

DO NOT REPRINT

© FORTINET



Advanced Analytics Lab Guide

for FortiSIEM 6.3

FORTINET

NSE Training Institute

Fortinet Training

<https://training.fortinet.com>

Fortinet Document Library

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

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

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguards.com>

Fortinet Network Security Expert Program (NSE)

<https://training.fortinet.com/local/staticpage/view.php?page=certifications>

Fortinet | Pearson VUE

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

Feedback

Email: askcourseware@fortinet.com



9/20/2021

TABLE OF CONTENTS

Network Topology	8
Lab 1: Customer Definition	9
Exercise 1: Adding Customers With Collectors	10
Define Customers With Collectors	10
Define Customers Without Collectors	12
Exercise 2: Discovering Devices Without a Collector	14
Verify the SNMP Service on Kali	14
Configure Device Credentials for an Organization Without a Collector	14
Discover a Device	17
Review Logs From an Organization Without a Collector	18
Exercise 3: Reviewing Multi-Tenancy on FortiSOAR	21
Review Tenants on FortiSOAR	21
Lab 2: Worker Configuration	23
Exercise 1: Adding a Worker	24
Add a Worker to the FortiSIEM Cluster	24
Exercise 2: Generating Incidents on FortiSIEM	26
Generate Incidents on FortiSIEM	26
Exercise 3: Configuring FortiSIEM Data Ingestion	28
Configure the FortiSIEM Connector	28
Lab 3: Administration and Management of Collectors	34
Exercise 1: Assigning Collectors to Organizations	35
Assign Collectors to Organizations	35
Verify Collector Health	38
Exercise 2: Registering Collectors	39
Register Collectors	39
Verify Collector Health	40
Exercise 3: Discovering FGT Banking through a Collector	42
Configure SNMP on FortiGate	42
Add Credentials for FortiGate	43
Discover Banking FortiGate	45
Approve FortiGate in CMDB	46
Exercise 4: Discovering FGT Aviation through a Collector	48
Configure Syslog on FGT Aviation	48

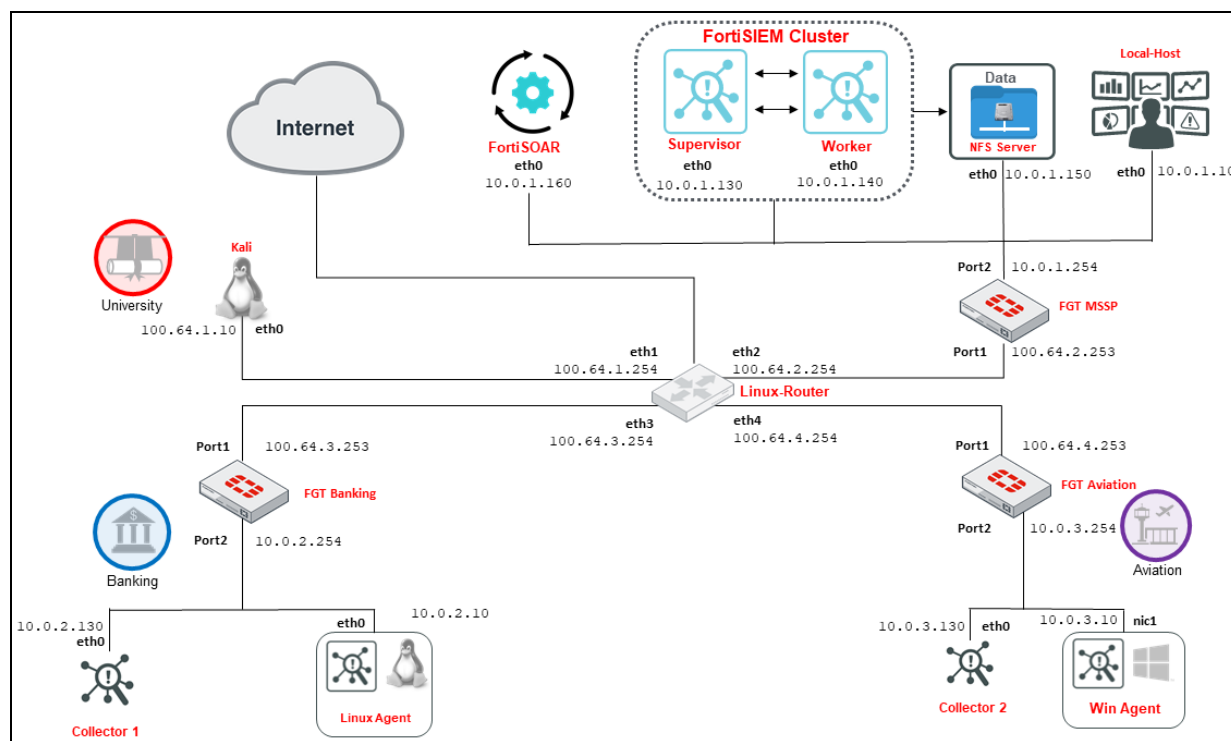
Configure SNMP on Aviation FortiGate.....	49
Add Credentials for Aviation FortiGate.....	50
Discover FortiGate.....	52
Approve FortiGate in CMDB.....	53
Lab 4: Administration and Management of Agents.....	54
Exercise 1: Adding a Windows Agent to an Organization.....	55
Configure Windows Agent Registration Credentials.....	55
Configure the Windows Agent Installation Settings File.....	56
Define an Audit Policy.....	57
Verify the Windows Agent Status.....	59
Exercise 2: Assigning Templates to Windows Agents.....	60
Create a Windows Agent Monitor Template.....	60
Associate a Host to a Template.....	61
Verify the Agent Status.....	62
Approve the Windows Agent.....	63
Exercise 3: Discovering LDAP Users.....	65
Discover LDAP Users and Groups.....	65
Review LDAP Users on FortiSIEM.....	67
Exercise 4: Adding a Linux Agent to an Organization.....	69
Configure Linux Agent Registration Credentials.....	69
Register the Linux Agent.....	70
Verify the Linux Agent Status.....	71
Exercise 5: Assigning Templates to Linux Agents.....	73
Create Linux Agent Monitor Templates.....	73
Associate a Host to a Template.....	74
Verify the Agent Status.....	75
Approve the Linux Agent.....	75
Lab 5: Discover Rules.....	76
Exercise 1: Analyzing Allowed Traffic.....	77
Log All Sessions on FortiGate.....	77
Analyze Traffic Events on FortiSIEM.....	77
Create a Rule From an Analytics Search.....	79
Exercise 2: Monitoring Firewall Sessions.....	83
Build an Analytics Search.....	83
Display the Average Firewall Session.....	84
Lab 6: Configuration of Single Pattern Security Rules.....	87
Exercise 1: Detecting Remote Desktop Access.....	88
Review the Remote Desktop From Internet Rule.....	88
RDP From the Internet.....	92
Review the RDP Incident.....	92
Exercise 2: Detecting Multiple VPN Logon Failures.....	95

Review the Multiple VPN Logon Failures Rule.....	95
Generate SSL VPN Login Failures.....	98
Verify VPN events on FortiGate.....	99
Review the Incident for Multiple VPN Logon Failures.....	100
Exercise 3: Detecting Locked Domain Accounts.....	102
Review the Domain Account Locked Rule.....	102
Review the Incident for Locked Domain Accounts.....	105
Exercise 4: Creating a New Security Rule.....	106
Create a Custom Rule.....	106
Log in to FortiGate From a Public IP Address.....	109
Lab 7: Configuration of Multipattern Security Rules.....	111
Exercise 1: Reviewing a VPN Login Event.....	112
Review the LDAP Users.....	112
Create a VPN Pool.....	113
Connect to the SSL VPN.....	114
Analyze the SSL VPN Event.....	115
Exercise 2: Reviewing an RDP Event.....	117
Run a Real-Time Analytics Search.....	117
Analyze an RDP Event.....	119
Exercise 3: Building a Multipattern Rule.....	120
Create a New Multipattern Rule.....	120
Establish an RDP Connection over SSL VPN.....	125
Review the Incident.....	126
Lab 8: Baseline Theory.....	128
Exercise 1: Reviewing Baseline Reports and Rules.....	129
Review Baseline Reports.....	129
Review Baseline Rules.....	130
Exercise 2: Determining What to Baseline.....	132
Determine Parameters to Baseline.....	132
Exercise 3: Creating a Baseline With the BaselineMate Script.....	136
Define an Event.....	136
Run the BaselineMate Script from Supervisor.....	137
Exercise 4: Verifying the Baseline Report.....	142
Verify the Baseline Report.....	142
Run the Script to Replay USB Events.....	143
Update the Daily and Profile Databases.....	143
Run the Baseline Report.....	145
Lab 9: Configuration of Baseline Rules.....	148
Exercise 1: Building a Baseline Rule.....	149
Build a Baseline Rule.....	149
Exercise 2: Preparing FortiSIEM for a Baseline Rule.....	155

Update the Profile Database.....	155
Exercise 3: Triggering a Baseline Rule.....	157
Trigger a Baseline Rule.....	157
Verify the Incident on FortiSIEM.....	158
Lab 10: UEBA.....	161
Exercise 1: Building a UEBA AI Model.....	162
Train the AI Engine.....	162
Exercise 2: Running the UEBA Demo.....	165
Run the UEBA Demo.....	165
Exercise 3: Reviewing UEBA Incidents.....	166
Review the UEBA Incidents.....	166
Review the UEBA Rules.....	169
Exercise 4: Reviewing the UEBA Dashboard.....	173
Review the UEBA Dashboards.....	173
Lab 11: MITRE ATT&CK Framework.....	181
Exercise 1: Creating Tags on FortiSIEM.....	182
Create Tags on FortiSIEM.....	182
Exercise 2: Generating Incidents on FortiSIEM.....	184
Generate Incidents on FortiSIEM.....	184
Exercise 3: Reviewing the MITRE ATT&CK Framework Support on FortiSIEM.....	185
Review the MITRE ATT&CK Incident Dashboard.....	185
Exercise 4: Reviewing the MITRE ATT&CK Framework Support on FortiSOAR.....	189
Review the MITRE ATT&CK Framework on FortiSOAR.....	189
Lab 12: Clear Conditions.....	192
Exercise 1: Reviewing Time-Based Clear Conditions.....	193
Review Rules With Clear Conditions.....	193
Review a Time-Based Clear Condition.....	194
Exercise 2: Configuring a Pattern-Based Clear Condition.....	195
Define a Pattern-Based Clear Condition.....	195
Modify the SNMP Ping Interval.....	196
Disable the SNMP Service.....	197
Run the Rule as a Query.....	198
Verify the Incident.....	199
Enable the SNMP Service.....	201
Run the Rule as a Query.....	201
Verify the Incident Status.....	201
Lab 13: Remediation.....	204
Exercise 1: Remediating an Incident.....	205
Execute the Remediation.....	205
Analyze the Remediation Result.....	207

- Exercise 2: Configuring the REST API on FortiGate..... 209**
 - Configure the REST API on FortiGate..... 209
 - Configure a New Web Filter Profile..... 210
- Exercise 3: Configuring the FortiGate Connector..... 212**
 - Configure the FortiGate Connector..... 212
 - Configure a Playbook to Use the FortiGate Connector..... 213
- Exercise 4: Mitigating Malicious IOCs..... 215**
 - Extract Indicators..... 215
 - Enrich Malicious Indicators..... 217
 - Block Malicious Indicators..... 220
- Appendix A..... 223**

Network Topology



See [Appendix A on page 223](#) for an enlarged network topology diagram.

Lab 1: Customer Definition

In this lab, you will add three organizations to FortiSIEM. Two of the organizations will be deployed with collectors, and the third one will be deployed without a collector. You will also discover a device for an organization without a collector, and then review the logs.

Objectives

- Manage organizational scopes
- Add organizations with a collector
- Add organizations without a collector
- Add credentials for organizations without a collector
- Discover devices for organizations without a collector
- Review multi-tenancy on FortiSOAR

Time to Complete

Estimated: 25 minutes

Exercise 1: Adding Customers With Collectors

In this exercise, you will add customers that have collectors in their infrastructure to the FortiSIEM supervisor node. You will also add customers that do not have collectors. Each new organization is automatically given an organization ID, which is included in every new event collected or received from that organization.

Define Customers With Collectors

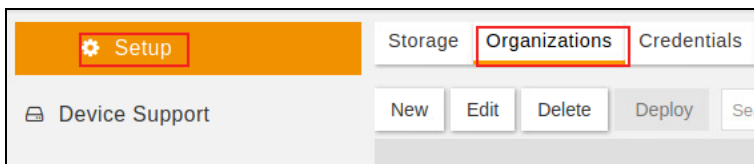
In a multi-tenant environment, you will add customers with different network infrastructures—some customers might have collectors and some might not. Now, you will add organizations that have collectors in their environment.

To add customers with collectors

1. On the supervisor FortiSIEM GUI, log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

2. Click **LOG IN**.
3. Click **ADMIN**.
4. In the left navigation pane, click **Setup**, and then click **Organizations**.



You will notice that there are no organizations defined by default.

5. Click **New** to create a new organization.
6. Configure the following settings:

Field	Value
Organization	Banking
Admin User	bankadmin

Field	Value
Admin Password	Password1!
Confirm Admin Password	Password1!
Admin Email	bankadmin@bank.lab

Your configuration should match the following example:

Organization Definition (Banking)

Organization: Banking

Full Name:

Admin User: bankadmin

Admin Password:

Confirm Admin Password:

Admin Email: bankadmin@bank.lab

Phone:

Account Number:

Support Tier:

Support Team:

Collectors:
New Edit Delete

Include IP/IP Range:

Exclude IP/IP Range:

Agent User:

Agent Password:

Confirm Agent Password:

Max Devices:

Address:

Account Type:

Account Status:

Account Manager:

- Click **Save**.
- Click **New** to create another organization.
- Configure the following settings:

Field	Value
Organization	Aviation
Admin User	flightadmin
Admin Password	Password1!
Confirm Admin Password	Password1!
Admin Email	flightadmin@aviation.lab

- Click **Save**.

Your organization configuration should match the following example. Note that FortiSIEM dynamically assigns the **Organization ID**.

Storage ▾	Organizations	Credentials	Discovery	Pull Events	Monitor Performance	STM	Maintenance
New	Edit	Delete	Deploy	Search...	Columns ▾	↺	1/1
ID	Organization	Full Name	Admin User	Admin Email	Collectors	Deployed	
2001	Aviation		flightadmin	flightadmin@aviation.lab		☒	
2000	Banking		bankadmin	bankadmin@bank.lab		☒	



When you register collectors in the upcoming labs, you require information, such as the organization name and the admin username and password that you configured for the organizations on the supervisor.

Define Customers Without Collectors

You will add an organization that does not have a collector in their environment. You will specify an IP address range to identify devices that belong to an organization without a collector.

To add customers without collectors

1. Continuing on the supervisor FortiSIEM GUI, click **New** to create a new organization.
2. Configure the following settings:

Field	Value
Organization	University
Admin User	uniadmin
Admin Password	Password1!
Confirm Admin Password	Password1!
Admin Email	uniadmin@university.lab
Include IP/IP Range	100.64.1.10

3. Click **Save**.
Your configuration should match the following example:

Storage ▾	Organizations	Credentials	Discovery	Pull Events	Monitor Performance	STM	Maintenance
New	Edit	Delete	Deploy	Search...	Columns ▾	↺	1/1 3
ID	Organization	Full Name	Admin User	Admin Email	Collectors	Deployed	
2001	Aviation		flightadmin	flightadmin@aviation.lab		☒	
2000	Banking		bankadmin	bankadmin@bank.lab		☒	
2002	University		uniadmin	uniadmin@university.lab		☒	



Organizations without collectors are defined by a unique IP address, which can be a single IP address, multiple IP addresses separated by commas, or an IP address range. Note that CIDR definitions are not supported here.

4. Log out of the supervisor FortiSIEM GUI.

Exercise 2: Discovering Devices Without a Collector

In this exercise, you will define credentials for devices for the University organization that does not have a collector, and then discover a device with those credentials.

Verify the SNMP Service on Kali

The SNMP service is preconfigured on Kali. You must restart the service, and then verify its status.

To verify the SNMP service on Kali

1. Go to the Kali VM.



The credentials for Kali are as follows:

- Username: root
- Password: toor

2. Open a terminal window.
3. Type the following command to restart the SNMP service:
`service snmpd restart`
4. Type the following command to check the SNMP service status:
`service snmpd status`

Verify that it is in a running state.

```
root@kali:~# service snmpd status
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; disabled; vendor preset:
   Active: active (running) since Tue 2021-04-27 01:56:46 EDT; 5s ago
     Process: 2003 ExecStartPre=/bin/mkdir -p /var/run/agentx (code=exited, statu
    Main PID: 2004 (snmpd)
       Tasks: 1 (limit: 2349)
      Memory: 9.5M
    CGroup: /system.slice/snmpd.service
            └─2004 /usr/sbin/snmpd -L0w -u Debian-snmp -g Debian-snmp -I -smux

Apr 27 01:56:46 kali systemd[1]: Starting Simple Network Management Protocol (SN
Apr 27 01:56:46 kali systemd[1]: Started Simple Network Management Protocol (SNM
```

5. Press Q.
6. Close the terminal window.

Configure Device Credentials for an Organization Without a Collector

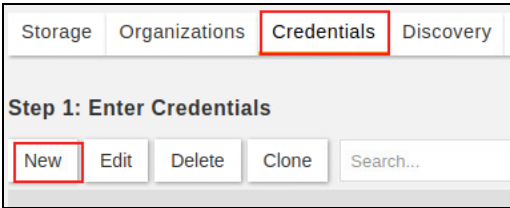
Before you can discover devices, you must define credentials for those devices. You must also associate the credentials with the IP address of those devices.

To configure credentials for an organization without a collector

1. On the supervisor FortiSIEM GUI, log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

2. Click **LOG IN**.
3. Click **ADMIN**.
4. In the left navigation pane, click **Setup**, and then click **Credentials**.



5. Click **New**.
6. Configure the following settings:

Field	Value
Name	Kali
Device Type	Generic
Access Protocol	SNMP
Port	161
Password config	manual
Community String	public
Confirm Community String	public

Your configuration should match the following example:

Access Method Definition

Name:Kali

Device Type:Generic

Access Protocol:SNMP

Port:161

Password config:Manual

Community String:*****

Confirm Community String:*****

Description:

7. Click **Save**.

To configure the IP range to credential association

1. Continuing on the **Credentials** tab, under the **Step 2: Enter IP Range to Credential Associations** section, click **New**.

StorageOrganizationsCredentialsDiscoveryPull Events

Step 1: Enter Credentials

NewEditDeleteClone

Search...

NameProtocol

KaliSNMP

Step 2: Enter IP Range to Credential Associations

NewEditDeleteTest

Search...

2. Configure the following settings:

Field	Value
IP/IP Range	100.64.1.10
Credentials	Kali

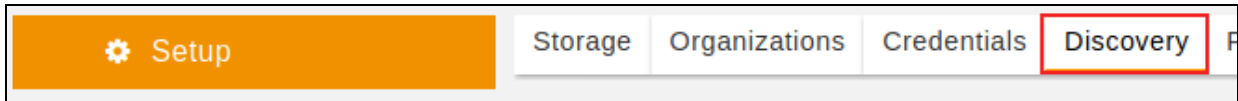
3. Click **Save**.

Discover a Device

You will discover a device, and the discovered device will be added automatically to the CMDB database.

To discover a device

1. Continuing on the supervisor FortiSIEM GUI, click **Discovery**.



2. Click **New**.
3. Configure the following settings:

Field	Value
Name	Kali
Discovery Type	Range Scan
Include	100.64.1.10
Name Resolution	SNMP/WMI first

4. Click **Save**.
5. Click **Discover**.

A screenshot of the FortiSIEM GUI showing a table of discovered devices. The 'Discover' button in the top navigation bar is highlighted with a red box. Below it is a table with columns: Name, Type, Root IPs, Include Range, Exclude Range, Last Discovery Time, and Schedule. One row is visible with the name 'Kali' and type 'Range Scan'.

After discovery is complete, the **Status** column displays **succeeded**.

A screenshot of the FortiSIEM GUI showing a window titled 'Discover - Kali'. It contains a table with columns: Organization, IP, Status, Name, Type, Access, and Sys Monitor. One row is visible with the status 'succeeded', which is highlighted with a red box. Below the table is a blue progress bar and a 'Close' button.

If for any reason the discovery fails, the **Status** column displays **fail**, along with the reason associated with that failure.

6. Click **Close**.

Review Logs From an Organization Without a Collector

After a device is discovered, FortiSIEM parses logs from that device and tags those events with the organization ID and organization name. You will analyze the logs that are being sent through SNMP from the Kali device to FortiSIEM.

