ3000F #
```

**FortiSoC**

Playbook Name	Status	Created Time	Modified Time
build playbook to get started	Enabled	06/25/2020	06/25/2020
build playbook to get started	Enabled	06/04/2020	06/04/2020
ng new new new	Enabled	01/30/2020	01/30/2020
build playbook to get started	Enabled	06/25/2020	06/25/2020
build playbook to get started	Enabled	06/24/2020	06/24/2020
k to run vulnerability scan on endpoint.	Disabled	06/03/2020	06/03/2020
build playbook to get started	Enabled	06/25/2020	06/25/2020
build playbook to get started	Enabled	06/25/2020	06/25/2020
build playbook to get started	Enabled	06/25/2020	06/25/2020

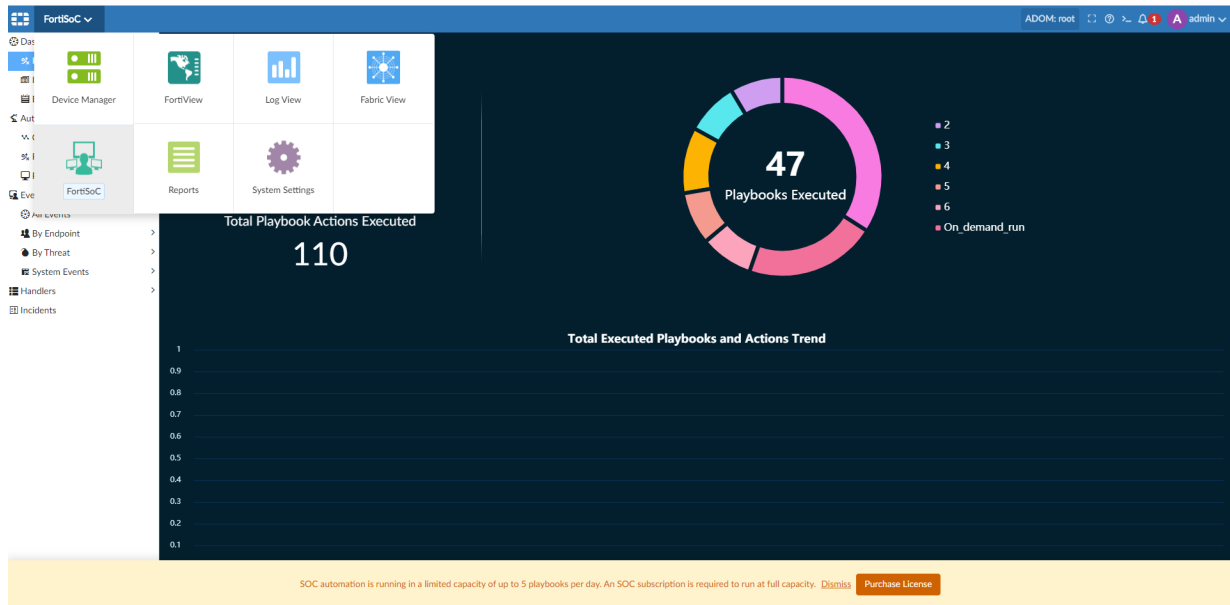
SOC automation is running in a limited capacity of up to 5 playbooks executed per day. An active SOC subscription is required to run at full capacity. The existing license expired on 07/04/2020. [Dismiss](#) [Purchase License](#)

## Try it Out feature for FortiSoC - 6.4.2

This new feature allows customers to access the FortiSoC module and try SOC automation features with some restrictions. Without a SOC subscription license, SOC automation will run in limited capacity with restricted number of playbooks to be executed per day.

### To use the Try it Out feature for FortiSoC:

1. Navigate to the FortiSoC module in FortiAnalyzer.  
When viewing FortiSoC without a SOC subscription license, a warning message and *Purchase License* option appears at the bottom of the page.



Without a license, up to five playbooks can be run per day. Additional playbooks will fail with a warning, and a local application log will be generated.

Invalid params: Playbook 'Shawn-2' cannot be launched, due to number of playbooks run has exceeded SOC license daily limit.

Name	Description	Status	Created Time	Modified Time
Compromised Host Incident	Playbook to create incident on FortiAnalyzer for det	Enabled	06/03/2020	06/05/2020
Quarantine Endpoint by EMS	Playbook to quarantine endpoint by EMS connector	Enabled	06/05/2020	06/05/2020
mzhao-test-license every 5 min	Custom build playbook to get started	Enabled	06/19/2020	06/19/2020
Run Vulnerability Scan on Endpoint	Playbook to run vulnerability scan on endpoint.	Enabled	06/05/2020	06/05/2020
Enrich Incident with Process List	Playbook to get running processes on endpoint by E	Enabled	06/05/2020	06/24/2020
Unquarantine Endpoint by EMS	Playbook to unquarantine endpoint by EMS connect	Enabled	06/05/2020	06/24/2020
Enrich Incident with Software Inventory	Playbook to get software inventory from endpoint b	Enabled	06/05/2020	06/24/2020
every 60 minute - 3	Custom build playbook to get started	Enabled	06/03/2020	06/24/2020
Update Asset and Identity Database	Playbook to automatically update FortiAnalyzer Ass	Disabled	06/05/2020	06/10/2020
mzhao-test-ems_get_endpoints	Custom build playbook to get started	Enabled	06/05/2020	06/10/2020
Shawn-2	Custom build playbook to get started	Enabled	06/24/2020	Last Friday at 10:18 AM
Run AV Scan on Endpoint	Playbo	Enabled	06/05/2020	06/05/2020
mzhao-test on schedule	Custom	Enabled	Yesterday at 4:22 PM	Yesterday at 5:43 PM
mzhao-test-license get events1	Custom	Enabled	06/19/2020	06/24/2020
ON Schedule-start 10:10	Custom	Enabled	06/12/2020	2020-07-08 16:45:51
mzhao-test-license get events	Custom	Enabled	06/19/2020	06/19/2020
Critical Intrusion Incident	Playbo	Enabled	06/03/2020	06/16/2020
mzhao-test-license every 6 min	Custom	Enabled	06/19/2020	06/19/2020
shawn-3-getevent-schedule	Custom	Enabled	06/24/2020	06/24/2020
Enrich Incident with Vulnerability List	Playbo	Enabled	06/05/2020	06/24/2020
mzhao-test-license every 7 min	Custom build playbook to get started	Enabled	06/19/2020	06/24/2020
Playbook Add_CnC_To_Blacklist	Custom build playbook to get started	Enabled	01/30/2020	06/05/2020
Attach Endpoint Vulnerability list to incident	Playbook to collect the list of endpoint vulnerabilit	Enabled	06/05/2020	06/05/2020

SOC automation is running in a limited capacity of up to 5 playbooks per day. An SOC subscription is required to run at full capacity. [Dismiss](#) [Purchase License](#)

Log View

#	Date/Time	Device ID	User	Sub Type	Event Type	Action	Description	Log ID	Level
1	16:46:16	FL-3KF3R16000119	system	playbook	run-stat	cancelled	Endpoints Re...	110100	notice
2	16:45:51	FL-3KF3R16000119	admin	playbook	run-stat	cancelled	Endpoints Re...	110050	warning
3	16:45:11	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
4	16:44:47	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
5	16:44:36	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
6	16:43:06	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
7	16:39:59	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
8	16:39:56	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
9	16:38:58	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
10	16:36:54	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
11	16:34:55	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
12	16:34:49	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
13	16:34:45	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
14	16:32:13	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
15	16:30:40	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
16	16:30:06	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
17	16:30:06	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
18	16:25:02	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
19	16:24:57	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
20	16:24:56	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
21	16:24:56	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
22	16:24:56	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
23	16:19:44	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
24	16:19:42	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
25	16:18:39	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
26	16:18:13	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
27	16:15:10	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
28	16:15:10	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110254	notice
29	16:13:02	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice
30	16:13:02	FL-3KF3R16000119	system	playbook	run-stat	Looking Up Ev...	Endpoints Re...	110100	notice

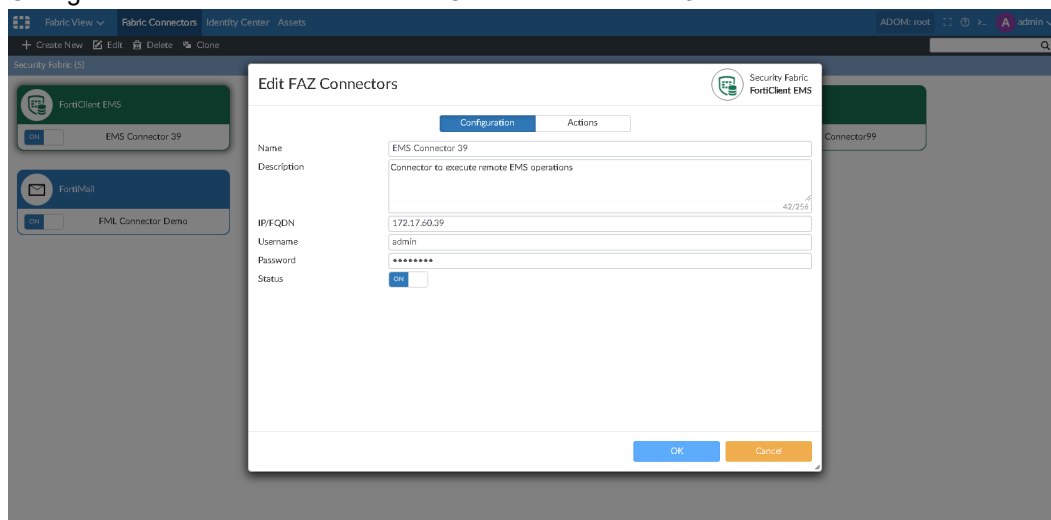
SOC automation is running in a limited capacity of up to 5 playbooks per day. An SOC subscription is required to run at full capacity. [Dismiss](#) [Purchase License](#)

## Vulnerabilities and software inventory data from EMS connector - 6.4.2

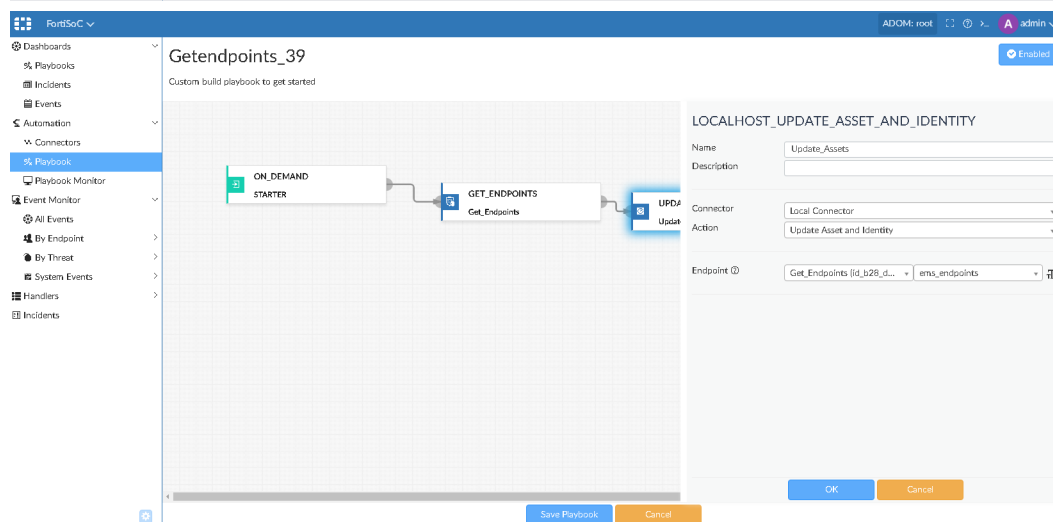
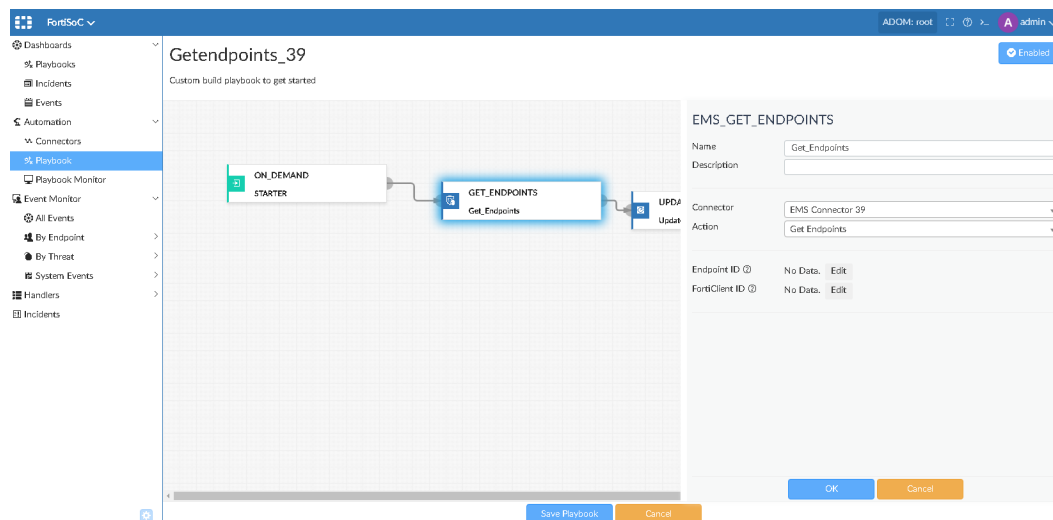
This new feature helps FortiAnalyzer to get more information, vulnerabilities and software inventory, from the FortiClient EMS server directly.

**To get endpoint data from an EMS connector:**

1. In *Fabric View > Fabric Connectors*, click *Create New* and select *FortiClient EMS*. Configure the connector details for FortiClient EMS and click *OK*.



2. Go to *FortiSoC > Automation > Playbook* and create a new playbook. Administrators can use wildcards to get all endpoints registered on the EMS server and then create another task to update *Fabric View > Assets*.



- Run the playbook, then go to *Fabric View > Assets*. The retrieved endpoints in the EMS server are displayed.

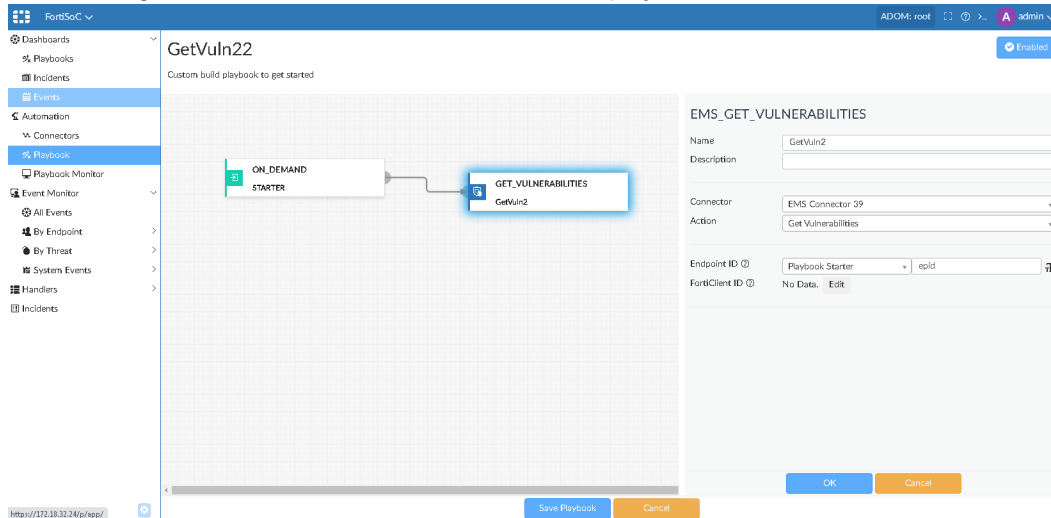
The screenshot shows the FortiAnalyzer Fabric View > Assets page. At the top, there are two green circles highlighting the 'Total Users' and 'Total Endpoints' counts. Below the counts, there is a table of discovered endpoints. The table has columns for Endpoint, Tags, User, MAC Address, IP Address, FortiClient UUID, Hardware / Software, Vulnerabilities, Network Location, and Last Update. The first row shows a user 'qa' with a 'Low' tag. The second row shows a user 'qa' with a 'Low' tag and an IP address of 172.17.00.5.

Endpoint	Tags	User	MAC Address	IP Address	FortiClient UUID	Hardware / Software	Vulnerabilities	Network Location	Last Update
DESKTOP-30B270R		qa				Details			2020-06-12 10:24:13
DESKTOP-M4H4T4I	Low	qa		172.17.00.5		WIN64 Details			2020-06-12 10:40:03

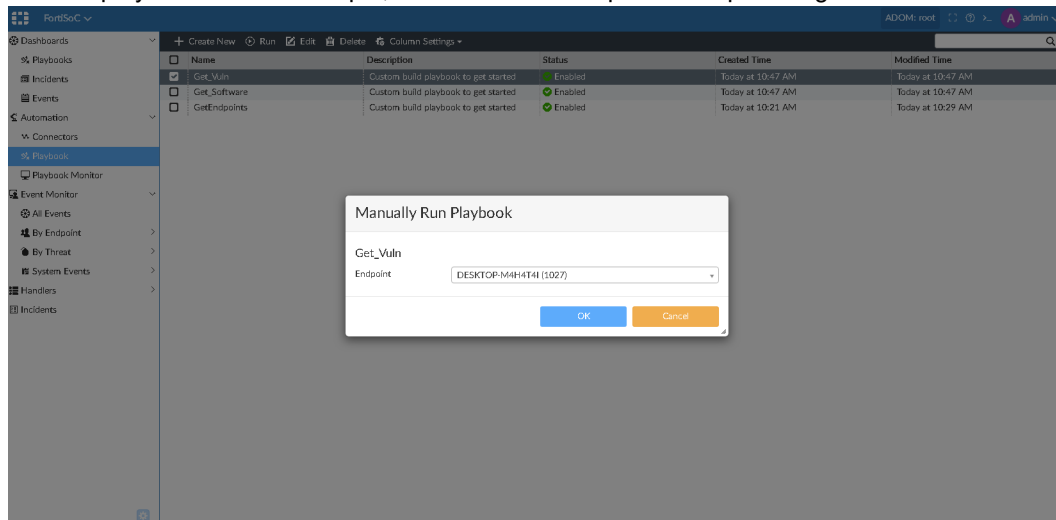


## To get vulnerability information from an EMS connector:

1. With a configured FortiClient EMS connector, create a playbook with an action to *Get Vulnerabilities*.



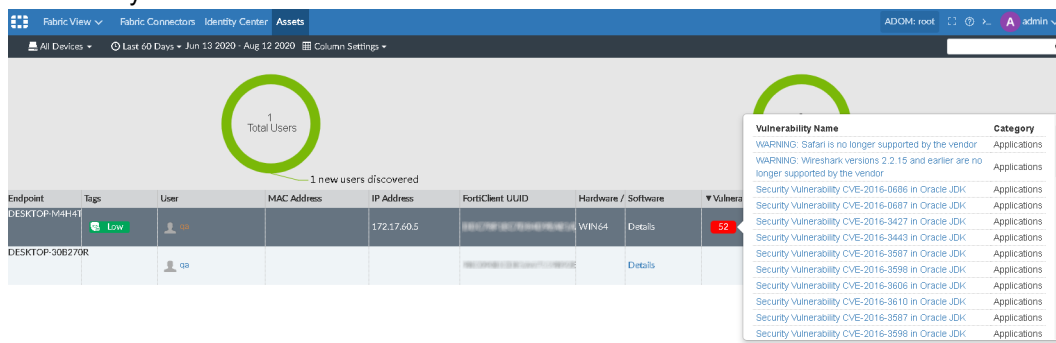
2. Run the playbook. In this example, the user selects a specific endpoint to get its vulnerabilities.



Confirm that the

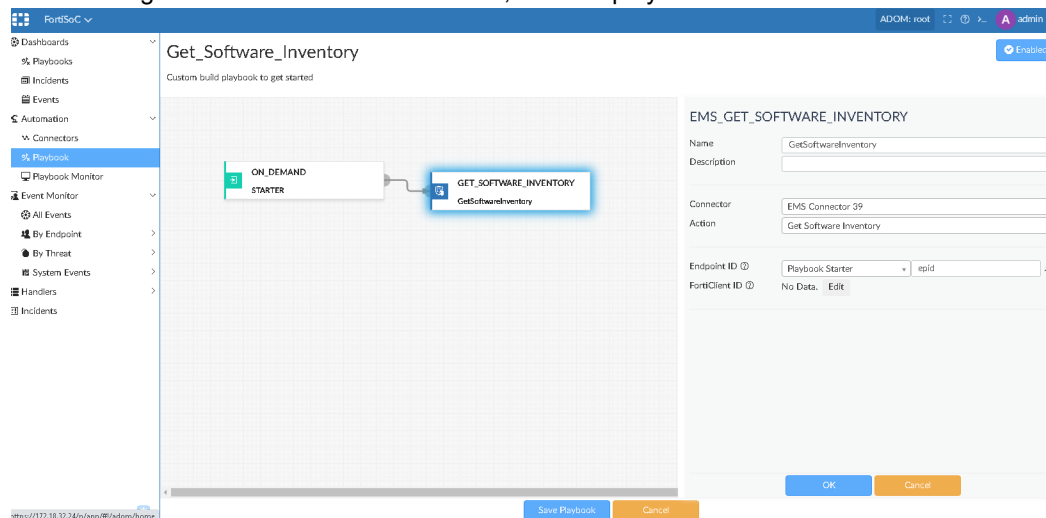
playbook has run successfully in *FortiSoC > Automation > Playbook Monitor*.

3. Go to *Fabric View > Assets*, and check the *Vulnerabilities* column. The number of *Critical* and *High* level vulnerabilities are displayed. Click on a number to view additional details. You can further drill-down on an individual vulnerability to see its details.

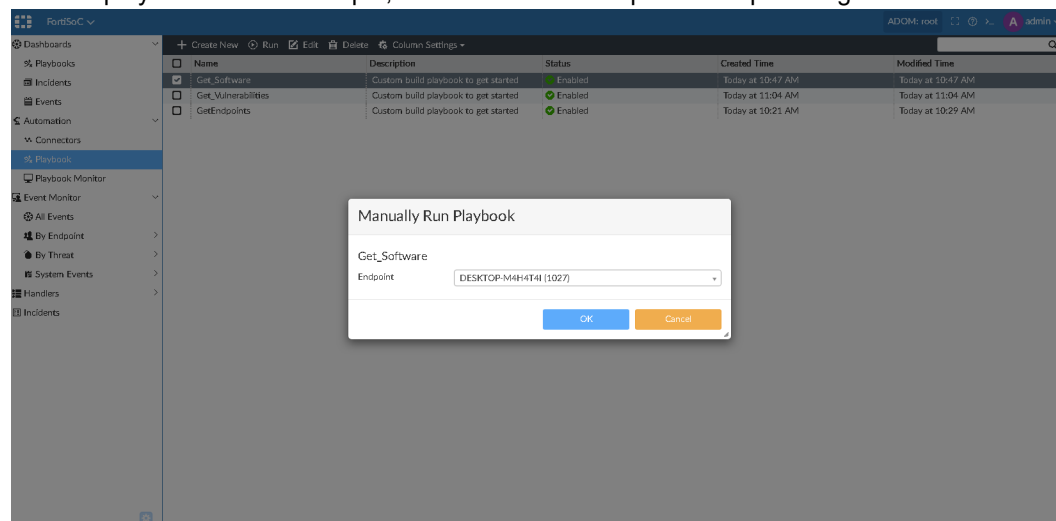


## To get software information from an EMS connector:

1. With a configured FortiClient EMS connector, create a playbook with an action to *Get Software Inventory*.



2. Run the playbook. In this example, the admin selects a specific endpoint to get its software inventory.



Confirm that the playbook has run successfully in *FortiSoC > Automation > Playbook Monitor*.

- Go to **Fabric View > Assets**, and check the **Software** column. Click on **Details** to display the software inventory retrieved from FortiClient EMS.

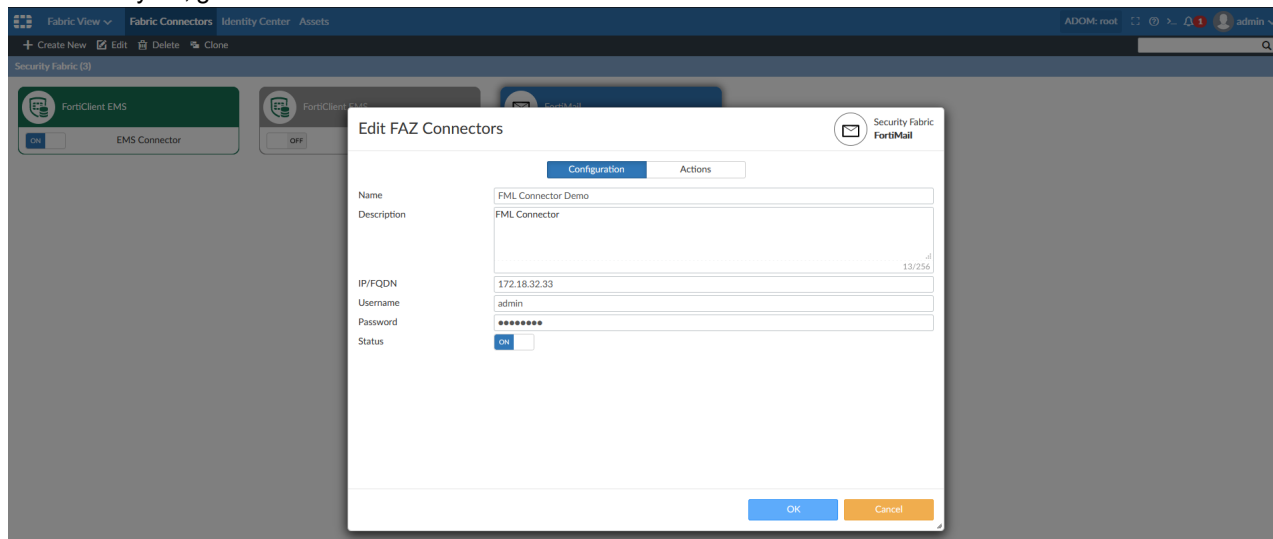
Software	Publisher	Version	Installation Path	Installation Date	First Seen	Last Seen
Add Folder Suggestions dialog	Microsoft Corporation	10.0.18362.449	C:\Windows\SystemApps\Micros	2020-05-18	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
App Installer	Microsoft Corporation	1.0.32912.0	C:\Program Files\WindowsApps\	2020-02-06	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Apple Application Support (S	Apple Inc.	3.1.3	C:\Program Files (x86)\Common I	2018-11-10	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Apple Mobile Device Support	Apple Inc.	9.0.0.26	C:\Program Files (x86)\Common I	2018-11-10	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Apple Software Update	Apple Inc.	2.1.4.131	C:\Program Files (x86)\Apple Soft	2018-11-10	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Assigned Access Lock app	Microsoft Corporation	1000.18362.449.0	C:\Windows\SystemApps\Micros	2020-05-18	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
AsyncTextService	Microsoft Corporation	10.0.18362.449	C:\Windows\SystemApps\Micros	2020-05-18	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Bonjour	Apple Inc.	3.0.0.10	C:\Program Files (x86)\Bonjour\	2018-11-10	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Candy Crush Saga	king.com	1.1800.1.0	C:\Program Files\WindowsApps\	2020-07-31	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Candy Crush Soda Saga	king.com	1.172.400.0	C:\Program Files\WindowsApps\	2020-07-31	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Captive Portal Flow	Microsoft Corporation	10.0.18362.449	C:\Windows\SystemApps\Micros	2020-05-18	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
CapturePicker	Microsoft Corporation	10.0.18362.449	C:\Windows\SystemApps\Micros	2020-05-18	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Connect	Microsoft Corporation	10.0.18362.449	C:\Windows\SystemApps\Micros	2020-05-18	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Cortana	Microsoft Corporation	1.13.0.18362	C:\Windows\SystemApps\Micros	2020-05-18	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Credential Dialog	Microsoft Corporation	10.0.18362.449	C:\Windows\SystemApps\Micros	2020-05-18	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Dolby Access	Dolby Laboratories	3.4.249.0	C:\Program Files\WindowsApps\	2020-07-31	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Email and accounts	Microsoft Corporation	10.0.18362.449	C:\Windows\SystemApps\Micros	2020-05-18	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Eye Control	Microsoft Corporation	10.0.18362.449	C:\Windows\SystemApps\Micros	2020-05-18	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Feedback Hub	Microsoft Corporation	1.1907.3152.0	C:\Program Files\WindowsApps\	2020-02-06	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00
Films & TV	Microsoft Corporation	10.20002.16211.0	C:\Program Files\WindowsApps\	2020-07-31	2020-06-12T14:00:57-07:00	2020-06-12T14:00:57-07:00

## FortiMail connector - 6.4.2

FortiMail connector on FortiAnalyzer allows playbooks to collect information from FortiMail and take containment action.

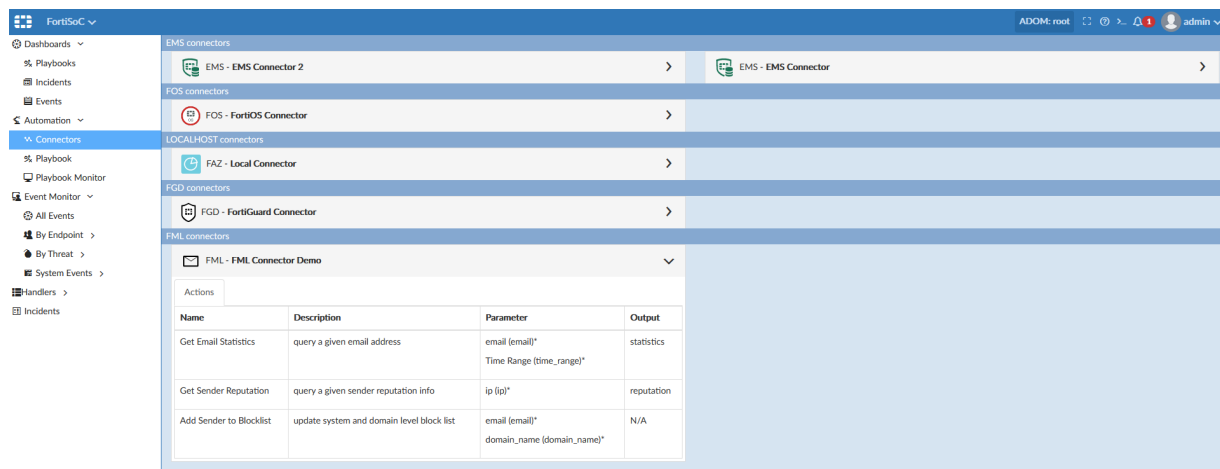
### To configure a FortiMail connector:

- Install a FortiMail device with the latest release.
- In FortiMail, create a domain and some users.
- In FortiAnalyzer, go to **Fabric View > Fabric Connectors** and create a FortiMail Connector.



- Go to **FortiSoC > Automation > Connectors** to view the actions available with the FortiMail connector. This connector supports three actions:
  - Get Email Statistics
  - Get Sender Reputation

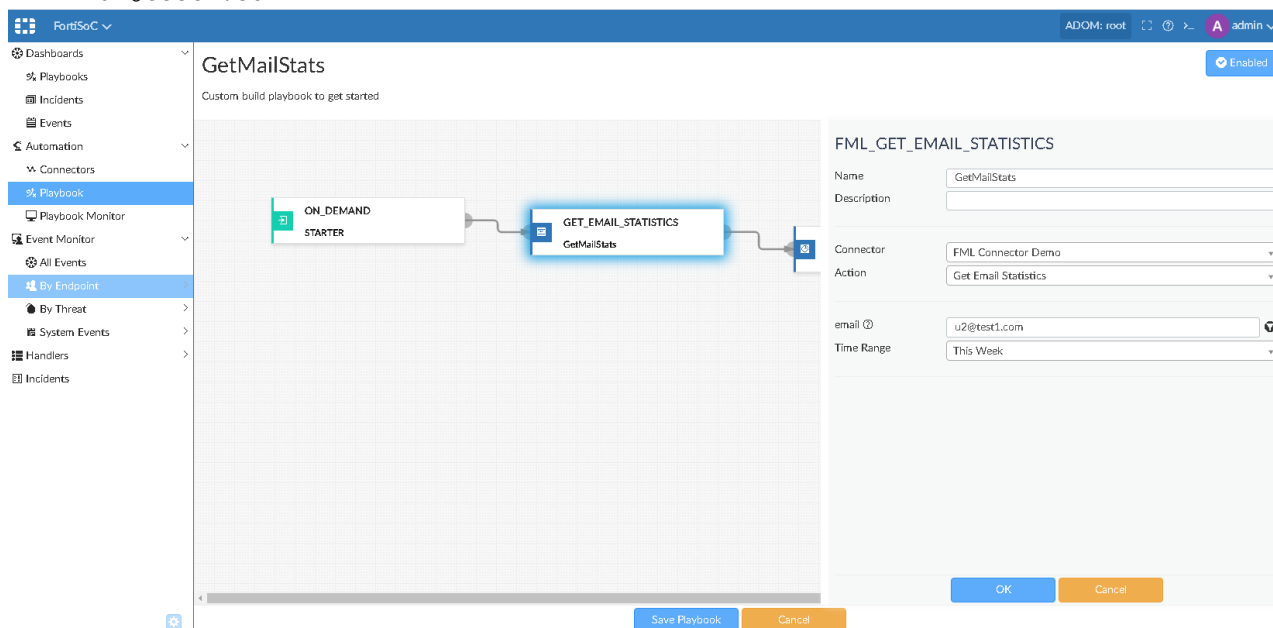
- Add Sender to Blocklist



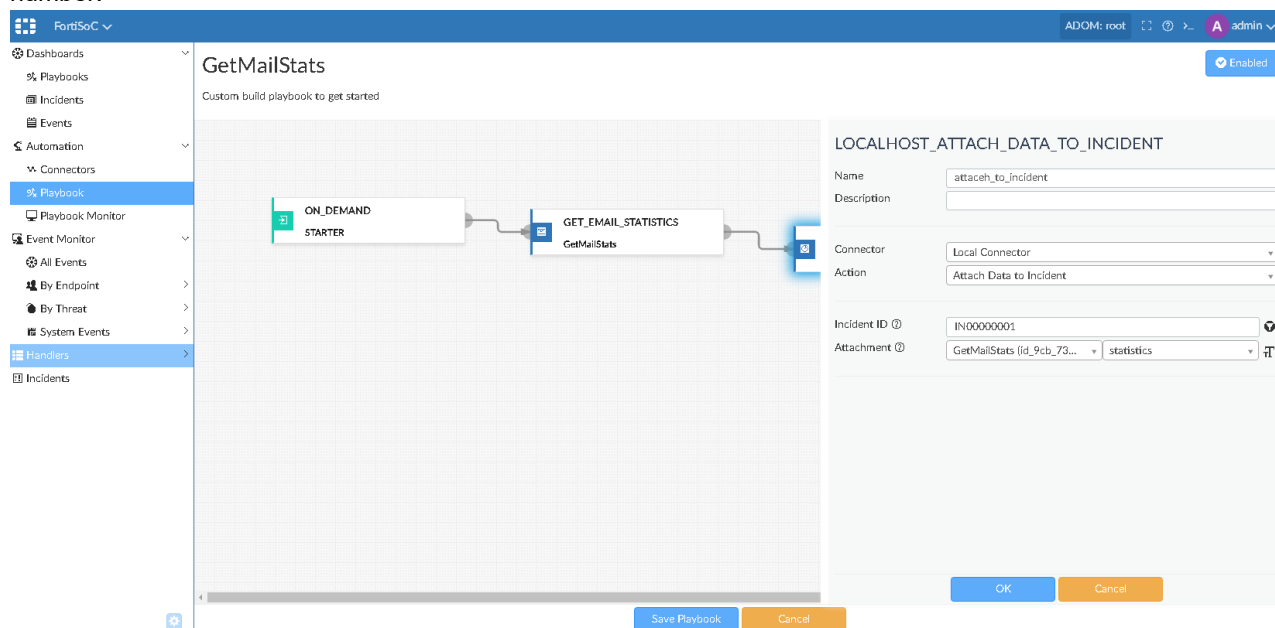
The following examples demonstrate how to create a FortiSoC playbook using FortiMail connector actions.

### To create a playbook using the Get Email Statistics action:

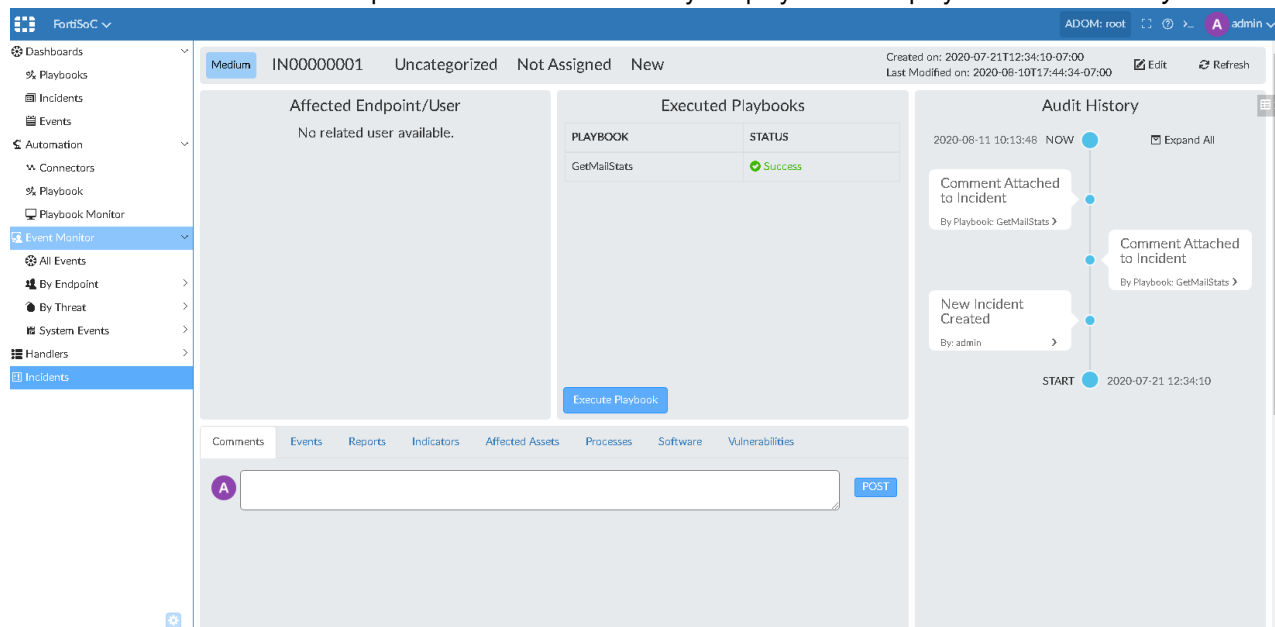
1. Go to *FortiSoC > Automation > Playbook* and create a new playbook from scratch.
2. Create a task with the action to *Get Email Statistics* using the FortiMail connector. This example gets email statistics for user `u2@test1.com`.



3. Create a second task with the action *Attach Data to Incident* using the local connector, and enter an incident number.



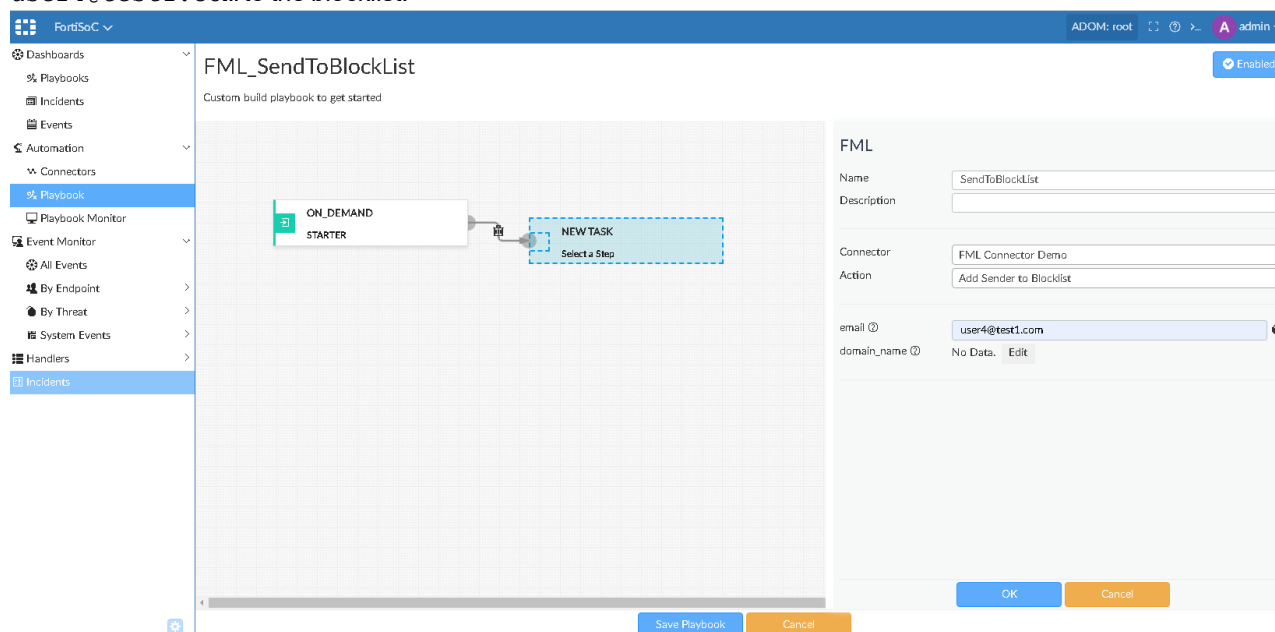
4. Save and run the playbook, and check the *Playbook Monitor* to confirm the playbook was run successfully.
5. Go to *FortiSoC > Incidents* and open the incident. The recently run playbook is displayed in *Executed Playbooks*.



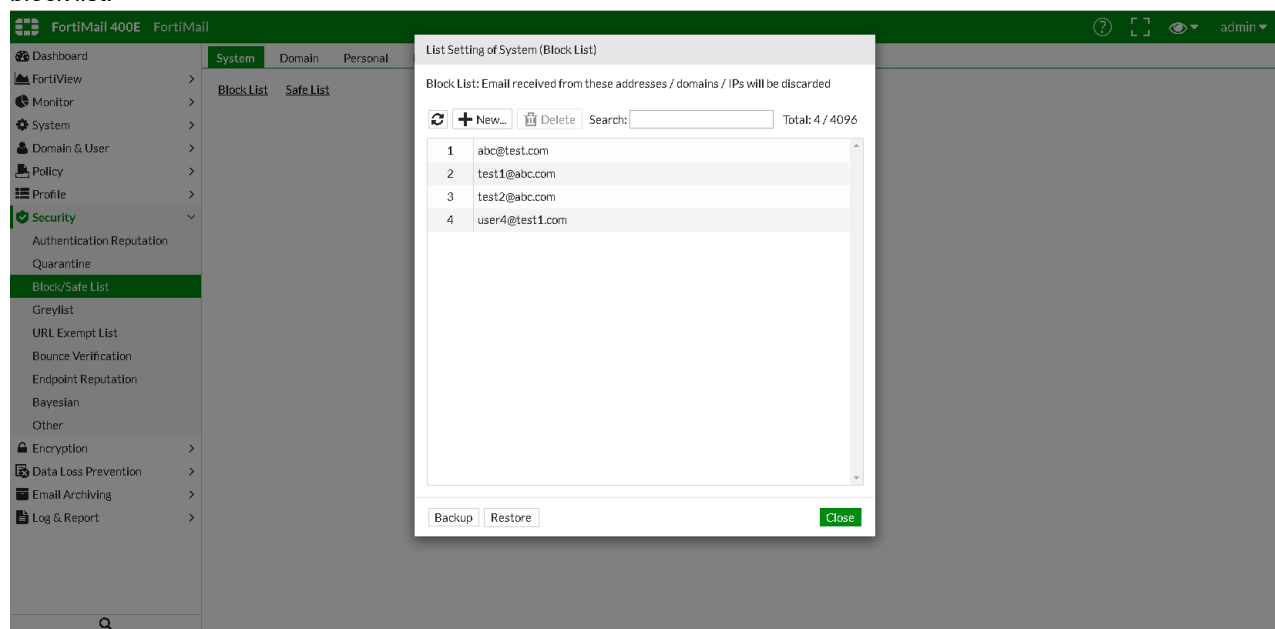
### To create a playbook using the Add Sender to Blocklist action:

1. Go to *FortiSoC > Automation > Playbook*, and create a new playbook from scratch.

2. Create a task with the action *Add Sender to Blocklist* using the FortiMail connector. This example adds user `user4@test1.com` to the blocklist.



3. Save and run the playbook, and check the *Playbook Monitor* to confirm the playbook was run successfully.
4. In FortiMail, go to *Security > Block/Safe List > System > Block List*. `user4@test1.com` has been added to the block list.



## Alerts on normalized logs - 6.4.3

Event handler support for SIEM normalized logs.

**To create an event handler for SIEM normalized logs:**

1. On FortiAnalyzer, go to *FortiSoC > Handlers > Event Handler List*, and create a new event handler.
2. Select *SIEM* in the *Log Device Type*, and complete the other settings like a normal FortiGate log based handler definition.

**Edit Handler: SIEM**

**Filter 1** ON 🗑️ ▼

Log Device Type: SIEM ▼

Log Type: SIEM Log ▼

Group By: Endpoint ▼ +  
Event Action (event\_action) ▼ 🗑️

Logs match: ☒ All ☐ Any of the following conditions

Log Field	Match Criteria	Value
<span>⊞</span> Event Type (event_type) ▼	Equal To ▼	utm + 🗑️
<span>⊞</span> Event Severity (event_severity) ▼	Greater Than or Equal To ▼	info + 🗑️

Generic Text Filter ?:   
0/1023

Generate Alert When: At least 3 Distinct ▼ Destination IP (dst\_ip) ▼ matches occurred  
over a period of 30 minutes

Event Message ?:

Event Status: ▼

☒ Allow FortiAnalyzer to choose

OK Cancel

Device and subnet filters are also supported for SIEM log handlers. Click **OK** to save the event handler.

FortiSoC

ADOM: root

admin

Dashboards

Playbooks

Incidents

Events

Automation

Connectors

Playbook

Playbook Monitor

Event Monitor

All Events

By Endpoint

By Threat

System Events

handlers

Event Handler List

FortiGate Event Handlers

Subnet List

Incidents

Edit Handler: SIEM

Status ☒

Name

Description

Devices

☐ All Devices
☒ Specify
☐ Local Device

☒ 192.168.1.1/24
☒ 192.168.1.1/24
☒ 192.168.1.1/24
☒ 192.168.1.1/24
☒ 192.168.1.1/24

Subnets

☐ All Subnets
☒ Specify

Include Subnets

☒

1 Entry Selected

Exclude Subnets

☒

1 Entry Selected

Filters (2) ☒

Filter 1 ☒

Log Device Type

Log Type

OK

Cancel

### 3. Go to **FortiSoC > Event Monitor > All Events** to check the event list for events generated by SIEM logs.

#	Event	Event ID	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler	Tags	Dt
1	Network.Service (2)											
	app_cat:Network.Service en...	2020090110000...		Others	3	Medium	2020-09-01 15:30:28	2020-09-01 15:40:28		SIEM		FV
2	192.168.22.6 (4)											
	app_cat:Network.Service en...	2020090110000...		Others	6	Medium	2020-09-01 15:00:28	2020-09-01 15:26:42		SIEM		FV
	this is a test for pass from , e...	2020090110000...		Others	45	Medium	2020-09-01 15:30:18	2020-09-01 15:42:35	extra-info: SSL...	SIEM	SIEM	FV
	this is a test for detected fro...	2020090110000...		Others	34	Medium	2020-09-01 15:30:11	2020-09-01 15:42:53	extra-info: []; fr...	SIEM	SIEM	FV
	this is a test for pass from , e...	2020090110000...		Others	86	Medium	2020-09-01 15:00:13	2020-09-01 15:29:37	extra-info: SSL...	SIEM	SIEM	FV
	this is a test for detected fro...	2020090110000...		Others	84	Medium	2020-09-01 15:00:11	2020-09-01 15:29:49	extra-info: []; fr...	SIEM	SIEM	FV
3	unscanned (8)											
	app_cat:unscanned endpoint:	2020090110000...		Others	1	Medium	2020-09-01 15:35:18	2020-09-01 15:35:18		SIEM		FV
	app_cat:unscanned endpoint:	2020090110000...		Others	1	Medium	2020-09-01 15:34:18	2020-09-01 15:34:18		SIEM		FV
	app_cat:unscanned endpoint...	2020090110000...		Others	1	Medium	2020-09-01 15:34:17	2020-09-01 15:34:17		SIEM		FV
	app_cat:unscanned endpoint...	2020090110000...		Others	224	Medium	2020-09-01 15:30:01	2020-09-01 15:42:52		SIEM		FV
	app_cat:unscanned endpoint:	2020090110000...		Others	2	Medium	2020-09-01 15:04:33	2020-09-01 15:22:43		SIEM		FV
	app_cat:unscanned endpoint:	2020090110000...		Others	2	Medium	2020-09-01 15:03:43	2020-09-01 15:19:08		SIEM		FV
	app_cat:unscanned endpoint...	2020090110000...		Others	2	Medium	2020-09-01 15:03:42	2020-09-01 15:19:07		SIEM		FV
	app_cat:unscanned endpoint...	2020090110000...		Others	794	Medium	2020-09-01 15:00:02	2020-09-01 15:29:59		SIEM		FV

Double-click a log to see related logs, or right click the log and select **View Log** from the context menu.

#	Date/Time	Data Source ID	Event Message	Event Type	Event Action	Event Severity	Source IP	Destination IP	Host
1	15:30:28	FGVM02TM2...	traffic	ip-conn		warning	::ffff:192.168.22.6	::ffff:10.2.125.18	

Data	Value
Data Parser Name	FortiGate parser
Data Source ID	FGVM02TM2...
Data Source Name	FW-93 root
Data Source Type	FortiGate
Data Timestamp	2020-09-01 15:30:31
Date/Time	15:30:28
Time Stamp	2020-09-01 15:30:28
Threat	
Threat Action	others
Threat Severity	low
Threat Type	Reconnaissance
User	
UEBA User ID	3
Network	
Destination Geo	Reserved
Destination IP	::ffff:10.2.125.18
Destination Interface	port2(lan)
Destination MAC	08:5b:0e:72:30:f2
Destination Port	514
Net Protocol	6
Net Session ID	7191260
Event	
Event Action	ip-conn
Event ID	11
Event Severity	warning
Event Sub Type	forward
Event Type	traffic
Host	
Host Hardware Vendor	Fortinet
Host IP	::ffff:192.168.22.6
Host Location	Reserved
Host MAC	00:0c:29:9b:d7:80
Host OS Family	FortiGate
Host OS Name	FortiOS
Host Type	Router
UEBA Endpoint ID	1042
Application	
Application Category	Network.Service
Application ID	41540
Application Name	SSL_TLSv1.2
Application Service	tcp/514
Others	

In the context menu, select **Search in Log View** to see all logs associated with the event.

#	Event	Event ID	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler	Tags	Dt
1	Network.Service (2)											
	app_cat:Network.Service en...	2020090110000...		Others	3	Medium	2020-09-01 15:30:28	2020-09-01 15:40:28		SIEM		FV
	app_cat:Netw...				6	Medium	2020-09-01 15:00:28	2020-09-01 15:26:42		SIEM		FV
2	192.168.22.6 (4)											
	this is a test f...				45	Medium	2020-09-01 15:30:18	2020-09-01 15:42:35	extra-info: SSL...	SIEM	SIEM	FV
	this is a test f...				34	Medium	2020-09-01 15:30:11	2020-09-01 15:42:53	extra-info: []; fr...	SIEM	SIEM	FV
	this is a test f...				86	Medium	2020-09-01 15:00:13	2020-09-01 15:29:37	extra-info: SSL...	SIEM	SIEM	FV
	this is a test f...				84	Medium	2020-09-01 15:00:11	2020-09-01 15:29:49	extra-info: []; fr...	SIEM	SIEM	FV
3	unscanned (8)											
	app_cat:unsc...				1	Medium	2020-09-01 15:35:18	2020-09-01 15:35:18		SIEM		FV
	app_cat:unsc...				1	Medium	2020-09-01 15:34:18	2020-09-01 15:34:18		SIEM		FV
	app_cat:unsc...				1	Medium	2020-09-01 15:34:17	2020-09-01 15:34:17		SIEM		FV
	app_cat:unsc...				224	Medium	2020-09-01 15:30:01	2020-09-01 15:42:52		SIEM		FV
	app_cat:unsc...				2	Medium	2020-09-01 15:04:33	2020-09-01 15:22:43		SIEM		FV
	app_cat:unscanned endpoint:	2020090110000...		Others	2	Medium	2020-09-01 15:03:43	2020-09-01 15:19:08		SIEM		FV
	app_cat:unscanned endpoint...	2020090110000...		Others	2	Medium	2020-09-01 15:03:42	2020-09-01 15:19:07		SIEM		FV
	app_cat:unscanned endpoint...	2020090110000...		Others	794	Medium	2020-09-01 15:00:02	2020-09-01 15:29:59		SIEM		FV



## Normalized logs for reports - 6.4.3

Normalized logs are supported in the report module.

### To create reports using normalized logs:

1. Go to **Reports > Report Definitions > Datasets**, and edit a dataset.  
The **Normalized** log type is available under the **SIEM** category in the **Log Type** dropdown.

**Reports** ▾ ADOM: Corp\_Logs admin ▾

**Generated Reports**  
**Report Definitions** ▾  
 All Reports  
 Templates  
 Chart Library  
 Macro Library  
**Datasets**  
 Advanced ▾  
 Language  
 Output Profile  
 Report Calendar

**Edit Dataset**

Dataset  
 Name: siem-top-source-by-count  