To review logs from an organization without a collector

1. Continuing on the supervisor FortiSIEM GUI, in the top navigation pane, click **ANALYTICS**.
2. Click **Edit Filters and Time Range**.
3. Select **Event Attribute** as the **Filter** type.
4. Configure the following settings:

Field	Value
Attribute	Reporting IP
Operator	=
Value	100.64.1.10
Time	Relative, Last 10 Minutes

5. Click **Apply & Run**.
6. Select the **System uptime for a device** event log.
7. In the **Raw Event Log** column, click the arrow icon (▾).

☐ Show Event Type
 ☐ Wrap Raw Events

Event Receive Time	Reporting IP	Event Name	Raw Event Log
Jul 22 2021, 11:25:10 AM	100.64.1.10	System uptime for a device	[PH_DEV_MON_SYS_UPTIME]:[eventSeverity]=PHL_INFO,
Jul 22 2021, 11:25:09 AM	100.64.1.10	SNMP Ping Statistics	[PH_DEV_MON_SNMP_PING_STAT]:[eventSeverity]=PHL_
Jul 22 2021, 11:24:49 AM	100.64.1.10	System process count for a device	[PH_DEV_MON_SYS_PROC_COUNT]:[eventSeverity]=PHL
Jul 22 2021, 11:24:14 AM	100.64.1.10	System uptime for a device	[PH_DEV_MON_SYS_UPTIME]:[eventSeverity]=PHL_INFO,
Jul 22 2021, 11:23:59 AM	100.64.1.10	Ping Statistics	[PH_DEV_MON_PING_STAT]:[eventSeverity]=PHL_INFO,
Jul 22 2021, 11:23:13 AM	100.64.1.10	SNMP Ping Statistics	[PH_DEV_MON_SNMP_PING_STAT]:[eventSeverity]=PHL_

8. Review the **Event Details**.

Notice that the **Collector ID** has a value of **1**, which is the default collector ID if an organization does not have any collectors.

Event Details

[PH_DEV_MON_SYS_UPTIME];[event:Severity]-PHL_INFO,[fileName]-phPerfJob.cpo,
[lineNumber]=1033,[hostName]=kali,[hostIpAddr]=100.64.1.10,[sysUpTime]=064007,
[sysUpTimePot]=100.000000,[sysDownTime]=0,[pollIntv]=56,[phLogDetail]=

Search...

Lines: 27

Display	Filter	Item	Value
☐	☐	Collector ID	1
☐	☐	Count	1
☐	☐	Event ID	5551108753201856664
☐	☐	Event Name	System uptime for a device
☐	☐	Event Parse Status	1
☐	☐	Event Parser Name	PHBoxParser
☒	☐	Event Receive Time	Dec 19 2019, 09:23:26 AM
☐	☐	Event Rule Trigger	1
☐	☐	Event Severity	1
☐	☐	Event Severity Category	LOW
☒	☐	Event Type	PH_DEV_MON_SYS_UP...

OKClose

9. Scroll down in the **Event Details** window, and then view the **Organization ID** and **Organization Name**.

Event Details

[PH_DEV_MON_SYS_UPTIME]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=1129,[hostName]=kali,[hostIpAddr]=100.64.1.10,[sysUpTime]=552,[sysUpTimePct]=100.000000,[sysDownTime]=0,[pollIntv]=60,[phLogDetail]=

Search...

Lines: 27

Display	Filter	Item	Value
☐	☐	File Name	phPerfJob.cpp
☐	☐	Host IP	100.64.1.10
☐	☐	Host Name	kali
☐	☐	Line Number	1129
☐	☐	Organization ID	2002
☐	☐	Organization Name	University
☐	☐	Polling Interval	60
☐	☐	Relaying IP	10.0.1.130
☐	☐	Reporting Device	kali
☒	☒	Reporting IP	100.64.1.10
☐	☐	Reporting Model	Linux
☐	☐	Reporting Vendor	Generic

The **Organization ID** may be different for you. You can filter logs using either the **Organization ID** or **Organization Name**, which will display all logs that are associated with that organization.

10. Click **Close**.
11. Log out of the supervisor FortiSIEM GUI.

Exercise 3: Reviewing Multi-Tenancy on FortiSOAR

In this exercise, you will review multi-tenancy on FortiSOAR.

Review Tenants on FortiSOAR

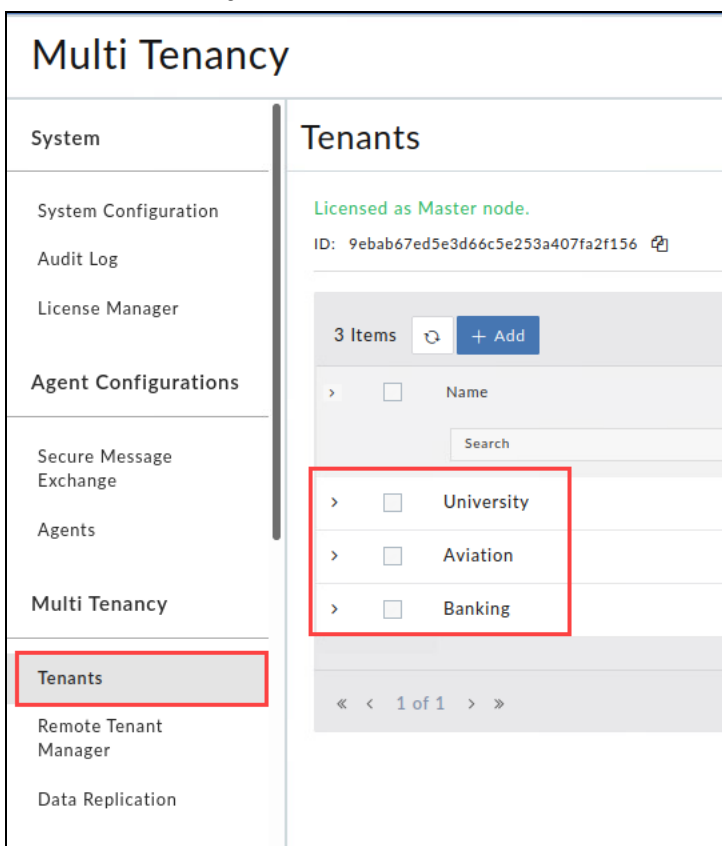
The tenants on FortiSOAR are already preconfigured. You will review them and verify that the tenant names match what is configured on FortiSIEM.

To review tenants on FortiSOAR

1. On the FortiSOAR management GUI, log in with the username `csadmin` and password `Fortinet1!`.
2. On the FortiSOAR GUI, in the top-right corner, click the **Settings** icon.



3. In the **Multi Tenancy** section, click **Tenants**.

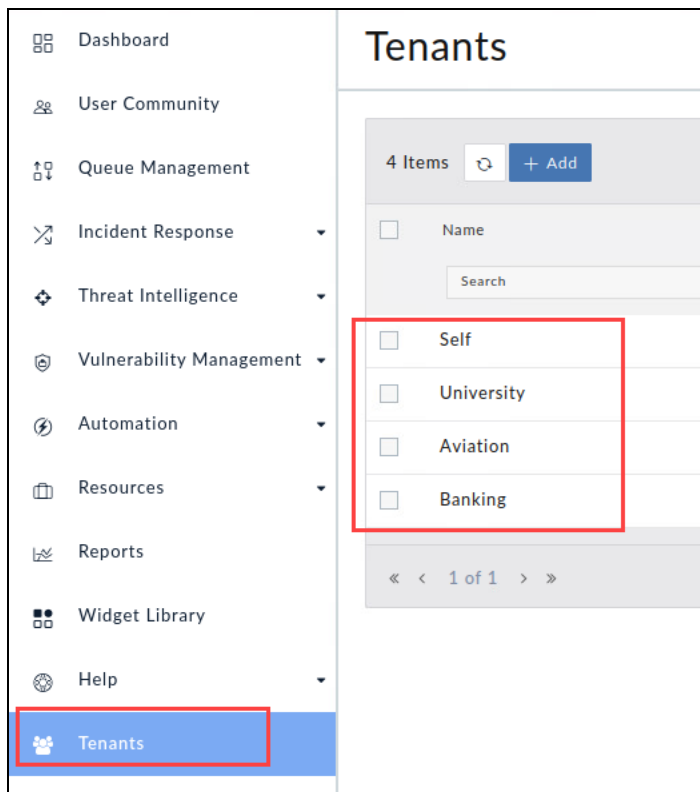


The three tenants that are configured on FortiSIEM are already configured on FortiSOAR.

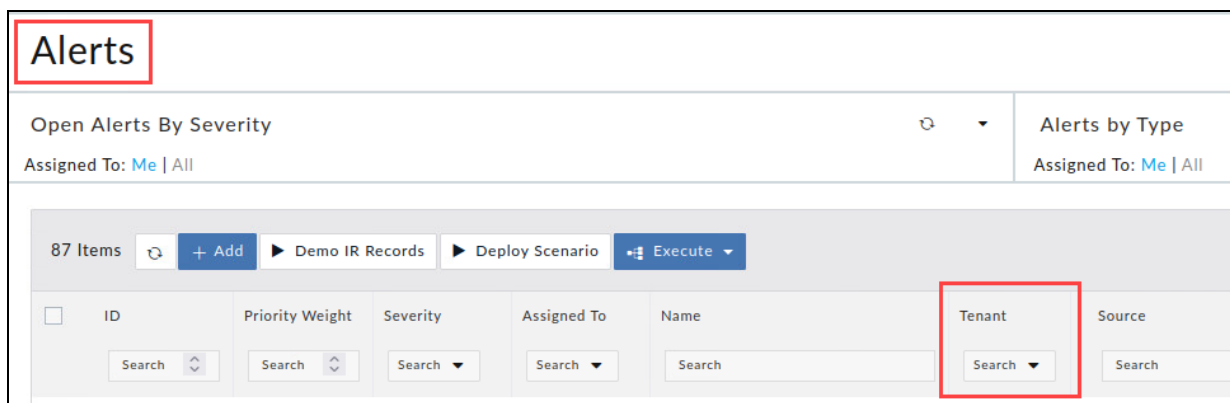
4. In the left navigation menu, click **Tenants**.

The same tenants can be viewed from this dedicated tenant menu.

The super organization is mapped to the **Self** tenant, which is the default tenant on FortiSOAR.



5. Continuing on the FortiSOAR GUI, click **Incident Response**.
6. Click **Alerts**.



There is a dedicated column to filter records by tenant name.

7. Log out of the FortiSOAR GUI.

Lab 2: Worker Configuration

In this lab, you will add a worker to the FortiSIEM cluster—the worker is already deployed and installed. Next, you will configure the FortiSIEM connector on FortiSOAR to ingest data from FortiSIEM to FortiSOAR. Finally, you will generate two incidents on FortiSIEM and ingest data to FortiSOAR to perform field mapping.

Objectives

- Add a worker to the FortiSIEM cluster
- Generate incidents on FortiSIEM
- Configure the FortiSIEM connector on FortiSOAR

Time to Complete

Estimated: 30 minutes

Exercise 1: Adding a Worker

In this exercise, you will add a worker to the FortiSIEM cluster. You cannot define collectors until you configure the worker upload address. Collectors receive this information during registration, and this value tells the collector which node it should upload the data to.

Add a Worker to the FortiSIEM Cluster

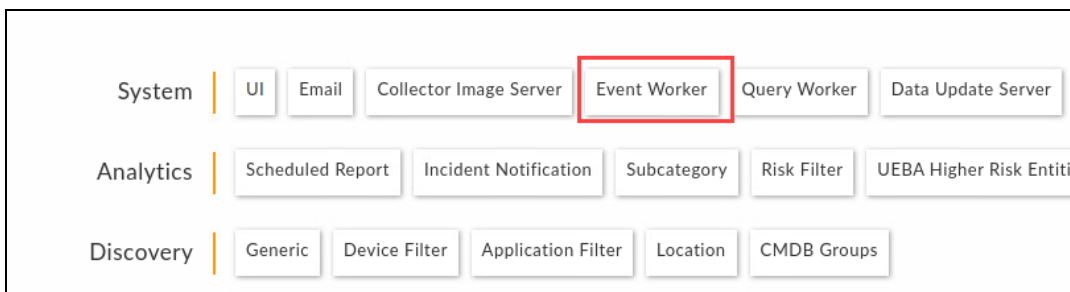
A worker enables the supervisor node to offload some of the log processing. You will add a worker to the FortiSIEM cluster.

To add a worker to the FortiSIEM cluster

1. On the supervisor FortiSIEM GUI, log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

2. Click **LOG IN**.
3. Click **ADMIN**.
4. In the left navigation pane, click **License**.
5. Click **Nodes**.
6. Click **Add**.
7. In the **Worker IP Address** field, type 10.0.1.140.
8. Click **OK**.
9. Continuing on the **ADMIN** tab, in the left navigation pane, click **Settings**.
10. Click **Event Worker**.



11. In the **Worker Address** field, type 10.0.1.140.
12. Click **Save**.

← All Settings > System > Event Worker

Worker Address: + -

Save

To view the health of the worker

- Continuing on the **ADMIN** tab, in the left navigation pane, click **Health**.

Cloud Health

Collector Health

Agent Health

Search...

Columns

Name	IP Address	Module Role	Health	Version	Load Average	CPU	Swap Used	Memory Size
super	10.0.1.130	Supervisor	Normal	6.3.0.0331	2.65,2.12,1.84	6%	0 KB	15.16 GB
worker.mssp.com	10.0.1.140	Worker	Normal	6.3.0.0331	0.59,1.09,0.7	3%	0 KB	7.58 GB

Search...

Columns

Process level metrics for worker.mssp.com (10.0.1.140)

Process Name	Status	Uptime	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorWorker	Up	3m 15s	0%	94 MB	1212 MB		
phParser	Up	3m 11s	0%	681 MB	2233 MB	99	148180
phEventForwarder	Up	3m 11s	0%	40 MB	534 MB		
phCheckpoint	Up	3m 11s	0%	35 MB	293 MB		
phPerfMonitor	Up	3m 11s	0%	75 MB	821 MB		
phIdentityWorker	Up	3m 11s	0%	62 MB	1044 MB	4	148180
phAgentManager	Up	3m 11s	0%	69 MB	1518 MB		

You can see the CPU and memory usage values for the worker and supervisor nodes, as well as the processes running on those nodes. The name of a node is the name that was assigned to the node during installation.

You will also notice that the supervisor node has a subset of more processes compared to the worker node.

- Log out of the supervisor FortiSIEM GUI.

Exercise 2: Generating Incidents on FortiSIEM

In this exercise, you will generate several different types of incidents on FortiSIEM using an incident generator script.

Generate Incidents on FortiSIEM

You will generate Windows security incidents using a script.

To generate incidents on FortiSIEM

1. On the Local-Host VM, open a terminal window (Ctrl+Alt+T).
2. Enter the following command to open an SSH connection to the FortiSIEM supervisor:
`ssh root@10.0.1.130`
3. Enter the password `Fortinet1!`.
4. Enter the following command to check your working directory—it should be `/root`:
`pwd`
5. Enter the following command, and then verify that the highlighted files are available:

```
ls -lrt
[root@super ~]# ls -lrt
total 58616
drwxr-xr-x 2 root root      69 Feb 21  2020 fixes
drwxr-xr-x 8 root root      91 Feb 21  2020 incidentSimData
-rw-r--r-- 1 root root    971 Jul  1 19:34 original-ks.cfg
-rw-r--r-- 1 root root   1610 Jul  1 19:34 anaconda-ks.cfg
-rw-r--r-- 1 root root 59760640 Jul  1 19:34 VBoxGuestAdditions.iso
-rwxr-xr-x 1 root root    485 Jul  1 19:36 zerofill.sh
-rw-r--r-- 1 root root   91316 Jul 13 20:52 fsmIncidentsSim.zip
-rw-r--r-- 1 root root   7037 Jul 13 20:52 fsmUebaDemo.zip
-rw-r--r-- 1 root root   58587 Jul 13 20:57 Lab.zip
-rw-r--r-- 1 root root    840 Jul 14 10:04 security_incident
-rw-r--r-- 1 root root   3460 Jul 14 10:04 security_sysmon_incident
-rw-r--r-- 1 root root   1427 Jul 14 10:04 security_user_incident
drwxr-xr-x 2 root root     87 Jul 27 10:12 fsmUebaDemo
-rw-r--r-- 1 root root    280 Jul 27 14:45 security_soar_incident
-rwxr-xr-x 1 root root   61456 Jul 27 15:11 fsmIncidentSimulator2_4.sh
drwxrwxr-x 5 root root     43 Jul 27 15:17 Lab
-rw-r--r-- 1 root root    539 Jul 27 18:44 incidentSimLog.log
[root@super ~]#
```

6. Enter the following command to run the incident generation script:
`./fsmIncidentSimulator2_4.sh security_soar_incident`
7. Close the SSH session tab.

To verify the incidents on FortiSIEM

1. On the supervisor FortiSIEM GUI, log in to the super organization with the following credentials:

Field	Value
User ID	admin

Field	Value
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

- 2. Click **INCIDENTS**.
- 3. Verify that you have two incidents with a **HIGH** severity.

Actions	Overview	List	Risk	Explorer	UEBA	MITRE ATT&CK	Timeline	
2 Web Traffic to FortiSandbox Malicious URLs Incidents for Last 2 Hours								
Severity Category	Last Occurred	Incident	Detail	Target	Tactics	Technique	Reporting	Source
HIGH	Jul 28 2021, 09:40:00 PM	Web Traffic to FortiSandbox Malicious URLs	Informational URL: https://upload.gumblar.cn	upload.gumblar.cn	Exfiltration	Exfiltration Over C2 ..	HCS* 372.56.1.0	172.16.8.105
HIGH	Jul 28 2021, 09:40:00 PM	Web Traffic to FortiSandbox Malicious URLs	Informational URL: https://upload.gumblar.cn	upload.gumblar.cn	Exfiltration	Exfiltration Over C2 ..	HCS* 372.56.1.0	172.16.8.105

- 4. Log out of the supervisor FortiSIEM GUI.

Exercise 3: Configuring FortiSIEM Data Ingestion

In this exercise, you will configure data ingestion from FortiSIEM.

Configure the FortiSIEM Connector

You will configure the FortiSIEM connector to automatically pull incidents from FortiSIEM to FortiSOAR on a scheduled basis.

To configure the FortiSIEM connector

1. On the FortiSOAR management GUI, log in with the username `csadmin` and password `Fortinet1!`.
2. Click **Automation > Connectors**.
3. In the **Installed** section, search for the `Fortinet FortiSIEM` connector, and then open it.
4. Configure the following settings:

Field	Value
Configuration Name	lab
Mark As Default Configuration	Enable
Server URL	https://10.0.1.130
Username	admin
Password	Fortinet1!
Organization	super
Verify SSL	Disable

5. Click **Save**.
6. Verify that the **CONFIGURATION** field is **COMPLETED** and the **HEALTH CHECK** field is **AVAILABLE**.

Fortinet FortiSIEM
Connector Version 4.1.1
Certified: Yes
Publisher: Fortinet

FortiSIEM provides integrations that allow you to query and make changes to the CMDB, query events, and send incident notifications. Provide actions like get incidents, comment incident, cleared incident, get device...

Active Deactivate Connector ✓ Compatible with your integration

Configurations **1** Actions 19 Playbooks 1 Agents 0

Select Configuration

lab Target Self Agent

CONFIGURATION: COMPLETED **HEALTH CHECK: AVAILABLE**

Configuration Name *

lab Configure Data Ingestion

☒ Mark As Default Configuration Visibility Public Private

Server URL: *

https://10.0.1.130

Username: *

admin

Password: *

Set Password

Password fields are write-only. If you do not change this field, your Password will not be overwritten.

Organization: *

Super

✓ Save ✕ Cancel Uninstall

7. Close the connector configuration window.

To configure data ingestion for FortiSIEM

1. Continuing on the FortiSOAR GUI, click **Automation > Connectors**.
2. Click **Data Ingestion**.
3. In the **lab** row, click **Configure Ingestion**.

Configuration	Status	Schedule	Last Data Pulled On	Actions
lab	AVAILABLE			Configure Ingestion

4. Click **Let's start by fetching some data**.
5. In the **Fetch Data** step, configure the following settings:

Field	Value
Fetch Mode	By Updates In Last X Minutes
Pull Incidents Creates/Updates In Last X Minutes	240
Maximum Events To Pull Per Incident	1
Configure Multi-Tenant Mappings	Select the checkbox.
Organization Mapping	{ "Super": "Self", "Banking": "Banking", "Aviation": "Aviation", "University": "University" }

Your configuration should match the following example:

Configurations

Inputs

Fetch Mode: ⓘ

By Updates In Last X Minutes ▾

Pull Incidents Creates/Updates In Last X Minutes: ⓘ

240

Maximum Events To Pull Per Incident: ⓘ

1

Filter Incidents: ⓘ

Select one or more options

Incident Status

Incident Category

Incident Sub Category

...

Configure Multi-Tenant Mappings:

☒

Organization Mapping: ⓘ

≡ ≡ ↶ ↷ Code ▾

1 {

2 "Super": "Self",

3 "Banking": "Banking",

4 "Aviation": "Aviation",

5 "University": "University"

6 }

Ln: 3 Col: 24

- Click **FETCH DATA**.
- In the **Field Mapping** step, in the **Module** drop-down list, select **Alerts**.

Advanced Analytics 6.3 Lab Guide
Fortinet Technologies Inc.

30

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

8. In the **Name** field, delete **eventType**.

The **Name** field should match the following example:

The screenshot shows the 'Field Mapping' section of the FortiSIEM interface. The 'Module' dropdown is set to 'Alerts'. The 'Name' field is highlighted with a red box and contains the value `{{vars.item.attributes.eventName}}`. The 'Fetch Data' button is visible in the top right corner.

9. In the search field, type **MITRE**.
10. Click inside the **MITRE ATT&CK ID** field.
11. In the **Sample Data** section, search for **Technique**.
12. Click **attackTechniqueId**.

The screenshot shows the 'Data Ingestion - Fortinet FortiSIEM' interface. The 'Field Mapping' section on the left has a search field containing 'MITRE'. Below it, the 'MITRE ATT&CK ID' field is highlighted with a red box and contains the value `[attributes].[attackTechniqueId]`. The 'MITRE Technique' field is empty. The 'Sample Data' section on the right has a search field containing 'Technique'. Below it, a list of incident data is displayed. The 'attackTechniqueId' field in the data is highlighted with a yellow box and contains the value 'T1048.001'.

The **attackTechniqueId** field in the **Sample Data** section is mapped to the **MITRE ATT&CK ID** field in the **Field Mapping** section.

13. Click inside the **MITRE Technique** field of the **Field Mapping** section.
14. In the **Sample Data** section, search for **Tactic**.
15. Click **attackTactic**.

The screenshot shows the FortiSIEM Field Mapping interface. The 'Field Mapping' section on the left has a search bar with 'MITRE' and a dropdown menu set to 'Alerts'. Below, the 'MITRE ATT&CK ID' field is mapped to '[\"attributes\"][\"attackTechniqueId\"]' and the 'MITRE Technique' field is mapped to '[\"attributes\"][\"attackTactic\"]'. The 'Sample Data' section on the right displays a JSON object with various fields, including 'attackTactic: Exfiltration' which is highlighted with a red box.

The **attackTactic** field in the **Sample Data** section is mapped to the **MITRE Technique** field in the **Field Mapping** section.

16. Click **Save Mapping & Continue**.
17. In the **Do you want to schedule the ingestion?** drop-down list, select **Yes**.
18. Click **Every X minutes**.
19. In the **minute** field, type ***/1**.
20. Type ***** for **hour**, **day of month**, **month**, and **day of week** if ***** is not already in those fields by default.

The screenshot shows the FortiSIEM Schedule Settings interface. The 'Do you want to schedule the ingestion?' dropdown is set to 'Yes'. The 'Configure Schedule Settings' section shows a frequency of '*/1' for 'minute', with other fields set to '*'. The text 'Every minute' is displayed below the fields.

21. Click **Save Settings & Continue**.
The **Quick Summary** page is displayed.
22. Review the **Quick Summary** section.

Data Ingestion Successfully Configured!

Playbook collection **Fortinet FortiSIEM [4.1.1]** is created and placed [here](#). You can rerun the wizard or edit the ingestion playbook to make further changes.

Quick Summary

- ✓ Connector 'Fortinet FortiSIEM' Configured
- ✓ Sample Data Fetched Successfully
- ✓ Field Mappings Added
- ✓ Schedule Created
- ✓ Ingestion Playbooks Created Successfully:
 - [FortiSIEM > Ingest](#) ACTIVE
 - [FortiSIEM > Fetch](#) ACTIVE

23. Click **Done**.

To verify the data ingestion schedule

1. Continuing on the FortiSOAR GUI, click **Automation > Schedules**.
2. Verify that the data ingestion scheduler for **Ingestion_fortinet-fortisiem** ran at least one time.
The **Total Run Count** must be **1** or more than 1.

To verify data ingestion from FortiSIEM

1. Continuing on the FortiSOAR GUI, click **Incident Response > Alerts**.
Alerts are displayed with a **Source** value of **Fortinet FortiSIEM**.

Alerts

Open Alerts By Severity ↕ Alerts by Type

Assigned To: [Me](#) | [All](#) Assigned To: [Me](#) | [All](#)

1 Items ↻ [+ Add](#) [▶ Demo IR Records](#) [▶ Deploy Scenario](#) [⚙ Execute](#)

☐	ID	Priority Weight	Severity	Assigned to	Name	source
☐	81	20	Critical	CS Admin	Web traffic to FortiSandbox Malicious URLs-PH_RULE_W...	Fortinet FortiSIEM



If you do not see the alerts, wait for a minute because the schedule runs every minute.

2. Log out of the FortiSOAR GUI.

Lab 3: Administration and Management of Collectors

In this lab, you will assign two collectors to one organization and a third collector to another organization. After you add the collectors on the supervisor node, you will register the collectors to the supervisor node.

Objectives

- Assign collectors to organizations
- Register collectors to the supervisor
- Add credentials for organizations with collectors
- Discover devices from organizations with collectors

Time to Complete

Estimated: 40 minutes

Exercise 1: Assigning Collectors to Organizations

In this exercise, you will assign collectors to organizations, and configure the guaranteed events per second (EPS) for each collector.

Assign Collectors to Organizations

Collectors must be defined for organizations that have collectors in their environment. Now, you will add collectors by editing the organizations that you created earlier.

To assign collectors to organizations

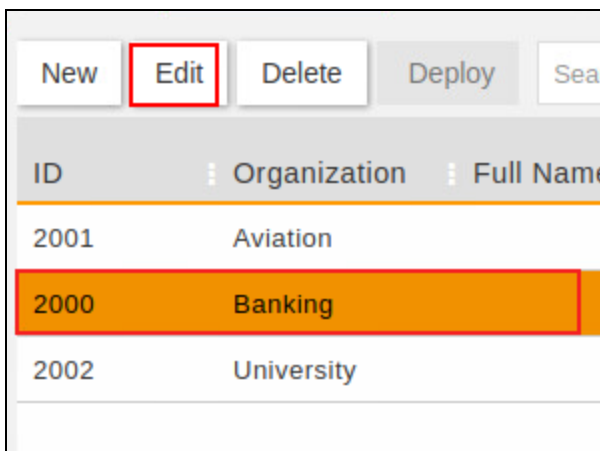
1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click the **ADMIN** tab.
5. In the left navigation pane, click **Setup**, and then click **Organizations**.



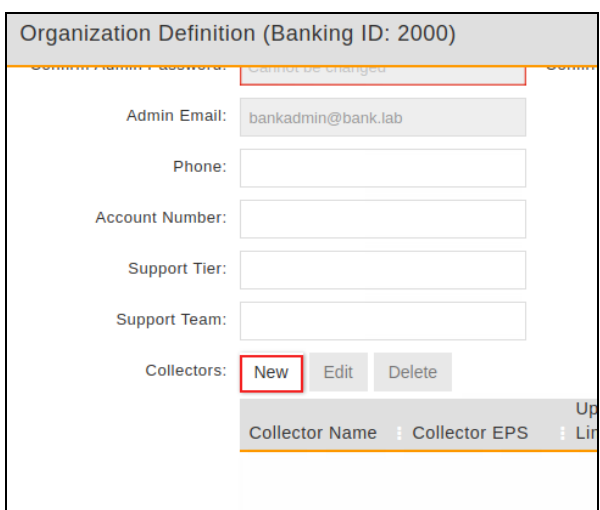
6. Select the **Banking** organization, and then click **Edit**.



A screenshot of a web interface showing a table of organizations. The table has columns for ID, Organization, and Full Name. The row with ID 2000 and Organization Banking is highlighted in orange. Above the table, there are buttons for New, Edit, Delete, Deploy, and Search. The 'Edit' button is highlighted with a red box.

ID	Organization	Full Name
2001	Aviation	
2000	Banking	
2002	University	

7. Scroll down, and click **New** to add a collector.



A screenshot of the 'Organization Definition (Banking ID: 2000)' form. The form contains fields for Admin Email (bankadmin@bank.lab), Phone, Account Number, Support Tier, and Support Team. Below these fields is a 'Collectors' section with buttons for New, Edit, and Delete. The 'New' button is highlighted with a red box. Below the buttons is a table with columns for Collector Name, Collector EPS, and Link.

Collector Name	Collector EPS	Link
----------------	---------------	------

8. Enter the following values:

Field	Value
Name	collector1
Guaranteed EPS	100
Start Time	Unlimited
End Time	Unlimited

9. Click **Save**.

Note the collector name. You will use this information during the collector registration.

Your configuration should match the following example:

Organization Definition (Banking ID: 2000)

Organization:	Banking	Include IP/IP Range:	
Full Name:		Exclude IP/IP Range:	
Admin User:	bankadmin	Agent User:	
Admin Password:	Cannot be changed	Agent Password:	
Confirm Admin Password:	Cannot be changed	Confirm Agent Password:	
Admin Email:	bankadmin@bank.lab	Max Devices:	0
Phone:		Address:	
Account Number:		Account Type:	
Support Tier:		Account Status:	
Support Team:		Account Manager:	
Collectors:	New Edit Delete	Lines: 1	

Collector Name	Collector EPS	UpLoad Rate Limit	Valid Start Date	Valid End Date
collector1	100	Unlimited	Unlimited	Unlimited

Save Cancel

10. Click **Save**.
Note the collector name. You will use this information during the collector registration.
11. Select the **Aviation** organization, and then click **Edit**.
12. Scroll down, and then click **New** to add a collector.
13. Enter the following values:

Field	Value
Name	collector2
Guaranteed EPS	150
Start Time	Unlimited
End Time	Unlimited

14. Click **Save**.
Note the collector name. You will use this information during the collector registration.
15. Click **Save**.

Verify Collector Health

Now, you will verify the health of collectors.

To verify collector health

1. Continuing on the **ADMIN** tab, on the left navigation pane, click **Health**.
2. Click **Collector Health**.

Cloud Health Collector Health Agent Health						
Show Processes Tunnels Action Search... Columns						
Organization	Name	IP Address	Status	Collector ID	CPU	Memory
Banking	collector1		No Connection	10000	0%	0%
Aviation	collector2		No Connection	10001	0%	0%

If you do not see the collectors, click the refresh icon (🔄).



The **Status** of all three collectors is **No Connection**. For the **Status** column to show a status of **up**, you must deploy, install, and register the collectors to the supervisor. The collectors have already been installed and IP addresses have been assigned. In the next lab exercise, you will register the collectors and verify that their **Status** is **up**.

3. Log out of the Supervisor FortiSIEM management GUI.

Exercise 2: Registering Collectors

In this exercise, you will register the collectors to the supervisor, and then verify that their status is up.

Register Collectors

Now, you will register the collectors to the supervisor. During registration, the collector is provided with information such as supervisor IP address, username, password, organization name, and collector name.

To register Collector1

1. Open an SSH connection to the Collector1 [10.0.2.130] FortiSIEM from Local-Host machine.
Log in to the collector1 with the following credentials:

Field	Value
Username	root
Password	Fortinet1!

2. Type the following commands to register Collector1 with the supervisor node:

```
phProvisionCollector --add bankadmin Password1! 10.0.1.130 Banking collector1
```

The collector will reboot to complete the registration process.

```
student@client:~$ ssh root@10.0.2.130
The authenticity of host '10.0.2.130 (10.0.2.130)' can't be established.
ECDSA key fingerprint is SHA256:h2Edjfd+q7XjekB6JYv0LxsdFxnzY9IK6ESKt+keGs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/student/.ssh/known_hosts).
root@10.0.2.130's password:
Last login: Tue Jul 13 13:27:06 2021
[root@collector1 ~]# phProvisionCollector --add bankadmin Password1! 10.0.1.130 Banking collector1
Continuing to provision the collector
This collector is registered successfully. Waiting for reboot...
[root@collector1 ~]# Connection to 10.0.2.130 closed by remote host.
Connection to 10.0.2.130 closed.
student@client:~$
```

3. Close the SSH session.

To register Collector2

1. Open an SSH connection to the Collector2 [10.0.3.130] FortiSIEM from Local-Host machine.
Log in to the collector2 with the following credentials:

Field	Value
Username	root
Password	Fortinet1!

2. Type the following commands to register Collector3 with the supervisor node:

```
phProvisionCollector --add flightadmin Password1! 10.0.1.130 Aviation collector2
```

The collector will reboot to complete the registration process.

```
student@client:~$ ssh root@10.0.3.130
The authenticity of host '10.0.3.130 (10.0.3.130)' can't be established.
ECDSA key fingerprint is SHA256:lrSz3PhPtDYNpaYZhJGPh7Ch6oxFoAqurWvjWWuq54w.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/student/.ssh/known_hosts).
root@10.0.3.130's password:
Last login: Tue Jul 13 13:29:15 2021
[root@collector2 ~]# phProvisionCollector --add flightadmin Password1! 10.0.1.130 Aviation collector2
Continuing to provision the collector
This collector is registered successfully. Waiting for reboot...
```

3. Close the SSH session.

Verify Collector Health

Now, you will verify the health of the collectors.

To verify collector health

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **ADMIN**.
5. In the left navigation pane, click **Health**, and then click **Collector Health**.
6. Click refresh (🔄).

Cloud Health Collector Health Agent Health											
Show Processes		Tunnels	Action	Search		Columns		Lines: 2 Last updated at 12:10:20 PM			
Organization	Name	IP Address	Status	Collector type	Health	Uptime	CPU	Memory	Allocated EPs	Incoming E/Ps	Version
Blinding	collector1	10.0.2.130	up	VM	Normal	9hr 24s	6%	32%	100	0	6.3.0.0531
Aviation	collector2	10.0.3.130	up	VM	Normal	3hr 24s	9%	32%	150	0	6.3.0.0531

The **Status** of all three collectors is **up**, the **Health** is **Normal**, and the correct IP address is associated with each collector.

7. Select any of the collector and click Show Processes to view the processes running on the collector and their status.

Cloud Health Collector Health Agent Health						
Show Processes Tunnels Action Search... Columns						
Organization	Name	IP Address	Status	Collector Type	Health	Uptime
Banking	collector1	10.0.2.130	up	VM	Normal	9m 24s
Aviation	collector2	10.0.3.130	up	VM	Normal	3m 24s
Close Panel Search... Columns						
Process Name	Status	Uptime	CPU	Physical Memory	Virtual Memory	
phMonitorAgent	Up	5m 1s	0%	562 MB	1117 MB	
phParser	Up	4m 35s	0%	679 MB	2225 MB	
phPerfMonitor	Up	4m 52s	0%	73 MB	796 MB	
phEventForwarder	Up	4m 52s	0%	38 MB	533 MB	
phDiscover	Up	4m 52s	0%	57 MB	533 MB	
phAgentManager	Up	4m 52s	0%	71 MB	1517 MB	
phCheckpoint	Up	4m 52s	0%	34 MB	292 MB	
Organization: Super User: admin Scope: Global						



If the status of any of the collectors is not **up**, open an SSH connection to the collector, and then reboot it using the following commands:

```
reboot -h now
```

- Log out of the Supervisor FortiSIEM management GUI.

Exercise 3: Discovering FGT Banking through a Collector

In this exercise, you will discover a FortiGate device in the banking organization that has two collectors.

Configure SNMP on FortiGate

Now, you will configure SNMP on FortiGate at the Banking organization. You will enable SNMP events that are critical for FortiSIEM to monitor.

Configure SNMP on FGT Banking

1. Go to the management GUI of the FGT Banking FortiGate.
2. Log in with the username `admin` and password `password`.
3. Click **System** > **SNMP**.
4. Enable **SNMP Agent**.
5. Enter the following values:

Field	Value
Description	FGT_Banking
Location	Ottawa

6. In the **SNMP v1/v2c** section, click **Create New**.
7. Enter the following values:

Field	Value
Community Name	public
Enabled	enable
IP Address	0.0.0.0/0
Host Type	Accept queries and send traps

8. Scroll down to the **SNMP Events** section, and verify that the following traps are enabled:

Field	Value
VPN tunnel is up	enable
VPN tunnel is down	enable
IPS detected an attack	enable

Field	Value
IPS detected an anomaly	enable
AV detected virus	enable
AV detected oversized file	enable
AV detected file matching pattern	enable
AV detected fragmented file	enable

9. Click **OK**.
10. Click **Apply**.

To enable the SNMP service on an interface

1. Continuing on the FGT Banking management GUI, click **Network > Interfaces**.
2. Select **port2**, and then click **Edit**.
3. In the **Administrative Access** section, enable **SNMP**.
4. Click **OK**.
5. Log out to the FGT Banking FortiGate management GUI.

Add Credentials for FortiGate

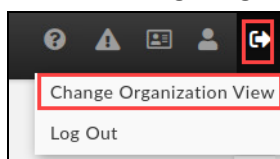
Now, you will add the FortiGate credentials on FortiSIEM. Using these credentials, FortiSIEM will be able to discover the FortiGate device.

To add credentials for FGT Banking

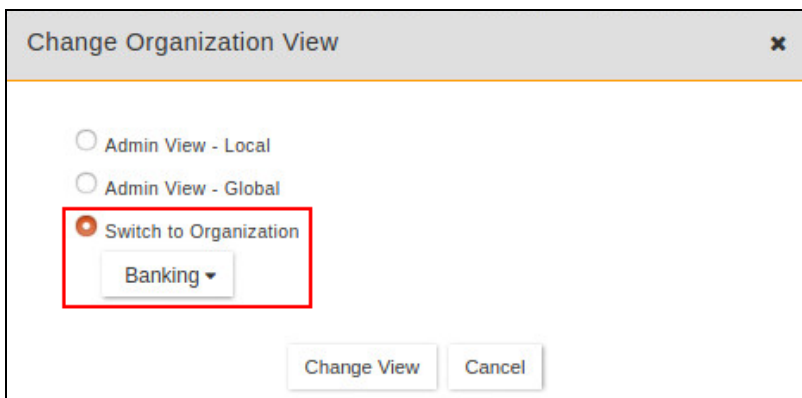
1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click the **Change Organization View** icon and, in the drop-down list, select **Change Organization View**.



5. Select **Switch to Organization** and in the drop-down list, select **Banking**.



6. Click **Change View**.
7. Click **ADMIN**.
8. In the left navigation pane, click **Setup**, and then click **Credentials**.
9. In the **Step 1: Enter Credentials** section, click **New**.
10. Enter the following values:

Field	Value
Name	Banking_FGT_SNMP
Device Type	Generic
Access Protocol	SNMP
Port	161
Password config	Manual
Community String	public
Confirm Community String	public

11. Click **Save**.
12. In the **Step 1: Enter Credentials** section, click **New** again.
13. Enter the following values:

Field	Value
Name	Banking_FGT_SSH
Device Type	Fortinet FortiOS
Access Protocol	SSH
Port	22
Password config	Manual

Field	Value
User Name	admin
Password	password
Confirm Password	password

- Click **Save**.
- In the **Step 2: Enter IP Range to Credential Associations** section, click **New**.
- Enter the following values:

Field	Value
IP/IP Range	10.0.2.254
Credential	Banking_FGT_SNMP Click +, and then select Banking_FGT_SSH .

- Click **Save**.
Your configuration should match the following example:

The screenshot displays the FortiGate web interface with the 'Credentials' tab selected. It shows two steps in the configuration process:

Step 1: Enter Credentials

Name	Protocol	Device Type	User Name	Description
Banking_FGT_SNMP	SNMP	Generic	admin	
Banking_FGT_SSH	SSH	Fortinet FortiOS	admin	

Step 2: Enter IP Range to Credential Associations

Name/IP/IP Range	Credential Name
10.0.2.254	Banking_FGT_SSH, Banking_FGT_SNMP

Discover Banking FortiGate

Now, you will discover the Banking FortiGate device.

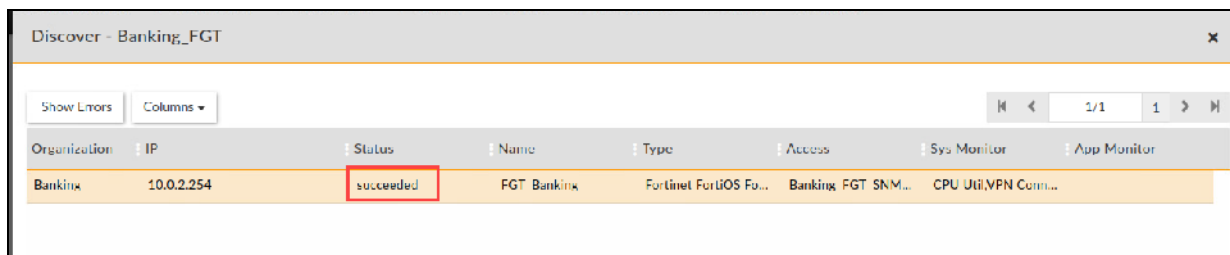
To discover FGT Banking

1. Continuing on the **Setup** page on FortiSIEM, click **Discovery**.
2. Click **New**.
3. Enter the following values:

Field	Value
Name	Banking_FGT
Discovery Type	Range Scan
Include	10.0.2.254
Name Resolution	SNMP/WMI first

4. Click **Save**.
5. Click **Discover**.

Wait for the discovery to complete.