 Log Type: **Normalized**  
 Query:   
 Variables:   
 Test query with specified devices and time period  
 Time Period: Last 7 Days  
 Devices: ☒ All Devices ☐ Specify  
 Test Result:   
 OK Cancel

2. Click **Test** to test the dataset and view the results. Click **OK** to save the dataset.

**Reports** ▾ ADOM: Corp\_Logs admin ▾

**Generated Reports**  
**Report Definitions** ▾  
 All Reports  
 Templates  
 Chart Library  
 Macro Library  
**Datasets**  
 Advanced ▾  
 Language  
 Output Profile  
 Report Calendar

**Edit Dataset**

Dataset  
 Name: siem-top-source-by-count  
 Log Type: Normalized  
 Query: `select data_sourceid, count(*) as total from $log where $filter group by data_sourceid order by total desc`  
 Variables:   
 Test query with specified devices and time period  
 Time Period: Last N Hours  
 N: 2  
 Devices: ☒ All Devices ☐ Specify  
 Test Result: 

data_sourceid	total
FG3MAETB1900075	615361
FGT37DHA15801346	309994
FGK0003P15801076	83717
FGK0003P15800925	20433
FGK0003P15801079	4661
FG3MAETB1900053	79

 OK Cancel

Charts including normalized log data can be created using the newly created dataset.

Reports

Generated Reports

Report Definitions

All Reports

Templates

Chart Library

Macro Library

Datasets

Advanced

Language

Output Profile

Report Calendar

ADOM: Corp\_Logs

admin

Edit Chart

Name

SIEM Top Source by Count

Description

Dataset

siem-top-source-by-count

Resolve

Inherit

Hostname

Chart Type

Table

Data

Table Type

Bindings

☒ Regular

☐ Ranked

☐ Drilldown

Columns

Click to add Column

Column 1

Title

data\_sourcecid

Width

0

% (0 for Auto)

Data Binding

data\_sourcecid

Format

Default

☐ Order By

Show Top (0 for all)

0

Column 2

Title

total

Width

0

% (0 for Auto)

Data Binding

total

Format

Counter (K/M/G)

☐ Order By

Show Top (0 for all)

0

OK

Cancel

Once created, the chart can be inserted into report layouts.

Reports

Generated Reports

Report Definitions

All Reports

Templates

Chart Library

Macro Library

Datasets

Advanced

Language

Output Profile

Report Calendar

ADOM: Corp\_Logs

admin

Edit: SIEM

View Report

Settings

Layout

Insert Chart

Insert Macro

Table

Text

Image

Code

Link

Unlink

Undo

Redo

Search

Save as Template

Normal

Font

Size

B

I

U

S

x

x<sup>2</sup>

A

A

Table

Text


Image

Code

Link

Unlink

SIEM Top Source by Count



Apply

Return

After the report has been run, you can view normalized log data in the report output.

SIEM Top Source by Count

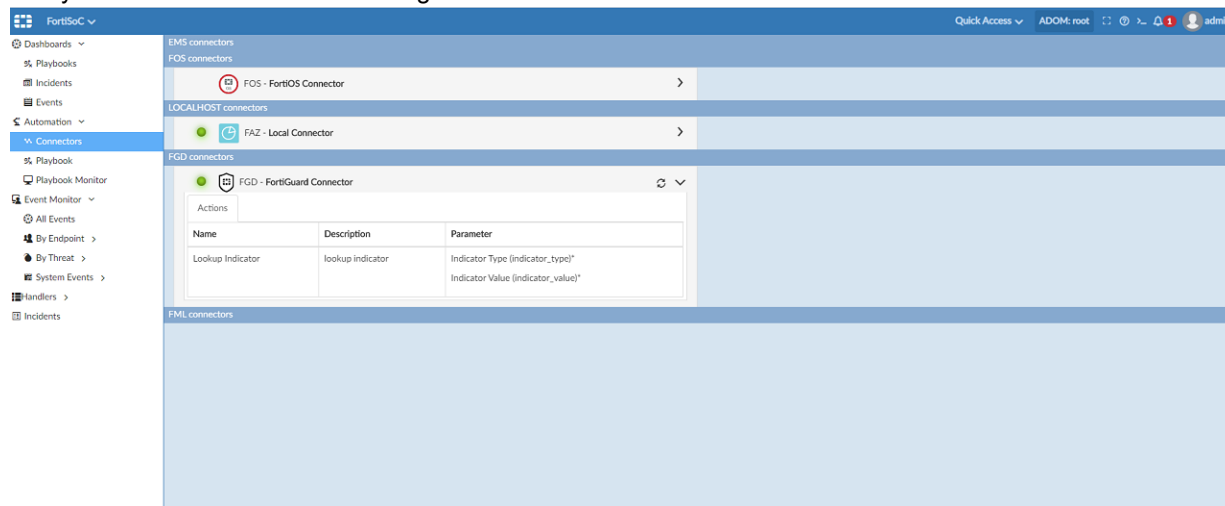
#	data_sourceid	total
1	Van_Office_FW1_Master(10.10.10.10)	832,920,593
2	Van_Office_FW2	386,010,947
3	Van_Office_FW1_Master(10.10.10.10)	374,522,855
4	Van_Office_Floor_1	138,982,273
5	New_Van_Office_Wifi	42,759,205
6	Van_Office_Floor_2	5,722,905
7	Van_Office_FW1_Master(10.10.10.10)	14,036

## FortiGuard connector - 6.4.3

The FortiGuard connector on FortiAnalyzer allows SOC playbooks to look up indicators and get threat intelligence information.

### To use the FortiGuard connector:

1. Go to *FortiSoC > Automation > Connectors* to view the FortiGuard connector.  
The FortiGuard connector is automatically installed with default actions. The FortiGuard connector is connected and ready for use when the status icon is green.



2. Go to *FortiSoC > Automation > Playbook*, and create a new playbook.

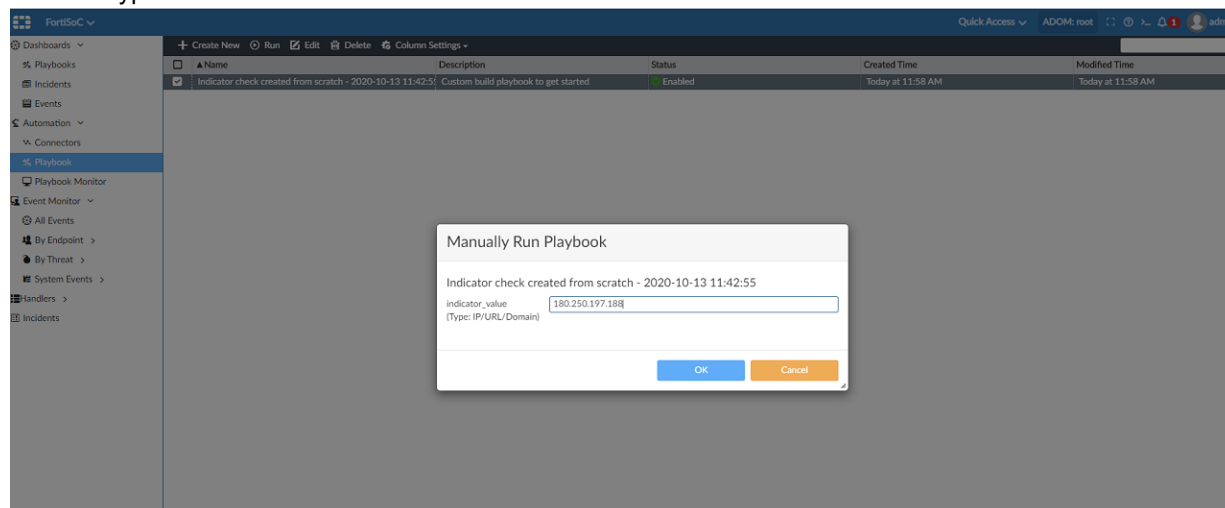
3. Create a task to perform a FortiGuard indicator lookup. Select the *FortiGuard Connector* type and the *Lookup Indicator* action. You can choose the indicator type based on your requirements (e.g. IP/URL/Domain).

The screenshot shows the FortiAnalyzer Playbook Editor interface. The left sidebar contains navigation options: Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, Handlers, and Incidents. The main canvas displays a playbook titled "Indicator check created from scratch - 2020-10-13 10:49:47". The playbook starts with an "ON\_DEMAND STARTER" block, followed by a "NEW TASK" block labeled "Select a Step". The right-hand configuration panel is set for the "FGD" connector. The "Name" field is "lookup indicator". The "Connector" is "FortiGuard Connector" and the "Action" is "Lookup Indicator". The "Indicator Type" is "IP/URL/Domain" and the "Indicator Value" is "indicator\_value".

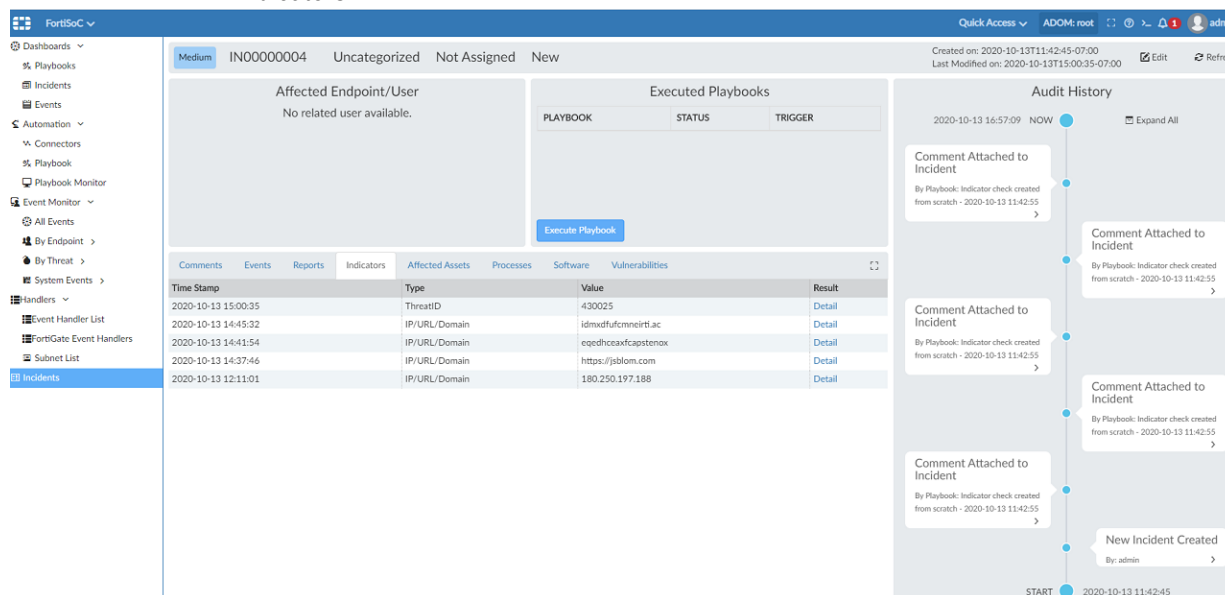
4. Create another task to attach data to an incident. Select the *Local Connector* type and *Attach Data to Incident* action. Enter an *Incident ID* and then save the playbook.

The screenshot shows the FortiAnalyzer Playbook Editor interface. The left sidebar is the same as in the previous screenshot. The main canvas displays a playbook titled "Indicator check created from scratch - 2020-10-13 11:42:55". The playbook starts with an "ON\_DEMAND STARTER" block, followed by an "FGD\_LOOKUP\_INDICATOR" block labeled "lookup indicator", and then a "NEW TASK" block labeled "Select a Step". The right-hand configuration panel is set for the "LOCALHOST" connector. The "Name" field is "attached result". The "Connector" is "Local Connector" and the "Action" is "Attach Data to Incident". The "Incident ID" field contains the value "IN00000004". The "Attachment" field is set to "lookup indicator [id\_a3c\_...]" under the "indicators" category.

5. Manually run the playbook. You will see a prompt to input the value of an indicator according to the configured indicator type.



6. Go to *FortiSoC > Automation > Playbook Monitor* to confirm that the playbook has run successfully. Once complete, go to *FortiSoC > Incidents* to view the incident you configured in the playbook. The FortiSoC indicators are attached to the incident in the *Indicators* tab.



Click *Detail* to drilldown for additional information about the indicator.

The screenshot shows the FortiSoC interface with an incident detail view. The incident is 'Medium' severity, 'IN00000004', 'Uncategorized', and 'Not Assigned'. It was created on 2020-10-13T11:42:45-07:00 and last modified on 2020-10-13T15:00:35-07:00. The interface shows a table of affected assets with columns for Time Stamp, Type, Value, and Result. An 'Information' modal is open on the right, displaying details for the indicator 'W32/Buzus.AEWtr', including its name, action, and analysis.

Time Stamp	Type	Value	Result
2020-10-13 15:00:35	ThreatID	430025	Detail
2020-10-13 14:45:32	IP/URL/Domain	idmxdofufcmncirtiac	Detail
2020-10-13 14:41:54	IP/URL/Domain	eqedhceafcapstenox	Detail
2020-10-13 14:37:46	IP/URL/Domain	https://jdlolm.com	Detail
2020-10-13 12:11:01	IP/URL/Domain	180.250.197.188	Detail

**Information**

**Name**  
W32/Buzus.AEWtr

**Action**

**FortiGate Systems**

- Check the main screen using the web interface for your FortiGate unit to ensure that the latest AV/NIIDS database has been downloaded and installed on your system - if required, enable the "Allow Push Update" option.

**FortiClient Systems**

- Quarantine/delete files that are detected and replace infected files with clean backup copies.

**Analysis**

W32/Buzus.AEWtr is classified as a Trojan.

Trojan has the capabilities to remote access connection handling, perform Denial of Service (DoS) or Distributed DoS (DDoS), capture keyboard inputs, delete file or object, or terminate process.

The Fortinet Anti-Virus Analyst Team is currently in the process of creating a detailed description for this virus.

**Miscellaneous**

ID	430025
Discovered	Feb 12, 2008
Created	Feb 12, 2008
Updated	Feb 12, 2008

Show Raw Data Close

## Connector's health check - 6.4.3

This enhanced feature provides visibility on the status of connectors.

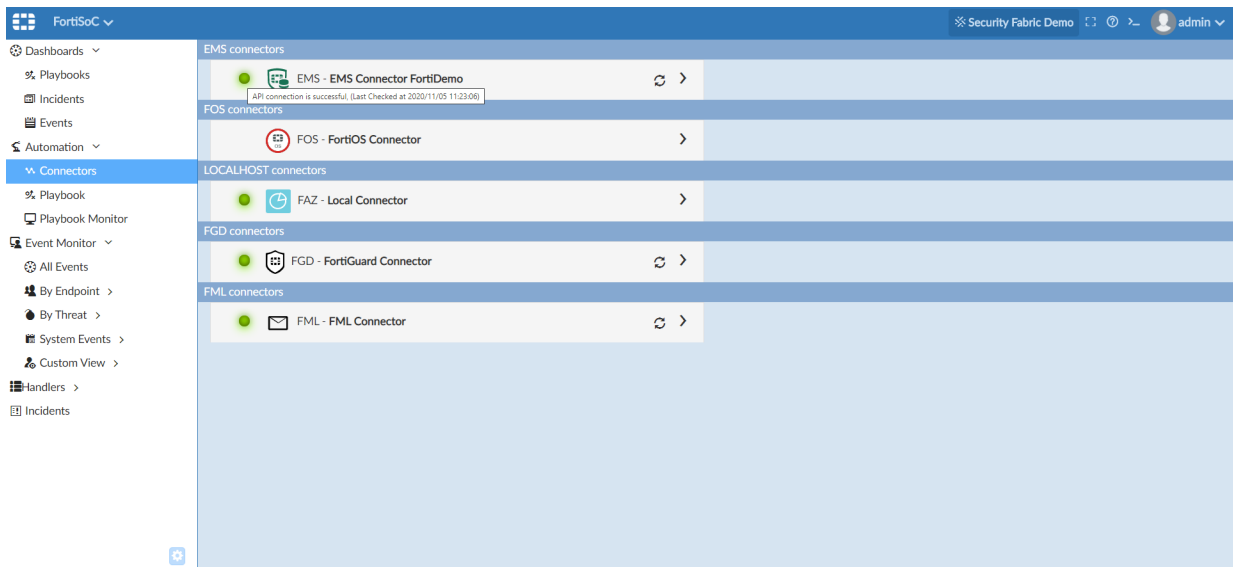
To view the status of FortiSoC connectors:

1. Go to *FortiSoC > Automation > Connectors*.

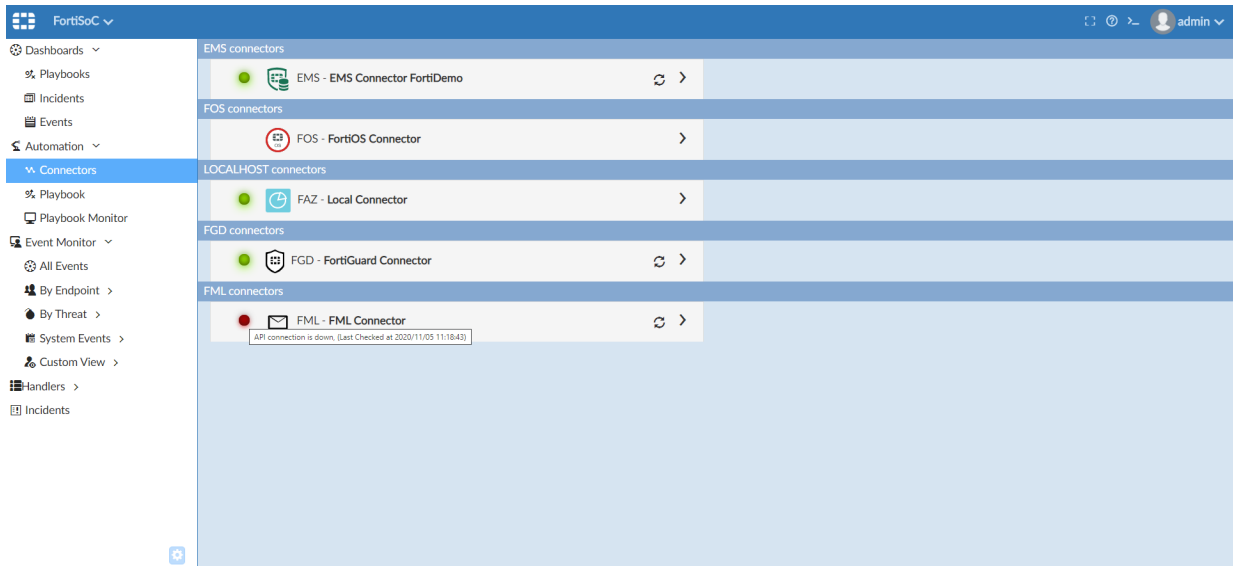
You can see health status and refresh icons for each connector.

The screenshot shows the FortiSoC Connectors page. The page displays a list of connectors categorized by type: EMS, FOS, LOCALHOST, FGD, and FML. Each connector has a health status icon (green for healthy, red for unhealthy) and a refresh icon. The connectors listed are: EMS - EMS Connector FortiDemo, FOS - FortiOS Connector, FAZ - Local Connector, FGD - FortiGuard Connector, and FML - FML Connector.

Click the refresh icon to refresh the status of a connector. Mouse over the health status icon to view detailed status information, including when the connector status was last updated.



When a connector is down, mouse over the health status icon to view additional information about why the connector is unavailable.



## FortiGuard outbreak and alert service - 6.4.6

The FortiGuard Outbreak Alert Service is available with a valid FOAS license to protect customers' networks against malware outbreaks. The Outbreak Alert content package consists of a FortiGuard Report for the outbreak, an Event Handler, and a Report Template to detect the outbreak.

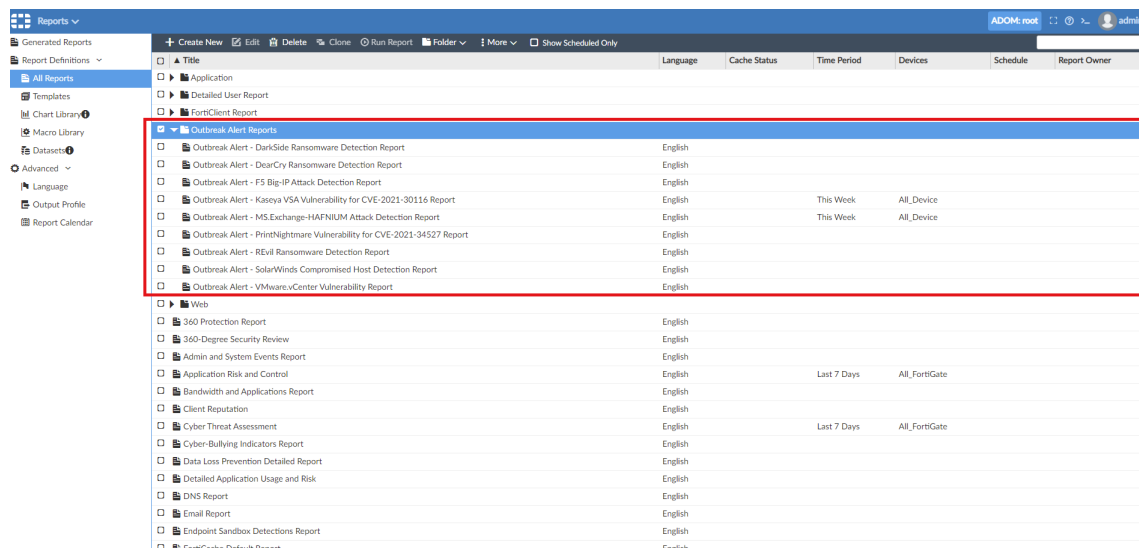
## To view outbreak alerts, reports, and event handlers:

1. Go to **FortiSoC > Outbreak Alerts**. Available outbreak alerts are displayed and can be browsed in all ADOMs.

2. Go to **FortiSoC > Handlers > Event Handler List**. Corresponding outbreak alert event handlers are installed and listed in related ADOMs automatically. The events can be triggered by logs which satisfy the event handlers' filter conditions.

3. Go to **Reports > Report Definitions > All Reports**.  
A new **Outbreak Alert Reports** folder is available in all ADOMs. All outbreak reports are stored in this folder. Right click a report to run the report. Reports can be generated in HTML, PDF, XML, and CSV formats.





Below is an example of the *Hafnium M.S.Exchange Attack Detection Report*.

### Summary

This report displays the findings on attack attempts to exploit MS. Exchange vulnerabilities from Fortigate.

This table shows detections by FortiGate IPS:

#### FortiGate IPS Detection

#	Device	Source	Destination	Attack	Total Count	First Seen	Last Seen
1	Van_Office_FW1_Master	172.16.68.21	111.206.21.0.75	HTTP.Unknown.Tunnelling	3	2021-04-13 18:12:50	2021-04-13 20:44:44
2	Van_Office_FW1_Master	172.18.34.2	74.125.124.94	TCP.PORT0	3	2021-04-13 18:12:50	2021-04-13 20:44:44
3	Van_Office_FW1_Master	172.16.197.102	10.50.0.0	TCP.PORT0	3	2021-04-13 18:12:50	2021-04-13 20:44:44
4	Van_Office_FW1_Master	172.16.171.64	172.18.22.4	MS.Exchange.Server.UM.Core.Remote.Co.de.Execution	3	2021-04-13 18:12:50	2021-04-13 20:44:44
5	FGT91E4Q16000534	172.16.68.21	111.206.21.0.75	HTTP.Unknown.Tunnelling	1	2021-04-13 18:15:19	2021-04-13 18:15:19
6	FGT91E4Q16000534	172.16.171.64	172.18.22.4	MS.Exchange.Server.UM.Core.Remote.Co.de.Execution	1	2021-04-13 18:15:19	2021-04-13 18:15:19
7	FGT91E4Q16000534	172.18.34.2	74.125.124.94	TCP.PORT0	1	2021-04-13 18:15:19	2021-04-13 18:15:19
8	FGT91E4Q16000534	172.16.197.102	10.50.0.0	TCP.PORT0	1	2021-04-13 18:15:19	2021-04-13 18:15:19

This table shows detections by FortiGate AV:

#### FortiGate AV Detection

#	Device	Source	Destination	Virus	Total Count	First Seen	Last Seen
1	Van_Office_FW1_Master	10.2.60.143	10.2.175.110	HTML/AgentA121ltr	1	2021-04-13 20:44:55	2021-04-13 20:44:55
2	Van_Office_FW1_Master	10.2.60.143	10.2.175.110	ASP/WebShell.cltr	1	2021-04-13 20:44:55	2021-04-13 20:44:55

4. When FortiAnalyzer does not have a valid FOAS license, a default Fortinet Outbreak Alert page is displayed with a warning that the service is not available in this ADOM yet.

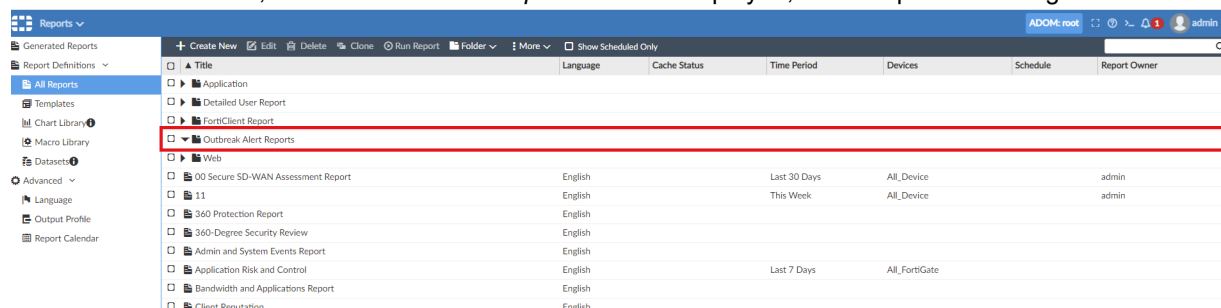


5. Go to **FortiSoC > Handlers > Event Handler List**.  
Without a valid license, no outbreak related event handlers are available.

Status	Name	Filters	Devices	Send Alert to	Events	Included Subnets	Excluded Subnets
✓	Local Device Event	> 1 Filter	Local Device		1802		
✓	Default-Botnet-Communication-Detection-By-Threat	> 9 Filters	All Devices				
✓	Default-Compromised Host-Detection-IOC-By-Threat	> 3 Filters	All Devices				
✓	Default-Malicious-Code-Detection-By-Threat	> 8 Filters	All Devices				
✓	Default-Risky-Destination-Detection-By-Threat	> 15 Filters	All Devices				
✓	Default-Risky-App-Detection-By-Threat	> 2 Filters	All Devices				
✓	Default-Malicious-File-Detection-By-Threat	> 8 Filters	All Devices				
✓	Default-Risky-App-Detection-By-Endpoint	> 4 Filters	All Devices				
✓	Default-Malicious-File-Detection-By-Endpoint	> 24 Filters	All Devices				
✓	Default-Malicious-Code-Detection-By-Endpoint	> 8 Filters	All Devices				
✓	Default-Risky-Destination-Detection-By-Endpoint	> 14 Filters	All Devices				
✓	Default-Compromised Host-Detection-IOC-By-Endpoint	> 3 Filters	All Devices				
✓	Default-Botnet-Communication-Detection-By-Endpoint	> 9 Filters	All Devices				
✗	Default-FFW System Events	> 8 Filters	All Devices				
✗	Default-FFW-Compromised Host-Detection-IOC-By-Threat	> 3 Filters	All Devices				
✗	Default-FFW-Risky-Destination-Detection-By-Threat	> 10 Filters	All Devices				
✗	Default-FFW-Risky-Destination-Detection-By-Endpoint	> 10 Filters	All Devices				
✗	Default-FFW-Compromised Host-Detection-IOC-By-Endpoint	> 2 Filters	All Devices				
✗	Default-FFW-Botnet-Communication-Detection-By-Endpoint	> 1 Filter	All Devices				
✗	Default-FFW-Threat-Detection-By-Hostname	> 4 Filters	All Devices				
✗	Default-FCT-Threat-Detection-By-Threat	> 2 Filters	All Devices				
✗	Default-FCT-Threat-Detection-By-Endpoint	> 3 Filters	All Devices				
✗	Default-FSA-Malware-Handler-By-Threat	> 6 Filters	All Devices				
✗	Default-FSA-Malware-Handler-By-Endpoint	> 4 Filters	All Devices				
✗	Default-FSA-System-Handler	> 3 Filters	All Devices				
✗	Default-FML-Threat-Detection-By-Email	> 11 Filters	All Devices				
✗	Default-FOS System Events	> 8 Filters	All Devices				
✗	Default-Data-Leak-Detection-By-Threat	> 2 Filters	All Devices				

## 6. Go to *Reports > Report Definitions > All Reports*.

Without a valid license, the *Outbreak Alerts Reports* folder is displayed, but no reports are assigned to it.



## Advanced threat protection

This section lists the new features added to FortiAnalyzer for advanced threat protection.

List of new features:

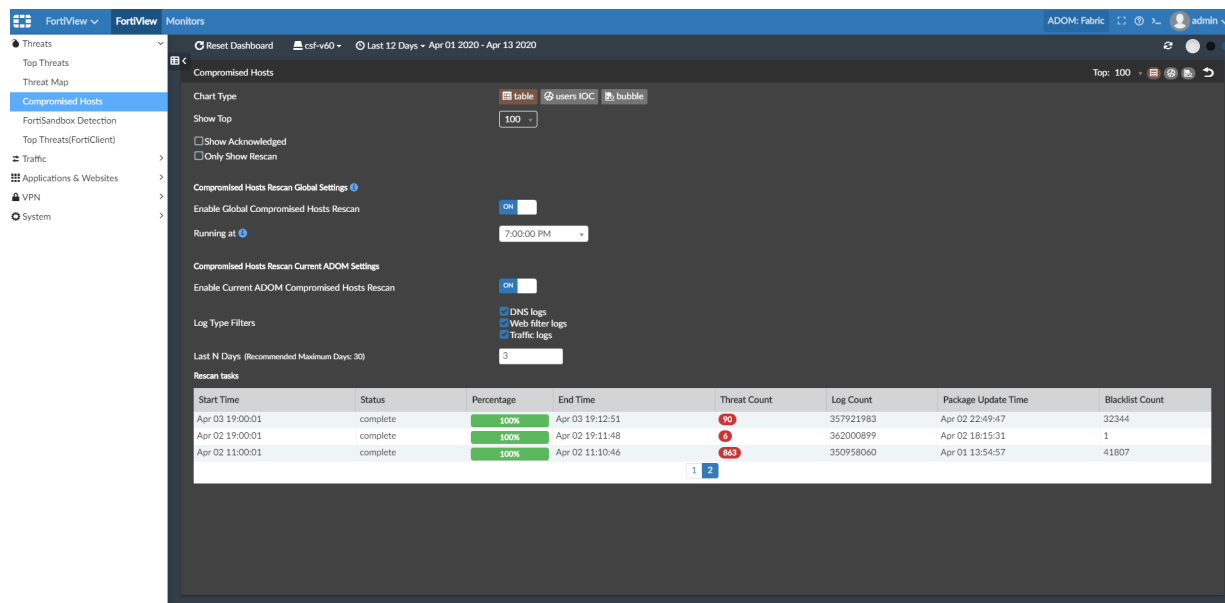
- [IoC re-scan events on page 101](#)
- [FortiDeceptor logging on page 105](#)
- [Unique count for event handler 6.4.2 on page 107](#)
- [FortiGate C&C Detection in SOC View 6.4.3 on page 108](#)
- [FortiADC logging 6.4.3 on page 111](#)

## IoC re-scan events

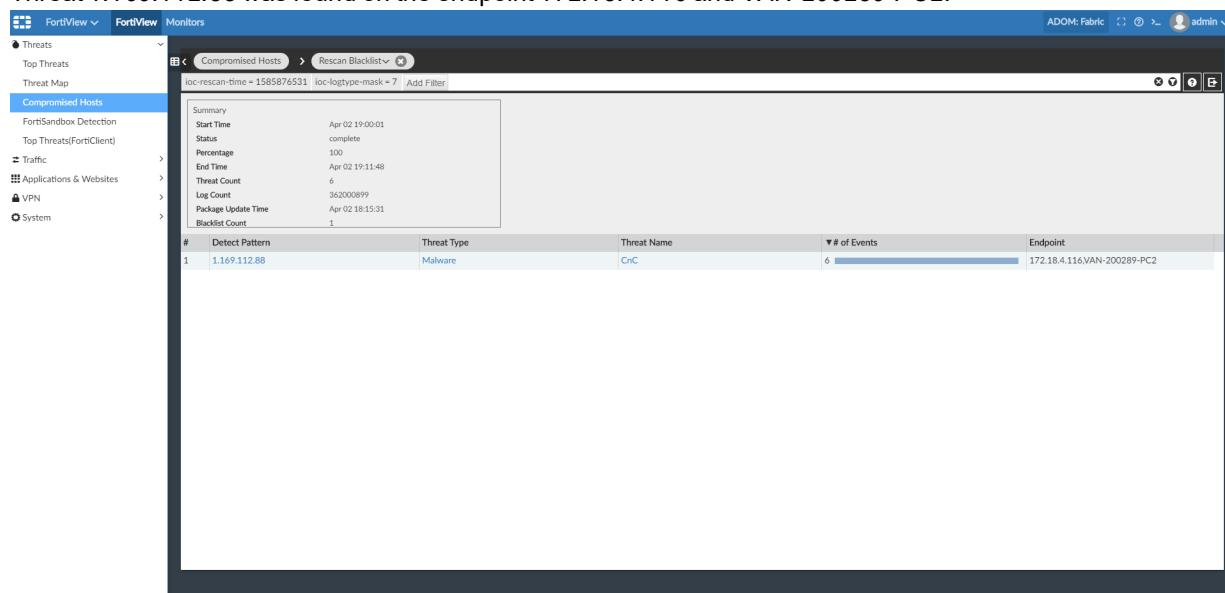
Event Handlers can generate events for compromised hosts detected by the IoC rescan feature.

### Example of viewing IoC re-scanned events:

1. Go to *FortiView > FortiView > Threats > Compromised Hosts*, and click the settings icon to configure global and ADOM rescan settings.

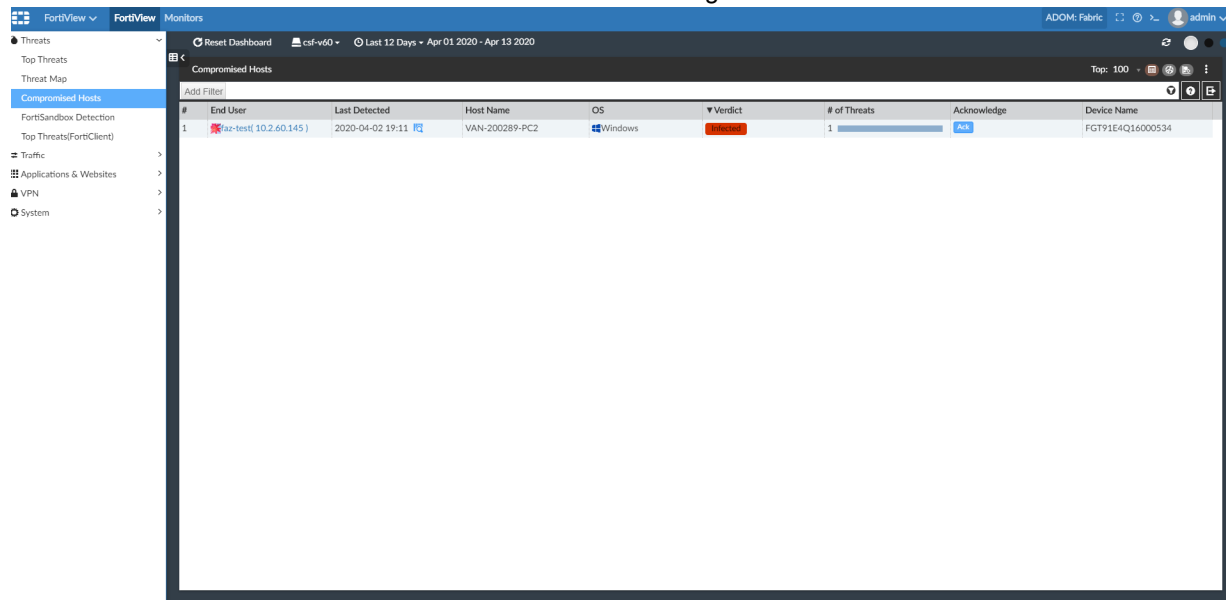


- In the rescan task list, select a task and click on a threat count (red circle) to view the rescan result. Threat 1.169.112.88 was found on the endpoint 172.18.4.116 and VAN-200289-PC2.

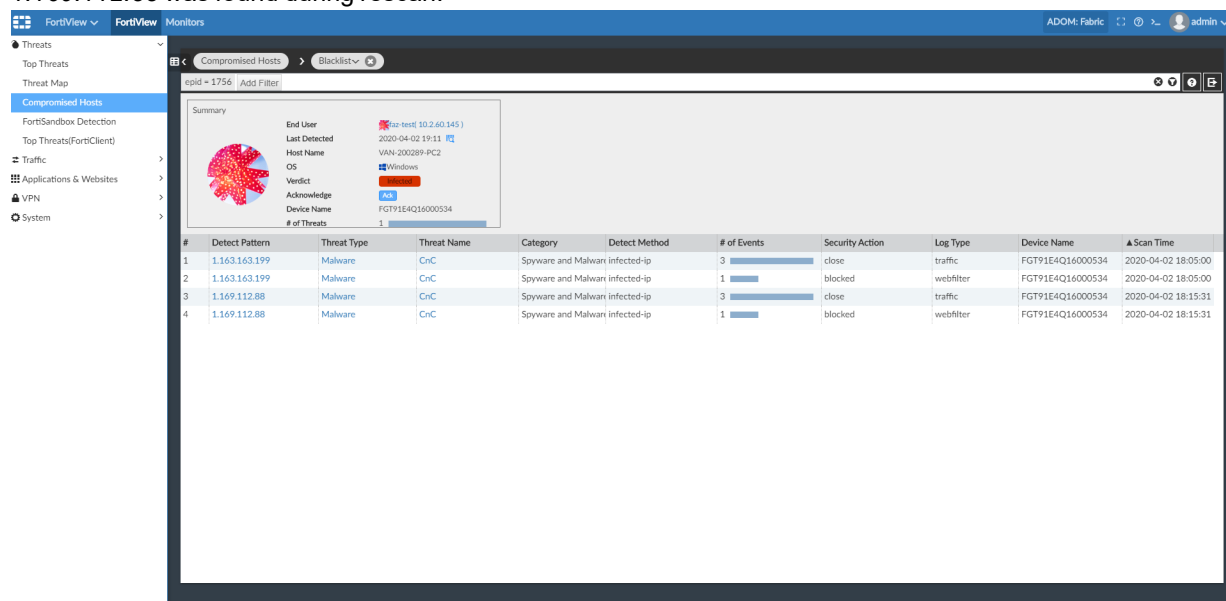


- Go to FortiView > FortiView > Threats > Compromised Hosts. For the end user faz-test(10.2.60.145) on endpoint VAN-200289-PC2, a rescan icon is displayed in the Last

*Detected* column to indicate that there were threats found during rescans.



4. Go to the drilldown view for the end user to view the detected threat patterns. For end user *faz-test(10.2.60.145)* there are two threat patterns: *1.163.163.199* was found by real-time logs, and *1.169.112.88* was found during rescans.



5. Go to *FortiSoC > Handlers > Event Handler List*. The *ioc\_rescan* tag is added in all filters for the following default event handlers: *Default-Compromised Host-Detection-IOC-By-Endpoint* and *Default-Compromised Host-Detection-IOC-By-Threat*. For comparison, there is no *ioc\_rescan* tag for any filters in the custom event handlers: *Copy of Default-Compromised Host-Detection-IOC-By-Endpoint* and *Copy of Default-Compromised Host-Detection-IOC-By-*

**Threat.**

Status	Name	Filters	Devices	Send Alert to	Events
✓	Default-Compromised Host-Detection-IOC-By-Threat	3 Filters Filter 1 (Default.By_Threat,IP,C&C,Ioc_Rescan) tdtype-infected Filter 2 (Default.By_Threat,C&C,URL,Ioc_Rescan) tdtype-infected Filter 3 (Default.By_Threat,C&C,Domain,Ioc_Rescan) tdtype-infected	All Devices		13248
✓	Default-Compromised Host-Detection-IOC-By-Endpoint	3 Filters Filter 1 (Default.By_Endpoint,IP,C&C,Ioc_Rescan) tdtype-infected Filter 2 (Default.By_Endpoint,C&C,URL,Ioc_Rescan) tdtype-infected Filter 3 (Default.By_Endpoint,C&C,Domain,Ioc_Rescan) tdtype-infected	All Devices		756
✓	Copy of Default-Compromised Host-Detection-IOC-By-Endpoint	3 Filters Filter 1 (IP,C&C) tdtype-infected Filter 2 (C&C,URL) tdtype-infected Filter 3 (C&C,Domain) tdtype-infected	All Devices		112
✓	Copy of Default-Compromised Host-Detection-IOC-By-Threat	3 Filters Filter 1 (IP,C&C) tdtype-infected Filter 2 (C&C,URL) tdtype-infected Filter 3 (C&C,Domain) tdtype-infected	All Devices		2222
✗	Default-FWB-Threat-Detection-By-Hostname	4 Filters	All Devices		
✗	Default-FCT-Threat-Detection-By-Threat	2 Filters	All Devices		
✗	Default-FCT-Threat-Detection-By-Endpoint	3 Filters	All Devices		
✗	Default-FSA-Malware-Handler-By-Threat	6 Filters	All Devices		

6. Go to **FortiSoC > Event Monitor > All Events** and view alerts for the Default-Compromised Host-Detection-IOC-By-Threat handler.

The *ioc\_rescan* tag exists for threat 1.169.112.88 because they are generated by rescan logs. There is no *ioc\_rescan* tag for threat 1.163.163.199 because they are generated by real-time logs.

#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler	Tags	Device Name
1	√ 1.169.112.88 (2)	Unhandled	Traffic	3	Critical	2020-04-02 18:10:45	2020-04-02 18:10:50	Traffic to C&C:1.16...	Default-Compromised H...	IP   C&C   Ioc_Rescan	HA91E_FGT91E
	Web traffic to C&C from ...	Unhandled	Web Filter	1	Critical	2020-04-02 18:10:43	2020-04-02 18:10:43	Traffic to C&C:1.16...	Default-Compromised H...	C&C   URL   Ioc_Rescan	HA91E_FGT91E
2	√ 1.163.163.199 (2)	Unhandled	Traffic	3	Critical	2020-04-02 18:05:34	2020-04-02 18:05:39	Traffic to C&C:1.16...	Default-Compromised H...	IP   C&C	HA91E_FGT91E
	Web traffic to C&C from ...	Unhandled	Web Filter	1	Critical	2020-04-02 18:05:32	2020-04-02 18:05:32	Traffic to C&C:1.16...	Default-Compromised H...	C&C   URL	HA91E_FGT91E

7. View alerts for the Copy of Default-Compromised Host-Detection-IOC-By-Threat handler.  
There are no alerts for threat 1.169.112.88 because the handler does not process rescan logs. There are alerts

without the `ioc_rescan` tag for threat `1.163.163.199` because the handler still processes real-time logs.

The screenshot shows the FortiAnalyzer interface with a table of events. The table has columns: #, Event, Event Status, Event Type, Count, Severity, First Occurrence, Last Update, Additional Info, Handler, Tags, and Device Name. Two events are listed for threat 1.163.163.199.

#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler	Tags	Device Name
1	Traffic to C&C from VAN...	Unhandled	Traffic	3	Critical	2020-04-02 18:05:34	2020-04-02 18:05:39	Traffic to C&C:1.16...	Copy of Default-Comp...	IP   C&C	HA91E_FGT91E
	Web traffic to C&C from ...	Unhandled	Web Filter	1	Critical	2020-04-02 18:05:32	2020-04-02 18:05:32	Traffic to C&C:1.16...	Copy of Default-Comp...	C&C   URL	HA91E_FGT91E

## FortiDeceptor logging

FortiDeceptor logs are supported on FortiAnalyzer.

**To view FortiDeceptor logs on FortiAnalyzer:**

1. On FortiDeceptor, go to *Log > Log Servers*, and click *Create New* to create a new remote log server.

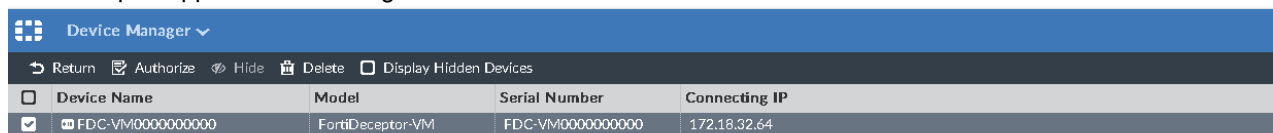
The screenshot shows the FortiDeceptor interface with the 'Log Servers' configuration page. The page has a sidebar with navigation options: Dashboard, Deception, Customization, Deception OS, Deployment Network, Deployment Wizard, Decoy & Lure Status, Decoy Map, Whitelist, Incident, Fabric, Network, System, Log, and Log Servers. The main content area is titled 'New Remote Log Server' and contains the following fields:

- Name: To\_Test\_FAZ
- Type: FortiAnalyzer
- Log Server Address: 172.18.32.65
- Port: 514
- Status: ☒ Enable ☐ Disable
- ☒ Alert Logs
- ☒ Critical Logs
- ☒ Error Logs
- ☒ Warning Logs
- ☒ Information Logs
- ☒ Debug Logs

At the bottom right, there are 'OK' and 'Cancel' buttons.

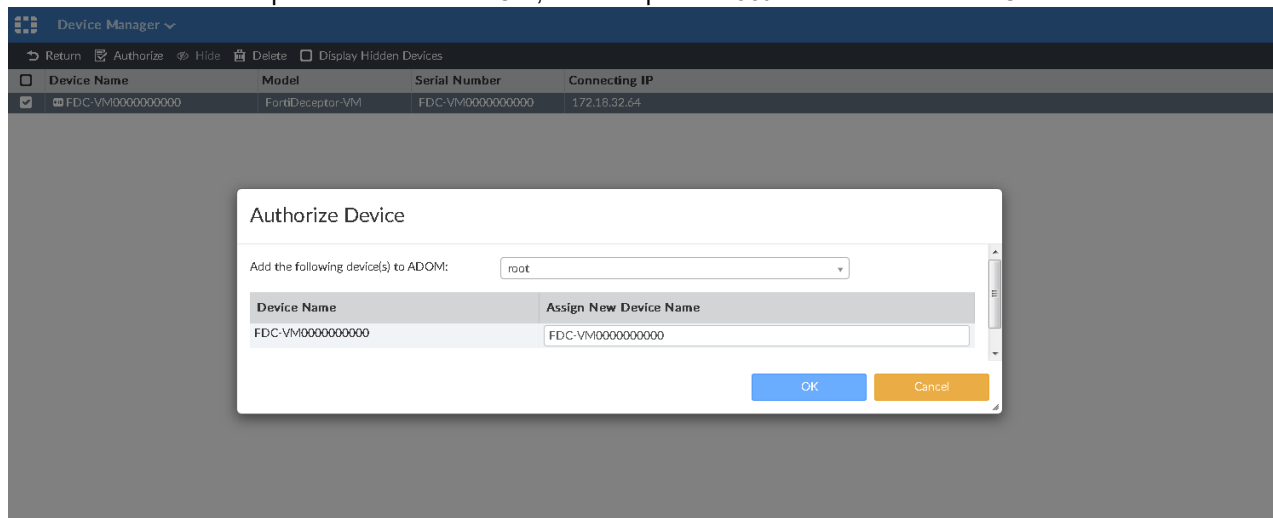
2. Configure the following details:
  - Enter a name for the remote log server. For example: `To_Test_FAZ`.
  - Select *FortiAnalyzer* as the server *Type*.
  - Keep the default settings for all other options.

3. On FortiAnalyzer, go to *Device Manager > Unauthorized*. FortiDeceptor appears in the unregistered devices table.



Device Name	Model	Serial Number	Connecting IP
FDC-VM0000000000	FortiDeceptor-VM	FDC-VM0000000000	172.18.32.64

4. Authorize the FortiDeceptor device to an ADOM, for example the *root* which is a Fabric ADOM.



Device Manager

Return Authorize Hide Delete Display Hidden Devices

Device Name	Model	Serial Number	Connecting IP
FDC-VM0000000000	FortiDeceptor-VM	FDC-VM0000000000	172.18.32.64

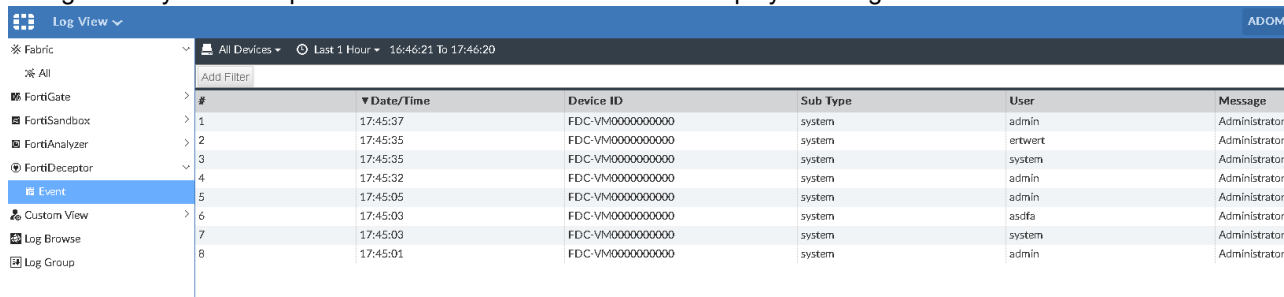
Authorize Device

Add the following device(s) to ADOM: root

Device Name	Assign New Device Name
FDC-VM0000000000	FDC-VM0000000000

OK Cancel

All logs sent by FortiDeceptor are stored in the root ADOM and displayed in Log View.



#	Date/Time	Device ID	Sub Type	User	Message
1	17:45:37	FDC-VM0000000000	system	admin	Administrator
2	17:45:35	FDC-VM0000000000	system	ertwert	Administrator
3	17:45:35	FDC-VM0000000000	system	system	Administrator
4	17:45:32	FDC-VM0000000000	system	admin	Administrator
5	17:45:05	FDC-VM0000000000	system	admin	Administrator
6	17:45:03	FDC-VM0000000000	system	asdfa	Administrator
7	17:45:03	FDC-VM0000000000	system	system	Administrator
8	17:45:01	FDC-VM0000000000	system	admin	Administrator

Below are sample raw logs from FortiDeceptor:

```
date=2020-03-12 time=16:54:01 id=6861604606372216836 itime=2020-08-16 08:30:17 euid=1
epid=1 dsteuid=1 dstepid=1 devhost=FDC-VM0000000552 tz=PDT logid=0106000001
type=event subtype=system level=information user=admin ui=GUI action=Logout
status=Success msg=Administrator admin logged out website successfully from
172.18.32.10 devid=FDC-VM0000000353 dtime=2020-03-12 16:54:01 itime_t=1597591817
devname=FDC-VM0000000353
```

```
date=2020-03-12 time=16:49:16 id=6861604602077249536 itime=2020-08-16 08:30:16 euid=1
epid=1 dsteuid=1 dstepid=1 devhost=FDC-VM0000000552 tz=PDT logid=0106000001
type=event subtype=system level=information user=admin ui=GUI action=Login
status=Success msg=Administrator admin logged into website successfully from
172.18.32.10 devid=FDC-VM0000000353 dtime=2020-03-12 16:49:16 itime_t=1597591816
devname=FDC-VM0000000353
```



## Unique count for event handler - 6.4.2

This is an enhancement to the *Generate Alert* threshold section of the event handlers which provides additional criteria (*Distinct* field value) for triggering events.

### To configure unique count in an event handler:

- When editing an event handler, there are two new options available in the *Generate Alert When* section:
  - Exact:** The legacy function. An event is triggered when the set number of logs meet the general condition defined in the event log filter.

The screenshot shows the 'Edit Handler: IPS' configuration page in FortiAnalyzer. The left sidebar contains navigation options like Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, and Handlers. The main panel is titled 'Edit Handler: IPS' and includes a 'Filter 1' section with 'Log Device Type' (FortiGate), 'Log Type' (IPS (ips)), and 'Group By' (Source Endpoint (endpoint)). The 'Logs match' section is set to 'Any of the following conditions'. The 'Generate Alert When' section is configured with 'At least 1' matches over a period of '30' minutes, using 'Exact' match criteria. The 'Event Message' is '(Blank)', 'Event Status' is 'Allow FortiAnalyzer to choose', and 'Event Severity' is 'Critical'. The 'Additional Info' section is set to 'Use system default'. The 'Notifications' section is set to 'Send Alert through Fabric Connectors'.

- Distinct:** An event is triggered when there are a set number of distinct values from the chosen log field, and the conditions of the general event log filter are met. In the example below, five distinct attacks within 30 minutes from the same endpoint will generate an event, allowing for strict criteria for an IPS event definition.

The screenshot shows the 'Edit Handler: IPS' configuration page in FortiAnalyzer. The left sidebar contains navigation options like Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, and Handlers. The main panel is titled 'Edit Handler: IPS' and includes a 'Filter 1' section with 'Log Device Type' (FortiGate), 'Log Type' (IPS (ips)), and 'Group By' (Source Endpoint (endpoint)). The 'Logs match' section is set to 'Any of the following conditions'. The 'Generate Alert When' section is configured with 'At least 5' matches over a period of '30' minutes, using 'Distinct' match criteria. The 'Event Message' is '(Blank)', 'Event Status' is 'Allow FortiAnalyzer to choose', and 'Event Severity' is 'Critical'. The 'Additional Info' section is set to 'Use system default'. The 'Notifications' section is set to 'Send Alert through Fabric Connectors'.

2. Generated events with associated first and last logs from before the trigger event is recorded are consolidated into the same event to a maximum of 50 logs. For a full log list, use *Search in Log View* from the event context menu.

The first screenshot shows the FortiGate SOC View interface. The left sidebar contains navigation options: Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbook, Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, Handlers, and Incidents. The main panel displays a table of events. The table has columns: #, Event, Event Status, Event Type, Count, Severity, First Occurrence, Last Update, Additional Info, Handler, Tags, and Device Name. The events are filtered by 'All Devices' and 'Last 30 Minutes'. The second screenshot shows the 'Log View' interface. The left sidebar is the same as the first screenshot. The main panel displays a table of logs. The table has columns: #, Date/Time, Device ID, Severity, Source, Attack Name, Destination IP, Action, Service, User, and Count. The logs are filtered by 'All FortiGate' and 'Custom' view. The third screenshot shows the 'Log View' interface with a search filter applied: '( epid=1060 ) AND ( ( type="uta" and subtype="ips" ) or ( type="anomaly" and subtype="anomaly" ) or ( type="uta" and subtype="anomaly" ) or type="ips" )'. The table displays logs for various services including LDAP, NBSS, and DNS.

#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler	Tags	Device Name
1	192.168.125.63 (1)										
2	MS.SMB2.Negotiation.Handler.Code.Executi...	Mitigated	IPS	18	Critical	2020-07-31 17:04:39	2020-07-31 17:12:44	Permission/Privilege/Ac...	IPS	IPS - Critical Severity-ren...	FW-93
3	up_src_session (4)		IPS	90	Critical	In an hour	In 2 hours	General	IPS - Critical Severity-ren...		FW-93
4	tcp_port_scan (4)		IPS	16	Critical	In an hour	In 2 hours	General	IPS - Critical Severity-ren...		FW-93
5	up_dst_session (4)		IPS	10	Critical	In an hour	In 2 hours	General	IPS - Critical Severity-ren...		FW-93

#	Date/Time	Device ID	Severity	Source	Attack Name	Destination IP	Action	Service	User	Count
1	17:04:39	FGVM02TM20003628	critical	192.168.125.63	MS.SMB2.Ne...	192.168.22.6	dropped	NBSS		
2	17:12:44	FGVM02TM20003628	low	192.168.125.63	LDAPInvalid...	192.168.22.6	detected	LDAP		

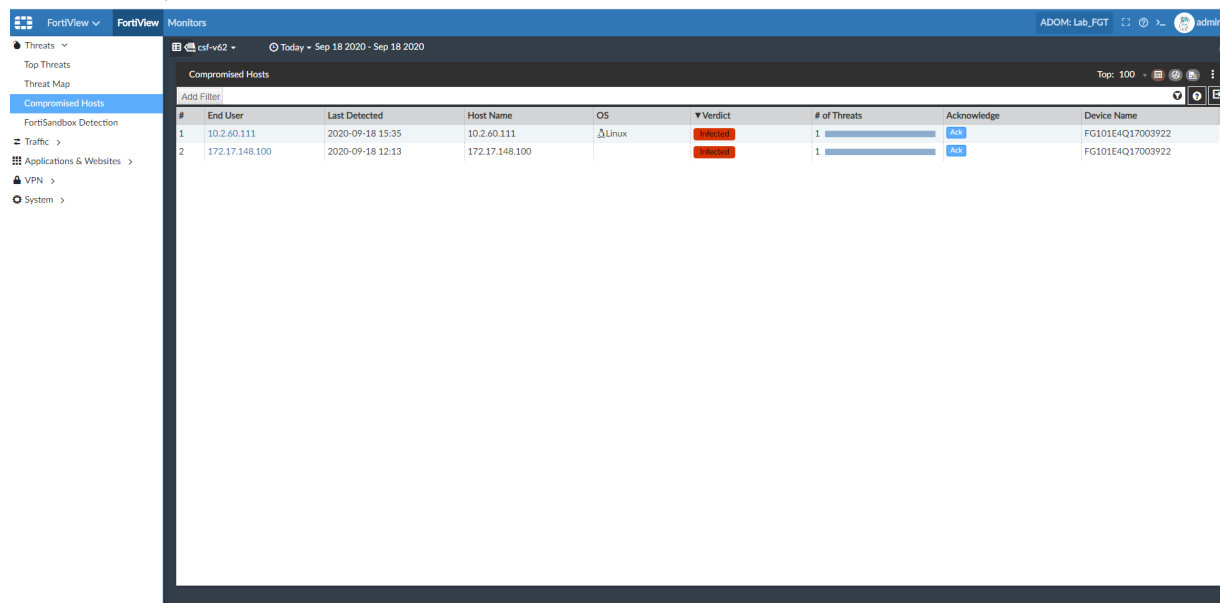
#	Date/Time	Device ID	Severity	Source	Attack Name	Destination IP	Action	Service	User	Count
1	17:12:44	FGVM02TM20003628	low	192.168.125.63	LDAP:Invalid Encod...	192.168.22.6	detected	LDAP		
2	17:12:29	FGVM02TM20003628	critical	192.168.125.63	MS.SMB2.Negotia...	192.168.22.6	dropped	NBSS		
3	17:11:49	FGVM02TM20003628	low	192.168.125.63	Walksam.Admin.Sc...	192.168.22.6	detected	NBSS		
4	17:11:44	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
5	17:11:44	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
6	17:11:44	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
7	17:11:44	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
8	17:11:44	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
9	17:11:44	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
10	17:11:34	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
11	17:11:34	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
12	17:11:29	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
13	17:11:29	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
14	17:11:24	FGVM02TM20003628	info	192.168.125.63	DNS.Undersized.ML...	192.168.22.6	detected	DNS		
15	17:11:24	FGVM02TM20003628	low	192.168.125.63	TCP.PORT0	192.168.22.6	detected	NONE		
16	17:11:19	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
17	17:11:19	FGVM02TM20003628	low	192.168.125.63	NBSS.Invalid.Fragm...	192.168.22.6	detected	NBSS		
18	17:04:39	FGVM02TM20003628	critical	192.168.125.63	MS.SMB2.Negotia...	192.168.22.6	dropped	NBSS		

## FortiGate C&C Detection in SOC View - 6.4.3

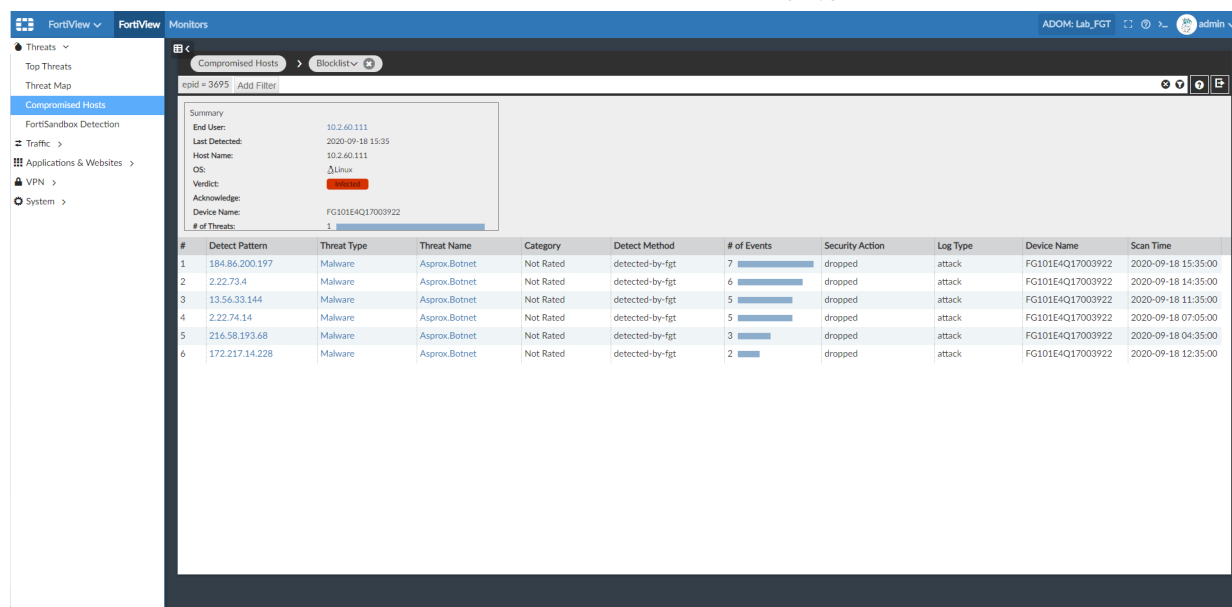
The IOC scan feature has been enhanced to allow FortiAnalyzer to include FortiGate C&C detection in Compromised Hosts in the SOC View.

## To view C&C attack logs:

1. Go to *FortiView* > *Compromised Hosts*.
2. Under *Verdict*, click *Infected*.



The C&C events have a *Detect Method* of detected-by-fgt and *Log Type* of attack.



### 3. Drilldown to view the log details. C&C logs will have an *Attack Name* matching \*.Botnet.

Summary

- End User: 10.2.40.111
- Last Detected: 2020-09-18 15:35
- Host Name: 10.2.40.111
- OS: Linux
- Verdict: Infected
- Acknowledge: FG101E4Q17003922
- Device Name: FG101E4Q17003922
- # of Threats: 1

#	Date/Time	Device ID	Severity	Source	Destination IP	Action	Service	Message	Attack Name
1	15:35:02	FG101E4Q17003922	critical	10.2.40.111	184.86.200.197	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
2	15:05:03	FG101E4Q17003922	critical	10.2.40.111	184.86.200.197	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
3	14:35:11	FG101E4Q17003922	critical	10.2.40.111	172.22.73.4	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
4	14:05:05	FG101E4Q17003922	critical	10.2.40.111	184.86.200.197	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
5	13:35:04	FG101E4Q17003922	critical	10.2.40.111	184.86.200.197	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
6	12:35:04	FG101E4Q17003922	critical	10.2.40.111	172.217.14.228	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
7	12:05:04	FG101E4Q17003922	critical	10.2.40.111	172.22.73.4	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
8	11:35:05	FG101E4Q17003922	critical	10.2.40.111	13.56.33.144	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
9	11:05:16	FG101E4Q17003922	critical	10.2.40.111	184.86.200.197	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
10	10:35:02	FG101E4Q17003922	critical	10.2.40.111	184.86.200.197	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
11	10:05:03	FG101E4Q17003922	critical	10.2.40.111	13.56.33.144	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
12	09:35:08	FG101E4Q17003922	critical	10.2.40.111	172.22.73.4	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
13	08:35:05	FG101E4Q17003922	critical	10.2.40.111	13.56.33.144	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
14	08:05:01	FG101E4Q17003922	critical	10.2.40.111	172.217.14.228	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
15	07:35:03	FG101E4Q17003922	critical	10.2.40.111	13.56.33.144	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
16	07:05:03	FG101E4Q17003922	critical	10.2.40.111	172.22.74.14	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
17	06:35:05	FG101E4Q17003922	critical	10.2.40.111	172.22.74.14	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet
18	06:05:01	FG101E4Q17003922	critical	10.2.40.111	172.22.73.4	dropped	HTTP	backdoor: Asprox.Botnet.	Asprox.Botnet

Total logs for analytics: 60 days 22 hours.

#### To view C&C message logs:

1. Go to *FortiView > Compromised Hosts*.
2. Under *Verdict*, click *Infected*. The C&C events have a *Detect Method* of detected-by-fgt and *Log Type* of attack.

Summary

- End User: 172.17.148.100
- Last Detected: 2020-09-18 12:13
- Host Name: 172.17.148.100
- OS: Linux
- Verdict: Infected
- Acknowledge: FG101E4Q17003922
- Device Name: FG101E4Q17003922
- # of Threats: 1

#	Detect Pattern	Threat Type	Threat Name	Category	Detect Method	# of Events	Security Action	Log Type	Device Name	Scan Time
1	141.255.150.0	Malware	njrat	Not Rated	detected-by-fgt	1	dropped	attack	FG101E4Q17003922	2020-09-18 12:12:00

### 3. Drilldown to see the log details. The C&C logs appear under *Message* as Botnet C&C.

The screenshot shows the FortiView Monitors interface. The left sidebar has a menu with options like Threats, Top Threats, Threat Map, and Compromised Hosts. The main area displays a summary for a compromised host (172.17.148.100) and a table of log entries. The log entry shows a critical severity event from source 172.17.148.100 to destination 141.255.150.0, with the message 'Botnet C&C Communication' and attack name 'Nirat'.

#	Date/Time	Device ID	Severity	Source	Destination IP	Action	Service	Message	Attack Name
1	12:12:48	FG101E4Q17003922	critical	172.17.148.100	141.255.150.0	dropped	HTTP	Botnet C&C Communication	Nirat

## FortiADC logging - 6.4.3

FortiADC logs are supported on FortiAnalyzer.

### To enable FortiADC logging:

#### 1. On FortiADC, go to *Logs & Report > Log Setting* and click the *Syslog Server* tab.

The screenshot shows the FortiADC Log Setting - Syslog Server tab. It displays a table with columns for ID, Status, Address, Port, and Log Level. There are two entries, both with Status 'Enable' and Log Level 'Information'. The first entry has Address 172.16.200.16 and Port 514. The second entry has Address 172.18.28.41 and Port 514. The interface also includes a 'Create New' button and a 'Show 25 entries' link.

ID	Status	Address	Port	Log Level
1	Enable	172.16.200.16	514	Information
2	Enable	172.18.28.41	514	Information

#### 2. Click *Create New* to create a remote log server. In the *Proto* field select *UDP*. FortiADC currently only supports this protocol. Click *Save* once complete.

**FortiADC - FortiADC-VM**

HA: Standalone V6.0.0 Build: 20038

**Syslog Server**

Status: ☒

Address: 172.16.200.15

Port: 514

Range: 0-65535

Proto: ☒ UDP ☐ TCP ☐ TCP SSL

Log Level: Information

CSV: ☐

Facility: Kern

Event: ☒

Event Category: ☒ Configuration ☒ Admin ☒ System ☐ User ☒ Health Check ☐ SLB ☐ LLB

☐ GLB ☐ Firewall ☐ Enable All

Required: Please select at least one category.

Traffic: ☒

Traffic Category: ☒ SLB ☒ GLB ☒ LLB ☒ Enable All

Required: Please select at least one category.

Security: ☒

Security Category: ☒ DDoS ☒ IPReputation ☒ WAF ☒ GEO ☒ AV ☒ IPS ☒ FW ☒ Enable All

Required: Please select at least one category.

**Save** **Cancel**

Once the remote log server is created and logs are generated on the FortiADC, the logs are sent to FortiAnalyzer.

Device Name	Model	Serial Number	Connecting IP
FADV040000002384	FortiADC-VM		172.16.81.1

- On FortiAnalyzer, go to the *Device Manager* and click the *Unauthorized* view to see the FortiADC device. Promote the FortiADC device to a Fabric ADOM, for example the root ADOM. FortiADC devices can only be added to Fabric ADOMs.

**Authorize Device**

Device Authorization

Total: 1/1, Success: 1, Warning: 0, Error: 0

**View Progress Report**

#	Name	Time Used	Status
1	FADV040000002384	1s	Initializing configuration database

**Close**

After the FortiADC device is registered in the *Device Manager*, the FortiADC's logs can be stored and displayed in *Log View*.

**Log View**

All FortiADC - Last 1 Hour - 15:18:46 to 16:18:45

#	Date/Time	Device ID	Type	Sub Type	ID	Virtual Domain	Protocol	Source Name	Destination
1	16:17:34	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
2	16:17:33	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
3	16:17:32	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
4	16:17:31	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
5	16:17:30	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
6	16:17:29	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
7	16:17:28	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
8	16:17:27	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
9	16:17:26	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
10	16:17:25	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
11	16:17:24	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100
12	16:17:14	FADV040000002384	traffic	slb_layer4	0100008000	root	6	20.20.0.1	20.20.0.100

Total logs for analysis: 6 hours.

10... 1 0.003 Second

## Sample FortiADC Logs:

### Traffic log:

```
id=6878052772042768384 itime=2020-09-29 16:17:34 euid=1 epid=1 dsteuid=1 dstepid=1
date=2020-08-19 time=17:13:37 type=traffic subtype=slb_layer4 log_id=0100008000
pri=information msg_id=8891139290341374 proto=6 src=20.20.0.1 src_port=55442
dst=20.20.0.100 dst_port=80 policy=VS1 action=none srccountry=United dstcountry=United
duration=3 ibytes=398 obytes=1075 service=tcp trans_src=20.20.0.1 trans_src_port=55442
trans_dst=20.20.2.3 trans_dst_port=80 real_server=pool1-3 device_id=FADV040000002384
vd=root dtime=2020-08-19 17:13:37 itime_t=1601421454 devname=FADV040000002384
```

### Security Log:

```
id=6878052935251525632 itime=2020-09-29 16:18:12 euid=1 epid=1 dsteuid=1 dstepid=1
date=2020-08-19 time=15:04:13 type=attack subtype=ip_reputation log_id=0200006001
pri=warning msg_id=8891139290340651 count=1 severity=high proto=6 service=http
src=20.20.0.1 src_port=55194 dst=20.20.0.100 dst_port=80 policy=VS1 action=deny
srccountry=United dstcountry=United msg=IP Reputation Violation: Botnet was detected.
device_id=FADV040000002384 vd=root dtime=2020-08-19 15:04:13 itime_t=1601421492
devname=FADV040000002384
```

### Event Log:

```
d=6878052845057212416 itime=2020-09-29 16:17:51 euid=1 epid=1 dsteuid=1 dstepid=1
date=2020-08-19 time=16:32:11 type=event subtype=config log_id=0000000100
pri=information msg_id=8891139290341031 user=admin ui=telnet(10.106.3.210) action=add
logdesc=Change msg=added cfgpath=system cfgobj=name cfgattr=HC_dnsv6 device_
id=FADV040000002384 vd=root dtime=2020-08-19 16:32:11 itime_t=1601421471
devname=FADV040000002384
```

## Dashboard/widgets/reports

This section lists the new features added to FortiAnalyzer for dashboards, widgets and reports.

### List of new features:

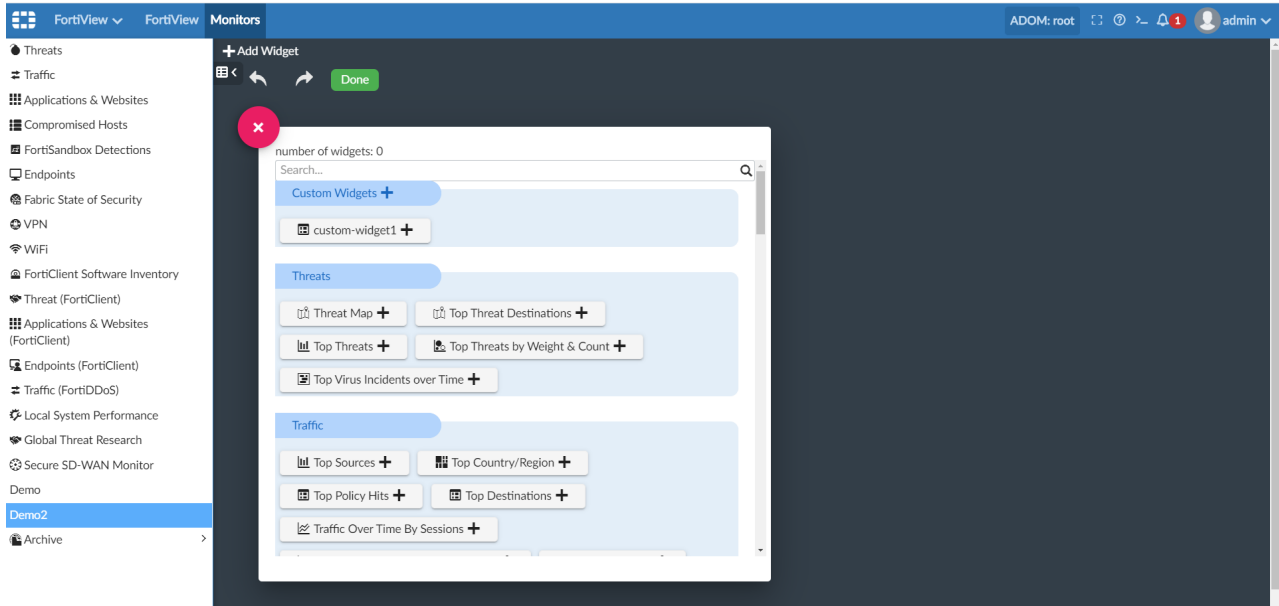
- [FortiView custom widgets 6.4.1 on page 114](#)
- [Extra caching for SOC reports 6.4.1 on page 117](#)
- [Asset tags on page 118](#)
- [Sankey Chart on page 120](#)
- [FortiPortal user summary report 6.4.2 on page 121](#)
- [FortiSandbox default report improvement 6.4.2 on page 123](#)
- [Improved SOC incident report 6.4.2 on page 124](#)
- [Add stackbar chart in FortiView 6.4.2 on page 126](#)
- [Interface bandwidth widgets 6.4.2 on page 128](#)
- [EMS classification tag 6.4.3 on page 130](#)
- [Throughput utilization billing reporting 6.4.3 on page 133](#)
- [Subnet list for reports 6.4.3 on page 135](#)
- [Asset & Identity View Improvement 6.4.3 on page 138](#)

## FortiView custom widgets - 6.4.1

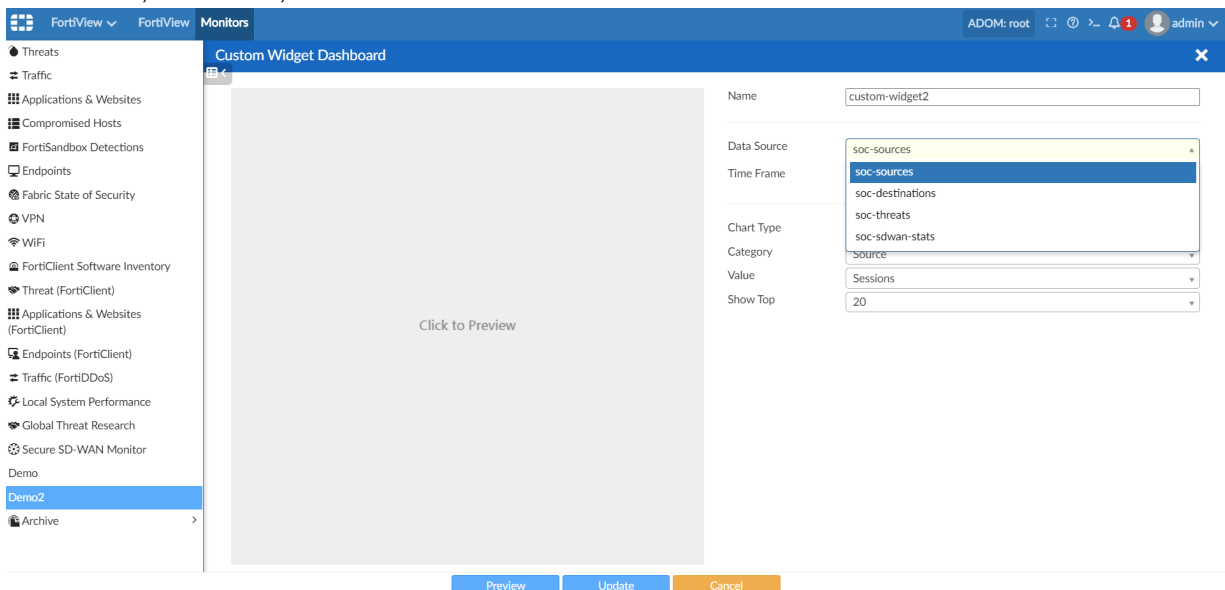
Custom widgets can be created from predefined Data sources and added to new dashboards in FortiView.

### To create a custom widget in FortiView Monitors:

1. Go to *FortiView > Monitors* and select or create a custom dashboard.
2. In the *Add Widget* window, select the plus icon next to *Custom Widgets* to create a new widget.

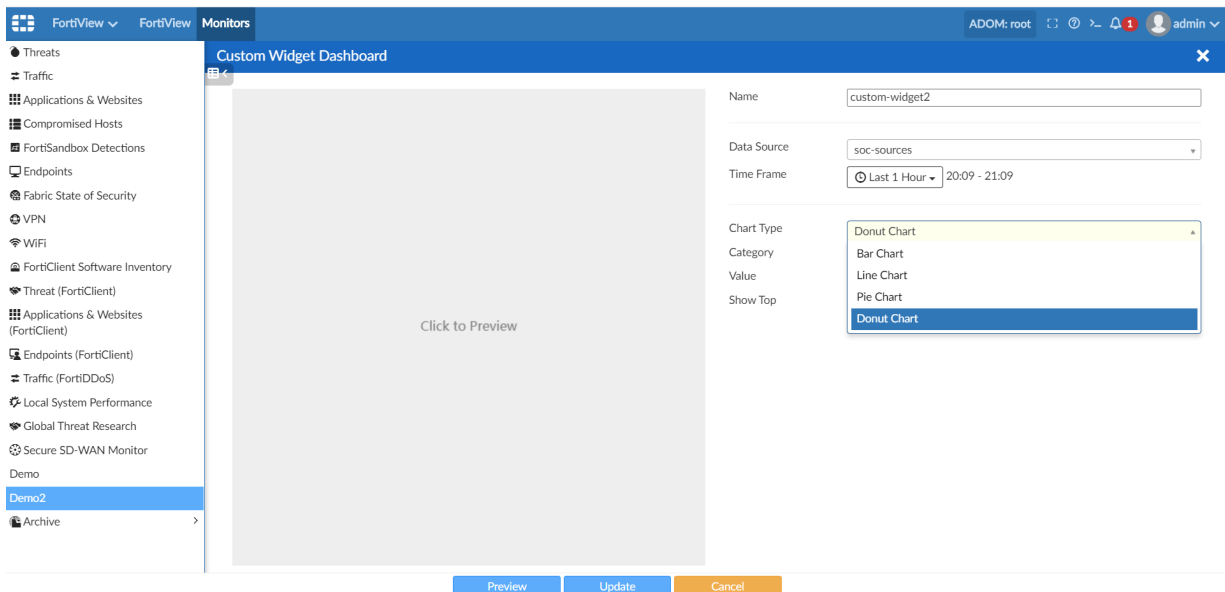


3. In the custom widget dashboard, enter the name of the custom widget, then select the *Data Source*, *Chart Type*, *X Axis* or *Category* field, and *Y Axis* or *Value* field.
  - a. For *Data Source*, one of four pre-defined data sources can be selected for a widget: *soc-sources*, *soc-destinations*, *soc-threats*, and *soc-sdwan-stats*.



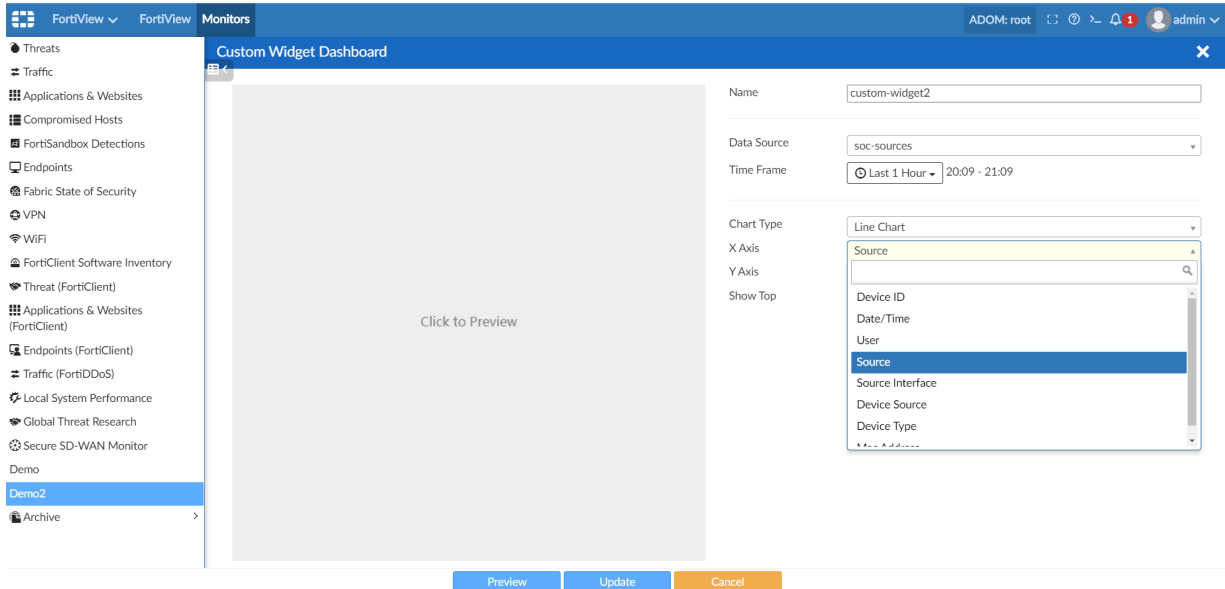


- b. For *Chart Type*, one of four chart types can be selected for a widget: *Bar Chart*, *Line Chart*, *Pie Chart*, and *Donut Chart*.



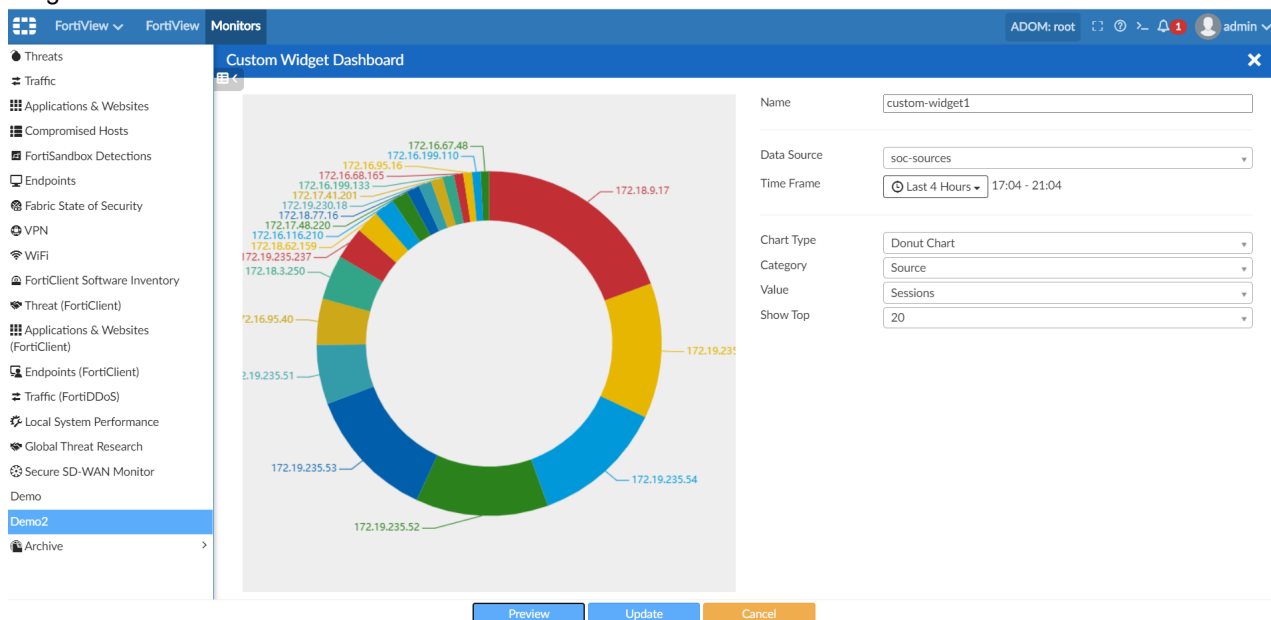
- c. The fields available in the *X Axis* and *Y Axis* or *Category* and *Value* fields vary depending on the data source selected.

For example, when the data-source is *soc-sources*, fields in the *X Axis* include *Device ID*, *Date/Time*, *User*, *Source*, *Source Interface*, *Device Source*, *Device Type*, *MAC Address*, and the fields in the *Y Axis* include *Threat Score*, *Threat Block*, *Threat Pass*, *Bandwidth*, *Traffic In*, *Traffic Out*, *Sessions*, *Session Block*, and *Session Pass*.

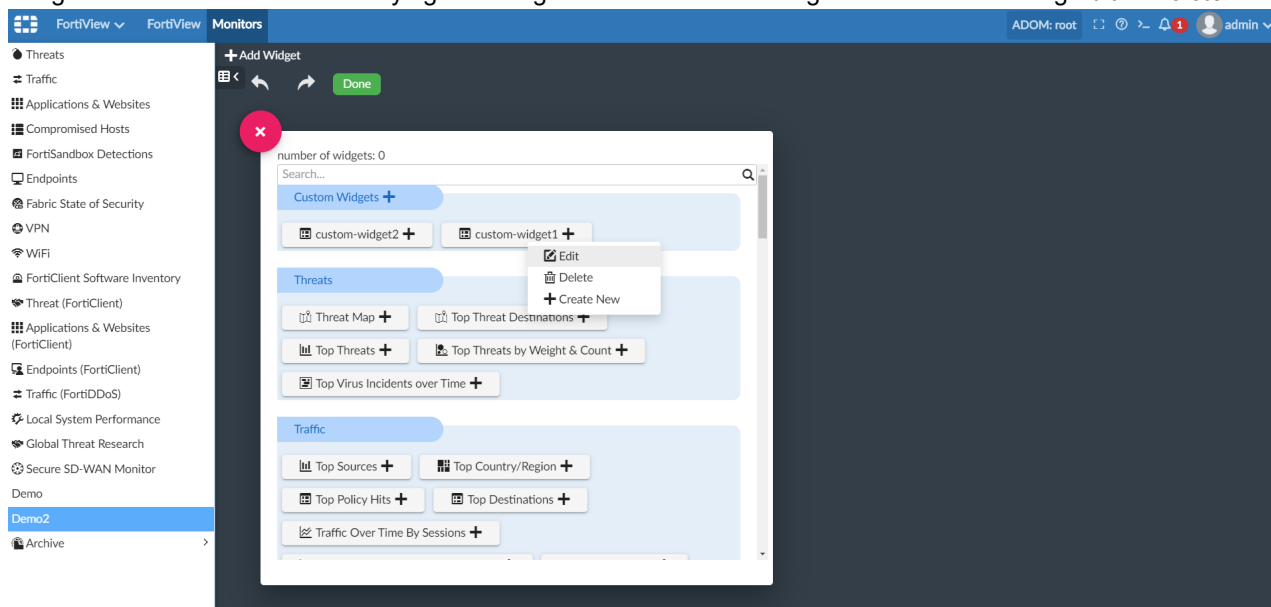


- d. For *Bar Chart* and *Line Chart*, *X Axis* is the name field and *Y Axis* is the value field. For *Pie Chart* and *Donut Chart*, *Category* is the name field and *Value* is the value field.

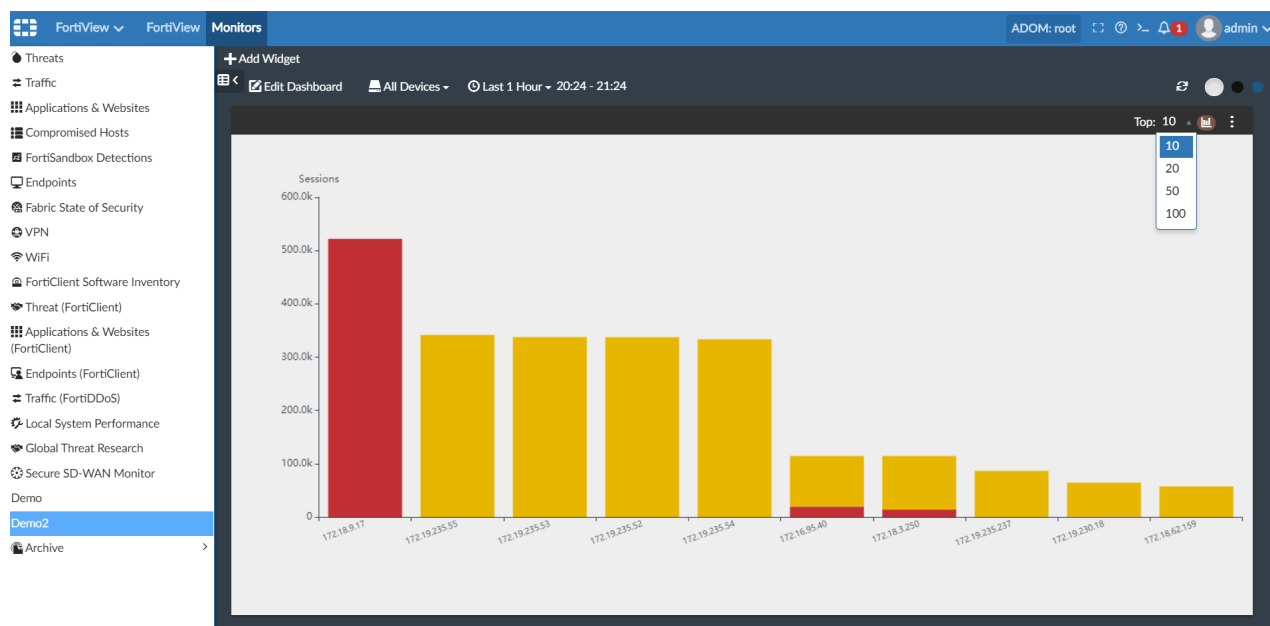
4. Before creating the widget, you can specify the *Time Frame* and *Show Top*, then click the *Preview* button to view the widget.



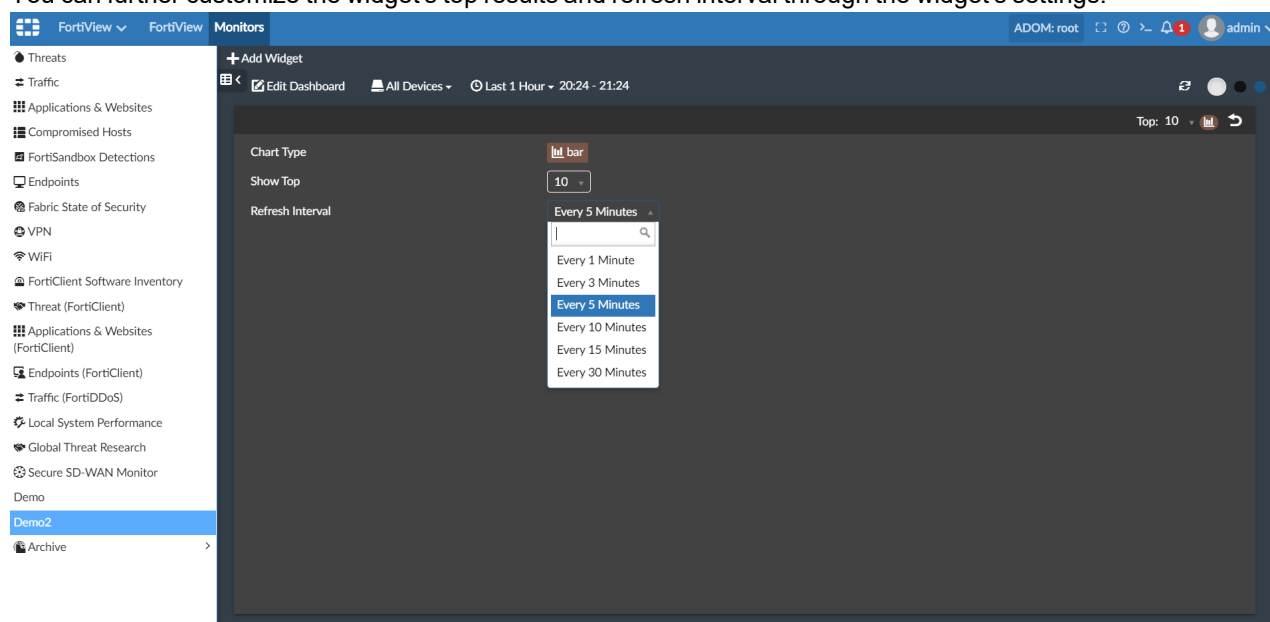
5. Click *Create* to create the widget or click *Cancel* to discard the widget. After the widget has been created, it will be listed in the *Add Widget* window under the *Custom Widgets* category. Widgets can be edited or deleted by right clicking them from the *Add Widget* window and clicking *Edit* or *Delete*.



After adding a widget to a custom dashboard, you can select the device, time period, and top results to display from the widget's toolbar.



You can further customize the widget's top results and refresh interval through the widget's settings.



## Extra caching for SOC reports - 6.4.1

Caching can be enabled for common log fields used for extended log filtering in reports. This feature is an enhancement for current report Auto Cache and report group function. After enabling this option, the following fields are added to each running report query:

- Device ID
- VDOM name
- Source Endpoint ID
- Source Enduser ID

- Source IP
- Destination IP

### To enable extended log filtering:

1. Go to *Reports > All Reports* and select a report.
2. Click the *Settings* tab.
3. Click *Enable Auto-cache*.  
The option to enable *Extended Log Filtering* is now available.
4. Enable *Extended Log Filtering*, and click *Apply*.

After it has been enabled, run the report and debug. You can see that `devid`, `vd`, `srcip`, `dstip`, `epid`, and `euid` are added to each report query.