The screenshot shows a window titled 'Discover - Banking_FGT'. It contains a table with the following data:

Organization	IP	Status	Name	Type	Access	Sys Monitor	App Monitor
Banking	10.0.2.254	succeeded	FGT_Banking	Fortinet FortiOS Fou...	Banking_FGT SNMP...	CPU Util,VPN Comm...	

6. Click **Close**.

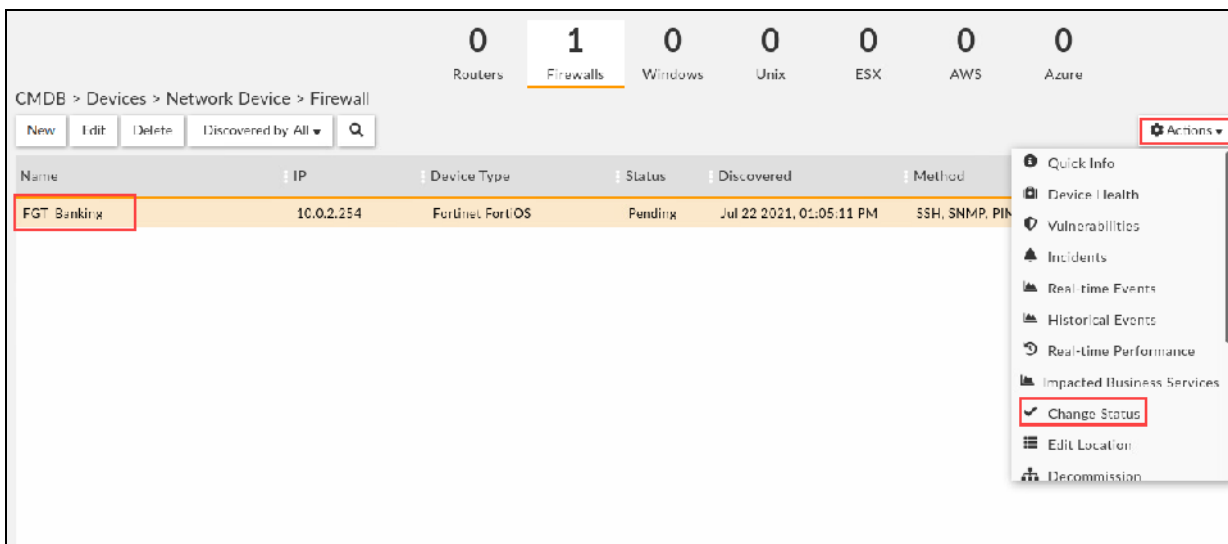
Approve FortiGate in CMDB

When FortiSIEM discovers devices, monitoring begins automatically, and incidents for those devices will be triggered automatically based on the rules associated with those devices. However, you can configure the discovery settings so incidents are triggered only for devices you approve.

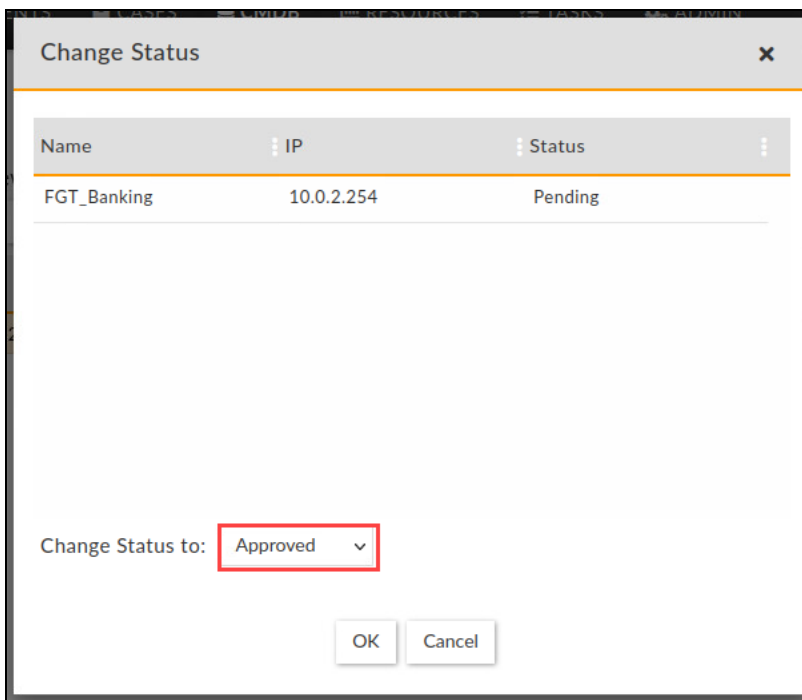
Since this is a lab environment with few devices, you can use the default settings.

To approve FGT Banking in CMDB

1. Continuing on the FortiSIEM management GUI, click **CMDB**.
2. In the left navigation pane, click **Devices > Network Device > Firewalls**.
3. Select **FGT_Banking**.
4. Click **Action**, and in the drop-down list, select **Change Status**.



5. Verify that the **Change Status to** setting is set to **Approved**.



6. Click **OK**.
7. Log out of the Supervisor FortiSIEM management GUI.

Exercise 4: Discovering FGT Aviation through a Collector

In this exercise, you will discover a FortiGate device from the aviation organization that has a collector.

Configure Syslog on FGT Aviation

Syslog is another method of sending logs to FortiSIEM. Now, you will configure Syslog on the Aviation FGT FortiGate device and enable only the essential logs that you want to monitor on FortiSIEM.

To configure Syslog on FGT Aviation

1. Go to the management GUI of FGT Aviation FortiGate.
2. Log in with the username `admin` and password `password`.
3. Click **Log & Report > Log Settings**.
4. Enable **Send logs to syslog**.
5. In the **IP Address/FQDN** field, type `10.0.3.130`.
6. In the **Event Logging** section, click **Customize**.
7. Enable the following events:
 - **System activity event**
 - **VPN activity event**
 - **User activity event**
 - **Router activity event**
8. In the **Local Traffic Log** section, click **Customize**.
9. Verify that the following events are disabled:
 - **Log Allowed Traffic**
 - **Log Local Out Traffic**
 - **Log Denied Unicast Traffic**
 - **Log Denied Broadcast Traffic**

Your configuration should match the following example:

Log Settings

Event Logging

All

Customize

☒ System activity event

☒ VPN activity event

☒ User activity event

☒ Router activity event

☐ WiFi activity event

☐ Explicit web proxy event

☐ Endpoint event

☐ HA event

☐ Security Rating event

☐ FortiExtender event

☐ SDN connector Event

☐ SD-WAN event

☐ CIFS event

☐ Switch controller event

Local Traffic Log

All

Customize

☐ Log Allowed Traffic

☐ Log Denied Unicast Traffic

☐ Log Local Out Traffic

☐ Log Denied Broadcast Traffic

10. Click **Apply**.

Configure SNMP on Aviation FortiGate

Now, you will configure SNMP on FGT Aviation and enable the SNMP events that you would like to monitor on FortiSIEM.

To configure SNMP on FGT Aviation

- 1. Continuing on the management GUI of FGT Aviation, click **System > SNMP**.
- 2. Enable **SNMP Agent**.
- 3. Enter the following values:

Field	Value
Description	FGT_Aviation
Location	London

- 4. In the **SNMP v1/v2c** section, click **Create New**.
- 5. Enter the following values:

Field	Value
Community Name	public
Enabled	enable

Field	Value
IP Address	0.0.0.0/0
Host Type	Accept queries only

6. Scroll down to the **SNMP Events** section, and disable all SNMP events except the following:
 - **IPS detected an attack**
 - **IPS detected an anomaly**
7. Click **OK**.
8. Click **Apply**.

To enable SNMP on an interface

1. Continuing on the management GUI of FGT Aviation, click **Network > Interfaces**.
2. Select **port2**, and then click **Edit**.
3. In the **Administrative Access** section, enable **SNMP**.
4. Click **OK**.
5. Log out of the FGT Aviation FortiGate management GUI.

Add Credentials for Aviation FortiGate

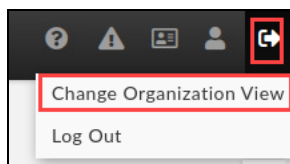
Now, you will add the FortiGate credentials on FortiSIEM so that FortiGate can be discovered through SNMP.

To add credentials for FGT Aviation

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click the **Change Organization View** icon, and in the drop-down list, select **Change Organization View**.



5. Select **Switch to Organization**, and in the drop-down list, select **Aviation**.
6. Click **Change View**.



If you are already logged in as an admin user of the banking organization, you must change the scope to **Global**, and then change the scope again to **Aviation**.

You can also log out and log back in as an admin user of the aviation organization.

7. Click **ADMIN**.
8. In the left navigation pane, click **Setup**, and then click **Credentials**.
9. In the **Step 1: Enter Credentials** section, click **New**.
10. Enter the following values:

Field	Value
Name	Aviation_FGT_SSH
Device Type	Fortinet FortiOS
Access Protocol	SSH
Port	22
Password config	Manual
User Name	admin
Password	password
Confirm Password	password

11. Click **Save**.
12. In the **Step 1: Enter Credentials** section, click **New** again.
13. Enter the following values:

Field	Value
Name	Aviation_FGT_SNMP
Device Type	Generic
Access Protocol	SNMP
Port	161
Password config	Manual
Community String	public
Confirm Community String	public

14. Click **Save**.
15. In the **Step 2: Enter IP Range to Credential Associations** section, click **New**.

16. Enter the following values:

Field	Value
IP/Host Name	10.0.3.254
Credential	Aviation_FGT_SSH Click + , and then select Aviation_FGT_SNMP .

17. Click **Save**.

Discover FortiGate

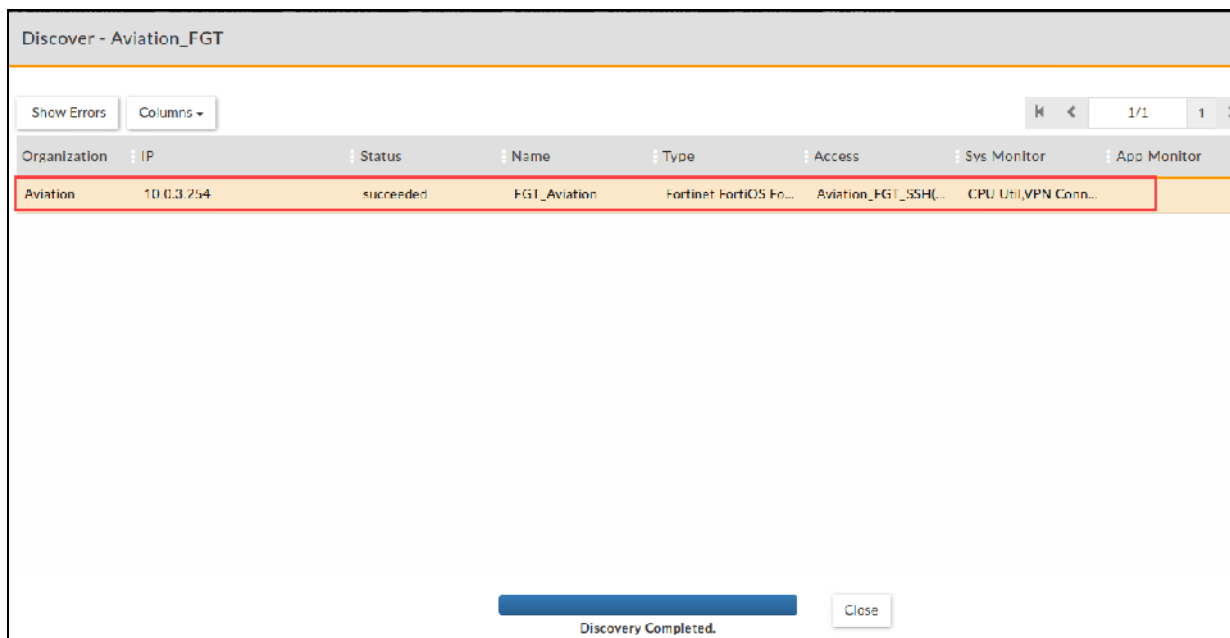
Now, you will discover the FortiGate device from Aviation organization on FortiSIEM.

To discover FGT Aviation

1. Continuing on the **Setup** page of FortiSIEM, click **Discovery**.
2. Click **New**.
3. Enter the following values:

Field	Value
Name	Aviation_FGT
Discovery Type	Range Scan
Include	10.0.3.254
Name Resolution	SNMP/WMI first

4. Click **Save**.
5. Click **Discover**.
Wait for the discovery to complete.



6. Click **Close**.

Approve FortiGate in CMDB

When FortiSIEM discovers devices, monitoring begins automatically, and incidents for those devices will be triggered automatically based on the rules associated with those devices. However, you can configure the discovery settings so incidents will be triggered only for devices you approve.

Since this is a lab environment with few devices, you can use the default settings.

To approve FGT Aviation in CMDB

1. Continuing in the aviation organization scope, click **CMDB**.
2. In the left navigation pane, click **Devices > Network Device > Firewall**.
3. Select **FGT_Aviation**.
4. Click **Action**, and in the drop-down list, select **Change Status**.
5. Verify that the **Change Status to** setting is set to **Approved**.
6. Click **OK**.
7. Log out of the Supervisor FortiSIEM management GUI.

Lab 4: Administration and Management of Agents

In this lab, you will add Windows and Linux agents to organizations.

Objectives

- Add agent credentials to organizations
- Register agents to a supervisor

Time to Complete

Estimated: 30 minutes

Exercise 1: Adding a Windows Agent to an Organization

In this exercise, you will add a Windows agent to the aviation organization. You will also configure audit policies on Windows so that appropriate security events will be sent to FortiSIEM for analysis.

Configure Windows Agent Registration Credentials

Before registering a Windows agent, you must define the administrator credentials for the organization through which the Windows agent will be managed.

To define Windows agent registration credentials

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **ADMIN**.
5. In the left navigation pane, click **Setup**, and then click **Organizations**.



6. Select **Aviation**, and then click **Edit**.
7. Enter the following values:

Field	Value
Agent User	admin
Agent Password	Password1!
Confirm Agent Password	Password1!

8. Click **Save**.
Note the aviation organization ID. You will need this ID during the agent registration process.

Configure the Windows Agent Installation Settings File

Using a text editor, you will edit the `InstallSettings.xml` file, which is located in the same folder as the Windows agent binaries. You will specify parameters such as organization name, organization ID, administrator username, administrator password, and supervisor IP.

To configure the `InstallSettings.xml` file

1. Go to the Win-Agent VM.
2. Click **Resource** > **FSM_WindowsAgent** > `InstallSettings.xml`.
Open the file in Notepad++.
3. Enter the following values:

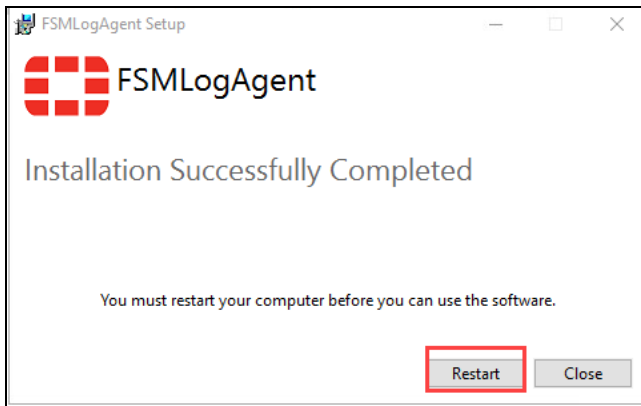
Field	Value
ORG_ID	Enter the aviation organization ID.
ORG_NAME	Aviation
SUPER_IP	10.0.1.130
ORG_NAME/AGENT_USER	Aviation/admin
AGENT_PASSWORD	Password1!

Your configuration file should match the following example, except for the organization ID.

```
<?xml version="1.0" encoding="utf-8"?>
<InstallConfig Version="1">
  <Org>
    <ID>2001</ID>
    <Name>Aviation</Name>
  </Org>
  <Super>
    <Name>10.0.1.130</Name>
    <Port>443</Port>
  </Super>
  <HostName>Win_Agent</HostName>
  <Registration>
    <Username>Aviation/admin</Username>
    <Password>Password1!</Password>
  </Registration>
  <Proxy>
    <Server></Server>
    <Port></Port>
  </Proxy>
  <SSLCertificate>ignore</SSLCertificate>
</InstallConfig>
```

4. Save the file (Ctrl + S).
5. Close the file.

- Return to the **FSM_WindowsAgent** folder, and double-click the MSI package `FSMLogAgent-v4.1.2-build0108`.
- Click **Install**.
The installer will display an install progress window.
- When installation is complete, click **Restart** to restart the Windows device.

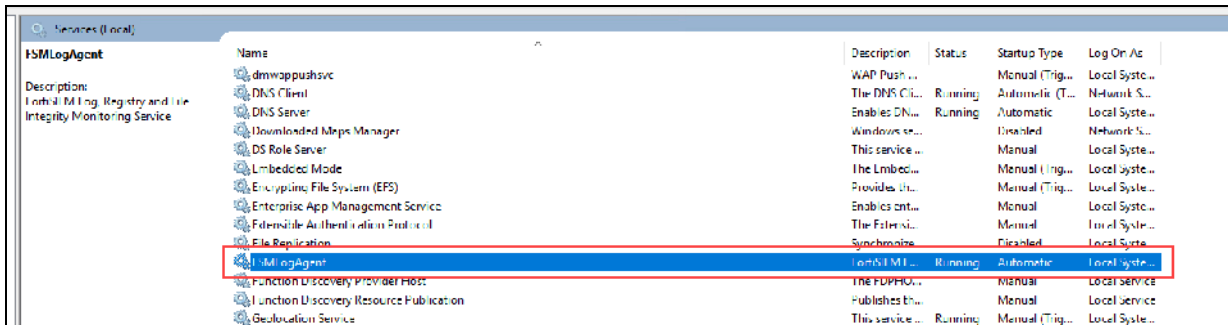


Wait for the windows server to come back up.

- On the Win-Agent VM task bar, click **Services**.



- Verify that the **FSMLogAgent** is **Running**.



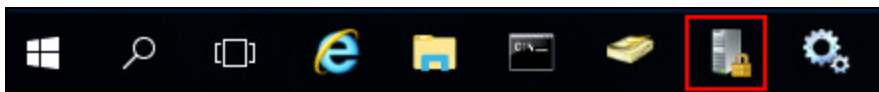
- Close the **Services** window.

Define an Audit Policy

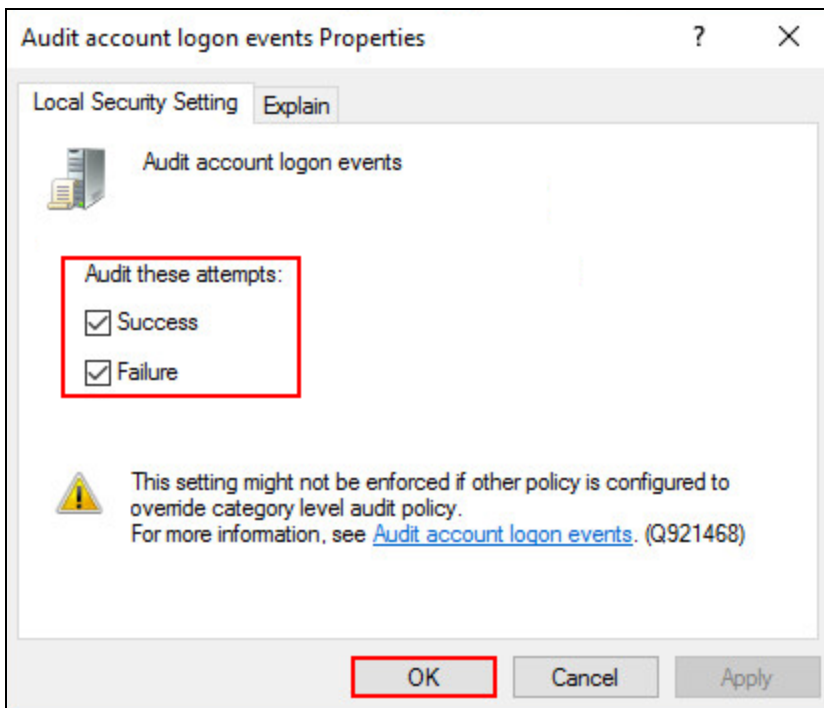
Since Windows generates a lot of security logs, you will specify the categories of events that you want to be logged and available for monitoring by FortiSIEM.

To define an audit policy

- On the Win-Agent VM taskbar, click **Local Security Policy**.



2. Click **Local Policies > Audit Policy**.
3. Double-click **Audit account logon events**.
4. Enable both **Success** and **Failure**.
5. Click **OK**.



6. Configure the following audit policies the same way:
 - **Audit logon events**
 - **Audit object access**
 - **Audit policy change**

Your configuration should match the following example:

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

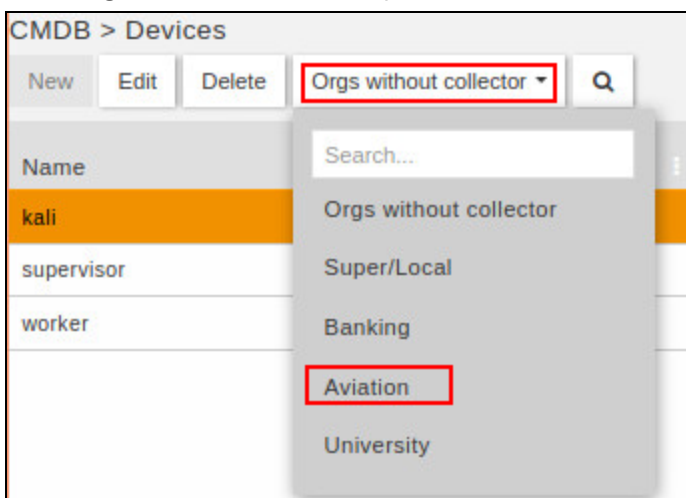
7. Close the **Local Security Policy** window.
8. Close the Win-Agent VM browser tab.

Verify the Windows Agent Status

Once an agent is installed, it appears in the CMDB. The **Agent Status** column may display various states initially, depending on whether a matching template is predefined or not. Now, you will verify the status of the Windows agent on FortiSIEM.

To verify the Windows agent status on CMDB

1. Return to the FortiSIEM management GUI, and click **CMDB**.
2. In the **Orgs without collector** drop-down list, select **Aviation**.



3. Click **Windows**.



The **Win_Agent** agent is displayed.

CMDB > Devices > Server > Windows									
New	Edit	Delete	Aviation ▾	Discovered by All ▾	⚙️ Action ▾ 📄 🔄 ⏮️ ⏪ 1/1 1 ⏩ ⏭️				
▲ Name	IP	Type	Status	Discovered	Method	Organization	Agent Policy	Agent Status	Monitor
Win_Agent	10.0.3.10	Microsoft Windows Server 2016 Standa...	Unmanaged	Mar 24 2020, 03:37:47 PM	AGENT	Aviation		Registered	

Notice that the **Method** used to discover the **Win_Agent** is listed as **AGENT**. The **Agent Status** is **Registered**, which means the agent has successfully registered but has not received a monitoring template. Therefore, at this point, a Windows agent license is not used and the **Status** of the device is **Unmanaged**.

4. Log out of the Supervisor FortiSIEM management GUI.

Exercise 2: Assigning Templates to Windows Agents

In this exercise, you will assign a template to the Windows agent.

Create a Windows Agent Monitor Template

Monitor templates define what type of logs the agent will monitor and upload, such as security event logs, system event logs, DNS logs, DHCP logs, custom application logs, file integrity monitoring logs, and so on.

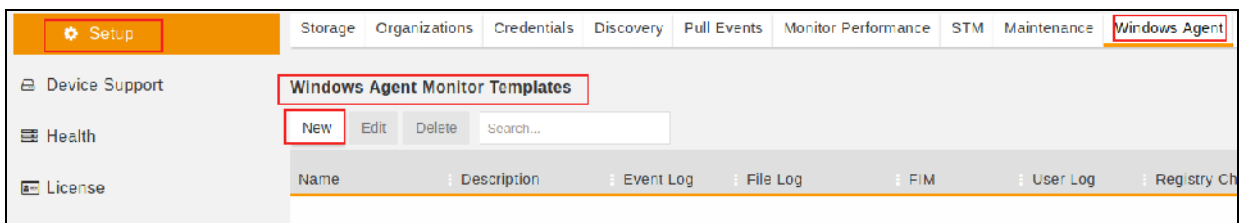
You will configure a security monitoring template for the Windows server.

To create a Windows agent monitor template

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

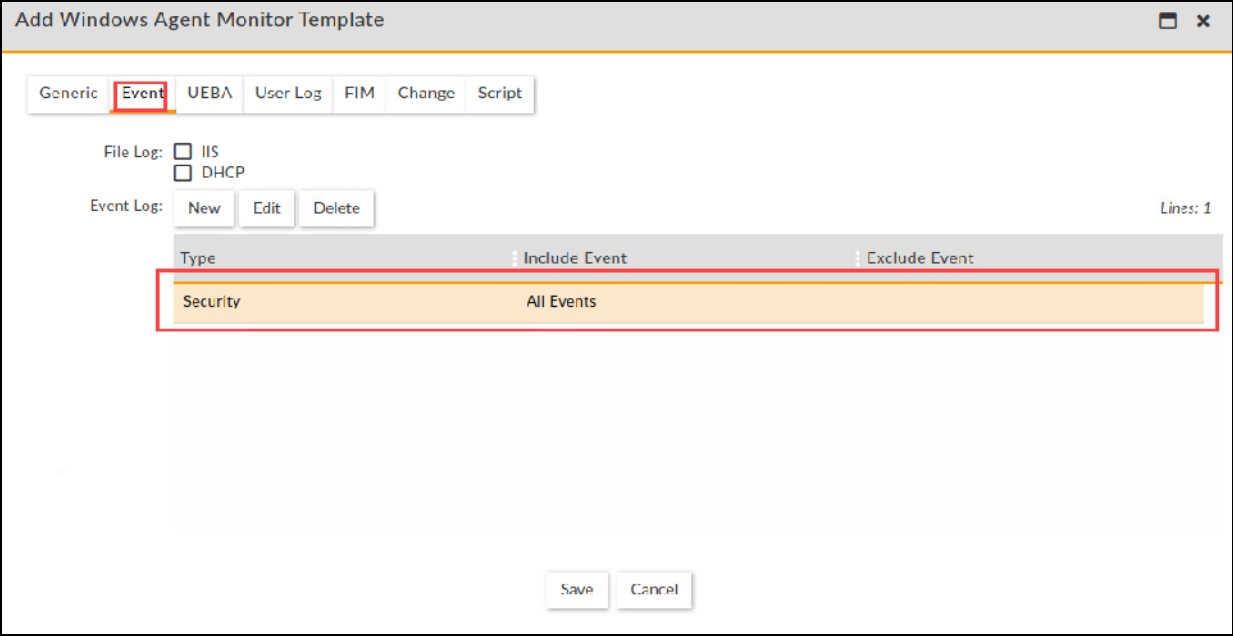
Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **ADMIN**.
5. In the left navigation pane, click **Setup**, then click **Windows Agent**.
6. In the **Windows Agent Monitor Templates** section, click **New**.



7. In the **Name** field, type `Security_Template`.
8. Click **Event**.
9. Click **New**.
10. In the **Type** drop-down list, select **Security**.
11. Click **Save**.

Your configuration should match the following example:



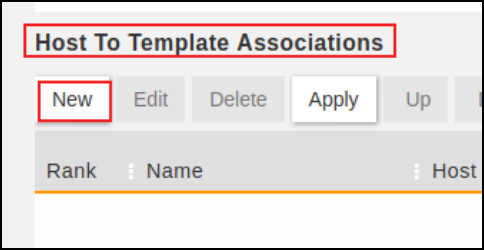
12. Click **Save**.

Associate a Host to a Template

After defining the monitoring templates, you must associate hosts to templates. You will be mapping organizations and hosts to templates and collectors.

To associate a host to a template

- 1. Continuing on the **Windows Agent** tab, in the **Host To Template Associations** section, click **New**.



- 2. Configure the following settings:

Field	Value
Name	Template_Server_2016
Organization	Aviation
Template	Security_Template
Collector	collector2

Your configuration should match the following example:

The screenshot shows the 'Host To Template Associations' dialog box. The 'Name' field is 'Template_Server_2016'. The 'Organization' section has a search bar and a list with 'Aviation' selected. The 'Host' dropdown is set to 'ANY'. The 'Template' section has a search bar and a list with 'Security_Template' selected. The 'Virtual Collectors' section has a search bar and a list with 'collector2' selected. The 'Collector' section has a search bar and a list with 'collector2' selected. The 'Save' and 'Cancel' buttons are at the bottom.

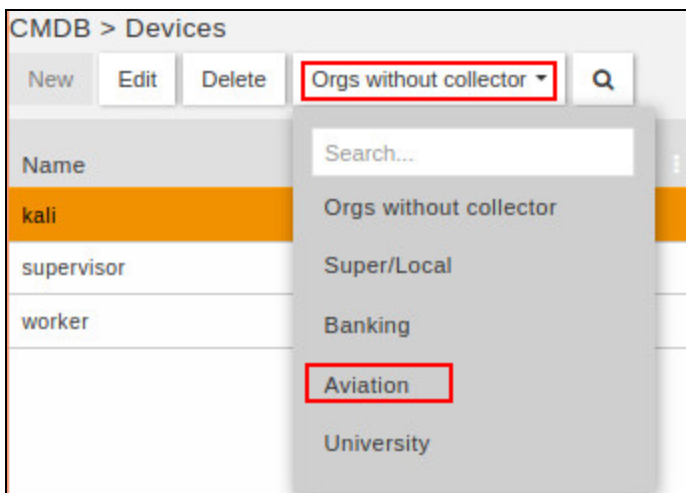
3. Click **Save**.

Verify the Agent Status

Now, you will verify the agent status after the template has been associated with it.

To verify the agent status

1. Continuing on the FortiSIEM management GUI, click **CMDB**.
2. In the **Orgs without collector** drop-down list, select **Aviation**.



3. Click **Windows**.

0	1	1	1	0	0	0
Routers	Firewalls	Windows	Unix	ESX	AWS	Azure

4. Click the refresh icon (🔄).

It will take a few minutes for the **Agent Status** column to change to **Running Active**.

Name	IP	Type	Status	Discovered	Method	Organization	Agent Policy	Agent Status	Monit
Win_Agent	10.0.3.10	Microsoft Windows Server 2...	Pending	Mar 24 2020, 03:37:47 PM	AGENT	Aviation	Template_Server_2016	Running Active	



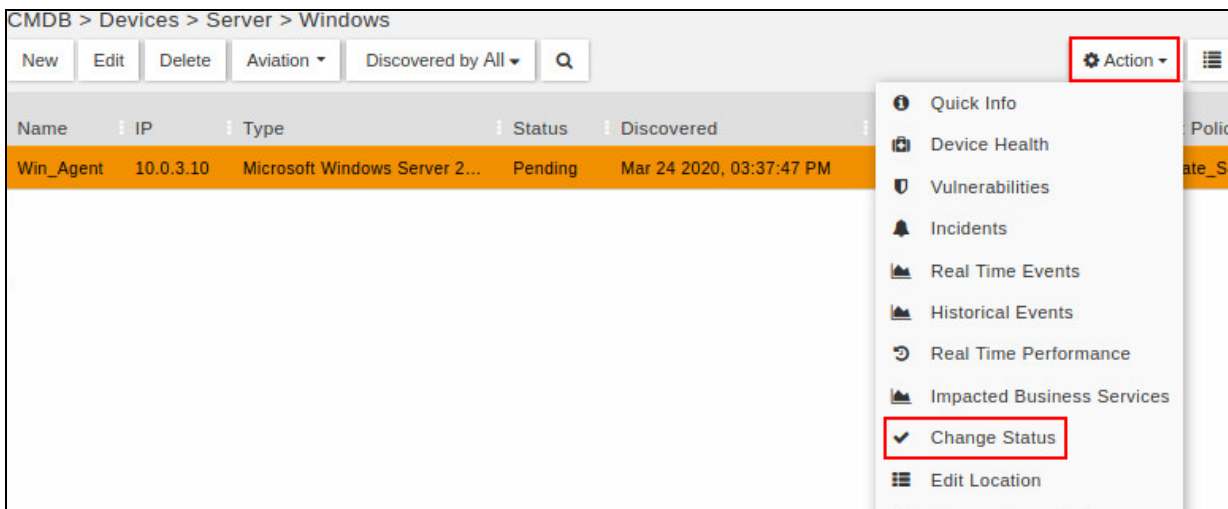
If for some reason the **Agent Status** changes to **Disconnected**, restart the Windows agent service on the Win-Agent VM.

Approve the Windows Agent

Now, you will approve the Windows agent. Monitoring of the agent begins automatically, and incidents for those devices will trigger automatically based on the rules associated with those devices.

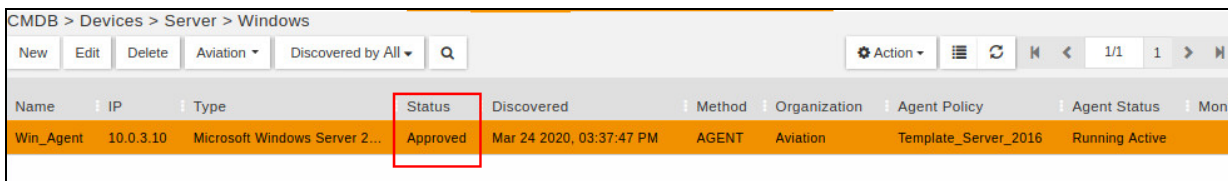
To approve the Windows agent

1. Continuing on the **CMDB** tab, select **Win_Agent**, and in the **Action** drop-down list, select **Change Status**.



2. Verify that the **Change Status to** setting is set to **Approved**, and then click **OK**.

Your configuration should match the following example:



3. Log out of the Supervisor FortiSIEM management GUI.

Exercise 3: Discovering LDAP Users

In this exercise, you will discover LDAP users and groups from FortiSIEM, which are preconfigured on the Windows Server.

Discover LDAP Users and Groups

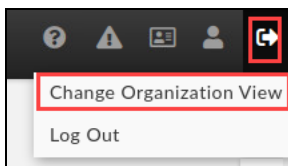
To add users to the FortiSIEM deployment from an Active Directory server over LDAP, you must first add the login credentials for your server and associate them to an IP range, and then run the discovery process on the Active Directory server. When the server is discovered successfully, all users in that directory will be added to your deployment.

To add credentials for LDAP

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click the **Change Organization View** icon, and in the drop-down list, select **Change Organization View**.



5. Select **Switch to Organization**, and in the drop-down list, select **Aviation**.
6. Click **Change View**.
7. Click **ADMIN**.
8. In the left navigation pane, click **Setup**, then click **Credentials**.
9. In the **Step 1: Enter Credentials** section, click **New**.
10. Enter the following values:

Field	Value
Name	LDAP Server

Field	Value
Device Type	Microsoft Windows Server 2016
Access Protocol	LDAP
Used For	Microsoft Active Directory
Server Port	389
Base DN	DC=Aviation,DC=lab
Password config	Manual
User Name	CN=Administrator,CN=Users,DC=Aviation,DC=lab
Password	Fortinet1!
Confirm Password	Fortinet1!

11. Click **Save**.
12. In the **Step 2: Enter IP Range to Credential Associations** section, click **New**.
13. Enter the following values:

Field	Value
IP/Host Name	10.0.3.10
Credentials	LDAP Server

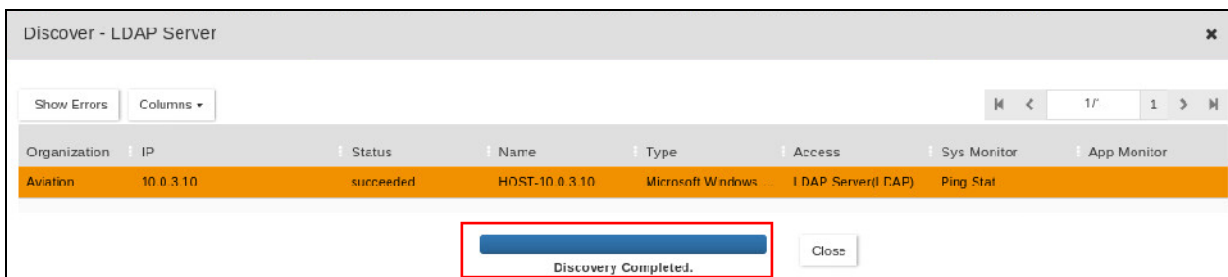
14. Click **Save**.

To discover LDAP users

1. Continuing on the **Setup** page, click **Discovery**.
2. Click **New**.
3. Enter the following values:

Field	Value
Name	LDAP Server
Discovery Type	Range Scan
Include	10.0.3.10
Name Resolution	SNMP/WMI first

4. Click **Save**.
5. Select **LDAP Server**, and then click **Discover**.
Wait for the discovery to complete.



- Click **Close**.

Review LDAP Users on FortiSIEM

Now, you will review the discovered LDAP users on FortiSIEM.

To review LDAP users

- Continuing on the FortiSIEM management GUI, click **CMDB**.
- Click **Users > DC=Aviation,DC=lab > OU=VPN Users,DC=aviation,DC=lab**.

The four users who are members of the VPN user group are displayed.

CMDB > Users > DC=Aviation,DC=lab > OU=VPN Users,DC=aviation,DC=lab						
New	Edit	Delete	Discovered by All	Search...	Action	
User Name	Full Name	System Role	Job Title	Work Phone	Mobile Phone	Email
Sarah	Sarah Smith			9874562165		sarah@aviation.lab
ben	Ben Jacobs			613258963		ben@aviation.lab
mike	Mike Jones			6132232654		mike@aviation.lab
tracey	Tracey Miller			2897564567		tracey@aviation.lab

- Select **Sarah**, and then click the arrow icon to review the **Summary**.

User Name	Full Name	System Role	Job Title	Work Phone	Mobile Phone	Email
Sarah	Sarah Smith			9874562165		sarah@aviation.lab
ben	Ben Jacobs			613258963		ben@aviation.lab
mike	Mike Jones			6132232654		mike@aviation.lab
tracey	Tracey Miller			2897564567		tracey@aviation.lab

You will notice that Sarah is a member of both the **VPN Users** and **Domain Admins** groups, unlike other users who are members of the **VPN Users** group only.

Summary

Contact

Member Of

☐ Auto expand

General

User Name: Sarah

Full Name: Sarah Smith

Job Title:

Company:

Employee ID:

Manager:

Domain: aviation.lab

Description:

Last Domain Logon: N/A

Advanced

Domain Password Last Set: Feb 19 20...

Domain Password Age: 34 days

Domain Account Control: Account E...

System Administrator: false

System Role:

Password Reset: N/A

Session Timeout: N/A

User Lockout: 15 minutes

Summary	Contact	Member Of	☐ Auto expand
Member of 3 Groups			
Group #1: CN=Domain Admins,CN=Users,DC=aviation,DC=lab			
Group #2: CN=VPN Users,OU=VPN Users,DC=aviation,DC=lab			
Group #3: OU=VPN Users,DC=aviation,DC=lab			

4. Log out of the Supervisor FortiSIEM management GUI.

Exercise 4: Adding a Linux Agent to an Organization

In this exercise, you will add a Linux agent to the banking organization.

Configure Linux Agent Registration Credentials

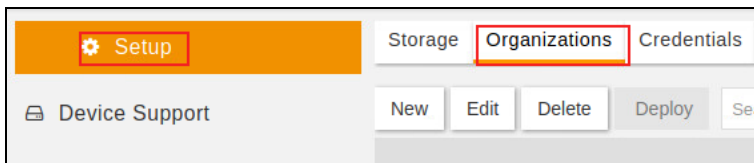
Before you register a Linux agent, you must define the administrator credentials for the organization through which the Linux agent will be managed.

To configure Linux agent registration credentials

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **ADMIN**.
5. In the left navigation pane, click **Setup**, and then click **Organizations**.



6. Select **Banking**, and then click **Edit**.
7. Enter the following values:

Field	Value
Agent User	admin
Agent Password	Password1!
Confirm Agent Password	Password1!

8. Click **Save**.
Note the banking organization ID. You will need this ID during the agent registration process.

Register the Linux Agent

To install a Linux agent, you must download the shell script for the Linux agent installer from the Fortinet Support site. For this lab, the installer is already downloaded.

The install script needs execute permissions and you must install it as a root user. You will specify parameters, such as supervisor IP address, organization ID, organization name, agent username, and agent password, before executing the script.