```
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:2324: Received request (from:0, type:2).
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:2894: Client sock '48' is accepted.
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:2324: Received request (from:0, type:2).
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:2894: Client sock '51' is accepted.
{1591653919} DEBUG: sqlreportd(976):pq_plugin.c:18: set PQconnectdb options parameter=[options='-c TimeZone=US/Pacific']
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:2324: Received request (from:0, type:2).
{1591653919} DEBUG: sqlreportd(976):pq_plugin.c:18: set PQconnectdb options parameter=[options='-c TimeZone=US/Pacific']
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:2324: Received request (from:0, type:2).
{1591653919} DEBUG: sqlreportd(976):pq_plugin.c:18: set PQconnectdb options parameter=[options='-c TimeZone=US/Pacific']
{1591653919} INFO: sqlreportd(976):dbplugin.c:2051: work_mem=1024MB, max_parallel_workers_per_gather=4
{1591653919} INFO: sqlreportd(976):dbplugin.c:2051: work_mem=1024MB, max_parallel_workers_per_gather=4
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:1514: Execute SQL query: insert into hcache."FGTADOM98224-HCACHE_18522"
select 96807 as hid, * from (/*HCACHE-R
FGTADOM98224-FGT-tlog-1591511700)/select "devid", "vd", "srcip", "dstip", "epid", "euid", count(*) as sessions, sum(coalesce(sentbyte, 0))+coalesce(recvbyte, 0) as bandwidth from (SE
LECT til.*, ti2."devid", ti2."vd", "devname", "csf" FROM "FGTADOM98224-FGT-tlog-1591511700" til LEFT JOIN "devtable" ti2 ON til.dvid=ti2.dvid ) ti where itime >= 1591513200 and (logflag1>0)
group by "devid", "vd", "srcip", "dstip", "epid", "euid" limit 100001) t
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:1514: Execute SQL query: insert into hcache."FGTADOM98224-HCACHE_18523"
select 96808 as hid, * from (/*HCACHE-R
FGTADOM98224-FGT-tlog-1591511700)/select "devid", "vd", "srcip", "dstip", "epid", "euid", app_group_name(app) as app_grp, count(*) as count from (SELECT til.*, ti2."devid", ti2."vd", "devname", "csf" FROM "FGTADOM98224-FGT-tlog-1591511700" til LEFT JOIN "devtable" ti2 ON til.dvid=ti2.dvid ) ti where itime >= 1591513200 and (logflag1>0) and nullifna(app) is not null gro
up by "devid", "vd", "srcip", "dstip", "epid", "euid", app_grp order by count desc limit 100001) t
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:1514: Execute SQL query: insert into hcache."FGTADOM98224-HCACHE_18524"
select 96810 as hid, * from (/*HCACHE-R
FGTADOM98224-FGT-tlog-1591511700)/select "devid", "vd", "srcip", "dstip", "epid", "euid", coalesce(nullifna("user"), nullifna("unauthuser"), ipstr("srcip")) as user_grp, count(*) as
count from (SELECT til.*, ti2."devid", ti2."vd", "devname", "csf" FROM "FGTADOM98224-FGT-tlog-1591511700" til LEFT JOIN "devtable" ti2 ON til.dvid=ti2.dvid ) ti where itime >= 1591513200 and
(logflag1>0) group by "devid", "vd", "srcip", "dstip", "epid", "euid", user_grp order by count desc limit 100001) t
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:1514: Execute SQL query: insert into hcache."FGTADOM98224-HCACHE_18527"
select 96813 as hid, * from (/*HCACHE-R
FGTADOM98224-FGT-tlog-1591511700)/select "devid", "vd", "srcip", "dstip", "epid", "euid", dstip, count(*) as count from (SELECT til.*, ti2."devid", ti2."vd", "devname", "csf" FROM "FGTADOM98224-
FGT-tlog-1591511700" til LEFT JOIN "devtable" ti2 ON til.dvid=ti2.dvid ) ti where itime >= 1591513200 and (logflag1>0) and dstip is not null group by "devid", "vd", "srcip", "epid", "eui
d", dstip order by count desc limit 100001) t
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:1514: Execute SQL query: insert into hcache."FGTADOM98224-HCACHE_18526"
select 96811 as hid, * from (/*HCACHE-R
FGTADOM98224-FGT-tlog-1591511700)/select "devid", "vd", "srcip", "dstip", "epid", "euid", to_char(from_time("itime"), 'YYYY-MM-DD') as dom, count(*) as sessions from (SELECT til.*,
ti2."devid", ti2."vd", "devname", "csf" FROM "FGTADOM98224-FGT-tlog-1591511700" til LEFT JOIN "devtable" ti2 ON til.dvid=ti2.dvid ) ti where itime >= 1591513200 and (logflag1>0) group by "d
evid", "vd", "srcip", "dstip", "epid", "euid", dom order by sessions desc limit 100001) t
{1591653919} DEBUG: sqlreportd(976):sqlreport_main.c:1514: Execute SQL query: insert into hcache."FGTADOM98224-HCACHE_18528"
select 96809 as hid, * from (/*tag:rrp_
base_t_bndwdth_rese*/select ("itime"/1800*1800) as timestamp, devid, vd, srcip, dstip, epid, euid, coalesce(nullifna("user"), nullifna("unauthuser"), ipstr("srcip")) as user_src, service,
```

## Asset tags

Asset tags from EMS and FortiNAC is available in FortiAnalyzer Assets view.

## To view asset tags in FortiAnalyzer:

1. In the FortiClient EMS Server, go to *Compliance Verification > Compliance Verification Rules*, and create a new rule.

In this example, the tag "QA Windows 10 Workstation" was created for OS Version: Windows 10.

FortiClient Endpoint Management Server

Compliance Verification Rule Set

Name: Rule1

Tag Endpoint As: QA Windows 10 Workstation

Enabled: ☒

Comments: Optional

Type	Value
Windows (1)	
OS Version	Windows 10

Buttons: Save, Cancel

Once saved, go to *Compliance Verification > Host Tag Monitor* to confirm the presence of the tag.

Below, the two endpoints using Windows 10 operating systems are tagged with *QA Windows 10 Workstation*.

Endpoint	User	OS	IP	Tagged on
QA Windows 10 Workstation (2)				
DESKTOP-6FPHU7	[User Icon]	Microsoft Windows 10 Professional Edition, 64-bit...	172.18.32.73	2020-04-15 17:39:28
DESKTOP-IE1AT7U	[User Icon]	Microsoft Windows 10 Professional Edition, 64-bit...	172.18.32.72	2020-04-15 17:38:49

2. On FortiAnalyzer, go to *Fabric View > Fabric Connectors*, and create a new *FortiClient EMS Connector*.

Fabric View | Fabric Connectors | Identity Center | Assets

+ Create New

Security Fabric (1)

FortiClient EMS - EMS Connector John

Configuration | Actions

Name: EMS Connector John

Description: Connector to execute remote EMS operations

IP/FQDN: 172.18.32.74

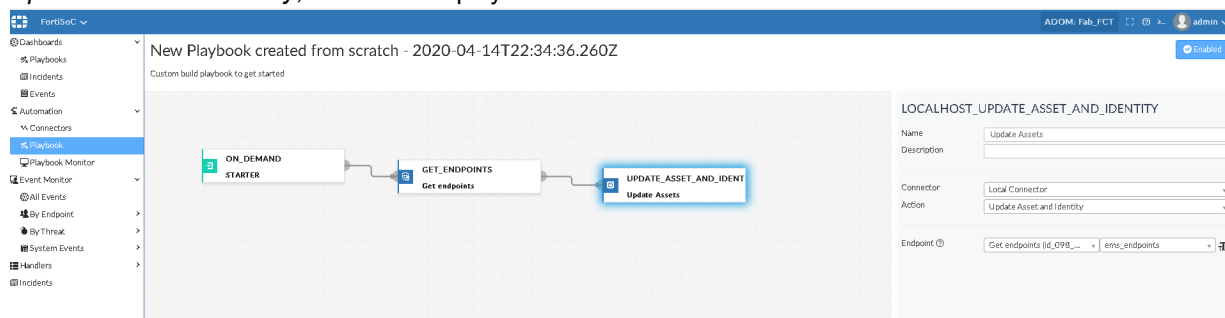
Username: admin

Password: [Masked]

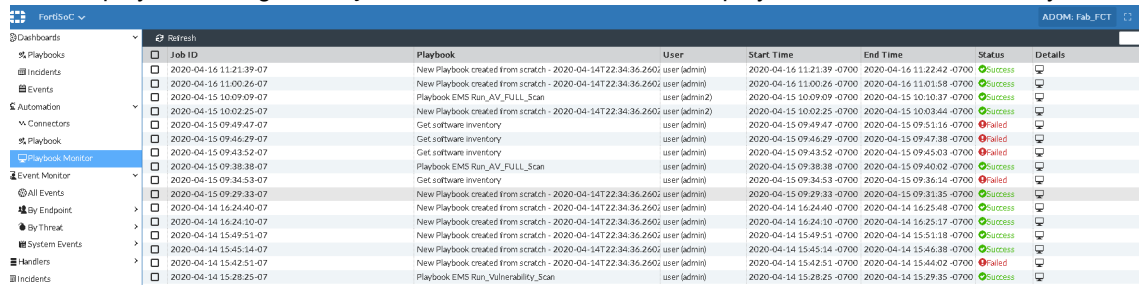
Status: ☒ Enabled

Buttons: OK, Cancel

3. Go to *FortiSoC > Automation > Playbook* and create a new customized playbook with a task using the action *Update Asset and Identity*, and save the playbook.



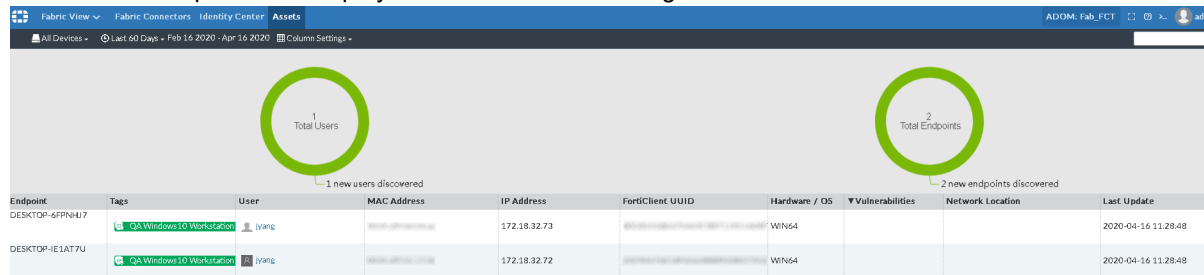
#### 4. Run the playbook and go to *Playbook Monitor* to confirm that the playbook was run successfully.



Job ID	Playbook	User	Start Time	End Time	Status	Details
2020-04-16 11:21:39 -0700	New Playbook created from scratch - 2020-04-14T22:34:36.2601	user (admin)	2020-04-16 11:21:39 -0700	2020-04-16 11:22:42 -0700	Success	
2020-04-16 11:00:26 -0700	New Playbook created from scratch - 2020-04-14T22:34:36.2601	user (admin)	2020-04-16 11:00:26 -0700	2020-04-16 11:01:58 -0700	Success	
2020-04-15 10:09:09 -0700	Playbook EMS Run_AV_FULL_Scan	user (admin2)	2020-04-15 10:09:09 -0700	2020-04-15 10:10:37 -0700	Success	
2020-04-15 10:02:25 -0700	New Playbook created from scratch - 2020-04-14T22:34:36.2601	user (admin2)	2020-04-15 10:02:25 -0700	2020-04-15 10:03:44 -0700	Success	
2020-04-15 09:49:47 -0700	Get software inventory	user (admin)	2020-04-15 09:49:47 -0700	2020-04-15 09:51:16 -0700	Failed	
2020-04-15 09:46:29 -0700	Get software inventory	user (admin)	2020-04-15 09:46:29 -0700	2020-04-15 09:47:38 -0700	Failed	
2020-04-15 09:43:52 -0700	Get software inventory	user (admin)	2020-04-15 09:43:52 -0700	2020-04-15 09:45:03 -0700	Failed	
2020-04-15 09:38:38 -0700	Playbook EMS Run_AV_FULL_Scan	user (admin)	2020-04-15 09:38:38 -0700	2020-04-15 09:40:02 -0700	Success	
2020-04-15 09:34:53 -0700	Get software inventory	user (admin)	2020-04-15 09:34:53 -0700	2020-04-15 09:36:14 -0700	Failed	
2020-04-15 09:29:33 -0700	New Playbook created from scratch - 2020-04-14T22:34:36.2601	user (admin)	2020-04-15 09:29:33 -0700	2020-04-15 09:31:35 -0700	Success	
2020-04-14 16:24:40 -0700	New Playbook created from scratch - 2020-04-14T22:34:36.2601	user (admin)	2020-04-14 16:24:40 -0700	2020-04-14 16:25:48 -0700	Success	
2020-04-14 16:24:10 -0700	New Playbook created from scratch - 2020-04-14T22:34:36.2601	user (admin)	2020-04-14 16:24:10 -0700	2020-04-14 16:25:17 -0700	Success	
2020-04-14 15:49:51 -0700	New Playbook created from scratch - 2020-04-14T22:34:36.2601	user (admin)	2020-04-14 15:49:51 -0700	2020-04-14 15:51:18 -0700	Success	
2020-04-14 15:45:14 -0700	New Playbook created from scratch - 2020-04-14T22:34:36.2601	user (admin)	2020-04-14 15:45:14 -0700	2020-04-14 15:46:38 -0700	Success	
2020-04-14 15:42:51 -0700	New Playbook created from scratch - 2020-04-14T22:34:36.2601	user (admin)	2020-04-14 15:42:51 -0700	2020-04-14 15:44:02 -0700	Failed	
2020-04-14 15:28:25 -0700	Playbook EMS Run_Vulnerability_Scan	user (admin)	2020-04-14 15:28:25 -0700	2020-04-14 15:29:35 -0700	Success	

After a few

moments, go to *Fabric View > Assets*. Tags are now displayed in the *Tags* column. In this example, the two Windows 10 endpoints are displayed in the table with the tag "QA Windows 10 Workstation".



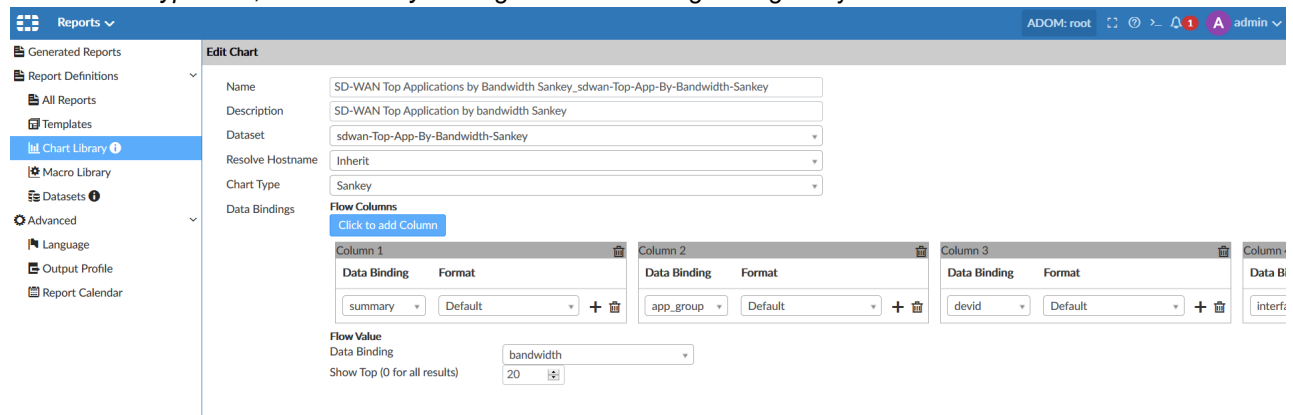
Endpoint	Tags	User	MAC Address	IP Address	FortiClient UUID	Hardware / OS	Vulnerabilities	Network Location	Last Update
DESKTOP-6FPN417	QA Windows 10 Workstation	lyang	08:00:27:00:00:00	172.18.32.73	0800270000000000	WIN64			2020-04-16 11:28:48
DESKTOP-IE1AT7U	QA Windows 10 Workstation	lyang	08:00:27:00:00:00	172.18.32.72	0800270000000000	WIN64			2020-04-16 11:28:48

## Sankey Chart

The *Sankey Chart* type is now available in FortiAnalyzer reports.

### To use a Sankey Chart in FortiAnalyzer reports:

1. Go to *Reports > Report Definitions > Chart Library*.
2. Click *Create New* to create a new sankey chart or select an existing sankey chart to edit.
3. In the *Chart Type* field, select *Sankey*. Configure the remaining settings for your chart and click *OK*.



**Report Definitions > Chart Library**

**Edit Chart**

Name: SD-WAN Top Applications by Bandwidth Sankey\_sdwan-Top-App-By-Bandwidth-Sankey

Description: SD-WAN Top Application by bandwidth Sankey

Dataset: sdwan-Top-App-By-Bandwidth-Sankey

Resolve Hostname: Inherit

Chart Type: Sankey

Data Bindings: Click to add Column

**Flow Columns**

Column 1: Data Binding: summary, Format: Default

Column 2: Data Binding: app\_group, Format: Default

Column 3: Data Binding: devid, Format: Default

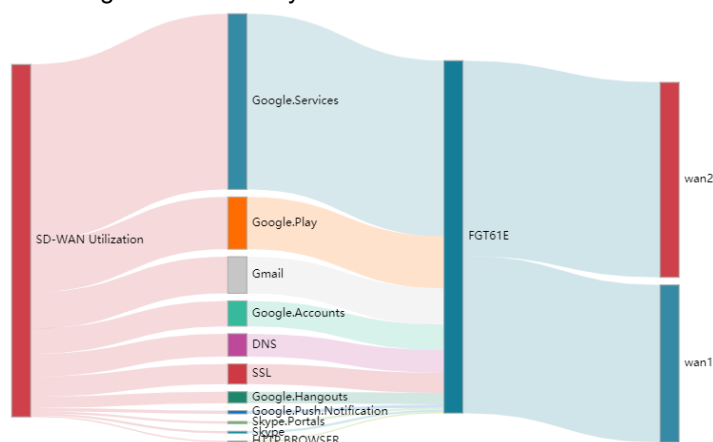
Column 4: Data Binding: interfac, Format: Default

**Flow Value**

Data Binding: bandwidth

Show Top (0 for all results): 20

Run the report to view the generated sankey chart.



## FortiPortal user summary report - 6.4.2

Existing customers can generate the same report "Default FortiPortal User Summary report" for deployments without collectors using FortiAnalyzer.

To view the FortiPortal User Summary report:

1. Go to *Reports > Report Definitions > Templates*.  
The *Template - FortiPortal User Summary Report* is displayed.

Reports

Generated Reports

Report Definitions

All Reports

Templates

Chart Library

Macro Library

Datasets

Advanced

Language

Output Profile

Report Calendar

Create New

View

Delete

Clone

Create Report

Install Template Pack

Title	Language	Description	Category	Preview
Vulnerability Scan Report				PDF
Template - FortiDDoS Default Report	English	Attacks and attackers by time period. Top 20 attacks, attack types, destinations and destinations by type.	FortiDDoS	HTML PDF
Template - FortiGate Performance Statistics Report	English	FortiGate Performance Statistics Report.	System	HTML PDF
Template - FortiMail Analysis Report	English	Statistics for Avg and Total mail size, number of mails and connections, delays, ip policies, recipient policies, top access list. Incoming filters for top spammed domains and users, classifiers by hour and disposition, and top subjects.	FortiMail	HTML PDF
Template - FortiMail Default Report	English	Top 10 client IP, senders, virus senders, local users, recipients and virus recipients	FortiMail	HTML PDF
Template - FortiNAC Endpoints and Network Report	English	FortiNAC Endpoints and Network Report.	FortiNAC	HTML PDF
Template - FortiPortal User Summary Report	English	FortiPortal User Summary Report.	Fabric	HTML PDF
Template - FortiProxy Default Report	English	Global bandwidth savings, cache rate, traffic and request timeline. Top 20 websites by bandwidth, bandwidth savings, cache rate, response time improvement.	FortiProxy	HTML PDF
Template - FortiProxy Security Analysis	English	User Security Analysis	FortiProxy	HTML PDF
Template - FortiProxy Web Usage Report	English	Web Usage Summary	FortiProxy	HTML PDF
Template - FortiSandbox Default Report	English	Threat rating distribution, job severity timeline, malware severity of targeted hosts, top 20 targeted hosts, top 20 malware, top 50 file type and brief job list	FortiSandbox	HTML PDF
Template - FortiWeb Default Report	English	Top sources, sources of attacks, event categories, login events by user, top destinations, attack destinations and event types	FortiWeb	HTML PDF

2. Go to *All Reports*.  
The *FortiPortal User Summary Report* is available.

Reports

Generated Reports

Report Definitions

All Reports

Templates

Chart Library

Macro Library

Datasets

Advanced

Language

Output Profile

Report Calendar

Create New

Edit

Delete

Clone

Run Report

Folder

More

Show Scheduled Only

Title	Language	Cache Status	Time Period	Devices	Schedule	Report Owner
FortiCache Security Analysis	English					
FortiCache Web Usage Report	English					
FortiDDoS Default Report	English		Last 7 Days	All_FortiDDoS		
FortiGate Performance Statistics Report	English					
FortiMail Analysis Report	English					
FortiMail Default Report	English					
FortiNAC Endpoints and Network Report	English					
Fortinet Email Risk Assessment	English					
FortiPortal User Summary Report	English					
FortiProxy Default Report	English					
FortiProxy Security Analysis	English					
FortiProxy Web Usage Report	English					
FortiSandbox Default Report	English					
FortiWeb Default Report	English					
FortiWeb Web Application Analysis Report	English					
GTP Report	English					
High Bandwidth Application Usage Report	English					
IPS Report	English					
PCI-DSS Compliance Review	English					
SaaS Application Usage Report	English					
Secure SD-WAN Report	English		Last 7 Days	All_FortiGate		
Security Analysis	English					
Security Events and Incidents Summary	English					

dtm

Highlight All

Match Case

Match Diacritics

Whole Words

More than 1000 matches

The FortiPortal User Summary Report includes the following table of contents.

Table of Contents	
1. Bandwidth and Application	2
Top Hostname by Traffic	2
Top Application Category by Count	2
Top Region Names by Traffic	2
Top Application by Traffic Chart	3
Top Protocols by Traffic	3
Bandwidth Summary	3
2. Web Usage	4
Top Websites by Count	4
3. Threats	5
Top Attacks by Count	5
Top Spams by Count	6
Top Viruses by Count	6
Antivirus Inspections	6
4. DLP	7
Top DLP by Count	7
5. Wireless	8
Top FAPs(Wireless) by Max Client Count	8
Top FAPs(Wireless) by Max Bandwidth	8
Top SSIDs(Wireless) by Max Traffic	8
6. Sandbox	9
FortiSandbox-Sandbox Scanning Statistics	9
FortiSandbox-Top Sandbox Hosts	9
FortiSandbox-Top Sandbox Malware	9
Appendix A	10
Devices	10

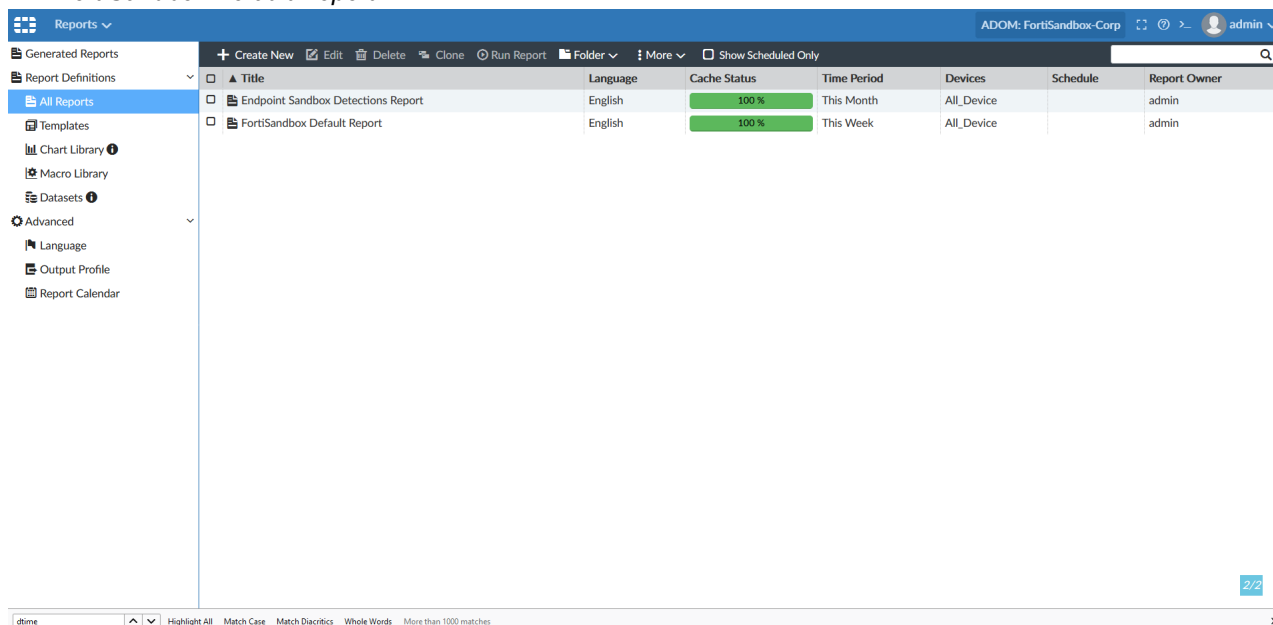


## FortiSandbox default report improvement - 6.4.2

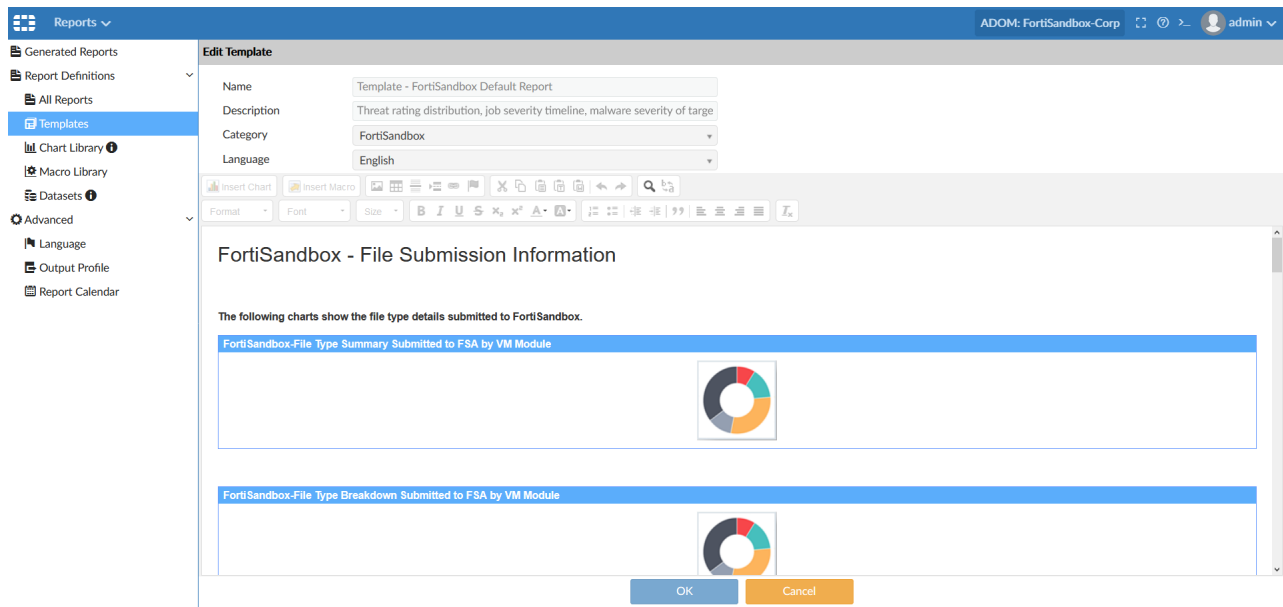
This report is an improved version of the "FortiSandbox Default Report" that provides more visibility on file submission to FSA, performance statistics and threat rating statistics.

### To view the improved FortiSandbox default report:

1. Go to *Reports > Report Definitions > All Reports*.  
The *FortiSandbox Default Report* is available.



2. In the *Layout Editor*, you can view the following new charts:
  - FortiSandbox - File Submission Information
    - File Type Summary Submitted to FSA by VM Module
    - File Type Breakdown Submitted to FSA by VM Module
    - File Type Summary Submitted to FSA
    - File Type Breakdown Submitted to FSA
  - FortiSandbox - Performance Statistics
    - Threat Rating Summary by VM Module
    - Threat Rating Breakdown by VM Module
    - Threat Rating Breakdown by File Type and VM Module
    - Threat Rating Breakdown by Time and VM Module
    - Average Threat Rating Duration by VM Module
    - Average Threat Rating Duration by Time and VM Module

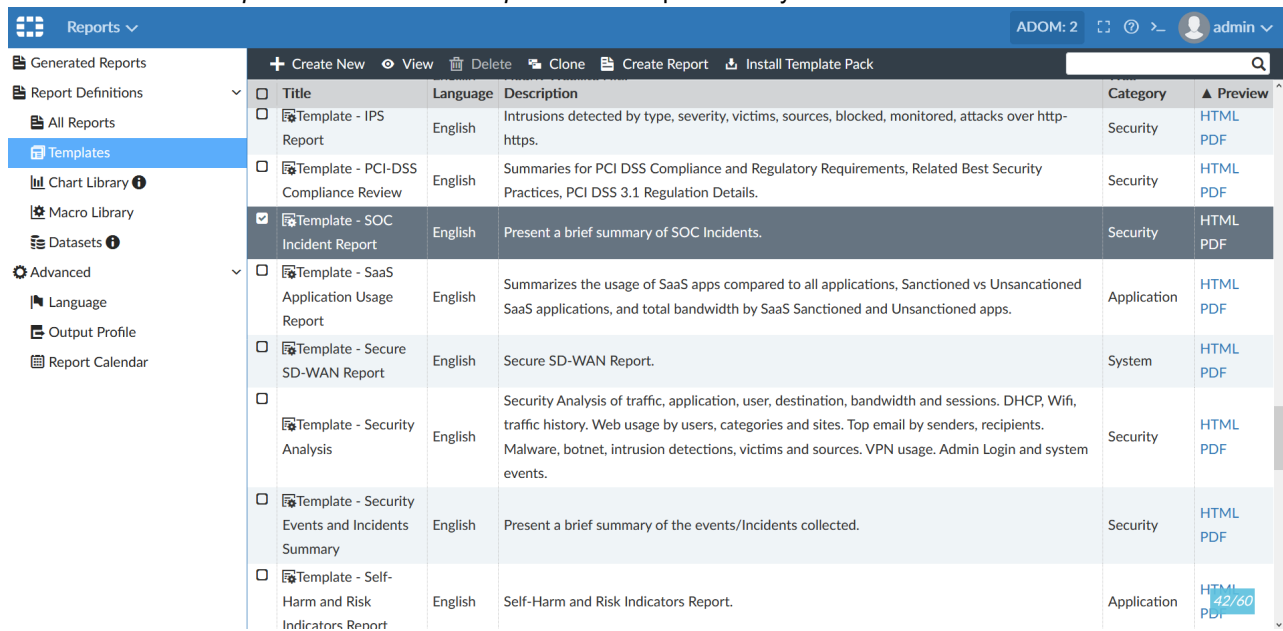


## Improved SOC incident report - 6.4.2

The SOC incident report has been added to the list of predefined report templates. This summary report will provide statistics on SOC incidents by their status, severity and category.

**To view the SOC incident report:**

1. Go to *Reports > Report Definitions > Templates*.  
You can see the *Template - SOC Incident Report* in the template library.



2. On the *All Reports* page, you can view the *SOC Incident Report*.

Reports									
ADOM: 2 [Icons] admin									
Generated Reports	<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Clone</a> <a href="#">Run Report</a> <a href="#">Folder</a> <a href="#">More</a> <a href="#">Show Scheduled Only</a>								
Report Definitions									
All Reports									
Templates									
Chart Library									
Macro Library									
Datasets									
Advanced									
Language									
Output Profile									
Report Calendar									
	Title	Language	Cache Status	Time Period	Devices	Schedule	Report Owner		
<input type="checkbox"/>	GTP Report	English							
<input type="checkbox"/>	High Bandwidth Application Usage Report	English							
<input type="checkbox"/>	IPS Report	English							
<input type="checkbox"/>	PCI-DSS Compliance Review	English							
<input type="checkbox"/>	SaaS Application Usage Report	English							
<input type="checkbox"/>	Secure SD-WAN Report	English		Last 7 Days	All_FortiGate				
<input type="checkbox"/>	Security Analysis	English							
<input type="checkbox"/>	Security Events and Incidents Summary	English							
<input type="checkbox"/>	Self-Harm and Risk Indicators Report	English							
<input type="checkbox"/>	Situation Awareness Report	English							
<input checked="" type="checkbox"/>	SOC Incident Report	English		Last 7 Days	All_FortiGate				
<input type="checkbox"/>	Social Media Usage Report	English							
<input type="checkbox"/>	Threat Report	English							
<input type="checkbox"/>	User Security Analysis	English							
<input type="checkbox"/>	VPN Report	English							
<input type="checkbox"/>	Web Usage Report	English							
<input type="checkbox"/>	What is New Report	English							
<input type="checkbox"/>	WiFi Network Summary	English							
<input type="checkbox"/>	Wireless PCI Compliance	English							

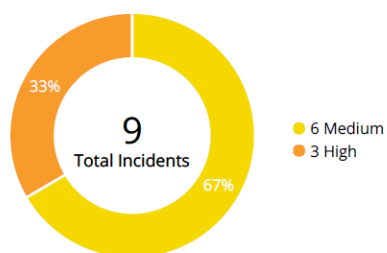
The SOC Incident Report contains new charts, including *Incidents by Severity*, *Incidents by Status*, *Unresolved Incidents by Category*, and *Unresolved Incidents by Severity*.

FORTINET

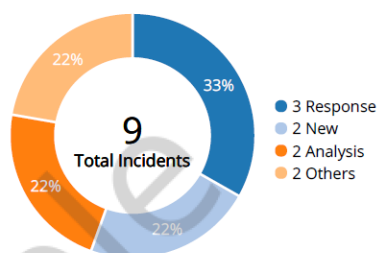
## SOC Incident Report

This report provides a summary of the SOC incidents between 2020-07-02 14:00:00 and 2020-07-03 13:59:59.

Incidents by Severity



Incidents by Status



Unresolved Incidents by Category



Unresolved Incidents by Severity

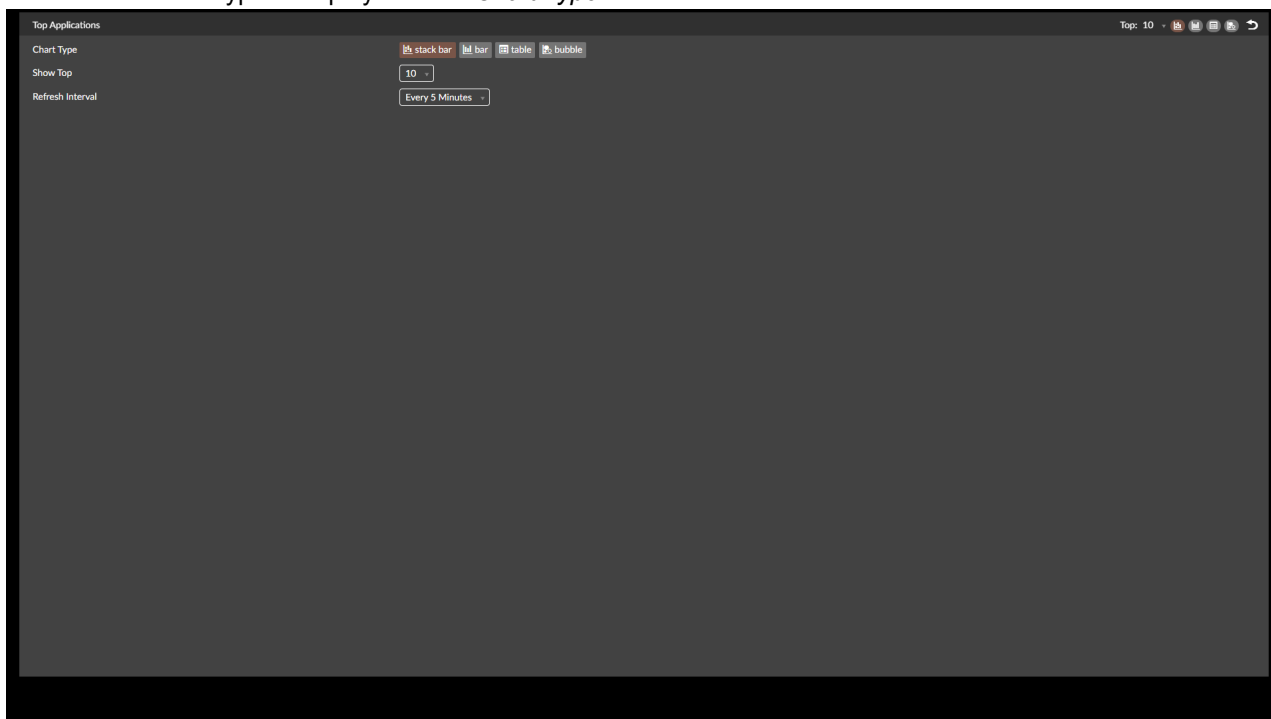


## Add stackbar chart in FortiView - 6.4.2

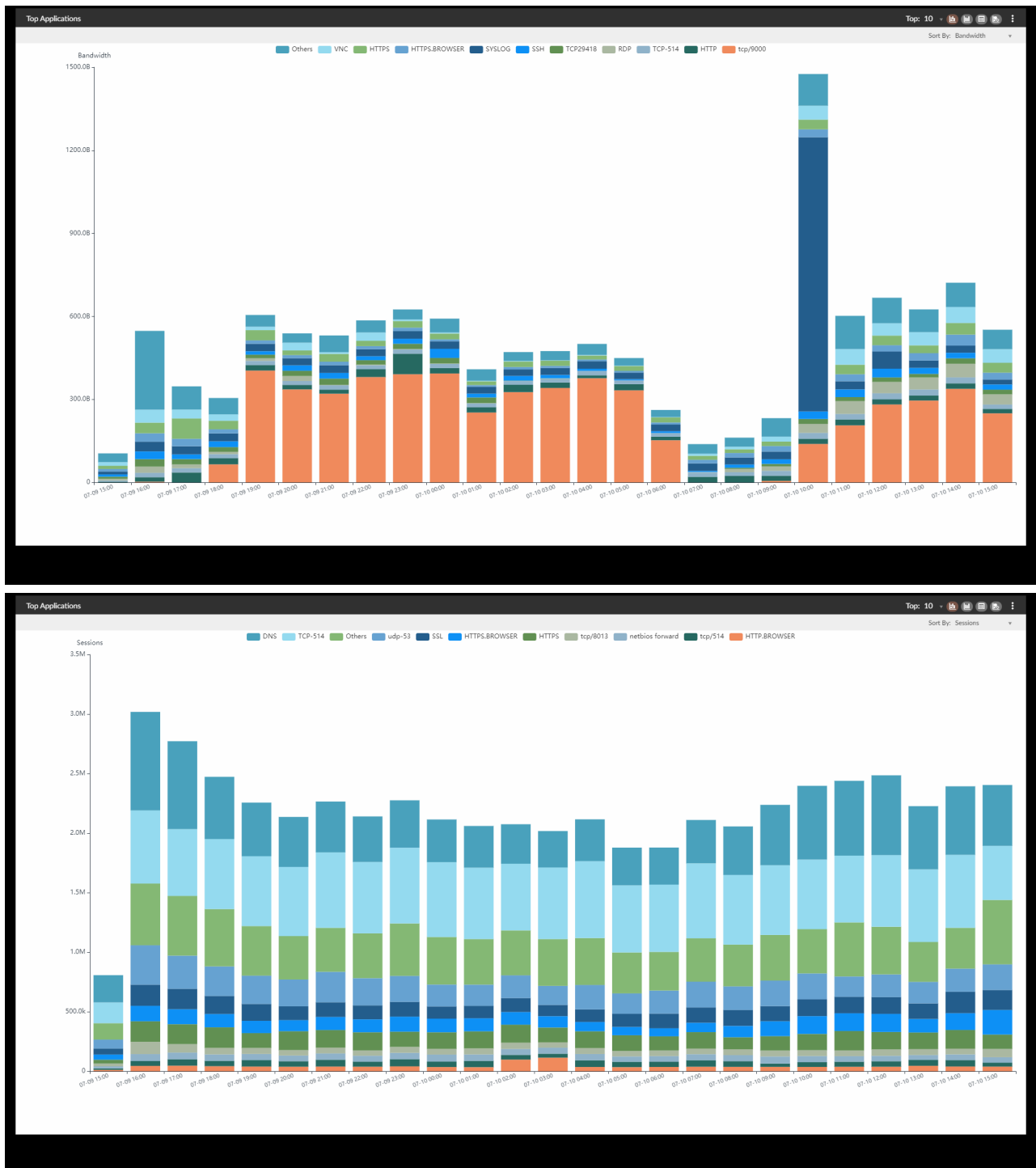
A new chart type, stack bar chart, is added to the *Top Application* widget under the *Applications & Websites* dashboard in *FortiView* to show the total bandwidth/session stacked by each application over time.

### To view the stackbar chart in FortiView:

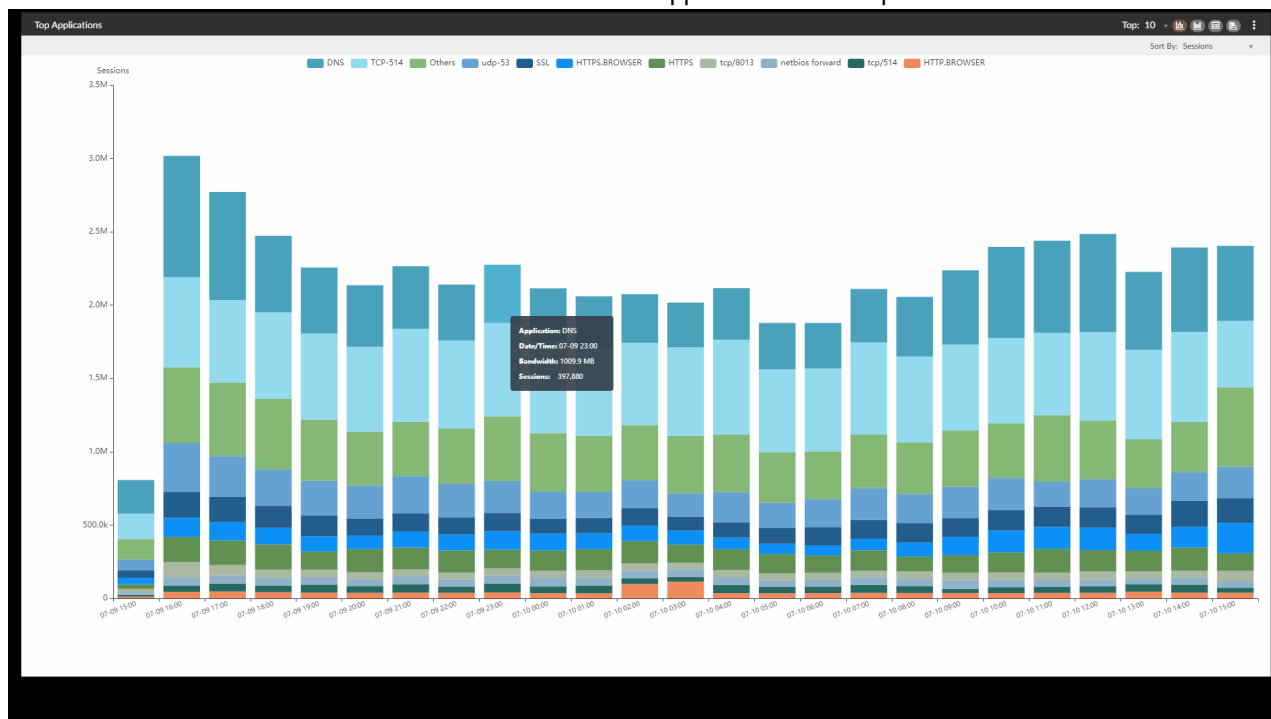
1. Go to *FortiView > Monitors > Applications & Websites > Top Applications* and select the settings icon. The stackbar chart type is displayed in the *Chart Type* list.



The stackbar chart shows stacked bars for the top 5/10 applications as well as other applications over the specified time period. The Y axis can be set as *Bandwidth* or *Sessions*. Each color in the stacked bar chart represents a different application.



2. Mouse over a bar in the chart to show details of the related application in a tooltip.



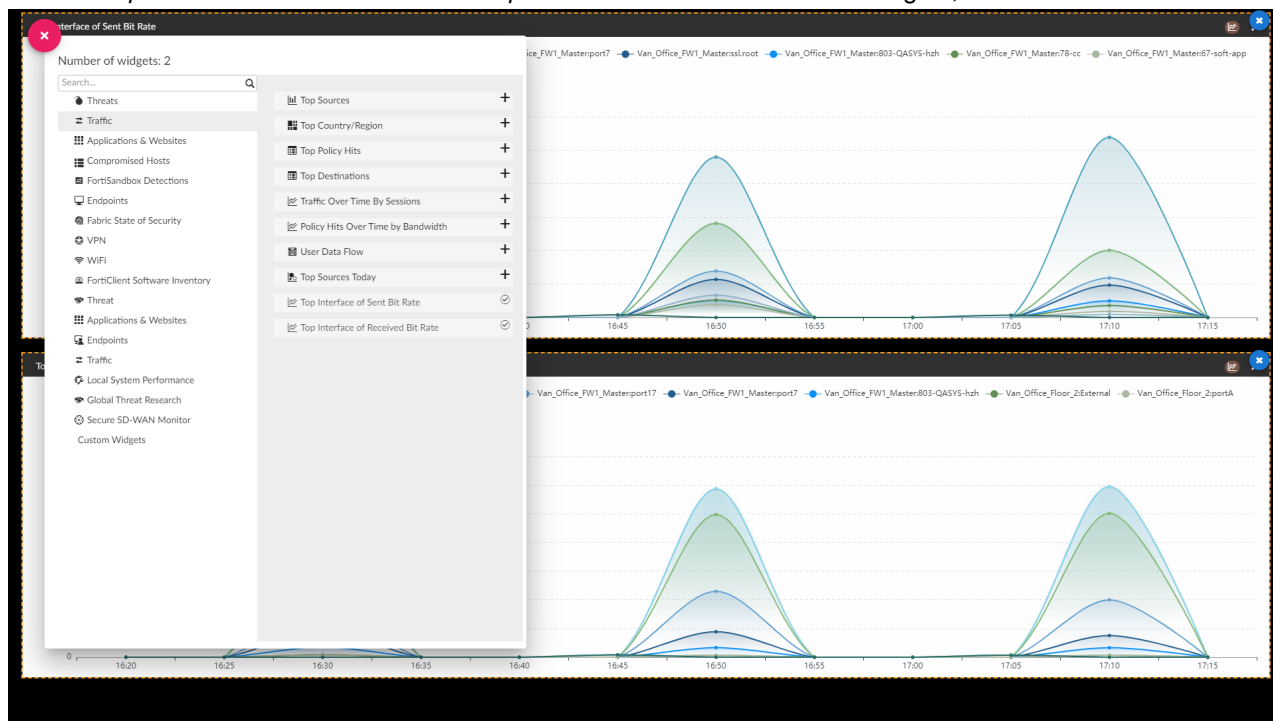
## Interface bandwidth widgets - 6.4.2

Two new widgets, *Top Interface of Sent Bit Rate* and *Top Interface of Received Bit Rate*, were added to *FortiView* under the *Traffic* category to provide bandwidth visibility on different interfaces over time.

### To add interface bandwidth widgets in the GUI:

1. Go to *FortiView* > *Monitors*, and click the *Traffic* category in the tree menu.
2. In the toolbar, click *Edit Dashboard* and then click the add icon.

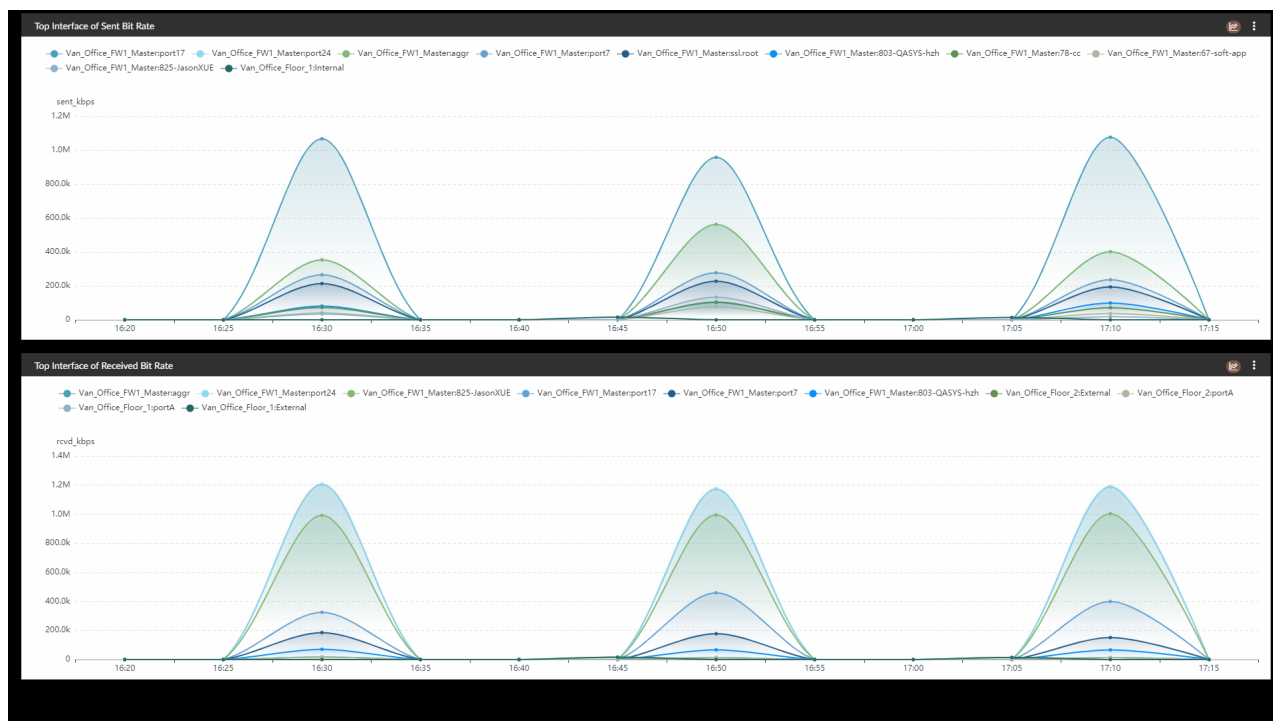
3. Add the *Top Interface of Sent Bit Rate* and *Top Interface of Received Bit Rate* widgets, and click *Done*.



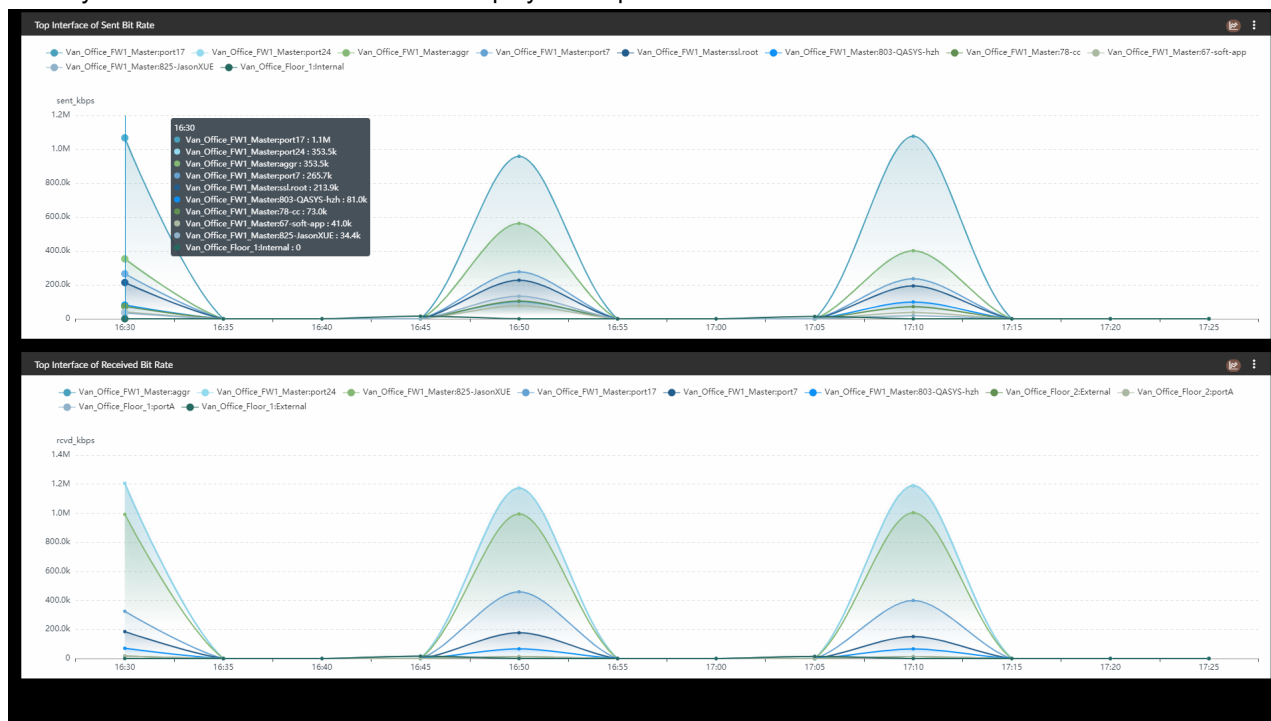
The *Top Interface of Sent Bit Rate* widget shows line charts for top 10 sent bit rate of interfaces during the specified time period.

The *Top Interface of Received Bit Rate* widget shows line charts for top 10 received bit rate of interfaces during the specified time period.

Different colors represent the different interfaces in both of the line charts.



4. Hover your mouse over the line charts to display a tooltip that shows the bit rate for each interface.



## EMS classification tag - 6.4.3

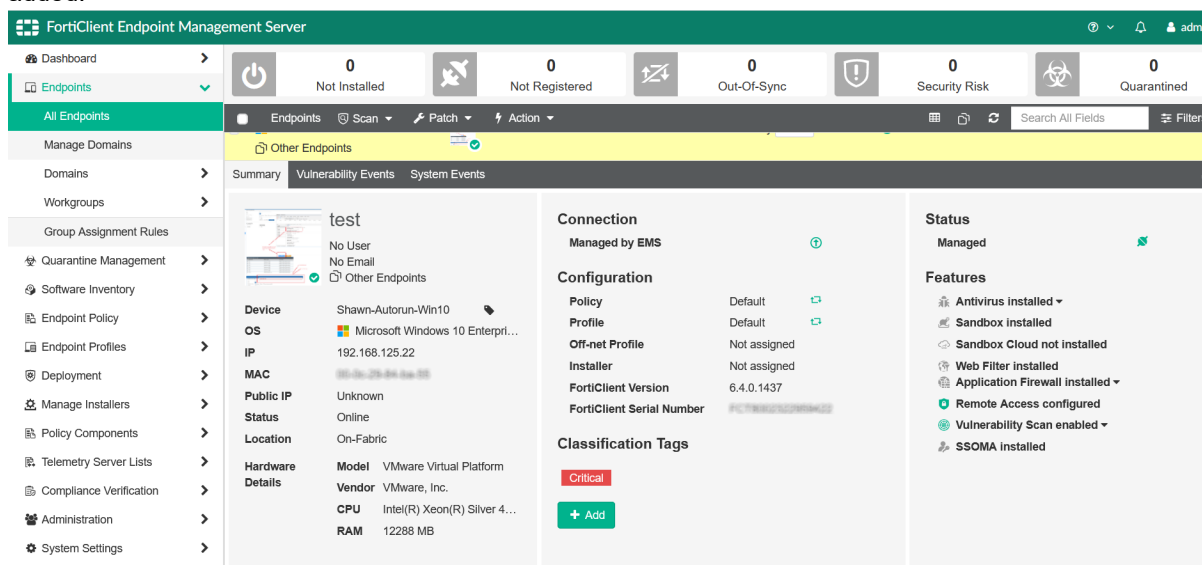
This is an enhancement to the Asset and Identity View enriching endpoints information with classification tags from EMS.

### To view EMS classification tags in Assets:

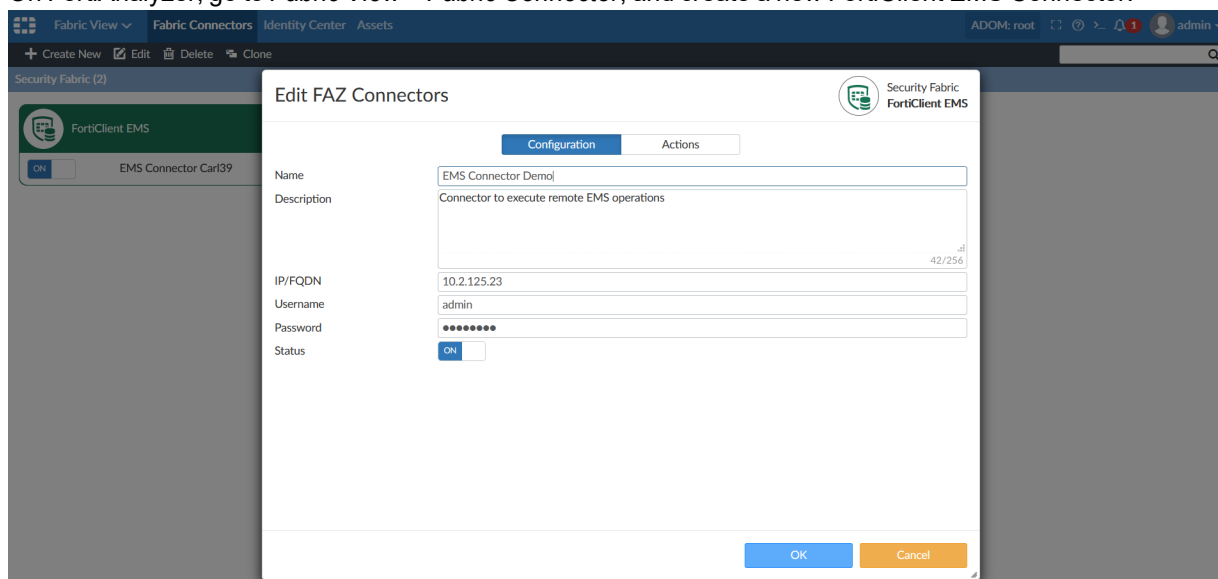
1. On the FortiClient EMS Server, go to *Endpoints > All Endpoints*, and select an endpoint.



2. In the *Summary* tab in the *Classification Tabs* category, click *Add* and add a tag. In this example, the *Critical* tag is added.



3. On FortiAnalyzer, go to *Fabric View > Fabric Connector*, and create a new FortiClient EMS Connector.



4. Go to *FortiSoC > Playbooks*, and create a customized playbook with a task to *Get Endpoints*, and a second task to *Update Asset and Identity*.

The image displays two screenshots of the FortiSoC interface, showing the configuration of a custom playbook named "GetEndpoints\_Demo".

**Top Screenshot:** The "GetEndpoints\_Demo" configuration window is shown. The left sidebar lists navigation options: Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbook, Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, Custom View, Handlers, and Incidents. The main area shows a custom build playbook to get started, with a diagram illustrating the flow: ON\_DEMAND STARTER → GET\_ENDPOINTS Get\_Endpoints. The right panel shows the configuration for the "GET\_ENDPOINTS" step:

- Name: Get\_Endpoints
- Description: (empty)
- Connector: EMS Connector Demo
- Action: Get Endpoints
- Endpoint ID: No Data. Edit
- FortiClient ID: No Data. Edit

**Bottom Screenshot:** The "GetEndpoints\_Demo" configuration window is shown again, but the right panel now shows the configuration for the "LOCALHOST\_UPDATE\_ASSET\_AND\_IDENTITY" step:

- Name: Update\_Assets
- Description: (empty)
- Connector: Local Connector
- Action: Update Asset and Identity
- Endpoint: Get\_Endpoints (id\_c7b\_b... | ems\_endpoints

Save and run the playbook, and check the *Playbook Monitor* to confirm the playbook was run successfully.

The screenshot shows the FortiSO interface. On the left is a navigation menu with options like Dashboards, Playbooks, Incidents, Events, Automation, Connectors, Playbook, Playbook Monitor, Event Monitor, All Events, By Endpoint, By Threat, System Events, Custom View, Handlers, and Incidents. The main area displays a table of Playbook tasks. A modal window titled 'Playbook Tasks' is open, showing a table with columns: Task ID, Task, Start Time, End Time, and Status.

Task ID	Task	Start Time	End Time	Status
id_6aa_9dc_0d2_bc0	Update_Assets	2020-09-18 11:53:44 -0700	2020-09-18 11:53:44 -0700	Success
id_c7b_b58_35d_33c	Get_Endpoints	2020-09-18 11:53:14 -0700	2020-09-18 11:53:19 -0700	Success

5. Go to **Fabric View > Assets** to check the endpoints. The applied tag (Critical) has been applied to the endpoint.

The screenshot shows the FortiSO Fabric View Assets page. At the top, there are two circular statistics: '2 Total Users' and '14 Total Endpoints'. Below these, there are two donut charts showing '2 new users discovered' and '3 new endpoints discovered'. The main area is a table with columns: Endpoint, Tags, User, MAC Address, IP Address, FortiClient UUID, Hardware Software, Vulnerabilities, Network Location, and Last. The table lists several endpoints, including Alice-Desktop-BK, WinServer\_2012, and Shawn-Autorun-Win10.

Endpoint	Tags	User	MAC Address	IP Address	FortiClient UUID	Hardware Software	Vulnerabilities	Network Location	Last
Alice-Desktop-BK	Low,all_registered_clients			192.168.22.5		WIN64			20
WinServer_2012	Low,all_registered_clients	Frank		192.168.22.6		WIN64			20
Shawn-Autorun-Win10	Critical,all_registered_clients	test		192.168.125.22		WIN64			20
10.2.60.64				10.2.60.64				FG101E-PF170/wan1	20
10.2.90.63				10.2.90.63				FG101E-PF170/wan1	20
10.2.90.64				10.2.90.64				FG101E-PF170/wan1	20

## Throughput utilization billing reporting - 6.4.3

This report enables users to generate the throughput consumption reporting for the billing purposes through utilizing interface bandwidth consumption information logged by FortiGate. You must also enable the "billing-report" option under interface-stats in the FortiAnalyzer CLI in order to use this report.

### Dependencies

- The FortiGate must be connected directly to the FortiAnalyzer.
- The FortiGate must have at least one interface configured with the WAN role.
- Before running this report, billing must be enabled for 24 hours or longer.

## To setup the FortiGate device and FortiAnalyzer:

1. In the FortiAnalyzer CLI, enter the following command to enable billing report config:

```
config system log interface-stats
  set billing-report enable
end
```
2. In the FortiGate device's CLI, enter the following command to connect the device to the FortiAnalyzer:

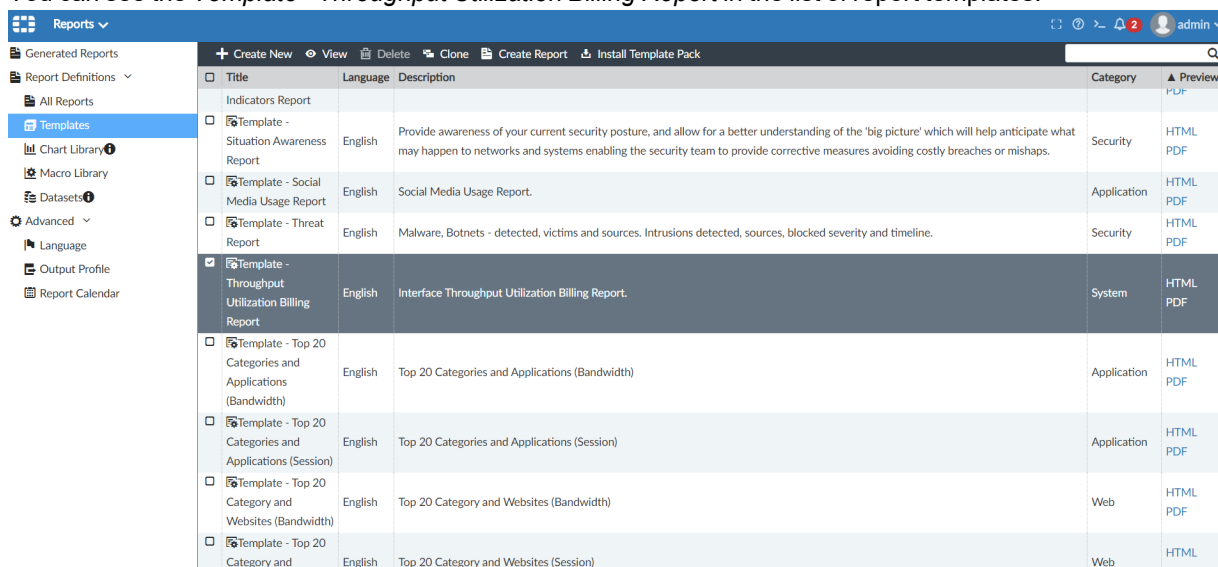
```
config log fortianalyzer setting
  set upload-option realtime
  set reliable enable
  set serial <FAZ-SN>
end
```

If you do not enter the FortiAnalyzer serial number in the above steps, you must configure the following in the FortiAnalyzer GUI:

1. Go to *Device Manager*, select the FortiGate device, and click *Edit*.
2. Set the *Admin User* and *Password* fields correctly for the device.
3. Click *OK*.

## To view the Throughput Utilization Billing Report:

1. On FortiAnalyzer, go to *Reports > Templates*.  
You can see the *Template - Throughput Utilization Billing Report* in the list of report templates.



Title	Language	Description	Category	Preview
Indicators Report				
Template - Situation Awareness Report	English	Provide awareness of your current security posture, and allow for a better understanding of the 'big picture' which will help anticipate what may happen to networks and systems enabling the security team to provide corrective measures avoiding costly breaches or mishaps.	Security	HTML PDF
Template - Social Media Usage Report	English	Social Media Usage Report.	Application	HTML PDF
Template - Threat Report	English	Malware, Botnets - detected, victims and sources. Intrusions detected, sources, blocked severity and timeline.	Security	HTML PDF
<b>Template - Throughput Utilization Billing Report</b>	English	Interface Throughput Utilization Billing Report.	System	HTML PDF
Template - Top 20 Categories and Applications (Bandwidth)	English	Top 20 Categories and Applications (Bandwidth)	Application	HTML PDF
Template - Top 20 Categories and Applications (Session)	English	Top 20 Categories and Applications (Session)	Application	HTML PDF
Template - Top 20 Category and Websites (Bandwidth)	English	Top 20 Category and Websites (Bandwidth)	Web	HTML PDF
Template - Top 20 Category and Websites (Session)	English	Top 20 Category and Websites (Session)	Web	HTML PDF

2. Go to *Reports > All Reports*.  
You can see the *Throughput Utilization Billing Report* in the list of reports.

Reports

Generated Reports

Report Definitions

All Reports

Templates

Chart Library

Macro Library

Datasets

Advanced

Language

Output Profile

Report Calendar

Create New

Edit

Delete

Clone

Run Report

Folder

More

Show Scheduled Only

Title	Language	Cache Status	Time Period	Devices	Schedule	Report Owner
FortiProxy Web Usage Report	English					
FortiSandbox Default Report	English					
FortiWeb Default Report	English					
FortiWeb Web Application Analysis Report	English					
GTP Report	English					
High Bandwidth Application Usage Report	English					
IPS Report	English					
PCI-DSS Compliance Review	English					
SaaS Application Usage Report	English					
Secure SD-WAN Report	English		Last 7 Days	All_Device		admin
Security Analysis	English					
Security Events and Incidents Summary	English					
Situation Awareness Report	English		This Week	All_Device		
Social Media Usage Report	English					
Threat Report	English					
Throughput Utilization Billing Report	English		This Week	Branch_Office_02		admin
User Security Analysis	English					
VPN Report	English					
Web Usage Report	English					
What is New Report	English					
WiFi Network Summary	English					
Wireless PCI Compliance	English					

In the report's *Settings* tab you can select the interface from *Physical Ports* or *VLAN*.

Reports

Generated Reports

Report Definitions

All Reports

Templates

Chart Library

Macro Library

Datasets

Advanced

Language

Output Profile

Report Calendar

View Report

Settings

Layout

Name

Throughput Utilization Billing Report

Time Period

This Week

Devices

All Devices

Specify

Device

Branch\_Office\_01

Branch\_Office\_02

Enterprise\_Core

Select Device

Type

Single Report

Multiple Reports

Enable Schedule

Enable Notification

Enable Auto-cache

Filters

Advanced Settings

Interface

Click here to select

Click here to select

Click here to select

Select Entries (Total: 14)

PHYSICAL PORTS (7)

port1

port2

port3

port4

port5

port6

port7

VLAN (7)

FNAC\_Isolation

onboarding

onboarding

OK Cancel

Apply

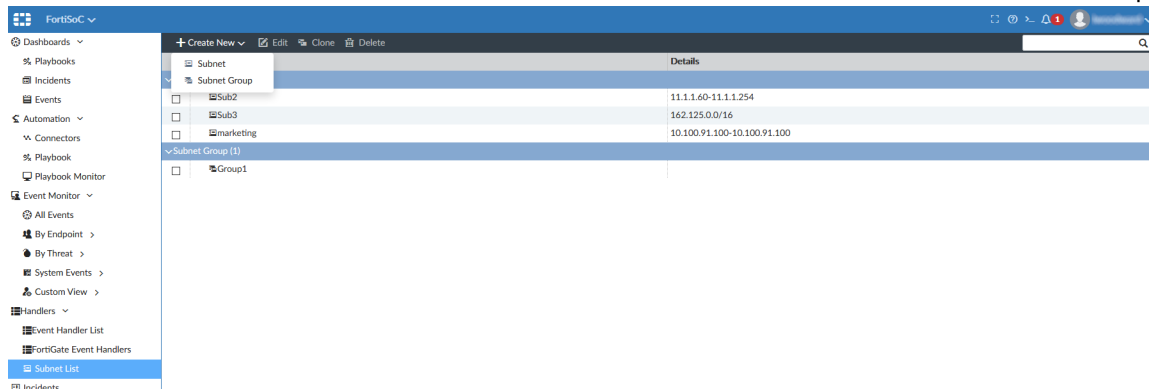
Return

### Subnet list for reports - 6.4.3

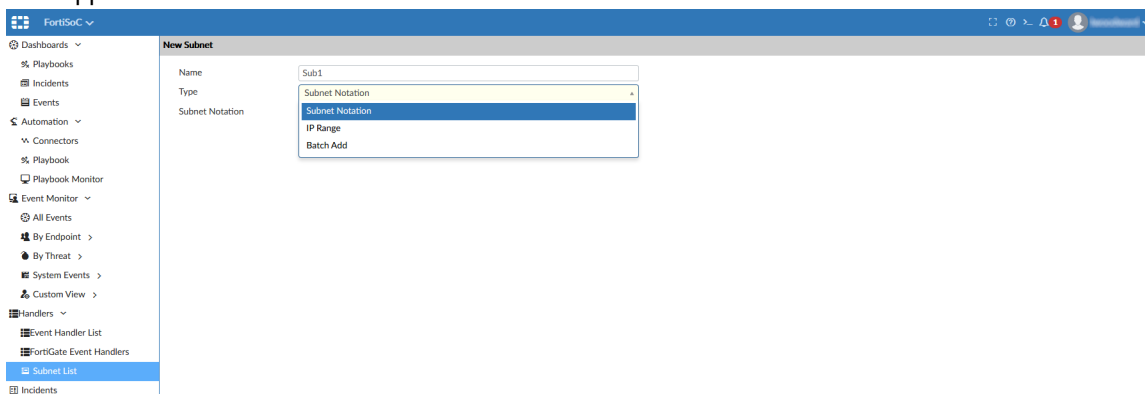
This new feature offers flexibility of filtering where specific subnets need to be included/excluded from reports.

## To configure subnet list for reports in the GUI:

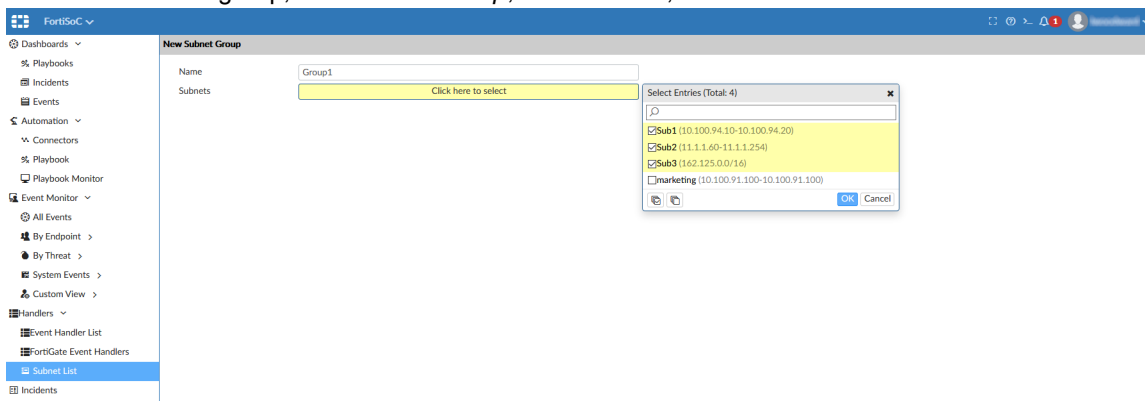
1. Go to *FortiSoC > Handlers > Subnet List* and click *Create New*. Create a new Subnet and Subnet Group:



- a. To create a subnet, click *Subnet*, enter a name, and select a *Type*. *Subnet Notation*, *IP Range*, and *Batch Add* are supported.



- b. To create a subnet group, click *Subnet Group*, enter a name, and select the subnet entries.



2. Go to *Reports > All Reports*, select a report, and click *Edit*.  
On the *Settings* tab you can see the *Subnets* setting which includes the options for *All Subnets* and *Specify*.
  - When *All Subnets* is selected, subnet and subnet groups are not specified and there is no filtering on `srcip` or `dstip` log fields based on subnets.

Reports ▾

Generated Reports  
Report Definitions ▾  
All Reports  
Templates  
Chart Library  
Macro Library  
Datasets  
Advanced ▾  
Language  
Output Profile  
Report Calendar

View Report Settings Layout

Name: 11cr\_test1

Time Period: Last N Days

N: 500

Devices: ☐ All Devices ☒ Specify

Subnets: ☒ All Subnets ☐ Specify

Type: ☒ Single Report ☐ Multiple Reports

☐ Enable Schedule  
☐ Enable Notification  
☐ Enable Auto-cache ⓘ

Filters >

Advanced Settings >

- When *Specify* is selected, the *Include Subnets* and *Exclude Subnets* options become available. You can specify which subnets and/or subnet groups are included and/or excluded from the list of available entries.

Reports ▾

Generated Reports  
Report Definitions ▾  
All Reports  
Templates  
Chart Library  
Macro Library  
Datasets  
Advanced ▾  
Language  
Output Profile  
Report Calendar

View Report Settings Layout

Name: 11cr\_test1

Time Period: Last N Days

N: 500

Devices: ☐ All Devices ☒ Specify

Subnets: ☒ All Subnets ☐ Specify

Include Subnets: Click here to select

Exclude Subnets: Click here to select

Type: ☒ Single Report ☐ Multiple Reports

☐ Enable Schedule  
☐ Enable Notification  
☐ Enable Auto-cache ⓘ

Filters >

Advanced Settings >

Select Entries (Total: 5)

SubNETS (4)

☒ marketing

☒ Sub1

☒ Sub2

☐ Sub3

SubNET GROUPS (1)

☐ Group1

OK Cancel

3. After the report settings are defined, run the report and check the results.  
Any logs with a `srcip` or `dstip` within the specified subnets are checked as analytical data for this report.

## Copy of Top Destinations by Bandwidth

#	Hostname(or IP)	Bandwidth	Sent	Received
1	dropbox.com			48.21 MB
2	dropboxapi.com			1.48 MB
3	162.125.34.129			501.84 KB
4	162.125.19.131			188.14 KB
5	162.125.18.133			60.71 KB
6	dropboxstatic.com			51.18 KB
7	162.125.1.3			41.11 KB
8	162.125.1.1			11.76 KB
9	162.125.36.1			9.49 KB
10	162.125.35.135			8.53 KB
11	162.125.7.1			7.12 KB
12	getdropbox.com			7.12 KB
13	162.125.1.7			7.09 KB
14	162.125.4.1			4.93 KB
15	162.125.68.1			4.93 KB
16	162.125.3.1			4.88 KB
17	162.125.64.1			4.88 KB
18	162.125.66.1			4.88 KB
19	162.125.67.1			4.88 KB
20	162.125.2.1			4.88 KB
21	162.125.70.1			4.88 KB
22	162.125.71.1			4.88 KB
23	162.125.72.1			4.88 KB
24	162.125.80.1			4.88 KB
25	162.125.81.1			4.88 KB
26	162.125.82.1			4.88 KB
27	162.125.9.1			4.88 KB
28	162.125.5.1			4.88 KB
29	162.125.6.1			4.88 KB
30	162.125.65.1			4.85 KB
31	162.125.69.1			4.84 KB
32	162.125.11.1			4.84 KB
33	162.125.83.1			4.84 KB
34	162.125.8.1			4.84 KB
35	162.125.35.134			2.39 KB
36	162.125.7.13			2.03 KB
37	162.125.19.9			708 B
38	162.125.2.7			416 B
39	162.125.19.130			416 B
40	162.125.2.13			416 B

Defined subnet information for included and excluded subnets is displayed in the report as *Appendix B*.

## Appendix B

## Subnets

# Include	Exclude
1 162.125.0.0-16	162.125.192.0-18

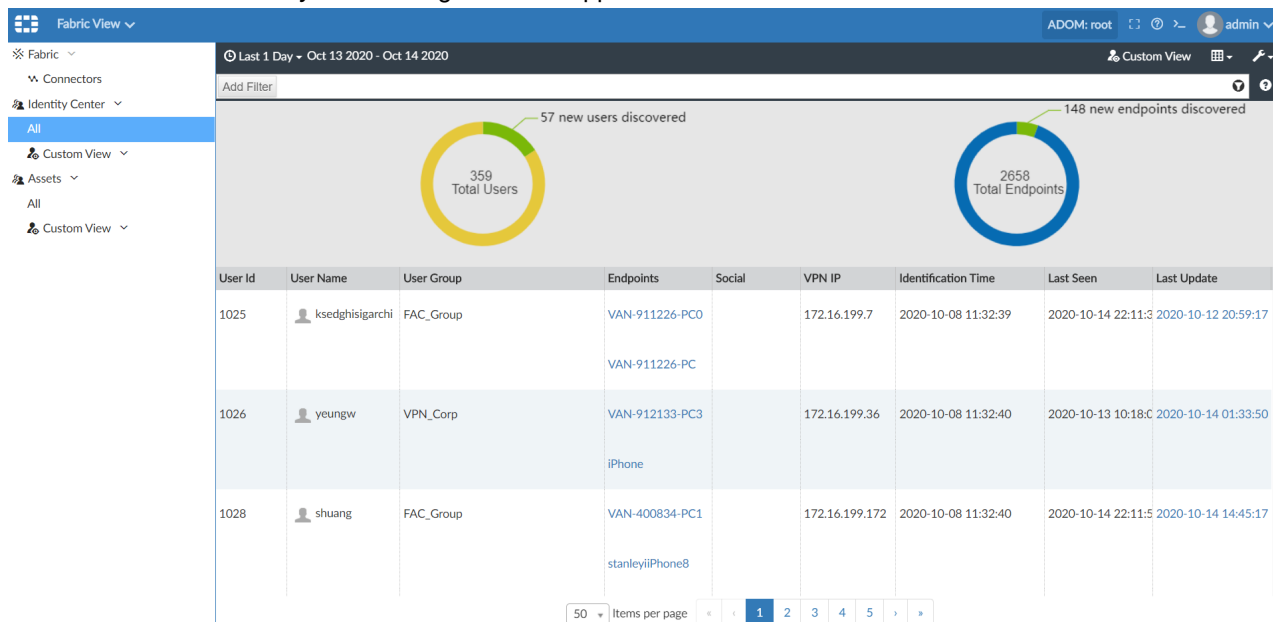
## Asset & Identity View Improvement - 6.4.3

These improvements offer more flexibility to the asset and identity views and address SOC operations limitations identified in the Asset and Identity center.

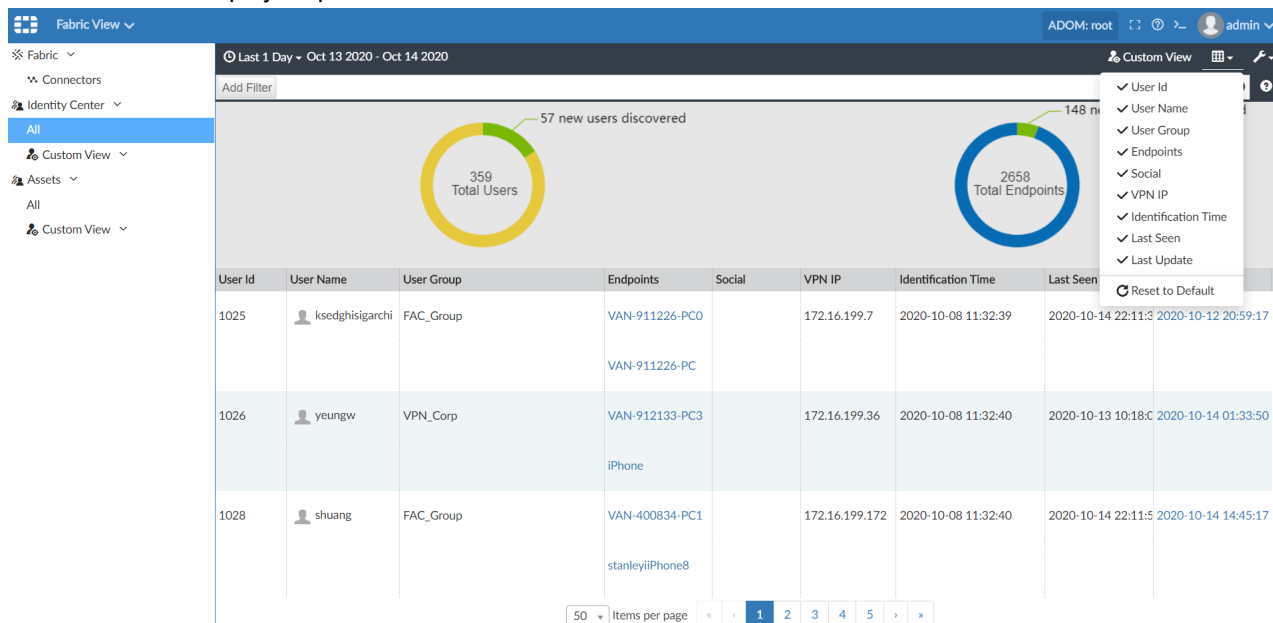


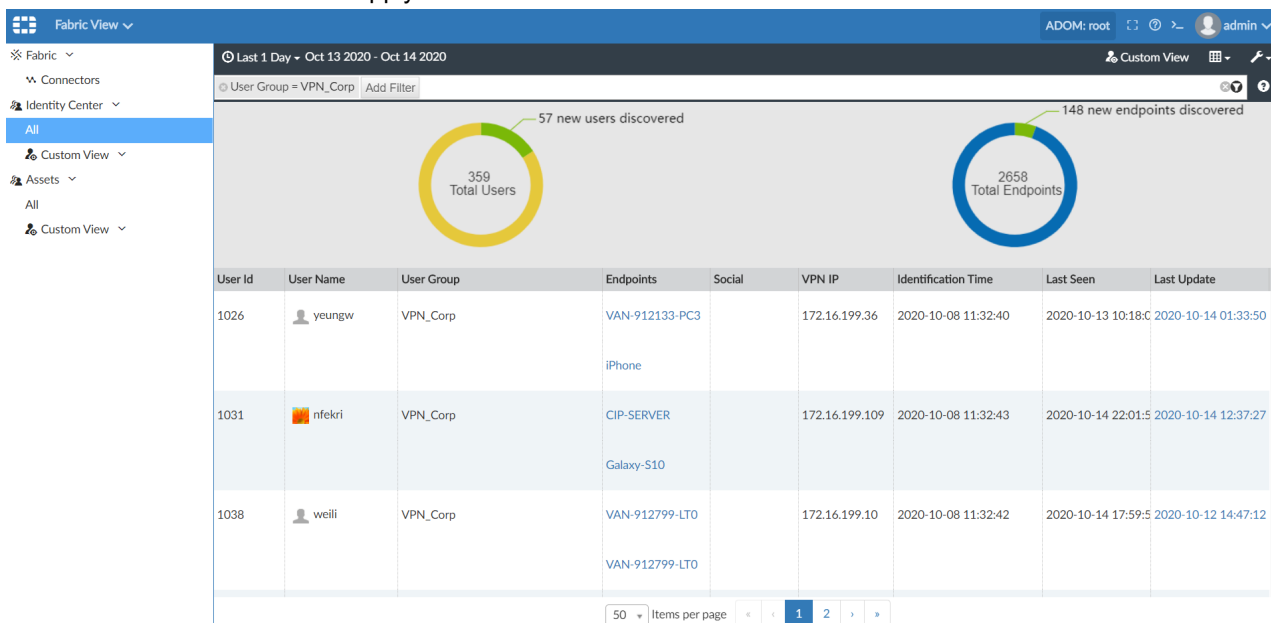
## To view the improvements in the Identity center:

1. Go to *Fabric View > Identity Center*. Pagination is supported and new columns such as *VPN IP* were added.



2. Click the column display dropdown to add or remove columns in the view.



3. Click **Add Filter** in the toolbar to apply a custom filter.

The filter is applied to the view

The screenshot shows the FortiAnalyzer Fabric View interface with the 'VPN\_Corp' filter selected in the left sidebar. The table lists five users: yeungw, nfekri, weilii, chenh, and zǎng, each with their respective endpoints and last seen dates.

User Id	User Name	User Group	Endpoints	Social	VPN IP	Identification Time	Last Seen	Last Update
1026	yeungw	VPN_Corp	VAN-912133-PC3 iPhone		172.16.199.36	2020-10-08 11:32:40	2020-10-13 10:18:00	2020-10-14 01:33:50
1031	nfekri	VPN_Corp	CIP-SERVER Galaxy-S10		172.16.199.109	2020-10-08 11:32:43	2020-10-14 22:01:50	2020-10-14 12:37:27
1038	weilli	VPN_Corp	VAN-912799-LT0 VAN-912799-LT0		172.16.199.10	2020-10-08 11:32:42	2020-10-14 17:59:50	2020-10-12 14:47:12
1040	chenh	VPN_Corp	haodeMBP		172.16.199.60	2020-10-08 11:32:42	2020-10-13 14:39:00	2020-10-14 21:30:39
1048	zǎng	VPN_Corp	Galaxy-S10 VAN-912386-PC0		172.16.199.66	2020-10-08 11:32:43	2020-10-13 14:39:00	2020-10-12 18:16:44

4. Click *Custom View* to save the current view.

Save as New Custom View

Name: VPN\_Corp

Time Period: Last 1 Day

Search: eugroup='VPN\_Corp'

OK Cancel

User Id	User Name	Identification Time	Last Seen	Last Update
1026	yeungw	2020-10-08 11:32:40	2020-10-13 10:18:5	2020-10-14 01:33:50
1031	nfekri	2020-10-08 11:32:43	2020-10-14 22:01:5	2020-10-14 12:37:27
1038	weili	2020-10-08 11:32:42	2020-10-14 17:59:5	2020-10-12 14:47:12

5. Click *OK*. The view is added to *Custom View* in the tree menu.

Custom View

468 Total Users

468 new users discovered

3408 Total Endpoints

3408 new endpoints discovered

Endpoint Id	Endpoint Name	User	MAC Address	IP Address	FortiClient UUID	Source	Hardware / C	Last Seen
1030	Leis-iPhone		9c:e3:3f:2f:40:d9	172.17.240.32		New_Van_Office_	iOS	2020-10-13 14:40:09
1031	Galaxy-A50		b0:6f:e0:61:72:f4	172.17.240.255		New_Van_Office_	Android	2020-10-14 09:33:08
1032	iPhone		74:1b:b2:43:61:93	172.17.241.41		New_Van_Office_	iOS	2020-10-14 10:31:46
1033	meow-phone		f8:95:ea:17:bd:af	172.17.241.35		New_Van_Office_	iOS	2020-10-14 10:15:53
1034	iCharing		36:2b:32:02:ac:8d	172.17.240.162		New_Van_Office_	iOS	2020-10-13 14:36:39
1035	Miphone		7e:74:d7:a9:43:f8	172.17.240.24		New_Van_Office_	iOS	2020-10-13 14:37:13

## To view Assets improvements:

1. Go to *Fabric View > Assets*. More options have been added to the column display dropdown.

468 Total Users

3408 Total Endpoints

468 new users discovered

3408 new endpoints discovered

Endpoint Id	Endpoint Name	User	MAC Address	IP Address	FortiClient UUID	Source	Hardware / OS
1026	Bruce-iPhone		96:98:ee:94:73:80	172.17.240.93		New_Van_Office	iOS
1027	VAN-911226-PC	ksedghisigarchi	d8:3b:bf:c6:0c:c3	172.17.240.45	FFB022F026104E669E1DF	New_Van_Office	Windows
1028	VAN-912133-PC3	yeungw	7c:b2:7d:6d:0f:ab	172.17.240.166	31ECE30059DC4FD7A8A7	New_Van_Office	Windows
1029	MiMIX3-JohnMix3		a4:50:46:4d:0e:dd	172.17.241.32		New_Van_Office	Android
1030	Leis-iPhone		9ce3:3f:2f:40:d9	172.17.240.32		New_Van_Office	iOS
1031	Galaxy-A50		b0:6f:e0:61:72:f4	172.17.240.255		New_Van_Office	Android

2. Click *Add Filter* in the toolbar, and select a value from the list.

3408 Total Endpoints

3408 new endpoints discovered

Endpoint Id	Endpoint Name	User	MAC Address	IP Address	FortiClient UUID	Source	Hardware / OS	Last Seen
1026	Bruce-iPhone		96:98:ee:94:73:80	172.17.240.93		New_Van_Office	iOS	2020-10-13 14:42:50
1027	VAN-911226-PC	ksedghisigarchi	d8:3b:bf:c6:0c:c3	172.17.240.45	FFB022F026104E669E1DF	New_Van_Office	Windows	2020-10-12 10:03:27
1028	VAN-912133-PC3	yeungw	7c:b2:7d:6d:0f:ab	172.17.240.166	31ECE30059DC4FD7A8A7	New_Van_Office	Windows	2020-10-13 10:18:09
1029	MiMIX3-JohnMix3		a4:50:46:4d:0e:dd	172.17.241.32		New_Van_Office	Android	2020-10-08 11:32:40
1030	Leis-iPhone		9ce3:3f:2f:40:d9	172.17.240.32		New_Van_Office	iOS	2020-10-13 14:40:09
1031	Galaxy-A50		b0:6f:e0:61:72:f4	172.17.240.255		New_Van_Office	Android	2020-10-14 09:33:08

### 3. Click *Tools > Download*, to export entries as CSV file.

The screenshot displays the FortiAnalyzer Fabric View interface. On the left, a navigation pane shows the hierarchy: Fabric View > Connectors > Identity Center > All. The main area shows a summary of 468 Total Users and 3408 Total Endpoints, both circled in green. Below the summary is a table of endpoints with columns: Endpoint Id, Endpoint Name, User, MAC Address, IP Address, FortiClient UUID, Source, Hardware / OS, and Last Seen. The table lists several endpoints, including Bruce-iPhone, VAN-911226-PC, VAN-912133-PC3, MiMIX3-JohnMix3, and Leis-iPhone. A 'Download' button is visible in the top right corner of the main area.

Endpoint Id	Endpoint Name	User	MAC Address	IP Address	FortiClient UUID	Source	Hardware / OS	Last Seen
1026	Bruce-iPhone		96:98:ee:94:73:80	172.17.240.93		New_Van_Office_	iOS	2020-10-13 14:42:50
1027	VAN-911226-PC	kyedghuapach	d8:3b:bf:c6:0c:c3	172.17.240.45	FFB022F026104E669E1DF	New_Van_Office_	Windows	2020-10-12 10:03:27
1028	VAN-912133-PC3	yeungw	7c:b2:7d:6d:0f:ab	172.17.240.166	31ECE30059DC4FD7A8A7	New_Van_Office_	Windows	2020-10-13 10:18:09
1029	MiMIX3-JohnMix3		a4:50:46:4d:0e:dd	172.17.241.32		New_Van_Office_	Android	2020-10-08 11:32:40
1030	Leis-iPhone		9c:e3:3f:2f:40:d9	172.17.240.32		New_Van_Office_	iOS	2020-10-13 14:40:09

## Cyber-Physical Security

This section lists the new features added to FortiAnalyzer for cyber-physical security.

List of new features:

- [Facial Recognition 6.4.1 on page 143](#)
- [Zoom function in FortiRecorder 6.4.1 on page 149](#)

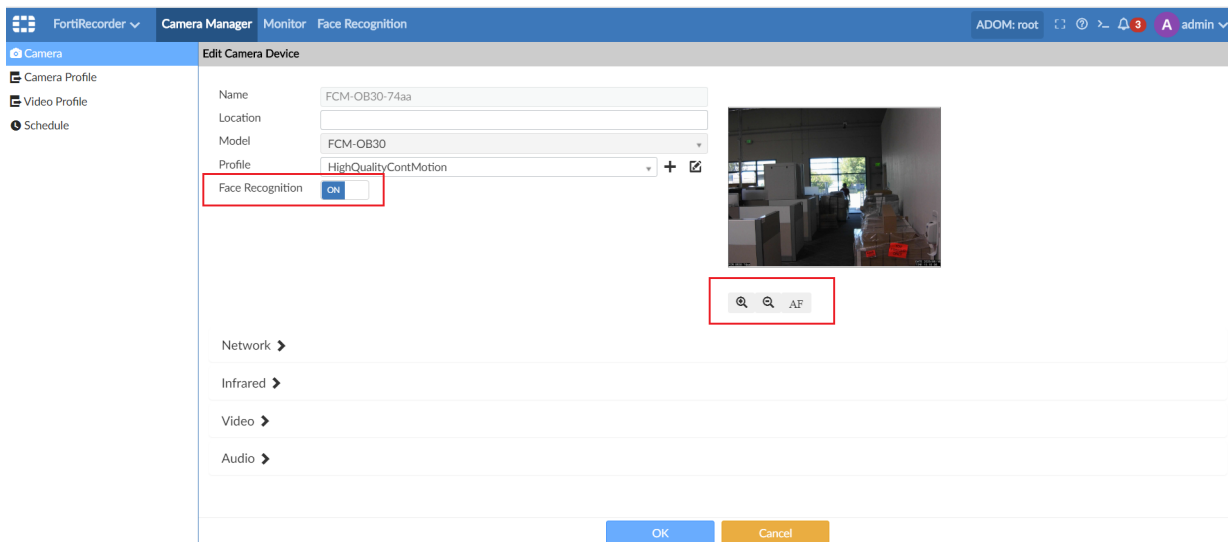
### Facial Recognition - 6.4.1

A new AI engine has been added to the FortiRecorder module to identify a person by analyzing patterns in the person's facial features. Faces detected by the camera can be used to enrich the *Assets and Identity* feature for UEBA correlation. The facial recognition feature allows SOC to easily perform video surveillance for its physical security from a single FortiAnalyzer console.

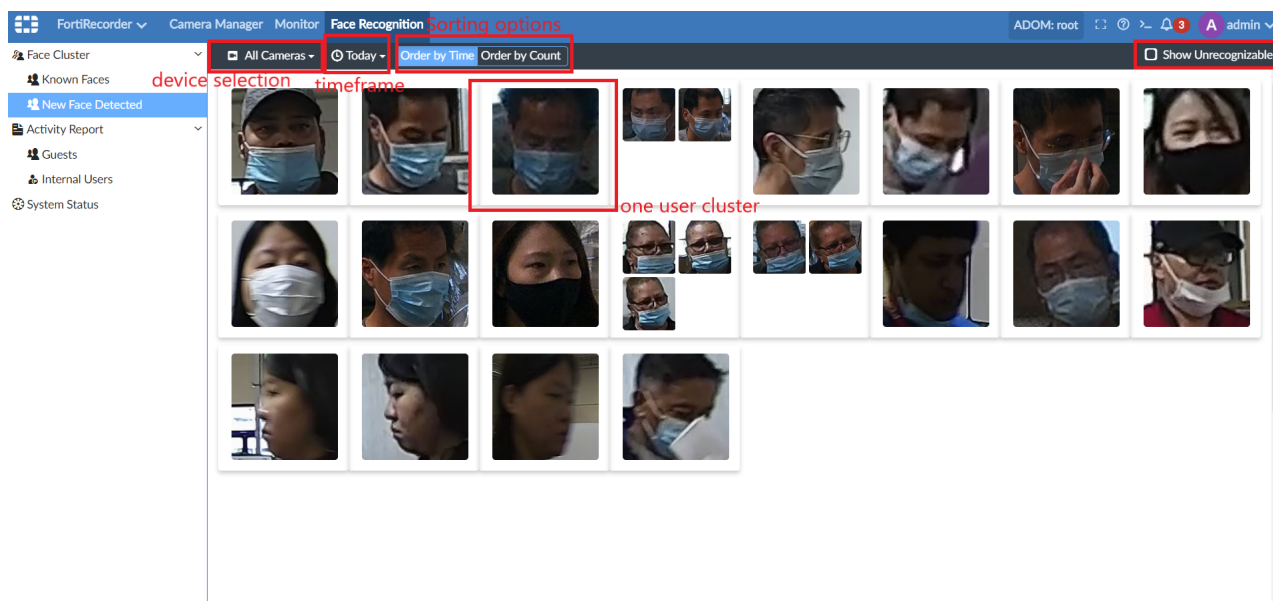
## GUI

### To enable face recognition in the GUI:

1. Go to *FortiRecorder* > *Camera Manager*.
2. In the tree menu, click *Camera* and select a managed camera in the pane.
  - a. Enable *Face Recognition*.
  - b. Click the *AF* icon to focus the camera.



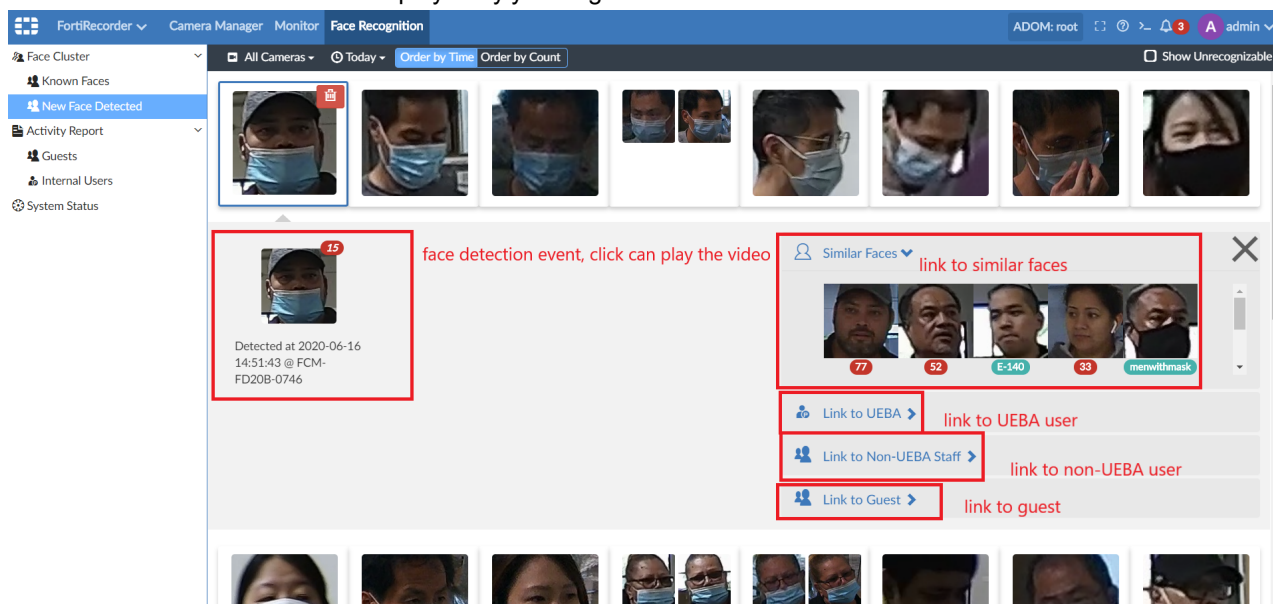
3. To view faces detected by the camera, go to *FortiRecorder* > *Face Recognition*, and click *New Face Detected* in the tree menu.
  - Similar faces are organized into clusters.
  - Each cluster represents a different user.
  - You can delete a face from a cluster or merge faces in a cluster.
  - Click the image in a cluster to watch a video of the user event.
  - Clusters can be ordered by count or time.



#### 4. Use the profile pane at the right side of the page to link faces to user profiles.

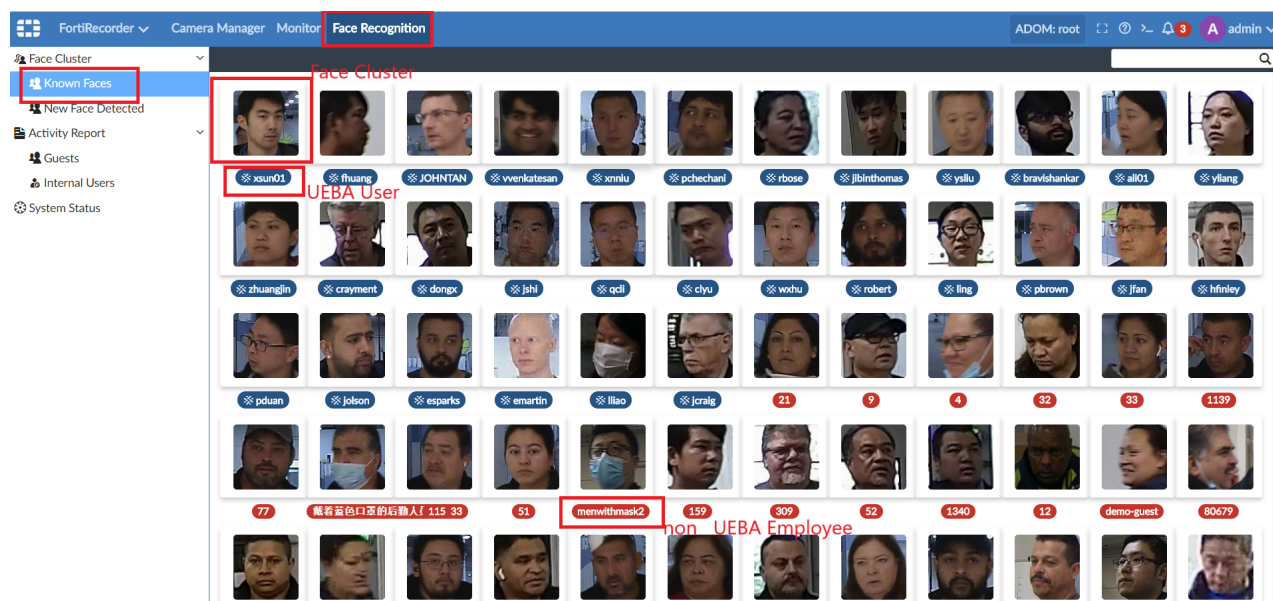
New faces can be linked to following profile types:

- **UEBA** : The user has an existing endpoint entry within FortiAnalyzer, and has information retrieved from FortiClient and FortiGate.
- **Non-UEBA Staff**: The user does not have an endpoint entry in FortiAnalyzer, but is employed by your organization. For example, a maintenance person.
- **Guest**: Someone who is not employed by your organization.



#### 5. In the tree menu, click *Known Faces* to view faces that are linked to a user profile.

- New events detected by the camera events are saved to the related known faces cluster.
- You can delete events from a cluster.
- Click the image to view a video of the event.
- You can order the clusters by count, or by the image time stamp.



### To view activity reports in the GUI:

1. In the tree menu, go to *Activity Report > Guests*.  
The report pane displays the user events.
  - a. Hover an event in the time line to view when the event was detected and the camera that detected it.
  - b. Click an event in the time line to watch a video of the event.
  - c. Use your scroll wheel to adjust the time frame.
  - d. Click *Reset Zoom* to reset the time line.

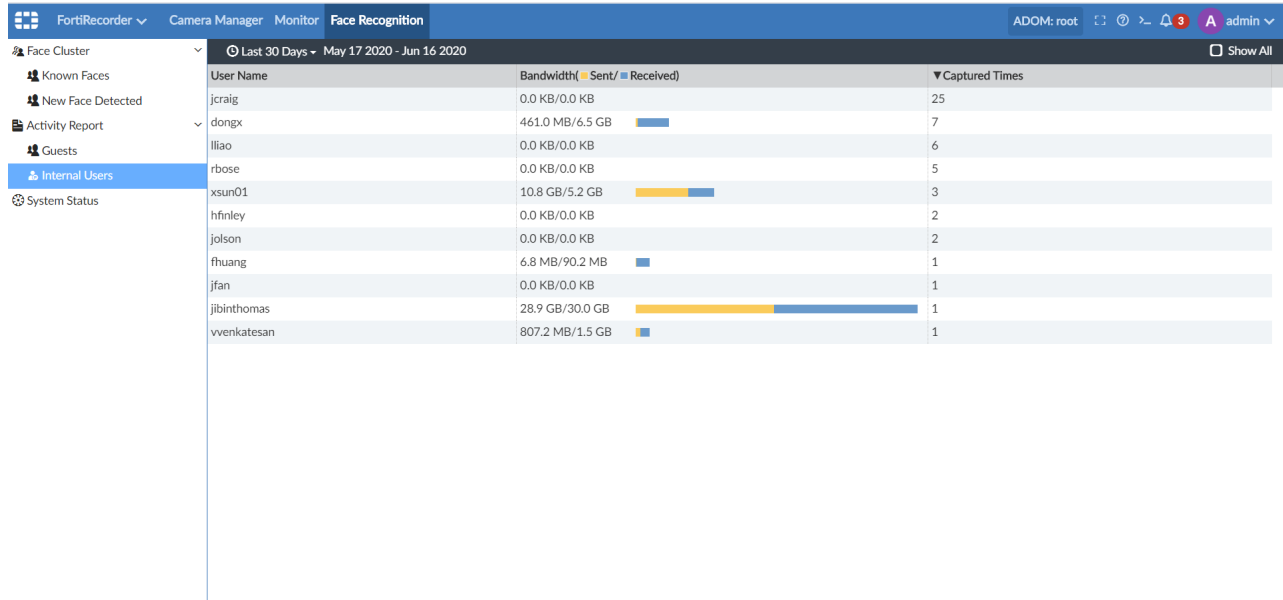


2. In the tree menu, go to *Activity Report > Internal Users*.  
Click a heading to sort a column in ascending or descending order. The following information is displayed:
  - *User Name*: The internal user name.
  - *Bandwidth (Sent/Received)*: The bandwidth sent and received from the camera in bytes.



- **Captured Times:** The number of times the camera captured an image of the user.

3. In the toolbar, click the time frame dropdown to specify the time period.



User Name	Bandwidth (Sent/Received)	Captured Times
jcraig	0.0 KB/0.0 KB	25
dongx	461.0 MB/6.5 GB	7
lliao	0.0 KB/0.0 KB	6
rbose	0.0 KB/0.0 KB	5
xsun01	10.8 GB/5.2 GB	3
hfinley	0.0 KB/0.0 KB	2
jolson	0.0 KB/0.0 KB	2
thuang	6.8 MB/90.2 MB	1
jfan	0.0 KB/0.0 KB	1
jibinthomas	28.9 GB/30.0 GB	1
vvenkatesan	807.2 MB/1.5 GB	1

## CLI

To enable and disable the AI module in the CLI:

```
config system global
# set disable-module
```



The disable-module command enables all of the AI modules.

To set the database and disk quota in the CLI:

1. Set disk quota for AI.

```
config system global
set ai-disk-quota value <disk limit in GB>
```

If the configuration is successful, the remaining available hard disk space shall be deducted accordingly.

2. Set database table item count limit.

```
execute face-recognition setting event_item_count_max <limit>
```

3. The *aisched* daemon cleans up the database and disk used by AI approximately once a day.

## CPU usage

CPU usage is managed by *nice*. The AI module has three daemons:

aid	Pre-processes videos with deep learning algorithms, which consumes lots of computational resources. The niceness is set to 19 (lowest priority).
-----	--

aiclusterd	Requires limited CPU/memory resource and is responsible for user interfaces. The niceness is set to default value 0.
aisched	Performs routine tasks,such as daily database clean up and requires very limited CPU/memory sources. The niceness is set to default value 0.

## Memory usage

Memory usage of daemon *aid* is controlled by *Cgroup*. If the limit is violated, daemon *aid* will be killed by Linux kernel.

The following CLI is used to update the maximum memory limitation. The default value is 4096.

```
config system global
    set ai-memory-quota <limit in MB>
end
```

## Face Recognition

Face recognition related CLIs have been added under the `execute face-recognition` command:

execute	face-recognition
backup	backup AI infos
log	AI log
process	process specific videos
restore	restore AI infos
setting	Show/Modify AI configuration

### To back up an AI user's personal information in the CLI:

```
execute face-recognition backup <ip:port> <filename><username><password>
```

Now we support restore from FTP server only.



Restoring an AI user's information is supported in the FTP server only.

---

### To insert a specific camera's into the AI database in the CLI:

```
execute face-recognition process <camera_name>
```

### To configure AI specific settings in the CLI:

Show all AI setting parameters:

```
execute face-recognition setting
```

Show a specific key value:

```
execute face-recognition setting <key>
```

Modify a specific key value:

```
execute face-recognition setting <key> <key_value>
```

## Event logs

Three log types have been added to the current log system:

LOG\_EVENT\_AID\_STATUS

LOG\_EVENT\_AID\_CONFIG

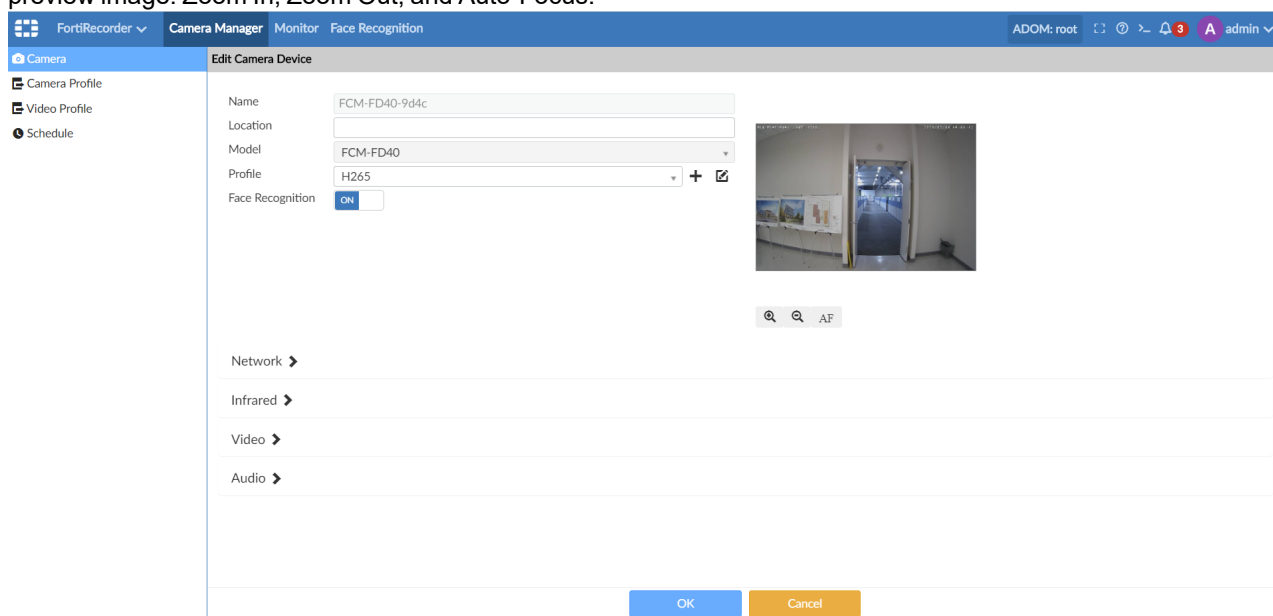
LOG\_EVENT\_AID\_UI

## Zoom function in FortiRecorder - 6.4.1

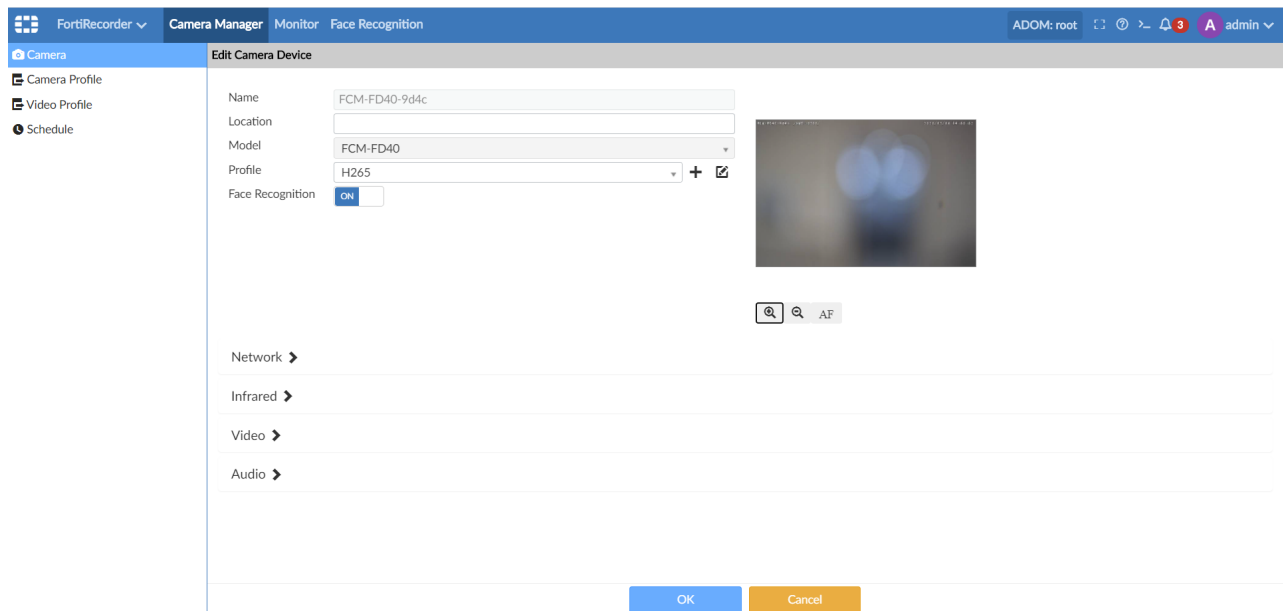
Zoom and auto focusing functions were added to the FortiRecorder module in FortiAnalyzer to improve the recorded video quality without manually focusing the cameras.

**To use the zoom and auto-focus functions in the GUI:**

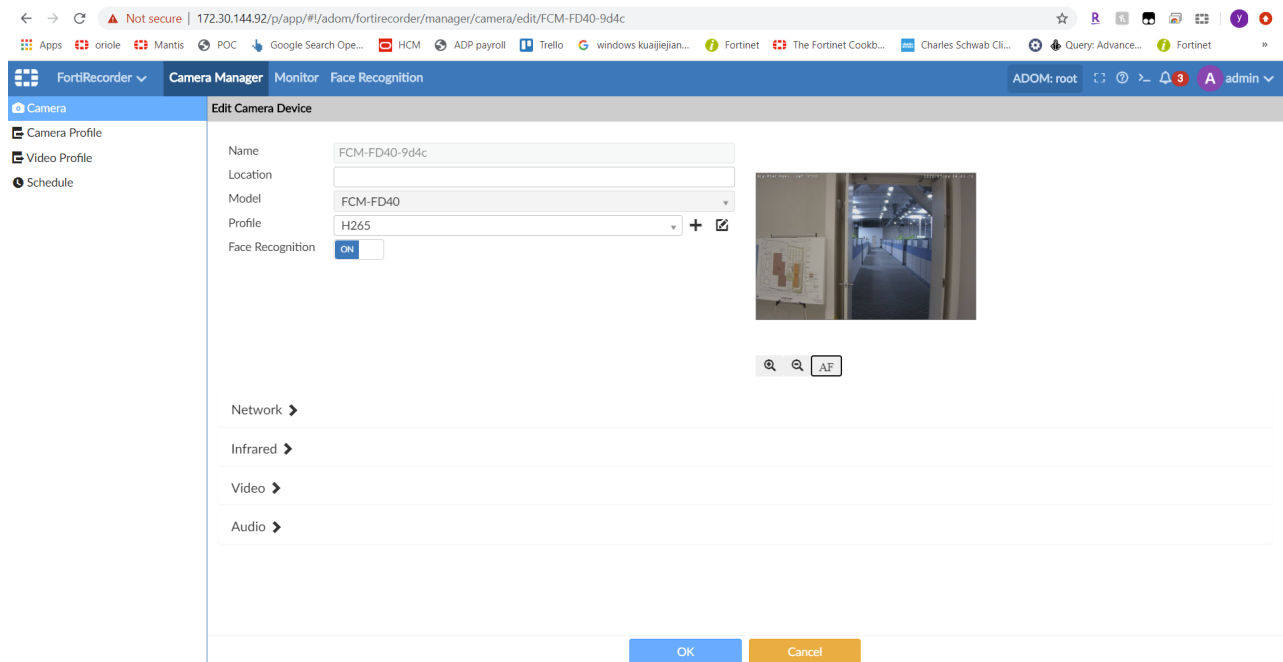
1. Go to *FortiRecorder > Camera Manager*.
2. In the tree menu, click *Camera*, and select an authorized camera from the list. Three new icons appear below the preview image: Zoom In, Zoom Out, and Auto-Focus.



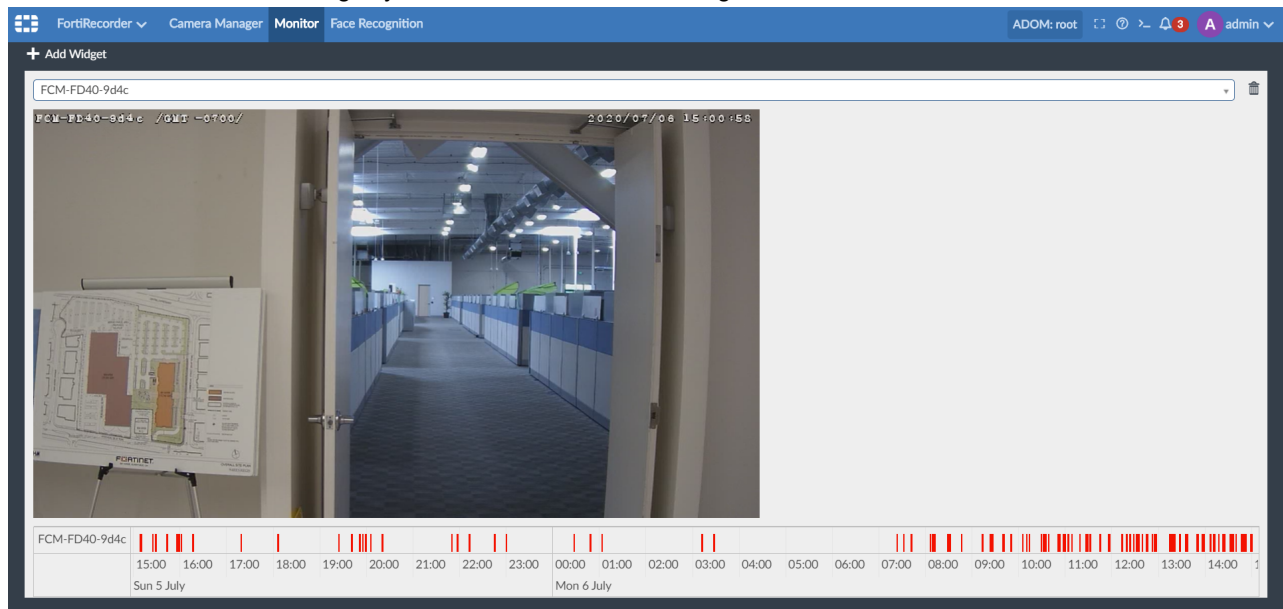
3. To zoom in, click the Zoom In icon several times, and then click the Auto-Focus icon. Wait several seconds for the camera to zoom in and auto-focus.



- To zoom out, click the Zoom Out icon several times, and then click the Auto-Focus icon. Wait several seconds for the camera to zoom out and auto-focus.



5. Click *Monitor* to view the changes you made to the camera settings.



# Fabric Management Platform

This section lists the new features added to FortiAnalyzer for Fabric Management Platform.

List of new features:

- [Single pane on page 152](#)
  - [Prompt admin to register FortiAnalyzer with FortiCloud on page 152](#)
  - [FortiManager support for FortiAnalyzer HA on page 158](#)
  - [Online update and verification for third-party certificates \(OCSP stapling\) on page 158](#)
  - [FortiAnalyzer firmware upgrade from FortiGuard servers on page 160](#)

## Single pane

This section lists the new features added to FortiAnalyzer for single pane.

List of new features:

- [Prompt admin to register FortiAnalyzer with FortiCloud on page 152](#)
- [FortiManager support for FortiAnalyzer HA on page 158](#)
- [Online update and verification for third-party certificates \(OCSP stapling\) on page 158](#)
- [FortiAnalyzer firmware upgrade from FortiGuard servers on page 160](#)
- [FortiAnalyzer GUI accessibility improvements 6.4.4 on page 161](#)

## Prompt admin to register FortiAnalyzer with FortiCloud

FortiAnalyzer VM users are now required to register their VM license or get a free trial license. You can register a hardware device directly from the *System Settings > Dashboard* pane with FortiCloud.

This topic contains the following section:

- [Registering a VM license on page 152](#)
- [Getting a trial VM license on page 153](#)
- [Registering a hardware device on page 155](#)
- [Viewing license information with the CLI on page 157](#)

### Registering a VM license

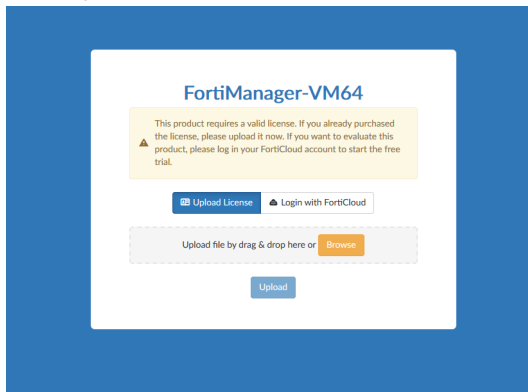


To download a VM license file, log in to FortiCloud, and click *Asset > Manage/View Products*. Select a device from the list, and click the link in the *License File* field.

---

**To register a VM license:**

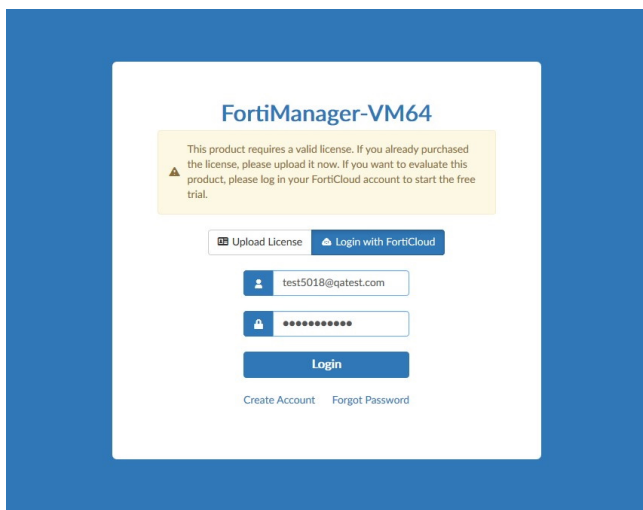
1. Go to the FortiAnalyzer VM login page.
2. Click *Upload License*, and take one of the following actions:
  - Drag and drop the license file onto the field.
  - Click *Browse* to navigate to the location of your license file on your computer.
3. Click *Upload*.

**Getting a trial VM license**

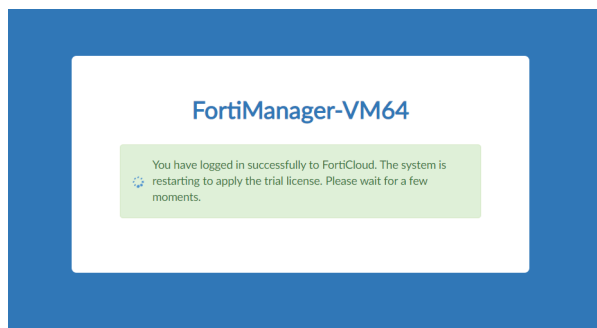
If a VM license is not associated with your FortiCloud account, you can get a free trial license for up to three devices. Trial licenses do not expire.

**To get a trial VM license:**

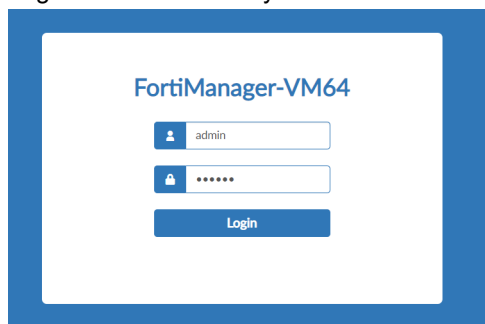
1. Go to the FortiAnalyzer VM login page.
2. Click *Login with FortiCloud*.
3. Enter your FortiCloud account credentials, and click *Login*. If you do not have a FortiCloud account, click *Create Account*.



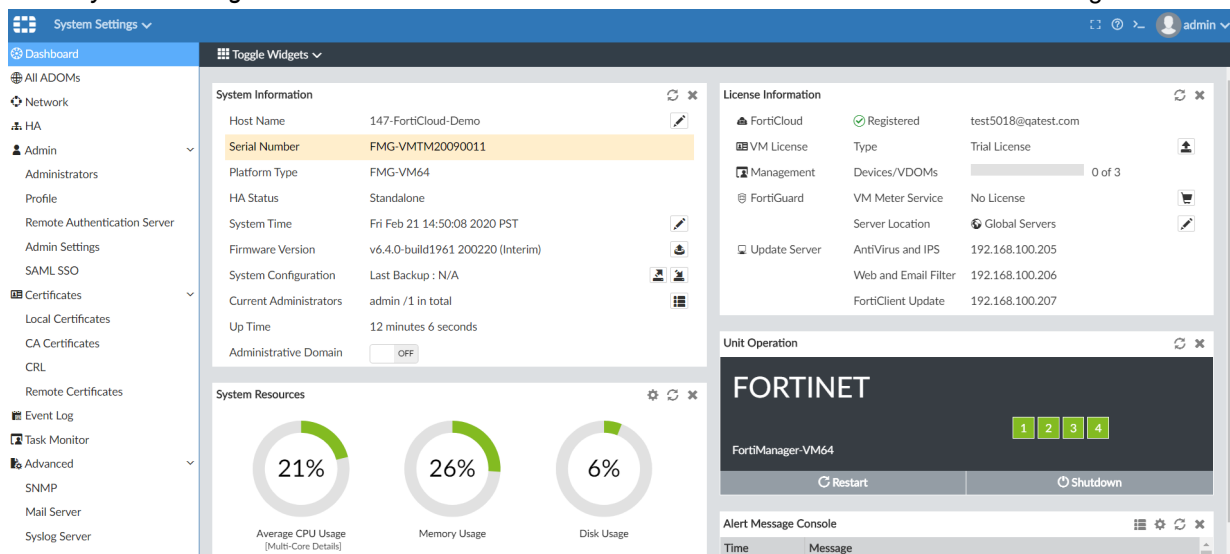
FortiAnalyzer VM connects to FortiCloud to get the trial license, and the system reboots.



- Log back into FortiAnalyzer VM.

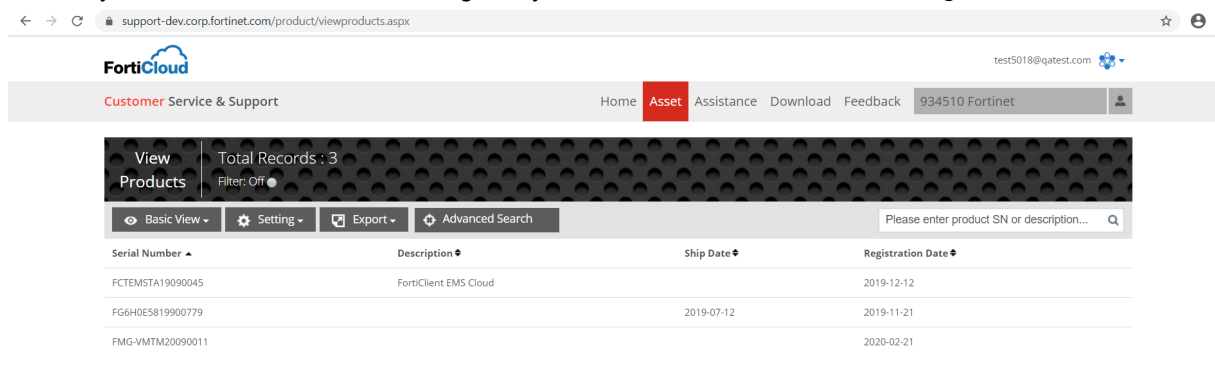


- Go to **System Settings > Dashboard** to view the license status in the **License Information** widget.





6. To view your trial license in FortiCloud, log in to your account, and click *Asset > Manage/View Products*.



FortiCloud  
Customer Service & Support

Home **Asset** Assistance Download Feedback 934510 Fortinet

test5018@qatest.com

View Products Total Records : 3 Filter: Off

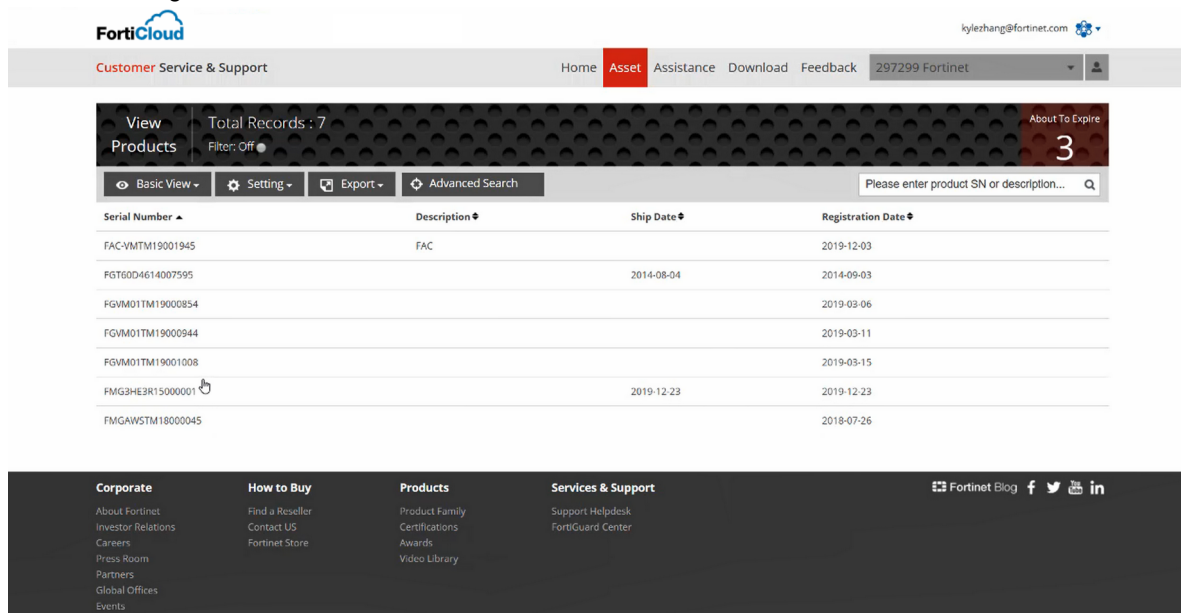
Basic View Setting Export Advanced Search Please enter product SN or description...

Serial Number	Description	Ship Date	Registration Date
FCTEMSTA19090045	FortiClient EMS Cloud		2019-12-12
FG6H0E5819900779		2019-07-12	2019-11-21
FMG-VMTM20090011			2020-02-21

## Registering a hardware device

To register a hardware device:

1. To verify the license is not registered, log in to FortiCloud, and click the *Assets* tab. If you do not see your device, then it is not registered.



FortiCloud  
Customer Service & Support

Home **Asset** Assistance Download Feedback 297299 Fortinet

kylezhang@fortinet.com

View Products Total Records : 7 Filter: Off About To Expire 3

Basic View Setting Export Advanced Search Please enter product SN or description...

Serial Number	Description	Ship Date	Registration Date
FAC-VMTM19001945	FAC		2019-12-03
FGT60D4614007595		2014-08-04	2014-09-03
FGVM01TM19000854			2019-03-06
FGVM01TM19000944			2019-03-11
FGVM01TM19001008			2019-03-15
FMG3HE3R15000001		2019-12-23	2019-12-23
FMGAWSTM18000045			2018-07-26

Corporate: About Fortinet, Investor Relations, Careers, Press Room, Partners, Global Offices, Events

How to Buy: Find a Reseller, Contact US, Fortinet Store

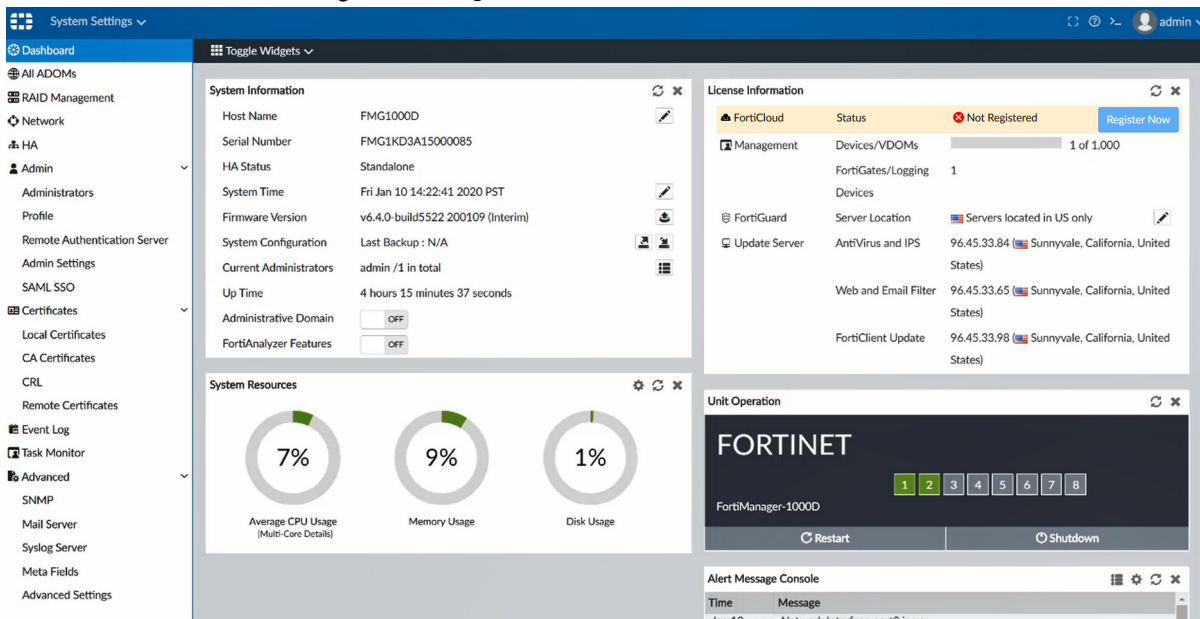
Products: Product Family, Certifications, Awards, Video Library

Services & Support: Support Helpdesk, FortiGuard Center

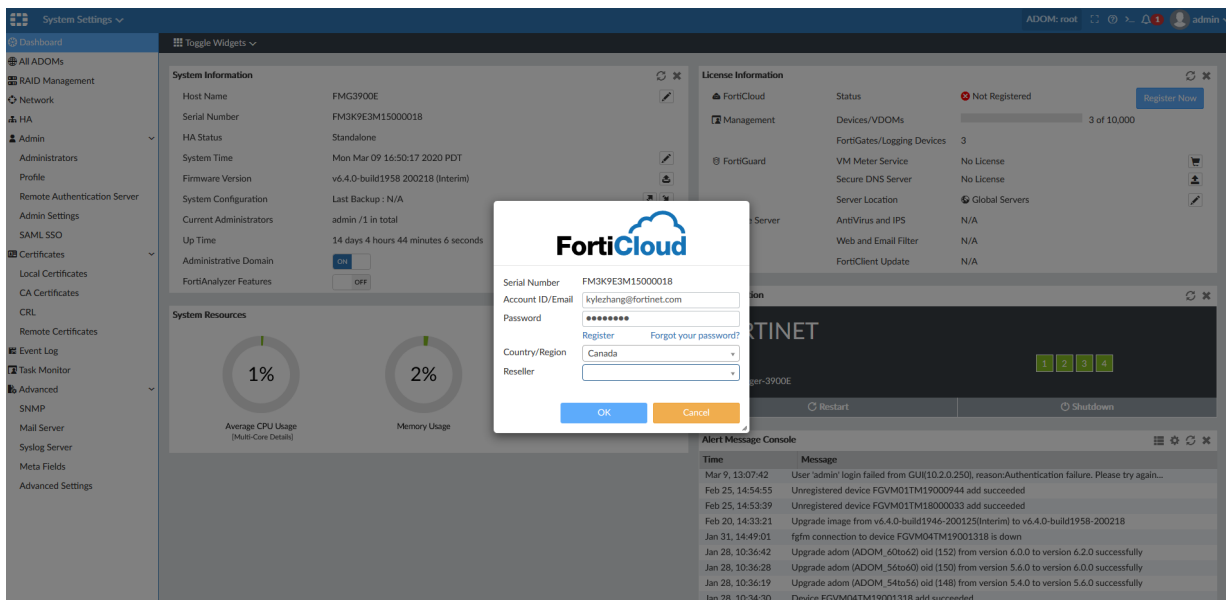
Fortinet Blog f t in

2. In FortiAnalyzer, go to *System Settings > Dashboard*.

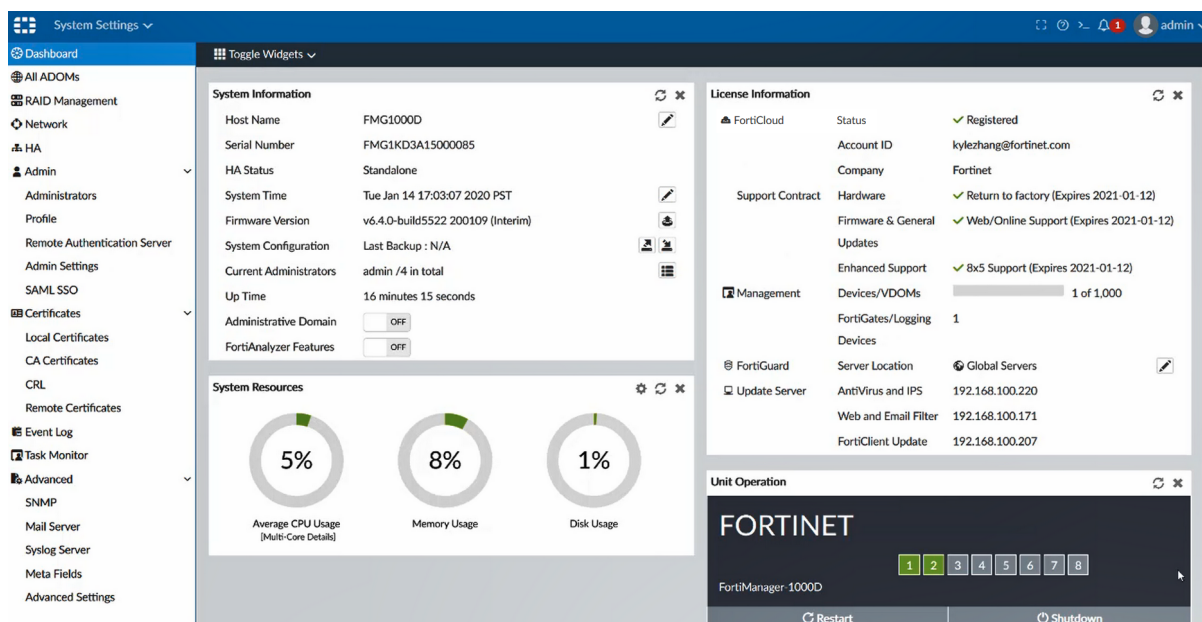
3. In the *License Information* widget, click *Register Now*.



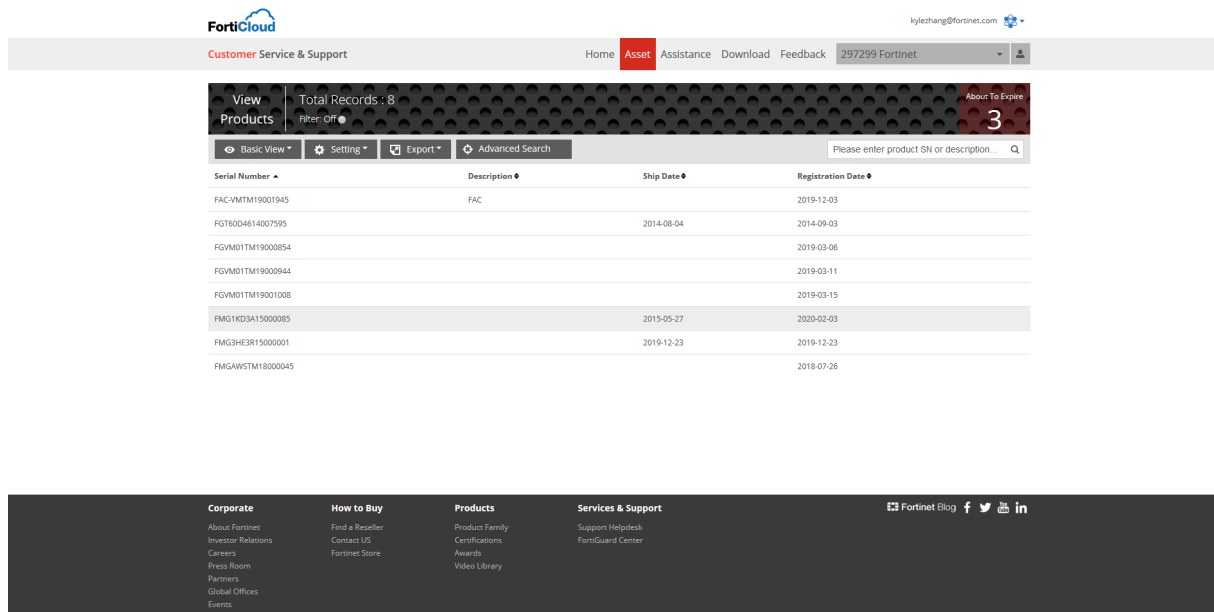
4. Enter your device information in the FortiCloud window, and click *OK*. FortiAnalyzer sends the information to FortiCloud.



After the information is synchronized, the *Status* changes to *Registered*.



5. Go back to the *Assets* page in FortiCloud to verify the device is registered.



## Viewing license information with the CLI

You can view the license status and information by using the CLI.

**To view the license status in the CLI:**