To register the Linux agent to a supervisor

1. Go to the Linux-Agent VM.
2. Open a terminal window (Ctrl + Alt + T).
3. Type the following command to change your working directory:

```
cd Desktop/Resource/FSM_LinuxAgent
```

4. Type `ls`, and verify that the `linux_agent.sh` file exists.

5. Type the following command to start the installer:

```
sudo ./linux_agent.sh
```

6. Type the password `password`.

The install options and install script syntax are displayed.

```
student@Linux_Agent:~/Desktop/Resource/FSM_LinuxAgent$ sudo ./linux_agent.sh
[sudo] password for student:
cat: /etc/system-release: No such file or directory

Please check the Below options you have passed to ./linux_agent.sh.

./linux_agent.sh -s <Supervisor-IP> -i <Organization-Id> -o <Organization-Name>
-u <Agent-User> -p <Agent-Password>

OPTIONS:
  -h      Show this message
  -s      Super IP/HostName
  -i      Organization Id
  -p      Agent Registration Password
  -u      Agent Registration User
  -o      Organization
  -v      Verify Super and Collector SSL Certificate during TLS handshake <Optional>
  -c      CA Certificate bundle file <Optional>
  -n      Hostname where agent is installed <Optional>
```

7. Type the following command to start the installation. Replace `<Organization-Id>` with the organization ID you noted earlier:

```
sudo ./linux_agent.sh -s 10.0.1.130 -i <Organization-Id> -o Banking -u admin -p
Password1!
```

An **INSTALLATION SUCCESS** message is displayed:

```
Mar 24 15:15:10 Linux_Agent systemd[1]: fortisiem-linux-agent.service: Ignoring
invalid environment assignment 'umask 0022; export PATH=/opt/fortinet/fortisiem/
linux-agent/bin:/sbin:/usr/sbin:$PATH': /opt/fortinet/fortisiem/linux-agent/bin/
fortisiem-linux-agent_env
Mar 24 15:15:10 Linux_Agent systemd[1]: Started FortiSIEM Linux Agent daemon.
INSTALLATION SUCCESS
INSTALL PATH:/opt/fortinet/fortisiem/linux-agent
```

8. Type the following command to check the agent service status:

```
systemctl status fortisiem-linux-agent.service
```

```
student@Linux_Agent:~/Desktop/Resource/FSM_LinuxAgent$ systemctl status fortisiem-linux-agent.service
● fortisiem-linux-agent.service - FortiSIEM Linux Agent daemon
   Loaded: loaded (/etc/systemd/system/fortisiem-linux-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-03-24 15:15:10 PDT; 4min 48s ago
     Main PID: 5589 (sh)
       Tasks: 9 (limit: 2311)
      CGroup: /system.slice/fortisiem-linux-agent.service
              └─5589 /bin/sh -c /opt/fortinet/fortisiem/linux-agent/bin/phLinuxAgent >> /opt/fortinet/fortis
                └─5591 /opt/fortinet/fortisiem/linux-agent/bin/phLinuxAgent
```

9. Press Ctrl + C, and then type the following command to change your working directory:

```
cd /opt/fortinet/fortisiem/linux-agent/bin
```

10. Enter ls, and verify that your directory listing matches the following example:

```
student@Linux_Agent:/opt/fortinet/fortisiem/linux-agent/bin$ ls
checkAgentRequirement.sh      fortisiem-linux-agent-stop.sh      signs.csv
fortisiem-linux-agent_env     fortisiem-linux-agent-uninstall.sh  VERSION
fortisiem-linux-agent-start.sh phLinuxAgent
```

There are several files for different purposes, such as starting the agent, stopping the agent, uninstalling the agent, checking the version number of the agent, and so on.

11. Close the terminal window.
12. Close the Linux-Agent VM browser tab.

Verify the Linux Agent Status

Now, you will verify the status of the Linux agent on FortiSIEM.

Once an agent is installed, it appears in the CMDB. The **Agent Status** column may display various states initially, depending on whether a matching template is predefined or not.

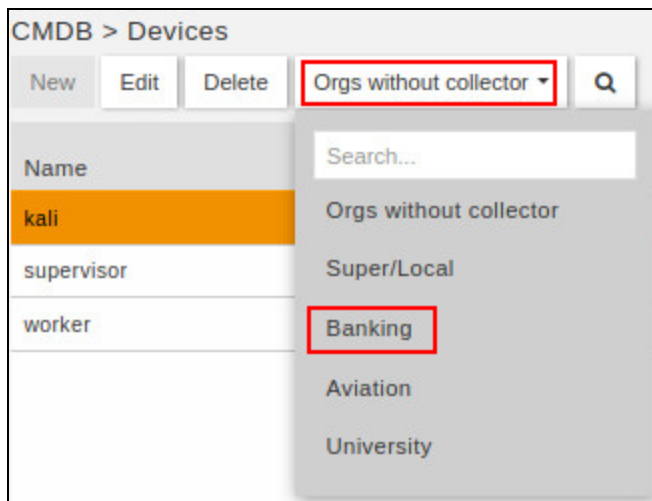
To verify the Linux agent status on CMDB

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!

Field	Value
Cust/Org Id	super
Domain	LOCAL

- Click **LOG IN**.
- Click **CMDB**.
- In the **Orgs without collector** drop-down list, select **Banking**.



- Click **Unix**.



The **Linux_Agent** agent is displayed.

							0	1	0	1	0	0	0
							Routers	Firewalls	Windows	Unix	ESX	AWS	Azure
CMDB > Devices													
New		Edit	Delete	Banking	Discovered by All								
Name	IP	Device Type		Status	Discovered	Method	Organization	Agent Status					
FGT_Banking	10.0.2.254	Fortinet FortiOS		Approved	Jul 22 2021, 01:05:11 PM	SSH, SNMP, PING	Banking						
Linux_Agent	10.0.2.10	Ubuntu Linux 18.04.4 LTS		Unmanaged	Jul 22 2021, 03:32:45 PM	AGENT	Banking	Registered					

Notice that the **Method** that **Linux_Agent** was discovered is **AGENT**. The **Agent Status** is **Registered**, which means the agent has successfully registered but has not received a monitoring template. Therefore, at this point, a Linux agent license is not used and the device **Status** shows **Unmanaged**.

- Log out of the Supervisor FortiSIEM management GUI.

Exercise 5: Assigning Templates to Linux Agents

In this exercise, you will assign a template to the Linux agent.

Create Linux Agent Monitor Templates

Linux templates define the type of logs the agent will monitor and upload, such as security event logs, system event logs, DNS logs, DHCP logs, custom application logs, file integrity monitoring logs, and so on.

To create a Linux agent monitor template

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL



You must be logged in to the FortiSIEM from the Local-Host VM.

3. Click **LOG IN**.
4. Click **ADMIN**.
5. In the left navigation pane, click **Setup**, and then click **Linux Agent**.
6. In the **Linux Agent Monitor Templates** section, click **New**.
7. In the **Name** field, type `FIM_Template`.
8. In the **Description** field, type `File Integrity and Monitoring`.
9. Click the **FIM** tab.
10. Click **New**.
11. In the **Include File/Directory** field, type `/home/student/Desktop/Resources`.
12. In the **Actions** section, select **Modify** and **Delete**.
13. On Modify select **Push Files** and **Compare Baseline**.
14. For compare baseline browse to the **Resource** folder on the Local-Host Desktop.
15. Open **lab4** folder.
16. Select **hello_world**.
17. Click **Open**.

Edit Linux Agent Monitor Template

Generic Syslog Log File **FIM** Process Monitoring

Include File/Directory: /home/student/Desktop/Resources

Exclude File/Directory: using ';' to separate multiple exclude

Actions: ☐ All ☐ Open ☐ Close ☐ Create ☒ Modify ☒ Delete ☐ Attribute Change

On Modify: ☒ Push Files ☒ Compare Baseline

Browse... hello_world
File Name: hello_world
File Hash: 8DDD8BE4B179A529AFA5F2FFAE4B9858

Save Cancel

18. Click **Save**.

19. Click **Save**.

Associate a Host to a Template

After you define the monitoring templates, you must associate hosts to that template. You will map organizations and hosts to templates and collectors.

To associate a host to a template

1. Continuing on the **Linux Agent** tab, in the **Host To Template Associations** section, click **New**.
2. Enter the following values:

Field	Value
Name	Template_Server_Linux
Organization	Banking
Template	FIM_Template
Collector	collector1

3. Click **Save**.

Verify the Agent Status

Now, you will verify the agent status after the template has been associated with it.

To verify the agent status

1. Continuing on the FortiSIEM management GUI, click **CMDB**.
2. In the **Orgs without collector** drop-down list, select **Banking**.
3. Click **Unix**.
4. Click the refresh icon (🔄) in the top left corner.

It will take a few minutes for the **Agent Status** column to change to **Running Active**.

0101000

RoutersFirewallsWindowsUnixESXAWSAzure

CMDB > Devices > Server > Unix

NewEditDeleteBankingDiscovered by All

Actions

1/1

Name	IP	Device Type	Status	Discovered	Method	Organization	Agent Policy	Agent Status
Linux_Agent	10.0.2.10	Ubuntu Linux 18.04.4 LTS	Pending	Jul 22 2021, 03:32:45 PM	AGENT	Banking	Template_Server_...	Running Active

Approve the Linux Agent

Now, you will approve the Linux agent. Monitoring of the agent begins automatically, and incidents for those devices will trigger automatically based on the rules associated with those devices.

To approve the Linux agent

1. Continuing on the **CMDB** tab, select **Linux_Agent**, and then in the **Action** drop-down list, select **Change Status**.
2. Verify that the **Change Status to** setting is set to **Approved**, and click **OK**.

Your configuration should match the following example:

0

Routers

1

Firewalls

0

Windows

1

Unix

0

ESX

0

AWS

0

Azure

CMDB > Devices > Server > Unix

New

Edit

Delete

Banking ▾

Discovered by All ▾

Q

⚙️ Actions ▾

📄

🔄

🏠

⏪

1/1

Name	IP	Device Type	Status	Discovered	Method	Organization	Agent Policy	Agent Status
Linux_Agent	10.0.2.10	Ubuntu Linux 18.04.4 LTS	Approved	Jul 22 2021, 03:32:45 PM	AGENT	Banking	Template_Server_...	Running Active

3. Log out of the Supervisor FortiSIEM management GUI.

Lab 5: Discover Rules

In this lab, you will learn the basics of FortiSIEM rules. You will analyze logs from FortiGate, and filter logs that you want to analyze.

Objectives

- Filter events from FortiGate on FortiSIEM
- Group events with similar attributes
- Apply aggregate conditions to events

Time to Complete

Estimated: 30 minutes

Exercise 1: Analyzing Allowed Traffic

In this exercise, you will generate HTTPS traffic on FortiGate and analyze the events on FortiSIEM.

Log All Sessions on FortiGate

In this task, you will enable all session logging on FGT_Aviation. By enabling this setting, FortiGate will create a log entry for every session that matches the policy. These logs are forwarded to the supervisor node by the collector. You will also generate some HTTPS traffic to generate traffic logs on FGT_Aviation.

To log all sessions on FGT_Aviation

1. Go to the FGT_Aviation FortiGate management GUI.
2. Log in with the username `admin` and password `password`.
3. Click **Policy & Objects > IPv4 Policy**.
4. Expand the **port2→port1** section.
5. Select the **Lan to Wan** policy, and then click **Edit**.
6. In the **Log Allowed Traffic** section, click **All Sessions**.
7. Click **OK**.
8. Close the FGT_Aviation FortiGate browser tab.

To generate HTTPS traffic

1. Go to the Win-Agent VM.
2. Open the Google Chrome browser, and then navigate to `https://www.fortinet.com`.
3. Close the Win-Agent VM browser tab.

Analyze Traffic Events on FortiSIEM

Now, you can view the traffic logs generated by FortiGate on FortiSIEM. You will run a historical search for events related to FortiGate allowed traffic.

After that, you will analyze the events and understand the log enrichment performed by FortiSIEM.

To filter allowed traffic events

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin

Field	Value
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

- Click **LOG IN**.
- Click **ANALYTICS**.
- Click the **Edit Filters and Time Range** field.
- In the **Filter** section, select **Event Attribute**.
- Enter the following values. Click the add icon (+) to add new rows.

Attribute	Operator	Value	Next
Reporting IP	=	10.0.3.254	AND
Event Type	=	FortiGate-traffic-allowed	AND
Destination TCP/UDP Port	=	443	AND

- In the **Time** section, select **Relative**, and set it to **2 Hours**.
Your filter setup should match the following example:

Reporting IP = 10.0.3.254 AND Event Type = FortiGate-traffic-allowed AND Destination TCP, [Add] [List] [Run]

Filter [Load] [Save] [Clear All]

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
[+]	Reporting IP	=	10.0.3.254	[+]	AND	[+]
[+]	Event Type	=	FortiGate-traffic-allowed	[+]	AND	[+]
[+]	Destination TCP/UDP Port	=	443	[+]	AND	[+]

☐ CMDB Attribute

Time Range

☐ Real-time

☒ Relative Last 2 Hours

☐ Absolute

Trend Interval: Auto

[Apply & Run] [Apply] [Cancel]

- Click **Apply & Run**.

To analyze the allowed traffic events

- Continuing on the **ANALYTICS** page, select any of the displayed events, and then click the arrow icon (→) in the **Raw Event Log** column.

The **Event Details** pop-up opens.

2. Scroll down and select the **Display** settings for **Organization ID** and **Organization Name**.

Event Details

```
<189>date=2020-03-25 time=08:40:23 devname="FGT3" devid="FGVM01TM19007953"
logid="0000000020" type="traffic" subtype="forward" level="notice" vd="root"
eventtime=1585150823870583321 tz="-0700" srcip=10.0.3.10 srcport=58046
srcintf="port2" srcintfrole="undefined" dstip=13.35.118.3 dstport=443 dstintf="port1"
dstintfrole="undefined" poluuid="dc833b94-531d-51ea-fcf4-a49eb61c3a02"
sessionid=52032 proto=6 action="accept" policyid=2 policytype="policy"
service="HTTPS" dstcountry="United States" srccountry="Reserved"trandisn="snat"
```

Search...

Lines: 60

Display	Filter	Item	Value
☐	☐	Member ID	0000000020
☐	☐	NAT Type	snat
☒	☐	Organization ID	2001
☒	☐	Organization Name	Aviation
☐	☐	Post-NAT Source IP	100.64.4.253
☐	☐	Post-NAT Source Port	58046

This adds the **Organization ID** and **Organization Name** columns to the event results.

3. Click **OK**.
4. Click **Run** again.

Reporting IP = 10.0.3.254 AND Event Type = Fortigate-traffic-allowed AND Destination TC

Q

Run

5. Click **Show Event Type**.

This will add an additional **Event Type** column to the event results.

☒ Show Event Type
 ☐ Wrap Raw Event

1/26

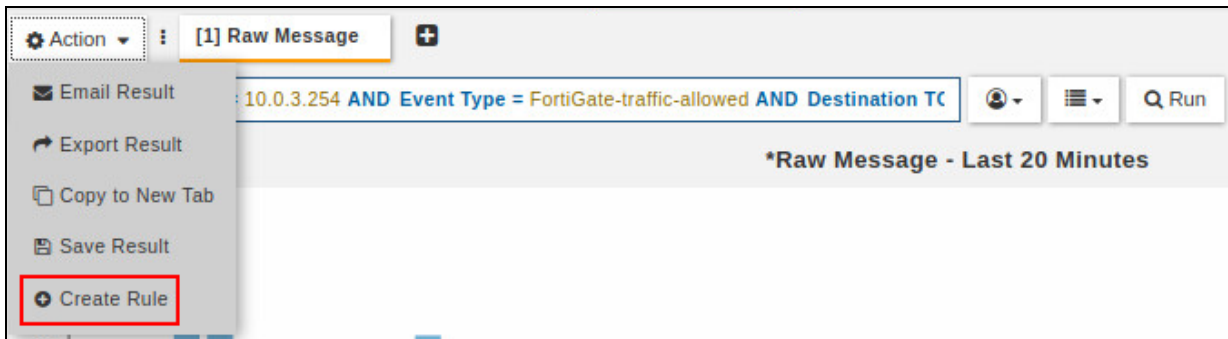
Event Receive Time	Reporting IP	Event Type	Event Name	Raw Event Log	Organization ID	Organization
Mar 25 2020, 11:48:00 AM	10.0.3.254	FortiGate-traffic-allowed	Permitted traffic	<189>date=2020-03-25 time=08:48:00 devname="FGT3" devid="TCVM01TM19007953"	2001	Aviation
Mar 25 2020, 11:48:00 AM	10.0.3.254	FortiGate-traffic-allowed	Permitted traffic	<189>date=2020-03-25 time=08:48:00 devname="FGT3" devid="TCVM01TM19007953"	2001	Aviation
Mar 25 2020, 11:47:39 AM	10.0.3.254	FortiGate-traffic-allowed	Permitted traffic	<189>date=2020-03-25 time=08:47:39 devname="FGT3" devid="FGVM01TM19007953"	2001	Aviation
Mar 25 2020, 11:47:07 AM	10.0.3.254	FortiGate-traffic-allowed	Permitted traffic	<189>date=2020-03-25 time=08:47:07 devname="FGT3" devid="FGVM01TM19007953"	2001	Aviation
Mar 25 2020, 11:47:00 AM	10.0.3.254	FortiGate-traffic-allowed	Permitted traffic	<189>date=2020-03-25 time=08:46:59 devname="FGT3" devid="FGVM01TM19007953"	2001	Aviation
Mar 25 2020, 11:46:09 AM	10.0.3.254	FortiGate-traffic-allowed	Permitted traffic	<189>date=2020-03-25 time=08:46:09 devname="FGT3" devid="FGVM01TM19007953"	2001	Aviation

Create a Rule From an Analytics Search

You can create a rule from the **ANALYTICS** tab, based on the filtered search criteria. Now, you will create a new rule without activating it. This is to save resources in the lab.

To create a rule from an analytics search

- Continuing on the **ANALYTICS** page, in the **Action** drop-down list, select **Create Rule**.



- In the **Rule Name** field, type `Excess HTTPS traffic`.
- Click **Step 2: Define Condition**.
- Change the time window to `120 seconds`.
- Click the pencil icon (✎) to edit the **Filter_1** subpattern.
- In the **Aggregate** section, change the **Value** setting to `100`.
- In the **Group By** section, configure the following values. Click the add icon (+) to add the following new rows:
 - Reporting IP**
 - Source IP**
 - Destination TCP/UDP Port**

Your configuration should match the following example:

Edit SubPattern

Name: Filter_1

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	Reporting IP	=	10.0.3.254	+	AND	+
	+	Event Type	=	FortiGate-traffic-allowed	+	AND	+
	+	Destination TCP/UDP Port	=	443	+	AND	+

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	COUNT(Matched Events)	>=	100	+		+

Group By:	Attribute	Row	Move
	Reporting IP	+	+
	Source IP	+	+
	Destination TCP/UDP Port	+	+

To configure **Aggregate** functions use the **Expression Builder**, available when you click on **Attribute** field for the **Aggregate** section.

1. Select **Function** from the drop-down list
2. Add **Function** to the expression
3. Select the **Event Attribute**
4. Add the **Event Attribute** to the expression
5. Click **Validate** and ensure the expression is valid
6. Finally click **OK** when the expression is ready



8. Click **Save**.
9. Click **Step 3: Define Action**.
10. In the **Severity** drop-down list, select **5 - MEDIUM**.
11. In the **Category** drop-down list, select **Security**.
12. In the **Subcategory** drop-down list, select **Impact**.
13. In the **Action** section, click the pencil icon (✎) to edit it.
14. In the **Incident Attributes** section, configure the following values:

Event Attribute	Subpattern	Filter Attribute
Source IP	Filter_1	Source IP

15. Click **Save**.
16. Click **OK**.
17. Click **RESOURCES**.
18. In the left navigation pane, click **Rules > Ungrouped**.

The **Excess HTTPS traffic** rule is displayed.

You will not be triggering any incidents for this rule. This exercise is to demonstrate the ability to create rules from the **ANALYTICS** search tab.

If you activate this rule, it will trigger incidents for hosts that have more than 100 sessions within a two minute window.



Do not activate this rule because it could consume excessive resources in the lab environment. Because the lab environment contains many devices, each device has been configured to run on minimum resources.

19. Log out of the Supervisor FortiSIEM management GUI.

Exercise 2: Monitoring Firewall Sessions

In this exercise, you will calculate the average firewall sessions from FGT2.

Build an Analytics Search

The FortiSIEM search functionality includes both real-time and historical search options of the information that is collected. With real-time search, you can see events as they happen, while historical search is based on information stored in the event database. Both types of searches include simple keyword searching, as well as structured searches that let you search based on specific event attributes and values, and then group the results by attributes.

To build an analytics search for firewall sessions

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **ANALYTICS**.
5. Click the **Edit Filters and Time Range** field.

If the attributes from the previous exercise appear in the field, click **Clear All**.

Reporting IP = 10.0.3.254 AND Event Type = Fortigate-traffic-allowed AND Destination TC

 Run

Filter

Saved Filters ...

Clear All

6. In the **Filter** section, select **Attribute**.
7. Enter the following values. Click the add icon (+) to add new rows.

Attribute	Operator	Value	Next
Reporting IP	=	10.0.2.254	AND

Attribute	Operator	Value	Next
Event Type	=	Select from CMDB	AND
		Search for PH_DEV_MON_FW_CONN_UTIL	
		Click the add item icon (➤) to select it.	

8. In the **Time** section, select **Relative**, and set it to **20 Minutes**.

Your filter setup should match the following example:

Filter Saved Filters ... Clear All

☐ Keyword

☒ Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Reporting IP	=	10.0.2.254	⊕ ⊖	AND	⊕ ⊖
⊕ ⊖	Event Type	=	PH_DEV_MON_FW_CONN_UTIL	⊕ ⊖	AND	⊕ ⊖

Time

☐ Real Time

☒ Relative Last 20 Minutes

☐ Absolute

9. Click **Apply & Run**.

All events related to firewall sessions from FGT_Banking are displayed.

☐ Show Event Type ☐ Wrap Row Event

Event: Receive Time	Reporting IP	Event: Name	Raw Event Log
Mar 25 2020, 02:45:45 PM	10.0.2.254	Firewall connection count stats for a device	[PH_DEV_MON_FW_CONN_UTIL][event:Severity]=PHL_INFO[fileName]=phPerfJob.cpp[lineNumber]=11848[hostNa...
Mar 25 2020, 02:42:49 PM	10.0.2.254	Firewall connection count stats for a device	[PH_DEV_MON_FW_CONN_UTIL][event:Severity]=PHL_INFO[fileName]=phPerfJob.cpp[lineNumber]=11848[hostNa...
Mar 25 2020, 02:39:53 PM	10.0.2.254	Firewall connection count stats for a device	[PH_DEV_MON_FW_CONN_UTIL][event:Severity]=PHL_INFO[fileName]=phPerfJob.cpp[lineNumber]=11848[hostNa...
Mar 25 2020, 02:36:57 PM	10.0.2.254	Firewall connection count stats for a device	[PH_DEV_MON_FW_CONN_UTIL][event:Severity]=PHL_INFO[fileName]=phPerfJob.cpp[lineNumber]=11848[hostNa...
Mar 25 2020, 02:34:00 PM	10.0.2.254	Firewall connection count stats for a device	[PH_DEV_MON_FW_CONN_UTIL][event:Severity]=PHL_INFO[fileName]=phPerfJob.cpp[lineNumber]=11848[hostNa...
Mar 25 2020, 02:31:04 PM	10.0.2.254	Firewall connection count stats for a device	[PH_DEV_MON_FW_CONN_UTIL][event:Severity]=PHL_INFO[fileName]=phPerfJob.cpp[lineNumber]=11848[hostNa...



If you don't see any events, check the FortiSIEM alerts (⚠) located in the top-right corner of the page. If there is a clock drift issue with a collector, open an SSH connection, and reboot the collector with the following command:

```
reboot -h now
```

Display the Average Firewall Session

Now, you will display only the average value for the firewall sessions.

To display the average firewall session

1. Continuing on the FortiSIEM management GUI, click the **Change Display Fields** icon (⚙️).
2. Click the add icon (+) to add a new row.

Attribute	Order	Display As	Row	Move
Event Receive Time	DESC		+	⬆️ ⬇️
Reporting IP			+	⬆️ ⬇️
Event Type			+	⬆️ ⬇️
Raw Event Log			+	⬆️ ⬇️

3. Click the empty **Attribute** field in the new row, and then select **Expression Builder**.

Attribute	Order	D
Event Receive Time	DESC	
Reporting IP		
Event Type		
Raw Event Log		
Type in attribute...		

4. In the **Expression** field, type `AVG(Firewall Session)`.
5. Click **Validate**.
A pop-up is displayed indicating that the expression is valid.

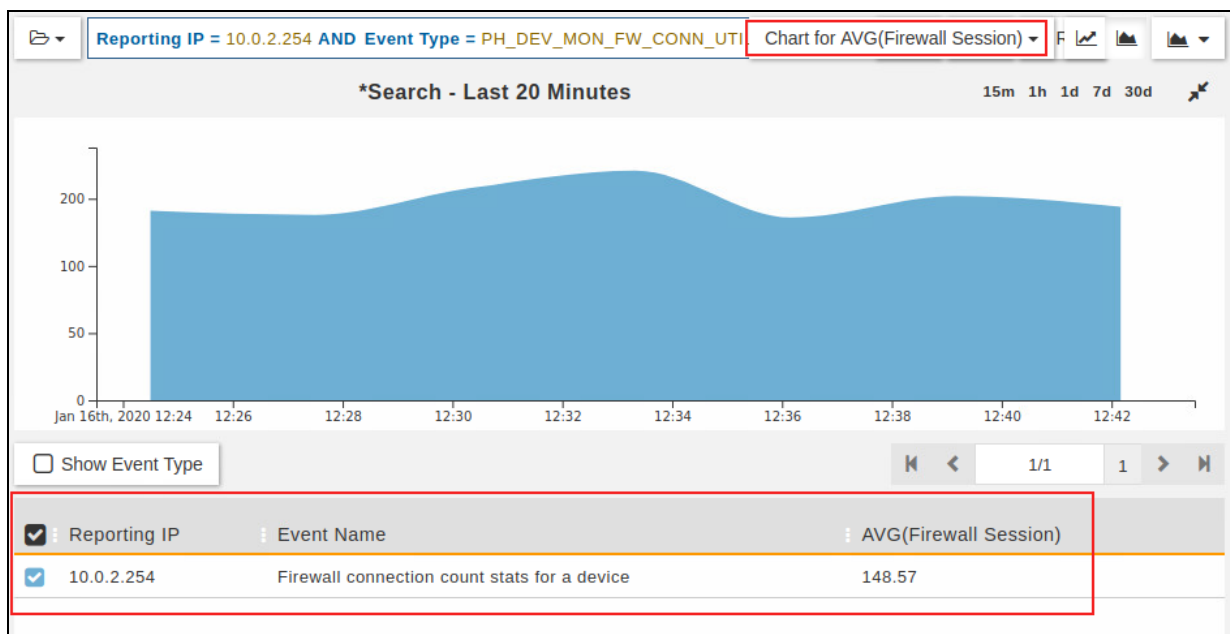
Expression is valid.

6. Close the pop-up message.
7. Click **OK**.
8. Click the remove icon (⊖) to delete the following rows:
 - **Raw Event Log**
 - **Event Receive Time**

These are unique attributes and cannot be considered for grouping events with similar attributes, and performing aggregate calculations.

9. Click **Apply & Run**.

The average firewall session count is displayed.



Note the display columns for **Reporting IP**, **Event Name**, and **AVG(Firewall Session)**. The average function calculates the average firewall session from all events related to firewall connection for the past 20 minutes.

10. Log out of the Supervisor FortiSIEM management GUI.

Lab 6: Configuration of Single Pattern Security Rules

In this lab, you will learn about single subpattern security rules. You will review some of the out-of-box rules, and create your own rules. You will also learn about the event filters, group by conditions, and aggregation conditions, that are required in a single subpattern rule.

Objectives

- Identify a single subpattern security rule
- Review a subpattern in a rule
- Understand out-of-the-box rules
- Define conditions in a rule
- Define actions for a rule
- Understand incident generation
- Review incident attributes
- Determine incident source and target

Time to Complete

Estimated: 30 minutes

Exercise 1: Detecting Remote Desktop Access

In this exercise, you will review the out-of-the-box rule which detects remote desktop access from the Internet, which is defined as anything outside the internal network. Remote desktop is detected from a Windows log or from a traffic flow to the RDP port.

Review the Remote Desktop From Internet Rule

You will review only the out-of-the-box rule, which detects remote desktop from the Internet. You will not be making any changes to this rule.

To review the Remote Desktop from Internet rule

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **RESOURCES**.
5. Click **Rules**.
6. In the search field, type `Remote Desktop from Internet`.
7. Select the rule, and then click **Edit > Selected Rule**.
The **Step 1: General** page has basic information such as the **Rule Name**, **Description** of the rule, **Event Type**, and **Remediation Note**.
8. Click **Step 2: Define Condition**.
This page displays the rule condition. This rule will trigger if the pattern **RDP** occurs within a 10 minute window.
9. Click the pencil icon () to edit the **RDP** subpattern.
10. Review the **Filters** for the rule.
The first two conditions state that the **Source IP** must not be part of the **Networks: Private Net** group and the **Destination IP** must be part of the **Networks: Private Net** group. For simplicity, and to understand it better, you can refer to these two conditions as Group 1.

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	Source IP	NOT IN	Networks: Private Net	+	AND	
	+	Destination IP	IN	Networks: Private Net	+	AND	
	((	Destination IP	IN	Devices: Windows	+	AND	
	+	Win Logon Type	=	10	+	AND	
	+	Event Type	IN	EventTypes: Dev Logon Failure, E	+	OR	
	(	Destination TCP/UDP Port	=	3389	+	AND	
	+	Event Type	IN	EventTypes: Bidirectional Netflow,	+	AND	

The next three filter conditions are grouped into one group, using parentheses. You can refer to these three conditions as Group 2. The **Destination IP** must be in the **Devices: Windows**, **Win Logon Type** must be equal to 10, and the **Event Type** must be part of **Dev Logon Failure** or **Dev Logon Success**.

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	Source IP	NOT IN	Networks: Private Net	+	AND	
	+	Destination IP	IN	Networks: Private Net	+	AND	
	((	Destination IP	IN	Devices: Windows	+	AND	
	+	Win Logon Type	=	10	+	AND	
	+	Event Type	IN	EventTypes: Dev Logon Success	+	OR	
	(	Destination TCP/UDP Port	=	3389	+	AND	
	+	Event Type	IN	EventTypes: Bidirectional Netflow,	+	AND	

The last two conditions are grouped into one group, using parentheses. You can refer to these two conditions as Group 3. The **Destination TCP/UDP Port** must be equal to **3389**, and the **Event Type** must be in the **Bidirectional Netflow** or **Permit Traffic** group.

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	Source IP	NOT IN	Networks: Private Net	+	AND	
	+	Destination IP	IN	Networks: Private Net	+	AND	
	((	Destination IP	IN	Devices: Windows	+	AND	
	+	Win Logon Type	=	10	+	AND	
	+	Event Type	IN	EventTypes: Dev Logon Failure, E	+	OR	
	(	Destination TCP/UDP Port	=	3389	+	AND	
	+	Event Type	IN	EventTypes: Bidirectional Netflow,	+	AND	

The Group 2 and Group 3 conditions are nested by other parentheses. There is an **OR** operator between Group 2 and Group 3, which means that either Group 2 or Group 3 conditions can be true. For this rule to trigger, Group 1 and either Group 2 or Group 3 must be true.

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row	
Group 1 AND Group 2 OR Group 3	+	Source IP	NOT IN	Networks: Private Net	+	AND	+	
	+	Destination IP	IN	Networks: Private Net	+	AND	+	
	+	((	Destination IP	IN	Devices: Windows	+	AND	+
	+	Win Logon Type	=	10	+	AND	+	
	+	Event Type	IN	Event Types: Dev Logon Failure, E	+	OR	+	
	+	(	Destination TCP/UDP Port	=	3389	+	AND	+
	+	Event type	IN	Event types: Bidirectional Netflow	+	AND	+	

11. Review the **Group By** attributes.

Group By:	Attribute	Row	Move
	Source IP	+	+
	Destination IP	+	+

The **Group By** attributes are set as **Source IP** and **Destination IP**. All the matching events that are defined in the filter will be grouped into two columns—**Source IP** and **Destination IP**.

12. Review the **Aggregate** conditions.

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	COUNT(Matched Events)	>=	1	+	AND	+

After the events are grouped, and if the **COUNT(Matched Events)** is equal to or greater than one, the rule will be triggered.

13. Click **Cancel**.
14. Click **Step 3: Define Action**.

Review the **Severity**, **Category**, **Subcategory**, **Technique**, and **Tactic**.

Remote Desktop from Internet - Edit Details

Step 1: General > Step 2: Define Condition > Step 3: Define Action

Severity: 9 - HIGH

Category: Security

Subcategory: Lateral Movement

Technique: 3 Selected

Tactics: Lateral Movement, Initial Access, Persistence, Command And Control

Action: Defined

Exception: Undefined

Tag:

15. Click the pencil icon (✎) to edit the **Action** setting.

16. Review the **Incident Attributes**.

Generate Incident for: Remote Desktop from Internet

Incident Attributes:	Event Attribute	Subpattern	Filter Attribute	Row
	Source IP	= RDP	Source IP	+
	Destination IP	= RDP	Destination IP	+

Insert Attribute: +

Incident Title: Remote Desktop from Internet \$srcIpAddr to \$destIpAddr

Triggered Attributes: Available: Search... 1/31

Selected:

- Event Receive Time
- Event Type
- Source IP
- Destination IP
- Win Logon Type
- Raw Event Log

Save Cancel

These will be more clear once the incident is triggered.

17. Click **Cancel**.
18. Click **Cancel**.

RDP From the Internet

Now, you will establish a remote desktop connection from the Local-Host VM. The RDP session will be translated to a public IP address by the FortiGate firewall. The rule will trigger an incident since the RDP session was sourced from a public IP address.

To establish an RDP connection to Win-Agent

1. Go to the Local-Host VM.
2. Open Remmina from the task bar.



3. Double-click **Server_2016_Administrator**.
This is a bookmark for an RDP session for 10.0.3.10.
4. If the bookmark prompts for credentials then enter the following credentials:

Field	Value
User name	Administrator
Password	Fortinet1!
Domain	Aviation

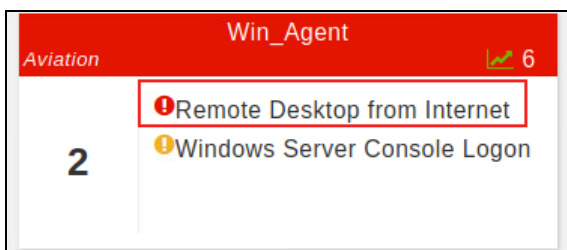
5. Click **OK**.
6. Accept any certificate warnings.
The RDP connection to the Win-Agent VM opens.
7. Close the RDP session.
8. Close the Win-Agent VM browser tab.

Review the RDP Incident

An incident will be generated, alerting the administrator that an RDP connection was established from the Internet. Any RDP connection from a public IP address is considered suspicious. You will review the incident in detail and the events that triggered this incident.

To review the RDP incident

1. Return to the Supervisor FortiSIEM management GUI, and click **INCIDENTS**.
2. Click **INCIDENTS**.
3. In the **Top Impacted Hosts - By Severity / Risk Score** section, find the **Win_Agent** widget, and click **Remote Desktop from Internet**.



It can take up to 30 seconds for the incident to display.

4. Select the rule and, at the bottom of the page, click **Details**.
5. Review the incident details.

Attributes	Search attribute name...	
Category: Security		
Count: 1		
Event Name: Remote Desktop from Internet		
Event Type: PH_RULE_INBOUND_REMOTE_DESKTOP		
First Occurred: Jul 22 2021, 05:01:30 PM		
Incident ID: 29		
Incident Title: Remote Desktop from Internet 100.64.2.253 to 10.0.3.10		
Reporting Device Status: Approved		
Reporting IP: 10.0.3.10		
Severity Category: HIGH		
Tactics: Persistence,Lateral Movement,Command And Control,Initial Access		
Technique: Remote Services: Remote Desktop Protocol, Remote Access Software, External Remote Services		
View Status: Read		
Last Occurred: Jul 22 2021, 05:01:30 PM		
Resolution: Open		
Incident Status: Active		
Organization: Aviation		
Reporting: HOST-10.0.3.10		
Severity: 9		
Source: 100.64.2.253		
Subcategory: Lateral Movement		
Target: 10.0.3.10		
Ticket Status: None		

6. Click **Events**.
7. Enable **Show Event Type**.
8. Select the **Win-Security-4624** event, and click the arrow icon (🔍) in the **Raw Event Log** column.
The **Event Details** window opens.

9. Review the enriched data.

```
Collector ID: 10003
Computer: WIN-GHSFO2BDOP4
Count: 1
Destination Host Name: Win_Agent
Destination IP: 10.0.3.10
Device Time: Jan 17 2020, 09:53:49 AM
Domain: AVIATION
Event ID: 9214787050068751952
Event Name: Windows logon success
Event Occur Time: Jan 17 2020, 03:53:49 PM
Event Parse Status: 1
Event Parser Name: WinOSWmiParser
Event Receive Time: Jan 17 2020, 09:53:59 AM
Event Rule Trigger: 1
Event Severity: 1
Event Severity Category: LOW
Event Source: Microsoft-Windows-Security-Auditing
Event Type: Win-Security-4624
External Event Receive Protocol: Windows Agent
Host Name: WIN-GHSFO2BDOP4.aviation.lab
Message: An account was successfully logged on.
Organization ID: 2007
Organization Name: Aviation
Process Name: User32
Relaying Device: Win_Agent
Relaying IP: 10.0.3.10
Reporting Device: Win_Agent
Reporting IP: 10.0.3.10
Reporting Model: Windows
Reporting Vendor: Microsoft
Software Name: User32
Source Host Name: WIN-GHSFO2BDOP4
Source IP: 100.64.2.253
Source TCP/UDP Port: 0
Source User: Administrator
Source User Full Name: Administrator
Status: Success
Subtype: Security
Win Logon Type: 10 (Remote interactive network logon using terminal services or remote desktop connection)
```

This event was reported by **Win_Agent**. The logon type code is **10**, and the RDP session was initiated from a public IP address to a private IP address. These conditions were enough to trigger the incident.

10. Click **Close**.
11. Click **Rule**, and review the rule that triggered this incident.
12. Analyze the **Pattern Definitions**.

Details Events Rule ☐ Auto expand

Pattern Definitions ▼

```
IF Source IP NOT IN Networks: Private Net AND Destination IP IN Networks: Private Net AND ((Destination IP IN Devices: Windows
AND Win Logon Type = 10 AND Event Type IN EventTypes: Dev Logon Failure, EventTypes: Dev Logon Success) OR
(Destination TCP/UDP Port = 3389 AND Event Type IN EventTypes: Bidirectional Netflow, EventTypes: Permit Traffic))
WHERE COUNT(Matched Events) >= 1
GROUPBY Source IP, Destination IP
```

These are the same definitions that were defined in the aggregate condition, event filter, and group by attributes in step 2 of the rule.

13. Click the left icon (◀) to return to the **Overview** page.
14. Log out of the Supervisor FortiSIEM management GUI.

Exercise 2: Detecting Multiple VPN Logon Failures

In this exercise, you will review the out-of-the-box rule which detects five consecutive VPN logon failures in a 10 minute evaluation period.

Review the Multiple VPN Logon Failures Rule

Now, you will review the out-of-the-box rule which detects five consecutive VPN logon failures in a 10 minute evaluation period.

To review the multiple VPN logon failures rule

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **RESOURCES**.
5. Click **Rules**.
6. In the search field, type `Multiple Logon Failures: VPN`.
7. Select the **Multiple Logon Failures: VPN** rule, and then click **Edit > Selected Rule**.
The **Step 1: General** page displays the **Rule Name**, **Description**, **Event Type**, and **Remediation Note**.
8. Click **Step 2: Define Condition**.
This page displays the rule condition. This rule will trigger if the **ExcessVPNLoginFailure** subpattern occurs within a 10 minute window.
9. Click the pencil icon (✎) to edit the **ExcessVPNLoginFailure** subpattern.
10. Review the **Filters** for the rule.

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	 	Event Type	IN	EventTypes: VPN Logon Failure	 	AND	 

There is only one filter. The **Event Type** must be from the **VPN Logon Failure** group.

11. Review the **Group By** attributes.

Group By:	Attribute	Row	Move
	Source IP		
	Reporting Device		
	Reporting IP		
	User		

The **Group By** attributes are **Source IP**, **Reporting Device**, **Reporting IP**, and **User**. All the matching events that are defined in the filter will be grouped into four columns, as defined in the **Group By** section.

- Review the **Aggregate** conditions.

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
		COUNT(Matched Events)	>=	5		AND	

After the events are grouped, and if the **COUNT(Matched Events)** is equal to or greater than 5, the rule will be triggered.

- Click **Cancel**.
- Click **Step 3: Define Action**.

Review the **Severity**, **Category**, **Subcategory**, **Technique**, and **Tactic**.

Multiple Logon Failures: VPN - Edit Details

Step 1: General > Step 2: Define Condition > Step 3: Define Action

Severity: 4 - LOW
Category: Security
Subcategory: Credential Access
Technique: [T1110.001] Brute Force: Password Guessing
Tactics: Credential Access
Action: Defined
Exception: Undefined
Tag:

- Click the pencil icon () to edit the **Action** setting.
- Review the **Incident Attributes**.