```
get system status
```

**To view the license information in the CLI:**

```
diagnose debug vminfo
```

**To connect the VM to FortiCloud when you set up the device:**

```
diagnose debug enable
diagnose debug application vmd <integer>
```

## Online update and verification for third-party certificates (OCSP stapling)

You can enable Anycast to optimize the routing performance to FortiGuard servers. Relying on Fortinet DNS servers, FortiAnalyzer obtains a single IP address for the domain name of each FortiGuard service. BGP routing optimization is transparent to FortiAnalyzer. The domain name of each FortiGuard service is the common name in that service's certificate. The certificate is signed by a third-party intermediate CA. The FortiGuard server uses the Online Certificate Status Protocol (OCSP) stapling technique, enabling FortiAnalyzer to always validate the FortiGuard server certificate efficiently.

This feature focuses on the Anycast option and TLS handshake using OCSP stapling when connecting to the FortiGuard server.

**To enable online update and verification for third party certificates:****1. Enable Anycast support:**

```
config fmupdate fds-setting
    set fortiguard-anycast enable
    set fortiguard-anycast-source {aws | fortinet}
end
```

When Anycast is enabled, FortiAnalyzer only completes the TLS handshake with a FortiGuard server that provides a *good* OCSP status for its certificate. Any other status will result in a failed SSL connection. Also, FortiGuard enforces connection only over port 443.

**FortiAnalyzer connecting to FortiGuard:**

1. FortiAnalyzer embeds CA bundle that includes third party intermediate CA and the root CA.
2. FortiAnalyzer finds FortiGuard IP address from the DNS.
3. FortiAnalyzer initiates TLS handshake with the FortiGuard IP address.
4. FortiGuard servers provide certificates with its OCSP status: good, revoked, or unknown.
5. FortiAnalyzer verifies CA against the root CA within the CA bundle.
6. FortiAnalyzer then verifies the intermediate CA's revoke status against the root CA's CRL.
7. Finally, FortiAnalyzer verifies the FortiGuard certificate OCSP status.

OCSP stapling is reflected on the signature interval (currently, 24 hours), and good means that the certificate is not revoked at that timestamp. The FortiGuard servers query the CA's OCSP responder every four hours and updates its OCSP status. If the FortiGuard server is unable to reach the OCSP responder, it keeps the last known OCSP status for seven days. This cached OCSP status is immediately sent out when a client connection request is made, which optimizes the response time.

## FortiManager support for FortiAnalyzer HA

You can manage FortiAnalyzer HA via FortiManager. FortiManager retrieves the cluster member list and updates the information whenever it changes, including FortiAnalyzer HA failover or a change in members.

### To enable support for FortiAnalyzer HA:

1. Go to *Device Manager > Device and Groups*.
2. Click the down arrow next to *Add Devices*. Select *Add FortiAnalyzer*.  
The *Add FortiAnalyzer* dialog opens.

**Add FortiAnalyzer**

**Discover**

Device will be probed using a provided IP address and credentials to determine model type and other important information

IP Address: 10.3.121.202

Username: admin

Password: [masked]

Next > Cancel

3. From the *Add FortiAnalyzer* box, add FortiAnalyzer HA to FortiManager DVM by HA cluster's VIP, and click *Next*.  
The FortiAnalyzer HA is discovered with its HA status information. Click *Next* to continue.

**Add FortiAnalyzer**

The following information has been discovered from the device:

IP Address	10.3.121.202
Host Name	FAZVM64-HA
SN	FAZ-VMTM20001379
Model	FortiAnalyzer-VM64
Firmware Version	6.4.0, build5792 (GA)
HA Status	Active - Passive
Administrator	admin

Please input the following information to complete addition of the device:

Name: FAZVM64-HA

Description: [empty]

Next > Cancel

FortiAnalyzer HA is added successfully. Click *Finish*.

#### Add FortiAnalyzer

Status:

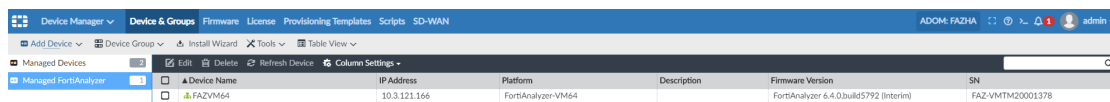
✔ FortiAnalyzer Added Successfully

Finish

4. In the tree menu, select *Managed FortiAnalyzer*. The device status icon is shown as the HA cluster and the SN is shown as the primary SN.

Device Name	IP Address	Platform	Description	Firmware Version	SN
FAZVM64	10.3.121.202	FortiAnalyzer-VM64		FortiAnalyzer 6.4.0, build5792 (Interim)	FAZ-VMTM20001379

FortiManager DVM gets an update after the failover on FortiAnalyzer in 300 seconds. Here, the previous primary "FAZ-VMTM20001379" becomes the secondary, and the new primary is "FAZ-VMTM20001378".



Device Name	IP Address	Platform	Description	Firmware Version	SN
FAZVM64	10.3.121.166	FortiAnalyzer-VM64	FortiAnalyzer 6.4.0.build5792 (Interim)	FortiAnalyzer 6.4.0.build5792 (Interim)	FAZ-VMTM20001378



You can get the HA status update immediately, select the FortiAnalyzer device and either click *Refresh Device* from the toolbar, or right-click and select *Refresh*.

### To check the DVM device list in the CLI:

1. View the DVM device list once FortiAnalyzer HA is added to FortiManager:  

```
diagnose dvm device list
```

It will have correct HA cluster information, including member list and role.
2. View the DVM device list after the failover on FortiAnalyzer:  

```
diagnose dvm device list
```

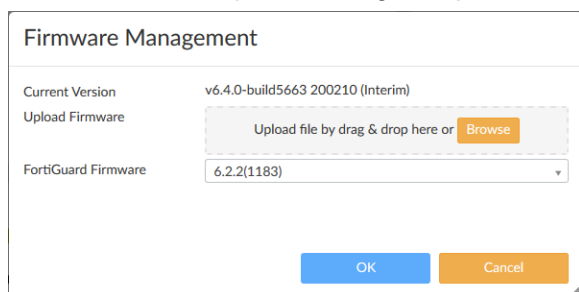
It will have the updated HA cluster information. The previous primary changes to secondary and vice versa.

## FortiAnalyzer firmware upgrade from FortiGuard servers

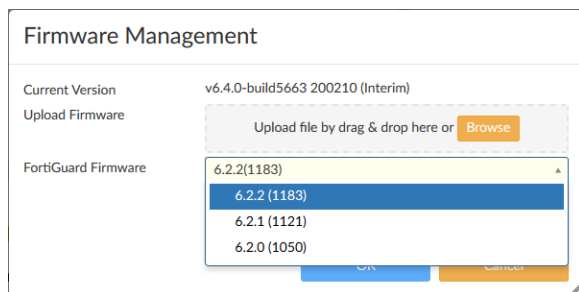
You can upgrade FortiAnalyzer firmware by using images available on FortiGuard servers. A green checkmark beside the available firmware images indicates the recommended FortiAnalyzer upgrade path. You can also upgrade to a firmware image that is not recommended if desired.

### To upgrade FortiAnalyzer firmware in the GUI:

1. Go to *System Settings*.
2. In the *System Information* widget, beside *Firmware Version*, click *Update Firmware*.  
The *Firmware Management* dialog box opens.

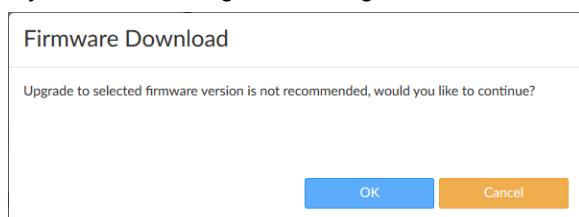


3. From the *FortiGuard Firmware* box, select the version of FortiAnalyzer for the upgrade, and click *OK*.  
The *FortiGuard Firmware* box displays all FortiAnalyzer firmware images available for upgrade. A green checkmark displays beside the recommended image for FortiAnalyzer upgrade.

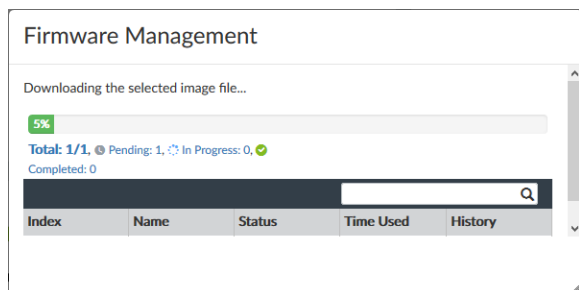


Because this image was captured before the release of FortiAnalyzer 6.4.0, a green checkmark is not yet available.

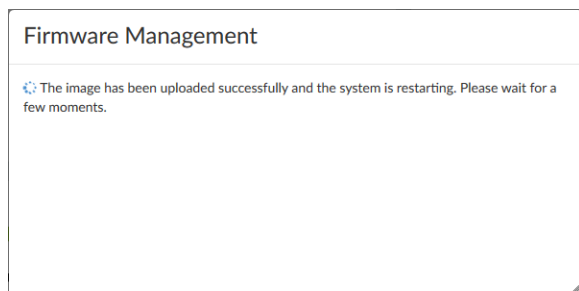
If you select an image without a green checkmark, a confirmation dialog box is displayed. Click OK to continue.



FortiAnalyzer downloads the firmware image from FortiGuard.



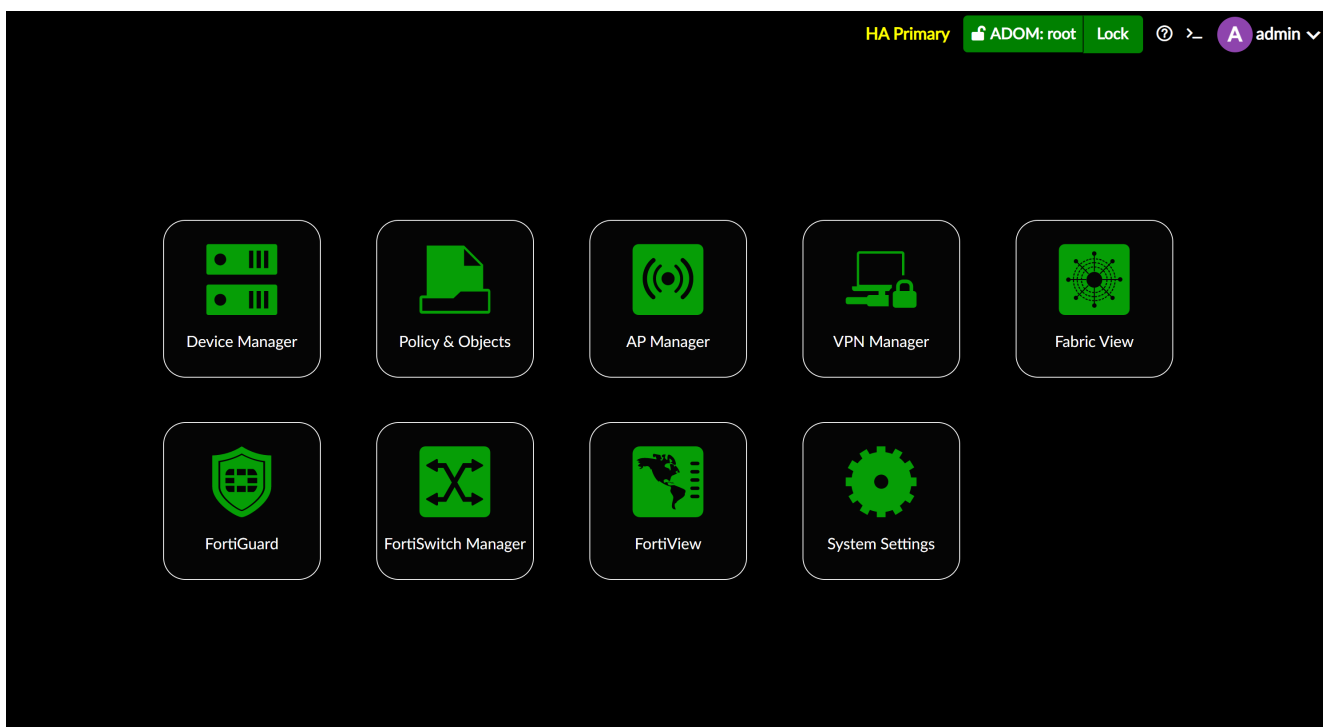
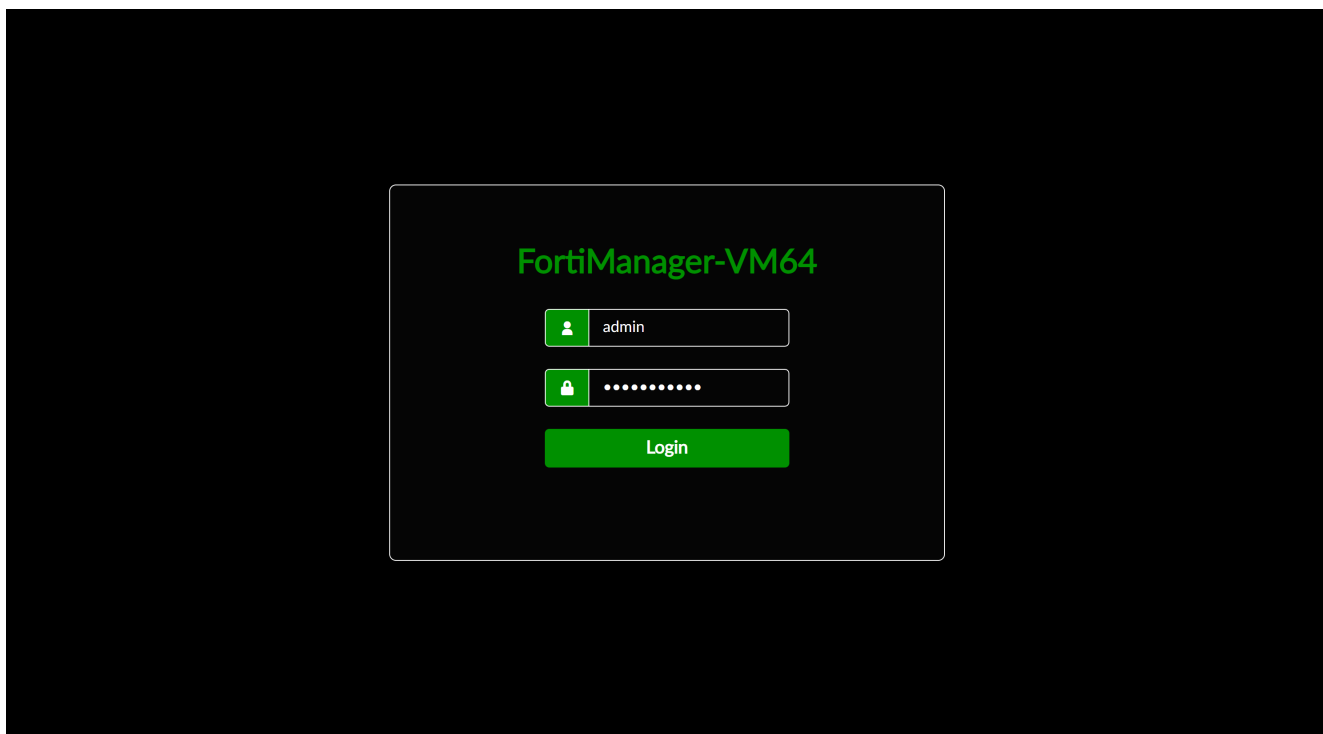
FortiAnalyzer uses the downloaded image to update its firmware, and then restarts.



After FortiAnalyzer restarts, the upgrade is complete.

## FortiAnalyzer GUI accessibility improvements - 6.4.4

FortiAnalyzer now implements a high contrast dark theme in order to make the FortiAnalyzer GUI more accessible, and to aid people with visual disability in using the FortiAnalyzer GUI.





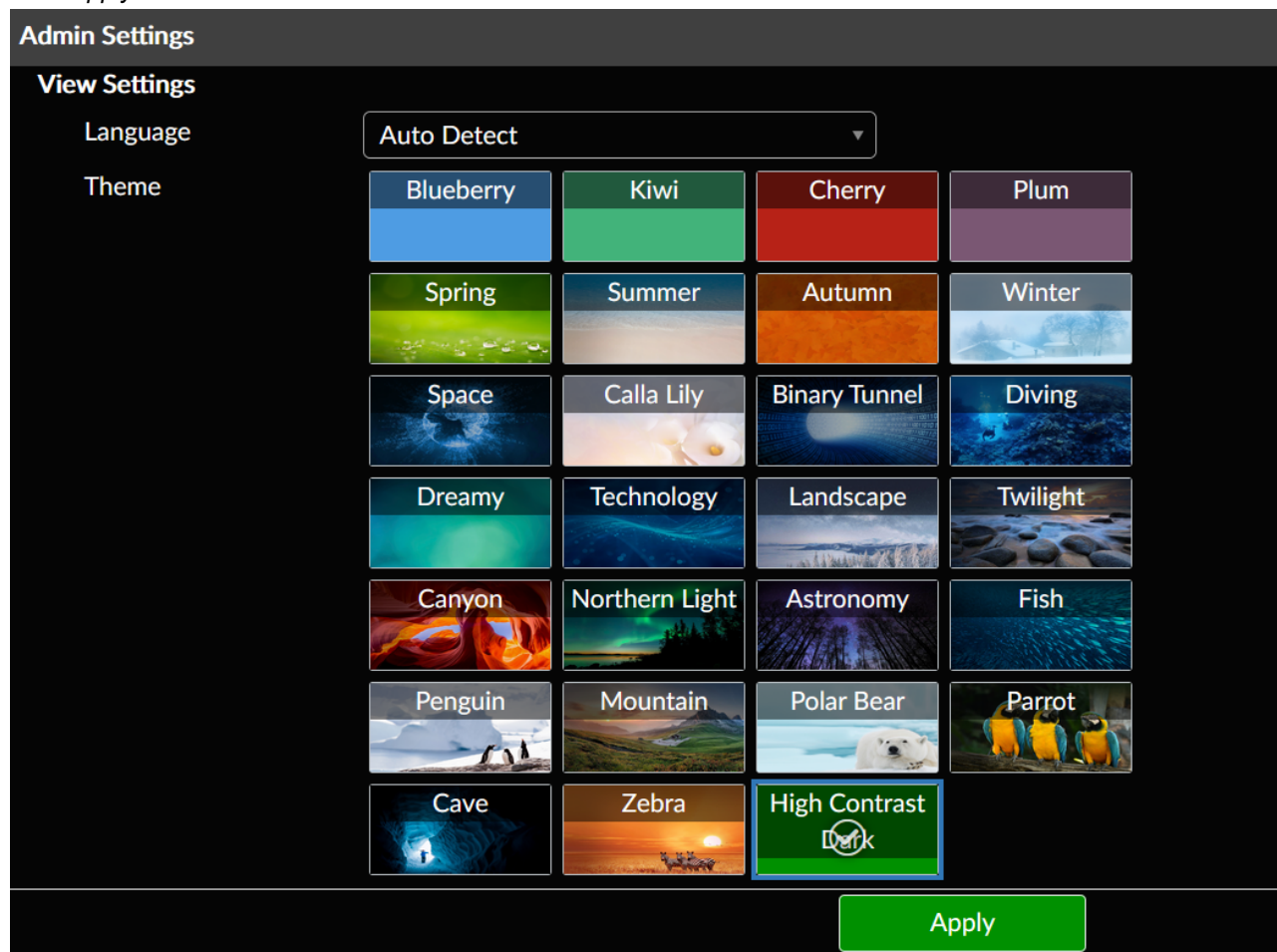
The screenshot displays the FortiAnalyzer Fabric Management Platform interface. The top navigation bar includes 'AP Manager', 'Managed APs', 'Monitor', 'Map View', and 'WiFi Profiles'. The 'WiFi Profiles' tab is active, showing 'HA Primary', 'ADOM: root', and 'Unlock' buttons. A user profile 'admin' is logged in. The left sidebar lists profile types: AP Profile, SSID (selected), WIDS Profile, Bluetooth Profile, QoS Profile, and Bonjour Profile. The main area is titled 'Create New SSID Profile' and contains the following configuration fields:

- Interface Name: SSID-Guest
- Alias: (empty)
- Traffic Mode: Tunnel (selected), Bridge, Mesh
- Address:
  - IP/Network Mask: 0.0.0.0/0.0.0.0
  - IPv6 Address: (empty)
- Administrative Access:
  - HTTPS (checked), PING (checked), SSH (checked)
  - SNMP (unchecked), HTTP (checked), TELNET (unchecked)
  - FMG-Access (unchecked), Auto-IPsec (unchecked), RADIUS Accounting (unchecked)
- IPv6 Administrative Access:
  - HTTPS (checked), PING (checked), SSH (checked)
  - SNMP (unchecked), HTTP (checked), TELNET (unchecked)
  - Any (unchecked), FMG-Access (unchecked)
- DHCP Server: OFF (selected), Server, Relay
- Networked Devices:
  - Device Detection: OFF (selected)
- WiFi Settings:
  - SSID: fortinet

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

To change the currently active theme to the *High Contrast Dark* theme:

1. Go to *System Settings > Admin > Admin Settings*.
2. Scroll to *View Settings > Theme*.
3. Select the *High Contrast Dark* theme tile from the available theme tiles.

4. Click *Apply*.

# Other

This section lists the other new features added to FortiAnalyzer.

List of new features:

- [FortiAnalyzer Application logs on page 165](#)

## FortiAnalyzer Application logs

FortiAnalyzer applications such as incident management and automation playbooks generate local audit logs, accessible in LogView under each ADOM.

Log View

ADOM: SOAR

admin

FortiGate

Traffic

Security

Antivirus

Intrusion Prevention

Application Control

Web Filter

DNS

VoIP

FortiClient

Event

SSL

Event

FortiClient

FortiAnalyzer

Application

Custom View

Log Browse

Log Group

All Devices

Last 7 Days

Mar 03 To Mar 10

Custom View

Add Filter

#	Date/Time	Device ID	User	Sub Type	Event Type	Action	Description	Message
1	03-03 17:52	FL3K9HE3M160001005		incident	attachment	add	Note Attached to Incident	Software...
2	03-03 17:52	FL3K9HE3M160001005	system	playbook	run-stat		Incident Attachment Added	Task 'At...
3	03-03 17:52	FL3K9HE3M160001005		incident	config	add	New Incident Created	Inciden...
4	03-03 17:52	FL3K9HE3M160001005		incident	config	add	New Incident Created	Inciden...
5	03-03 17:52	FL3K9HE3M160001005	system	playbook	run-stat		Incident Created	Task 'Cr...
6	03-03 17:52	FL3K9HE3M160001005	system	playbook	run-stat		Incident Created	Task 'Cr...
7	03-03 17:52	FL3K9HE3M160001005	system	playbook	run-stat		Looking Up Events	Task 'Gr...
8	03-03 17:52	FL3K9HE3M160001005	system	playbook	trigger	triggered	Playbook Triggered by Incident	Playbo...
9	03-03 17:52	FL3K9HE3M160001005	system	playbook	trigger	triggered	Playbook Triggered by Incident	Playbo...
10	03-03 17:52	FL3K9HE3M160001005	system	playbook	trigger	triggered	Playbook Triggered by Incident	Playbo...
11	03-03 17:52	FL3K9HE3M160001005	system	playbook	trigger	triggered	Playbook Triggered by Incident	Playbo...
12	03-03 17:52	FL3K9HE3M160001005	system	playbook	run-stat		Report Scheduled	Task 'Rl...
13	03-03 17:52	FL3K9HE3M160001005	system	playbook	run-stat		Endpoint Vulnerability Scan Requested	Task 'Rl...
14	03-03 17:52	FL3K9HE3M160001005	system	playbook	run-stat		Endpoint AV Quick Scan Requested	Task 'A...
15	03-03 17:52	FL3K9HE3M160001005	system	playbook	run-stat		Endpoint Software Inventory Requested	Task 'Gr...
16	03-03 17:52	FL3K9HE3M160001005	incident	attachment	add		Note Attached to Incident	Note at...
17	03-03 17:52	FL3K9HE3M160001005	system	playbook	run-stat		Incident Attachment Added	Task 'At...
18	03-03 17:52	FL3K9HE3M160001005	system	playbook	run-stat		Looking Up Events	Task 'Gr...
19	03-03 17:52	FL3K9HE3M160001005	incident	attachment	add		Report Attached to Incident	Report...

Total logs for analytics: 56 days 6 hours.

50

Items per page

1 2 3 4 5

0.008 Second

In the root ADOM, administrators can view the local event logs and the application logs of the root ADOM.

Log View

ADOM: root

FortiAnalyzer

FAZ3900E(Local)

Last 7 Days - Mar 03 To Mar 10

Custom View

Event

Application

Custom View

Log Browse

Log Group

#	Date/Time	Device ID	Sub Type	User	Message
1	03-03 16:59	FL3M79E284F5A0001035	logfile	system	Rolled log file tlog.1583283537.log of device ...
2	03-03 16:59	FL3M79E284F5A0001035	report	system	Start generating SQL report [S-10007_t1000...
3	03-03 16:59	FL3M79E284F5A0001035	report	system	Report [S-10007_t10007-IPS Report-2020-0...
4	03-03 16:59	FL3M79E284F5A0001035	report	system	report[S-10007_t10007-IPS Report-2020-03...
5	03-03 17:00	FL3M79E284F5A0001035	report	system	Start generating SQL report [S-10025_t1002...
6	03-03 17:00	FL3M79E284F5A0001035	report	system	Report [S-10025_t10025-Cyber Threat Asses...
7	03-03 17:00	FL3M79E284F5A0001035	report	system	report[S-10025_t10025-Cyber Threat Assess...
8	03-03 17:00	FL3M79E284F5A0001035	logfile	system	Rolled log file tlog.1583283608.log of device ...
9	03-03 17:00	FL3M79E284F5A0001035	report	system	Start generating SQL report [S-10007_t1000...
10	03-03 17:00	FL3M79E284F5A0001035	report	system	Report [S-10007_t10007-IPS Report-2020-0...
11	03-03 17:00	FL3M79E284F5A0001035	report	system	report[S-10007_t10007-IPS Report-2020-03...
12	03-03 17:01	FL3M79E284F5A0001035	report	system	Start generating SQL report [S-10007_t1000...
13	03-03 17:01	FL3M79E284F5A0001035	report	system	Start generating SQL report [S-10007_t1000...
14	03-03 17:01	FL3M79E284F5A0001035	report	system	Report [S-10007_t10007-IPS Report-2020-0...
15	03-03 17:01	FL3M79E284F5A0001035	report	system	report[S-10007_t10007-IPS Report-2020-03...
16	03-03 17:01	FL3M79E284F5A0001035	report	system	report[S-10007_t10007-IPS Report-2020-03...
17	03-03 17:01	FL3M79E284F5A0001035	report	system	Report [S-10007_t10007-IPS Report-2020-0...
18	03-03 17:01	FL3M79E284F5A0001035	logfile	system	Rolled log file tlog.1583283684.log of device ...
19	03-03 17:02	FL3M79E284F5A0001035	report	system	Start generating SQL report [S-10007_t1000...
20	03-03 17:02	FL3M79E284F5A0001035	report	system	Report [S-10007_t10007-IPS Report-2020-0...
21	03-03 17:02	FL3M79E284F5A0001035	report	system	report[S-10007_t10007-IPS Report-2020-03...
22	03-03 17:02	FL3M79E284F5A0001035	report	system	Start generating SQL report [S-10007_t1000...
23	03-03 17:02	FL3M79E284F5A0001035	report	system	Report [S-10007_t10007-IPS Report-2020-0...
24	03-03 17:02	FL3M79E284F5A0001035	report	system	report[S-10007_t10007-IPS Report-2020-03...
25	03-03 17:02	FL3M79E284F5A0001035	report	system	report[S-10007_t10007-IPS Report-2020-03...

Total logs for analytics: 60 days 13 hours.

50 Items per page

1 2 3 4 5

0.002 Second

Use **Log Browse** to find application log files.

Log View

ADOM: SOAR

FortiGate

FAZ3900E(FL3M79E284F5A0001035)

Last 1 Day

Display Delete Download Import

Traffic

Security

Antivirus

Intrusion Prevention

Application Control

Web Filter

DNS

VoIP

FortiClient

Event

SSL

Event

FortiClient

FortiAnalyzer

Application

Custom View

Log Browse

Log Group

#	Device Name	Serial Number	VDOM	Type	File Name	From	To	Size
1	.self	FL3M79E284F5A0001035	SOAR	App Events	rlog.1583790046.log.gz	2020-03-09 14:40:4	2020-03-10 14:3	1.3M
2	.self	FL3M79E284F5A0001035	SOAR	App Events	rlog.log	2020-03-10 14:40:1	2020-03-10 16:5	3.5M



**FORTINET®**



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.