Generate Incident for: Multiple Logon Failures: VPN

Incident Attributes:

Event Attribute		Subpattern	Filter Attribute	Row
Source IP	=	ExcessVPNLoginFailure	Source IP	+ -
Destination Host Name	=	ExcessVPNLoginFailure	Reporting Device	+ -
Destination IP	=	ExcessVPNLoginFailure	Reporting IP	+ -
User	=	ExcessVPNLoginFailure	User	+ -
Triggered Event Count	=	ExcessVPNLoginFailure	COUNT(Matched Events)	+ -

Insert Attribute: +

Incident Title: \$incidentCount VPN logon failures for user \$user from \$srcIpAddr on server \$destName

Triggered Attributes: Available: Search... 1/31

Selected:

- Event Receive Time
- Event Type
- Reporting Device
- Reporting IP
- Source IP

Save Cancel

This will be more clear after the incident is triggered.

- Click **Cancel**.
- Click **Cancel**.

To review event types for VPN logon failure

- Continuing on the FortiSIEM GUI, on the left navigation pane, click **Event Types > Security > Logon Failure > VPN Logon Failure**.

Resources > Event Types > Security > Logon Failure > VPN Logon Failure

Event Type	Description	Device Type	CVE IDs	Severity	Scope
ASA-113005	IPsec/VPN/VPN AAA user authentication failed	Cisco ASA		Medium (Sev5)	System
ASA-611311	VNPDClient: XAUTH Failed	Cisco ASA		Medium (Sev6)	System
ASA-713166	Hardware Client IPsec Xauth authentication failed	Cisco ASA		Medium (Sev5)	System

There are 107 different types of VPN logon failures that can trigger this rule. These are the event types that are built in to FortiSIEM. You cannot delete them, but you can create your own event types in the appropriate category.

- In the search field, type FortiGate.

NewEditDelete

FortiGate

</

You will trigger a tunnel-mode SSL VPN logon failure.

Generate SSL VPN Login Failures

Now, you will generate five or more SSL VPN login failures by entering an incorrect password. FortiGate will send those failed logon events to FortiSIEM.

To initiate five consecutive SSL VPN login failures

1. Go to the Local-Host VM.
2. Open FortiClient from the task bar.



If the system prompts for password to run FortiClient then enter `password`.

3. Connect to the Aviation organization through SSL VPN with the following credentials:

Field	Value
VPN Name	SSL_VPN_Aviation
User	Sarah
Password	123456

This is an incorrect password for the VPN which will generate the failed logon events.

4. Click **Connect**.
5. Click **Continue**.
6. Click **OK**.
7. Continue attempting to log in four more times with different incorrect passwords.



Pause for 30 seconds after each login attempt. This ensures that FortiGate records the events and forwards them to FortiSIEM.

8. Close FortiClient.
9. Close the Local-Host VM browser tab.

Verify VPN events on FortiGate

Now, on FortiGate, you will verify the failed SSL VPN events. You must ensure that there are at least five failed logon events within a 10 minute period.

To verify the VPN events on FGT3

1. Go to the FGT_Aviation FortiGate management GUI.
2. Log in with the username `admin` and password `password`.
3. Click **Log & Report > Events**.
4. Click **System Events**
5. From the drop-down list, select **VPN Events**.
6. Click **Add Filter > Action > ssl-login-fail**.

The failed SSL VPN login events are displayed.

		x Action: ssl-login-fail	OR NOT	Add Filter	x	VPN Events ▾
Date/Time	Level	Action	Status	Message		
2020/03/26 13:08:28		ssl-login-fail		SSL user failed to logged in		
2020/03/26 13:07:24		ssl-login-fail		SSL user failed to logged in		
2020/03/26 13:07:11		ssl-login-fail		SSL user failed to logged in		
2020/03/26 13:04:29		ssl-login-fail		SSL user failed to logged in		
2020/03/26 13:03:54		ssl-login-fail		SSL user failed to logged in		
2020/03/26 13:02:32		ssl-login-fail		SSL user failed to logged in		
2020/03/26 13:02:24		ssl-login-fail		SSL user failed to logged in		

There must be at least five failed SSL VPN login attempts within a 10 minute period.

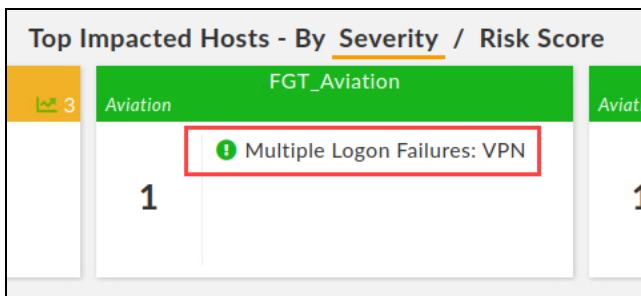
7. Log out of the FGT_Aviation FortiGate management GUI.

Review the Incident for Multiple VPN Logon Failures

Now, you will review the incident that is generated because there were five or more SSL VPN logon failures. You will review the incident source, target, and details.

To review the incident for multiple VPN logon failures

1. Return to the Supervisor FortiSIEM management GUI, and click **INCIDENTS**.
2. In the **Top Impacted Host - By Severity / Risk Score** section, find the **FGT_Aviation** widget, and then click **Multiple Logon Failures: VPN**.



3. Select the incident, and at the bottom of the page, click **Details**.
4. Review the incident details.
5. Click the **Events** tab to view the events that triggered this incident.

Incident Multiple Logon Failures: VPN for FGT_Aviation for Last 2 Hours							
Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target
LOW	Jul 23 2021, 10:40:30 AM	Multiple Logon Failures: VPN	Credential Access	Brute Force: Pass...	FGT_Aviation	100.64.2.253	FGT_Aviation 10.0.3.254 User: Sarah
Details	Events	Rule	Subpatient: ExcessVPNLoginFailure				
			☐ Auto expand	☐ Wrap Raw Events	☒ Show Event Type	☐ Show Raw Event Only	Compare Distribution
Event Receive Time	Event Type	Event Name	Reporting Device	Reporting IP	Source IP	User	
Jul 23 2021, 10:39:11 AM	FortiGate-ssl-vpn-user-ssl-login-fail	FortiGate-ssl-vpn-user-ssl-login-f...	FGT_Aviation	10.0.3.254	100.64.2.253	Sarah	
Jul 23 2021, 10:37:51 AM	FortiGate-ssl-vpn-user-ssl-login-fail	FortiGate-ssl-vpn-user-ssl-login-f...	FGT_Aviation	10.0.3.254	100.64.2.253	Sarah	
Jul 23 2021, 10:37:27 AM	FortiGate-ssl-vpn-user-ssl-login-fail	FortiGate-ssl-vpn-user-ssl-login-f...	FGT_Aviation	10.0.3.254	100.64.2.253	Sarah	
Jul 23 2021, 10:34:19 AM	FortiGate-ssl-vpn-user-ssl-login-fail	FortiGate-ssl-vpn-user-ssl-login-f...	FGT_Aviation	10.0.3.254	100.64.2.253	Sarah	
Jul 23 2021, 10:33:56 AM	FortiGate-ssl-vpn-user-ssl-login-fail	FortiGate-ssl-vpn-user-ssl-login-f...	FGT_Aviation	10.0.3.254	100.64.2.253	Sarah	

Because FGT_Aviation FortiGate reported five or more VPN logon failures, FortiSIEM generated this incident.

6. Review the **Source**, **Target**, and **Detail** for the incident.

Incident Multiple Logon Failures: VPN for FGT Aviation for Last 2 Hours								
Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target	Detail
LOW	Jul 23 2021 10:40:30 AM	Multiple Logon Failures: VPN	Credential Access	Brute Force: Pass...	FGT Aviation	100.64.2.253	FGT Aviation 10.0.3.254 User: Sarah	Triggered Event Count: 5

This incident was generated because of failed VPN logon attempts from the IP address 100.64.2.253 and the target was the FortiGate IP address 10.0.3.254. The user **Sarah** was also a target because someone tried to use her username to log in to the VPN. The **Detail** section provides you with the number of events that it took to trigger this incident.

7. Log out of the Supervisor FortiSIEM management GUI.

Exercise 3: Detecting Locked Domain Accounts

In this exercise, you will review the out-of-the-box rule which detects account lockout caused by excessive logon failures in a 10 minute window.

Review the Domain Account Locked Rule

You will review the **Account Locked: Domain** out-of-the-box rule which detects account lockout caused by excessive logon failures.

To review the domain account locked rule

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **RESOURCES**.
5. Click **Rules**.
6. In the search field, type `Account Locked: Domain`.
7. Select the **Account Locked: Domain** rule, and then click **Edit > Selected Rule**.
The **Step 1: General** page shows the **Rule Name**, **Description**, **Event Type**, and **Remediation Note**.
8. Click **Step 2: Define Condition**.
This page displays the rule condition. This rule will trigger if the **DomainAcctLockout** subpattern occurs within a 10 minute window.
9. Click the pencil icon (✎) to edit the **DomainAcctLockout** subpattern.
10. Review the **Filters** for this rule.

Name: DomainAcctLockout

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
+ -	Event Type	IN	EventTypes: Domain Account Lock	+ -	AND	+ -
+ -	Reporting IP	IN	Applications: Domain Controller	+ -	AND	+ -

The **Event Type** attribute must be in the **Domain Account Locked** group, and the **Reporting IP** must be in the **Domain Controller** group.

11. Review the **Group By** attributes.

Group By:	Attribute	Row	Move
	Reporting Device	 	 
	Reporting IP	 	 
	User	 	 

The **Group By** attributes are **Reporting Device**, **Reporting IP**, and **User**. All the matching events that are defined in the filter will be grouped into four columns, as defined in the **Group By** section.

12. Review the **Aggregate** conditions.

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	 	COUNT(Matched Events)	>=	1	 	AND	 

After the events are grouped, and if the **COUNT(Matched Events)** is equal to or greater than 1, the rule will be triggered.

13. Click **Cancel**.
14. Click **Step 3: Define Action**.

Review the **Severity**, **Category**, **Subcategory**, **Technique**, and **Tactics**.

Account Locked: Domain - Edit Details

Step 1: General > Step 2: Define Condition > Step 3: Define Action

Severity: 10 - HIGH
Category: Security
Subcategory: Credential Access
Technique: [T1110.001] Brute Force: Password Guessing
Tactics: Credential Access

Action: Defined
Exception: Undefined
Tag:

15. Click the pencil icon () to edit the **Action** setting.
16. Review the **Incident Attributes**.

Generate Incident for: Account Locked: Domain

Incident Attributes:

Event Attribute	Subpattern	Filter Attribute	Row
Destination Host Name	= DomainAcctLockout	Reporting Device	☐ ☐
Destination IP	= DomainAcctLockout	Reporting IP	☐ ☐
User	= DomainAcctLockout	User	☐ ☐
Triggered Event Count	= DomainAcctLockout	COUNT(Matched Events)	☐ ☐

Insert Attribute: +

Incident Title: \$user domain account locked on \$destName

Triggered Attributes: Available: Search... 1/31

Selected:

- Event Receive Time
- Event Type
- Reporting IP
- Source IP
- User
- Computer

Save Cancel

17. Click **Cancel**.

18. Click **Cancel**.

To review the domain account locked event types

- Continuing on the **RESOURCE** page, on the left navigation pane, click **Event Types > Security > Logon Failure > Domain Account Locked**.

There are three different types of domain account lockout events that are built in to FortiSIEM.

Resources > Event Types > Security > Logon Failure > Domain Account Locked

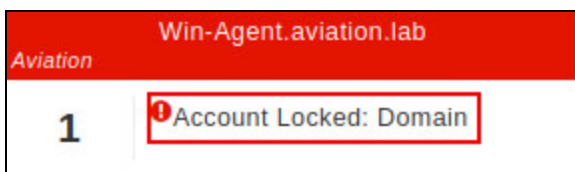
Name	Description
Win-Security-4740	A user account was locked out
Win-Security-539	Windows logon failure - account locked out
Win-Security-644	Windows user account locked out - excessive failed logins

Review the Incident for Locked Domain Accounts

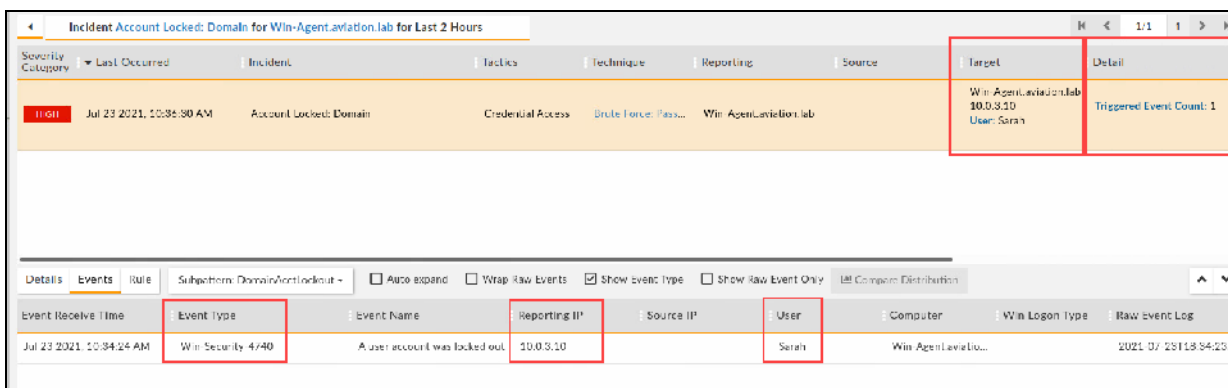
The incident for this rule was already triggered when you tried to log in to the SSL VPN and failed five times using the username Sarah. The domain policy is configured to lock user accounts after five failed attempts.

To review the incident for locked domain accounts

1. Continuing on the FortiSIEM GUI, click **INCIDENTS**.
2. In the **Top Impacted Host - By Severity / Risk Score** section, find the **Win-Agent.aviation.lab** widget, and click **Account Locked: Domain**.



3. Select the incident, and at the bottom of the page, click **Events**.



The **Event Type** is **Win-Security-4740**, and it is reported from an IP address that belongs to the domain controller group.

4. Log out of the Supervisor FortiSIEM management GUI.

Exercise 4: Creating a New Security Rule

In this exercise, you will build a new security rule which monitors for successful login events reported by a network device from a public IP address.

Create a Custom Rule

Creating a new rule involves defining the attributes of the incident that is triggered by the rule, as well as the triggering conditions and any exceptions or clear conditions. You can also create a rule by cloning an existing rule.

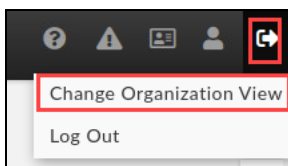
In this task, you will create a new rule to detect successful admin logins to FortiGate from a public IP address.

To create a custom rule

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click the **Change Organization View** icon, and in the drop-down list, select **Change Organization View**.



5. Select **Switch to Organization**, and in the drop-down list, select **Aviation**.
6. Click **Change View**.
7. Click **RESOURCES**.
8. In the left navigation pane, click **Rules > Security**.
9. Click **New**.
10. In **Step 1: General**, enter the following:

Field	Value
Rule Name	Admin login to FortiGate from a public IP address
Description	Detects successful admin login to FortiGate from public IP addresses

11. Click **Step 2: Define Condition**.
12. Click the pencil icon (✎) to edit the **Subpattern**.
13. In the **Name** field, type `FgtLoginPublic`.
14. Configure the following **Filters**:

Attribute	Operator	Value	Next
Source IP	NOT IN	Select from CMDB. Click Networks > Private Net . Click the add item icon (») to select it.	AND
Event Type	=	Select from CMDB. Search for FortiGate-event-admin-login-success. Click the add item icon (») to select it.	AND

15. Configure the following **Aggregate** function:

Attribute	Operator	Value	Next
COUNT(Matched Events)	>=	1	AND

To configure **Aggregate** functions use the **Expression Builder**, available when you click on **Attribute** field for the **Aggregate** section.

1. Select **Function** from the drop-down list
2. Add **Function** to the expression
3. Select the **Event Attribute**
4. Add the **Event Attribute** to the expression
5. Click **Validate** and ensure the expression is valid
6. Finally click **OK** when the expression is ready



16. Add the following **Group By** attributes:

- User
- Reporting Device

- Reporting IP
- Source IP

- Click **Save**.
- Click **Step 3: Define Action**.
- Configure the following values:

Field	Value
Severity	9-HIGH
Category	Security
Subcategory	Suspicious Activity
Technique	[T1190] Exploit Public-Facing Application

- Click the pencil icon (✎) to edit the **Action** setting.
- Configure the following **Incident Attributes**:

Event Attribute	Subpattern	Filter Attribute
Destination IP	FgtLoginPublic	Reporting IP
Destination Host Name	FgtLoginPublic	Reporting Device
User	FgtLoginPublic	User
Source IP	FgtLoginPublic	Source IP

- Set the **Incident Title** as follows:
\$srcIpAddr attempted to log into FortiGate \$destIpAddr from a public IP address
 You can populate the Source IP and Destination IP using the Insert Attribute drop-down list
- Select the following **Triggered Attributes**:
 - **Event Receive Time**
 - **Event Type**
 - **Reporting IP**
 - **Raw Event Log**
 - **Source IP**
- Click **Save**.
- Click **Save** again.
- Click the checkbox to activate your custom rule.

Resources > Rules > Security					
New	Edit	Delete	Clone	Search...	Insert Export
Active	Severity	Name	Description	Tactics	Technique
☐	9 - HIGH	Admin login to FortiGate from a public IP address	Detects successful admin login to FortiGate from public IP addresses		Exploit Public-Facing Application
					User

- Click **Continue**.

Log in to FortiGate From a Public IP Address

Now, you will trigger an incident by logging in to FGT_Aviation from a public IP address.

To log in to FortiGate from Kali

1. Go to the Kali VM.
2. Open a terminal session.
3. Type the following commands to open an SSH connection to FGT_Aviation

```
ssh admin@100.64.4.253
```

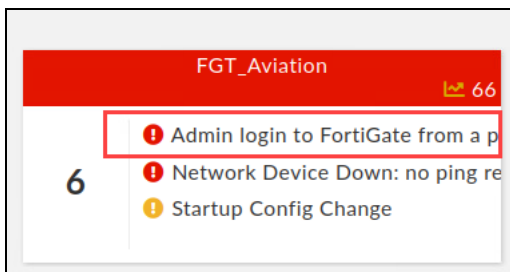


Accept any security warnings.

4. Log in with the password `password`.
5. Close terminal window.
6. Close the Kali VM browser tab.

To review the incident for the rule

1. Return to the Supervisor FortiSIEM management GUI, and click **INCIDENTS**.
2. In the **Top Impacted Host - By Severity / Risk Score** section, find the **FGT_Aviation** widget, and click **Admin login to FortiGate from a public IP address**.



3. Select the incident, and at the bottom of the page, click **Details**.
4. Review the incident details.
5. Click the **Events** tab to view the events that triggered this incident.
6. Review the **Source**, **Target**, and **Detail** for the incident.

Incident Admin login to FortiGate from a public IP address for FGT_Aviation for Last 2 Hours							
Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target
HIGH	Jul 23 2021, 12:59:00 PM	Admin login to FortiGate fr...	Initial Access	Exploit Public-Fac...	FGT_Aviation	100.64.1.10	10.0.3.254 FGT_Aviation User: admin

This incident was generated because the administrator of FGT_Aviation logged in from a public network. The source IP address 100.64.1.10 is a public IP address and is not part of the private network group on FortiSIEM.

7. Log out of the Supervisor FortiSIEM management GUI.

Lab 7: Configuration of Multipattern Security Rules

In this lab, you will build a multipattern rule to detect events where a user successfully authenticates to a VPN, and then successfully performs RDP authentication, using LDAP accounts not in a specific service accounts group, over a one hour time period.

Objectives

- Review a multisubpattern rule
- Build a multisubpattern rule from an analytics search
- Trigger an incident for the multisubpattern rule

Time to Complete

Estimated: 30 minutes

Exercise 1: Reviewing a VPN Login Event

In this exercise, you will review an LDAP user group, and create a VPN IP pool. Then, you will log in to the SSL VPN, and study the attributes that you will use to create the subpattern.

Review the LDAP Users

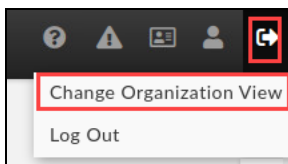
You will review the LDAP users that were imported from the Active Directory server.

To review the LDAP users

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click the **Change Organization View** icon, and in the drop-down list, select **Change Organization View**.



5. Select **Switch to Organization**, and in the drop-down list, select **Aviation**.
6. Click **Change View**.
7. Click **CMDB**.
8. In the left navigation pane, expand **Users > DC=Aviation,DC=lab**.
You will see all the user groups from the LDAP server that you discovered in a previous lab.

CMDB > Users > DC=Aviation,DC=lab						
New	Edit	Delete	Discovered by All	Search...	Action	1/1 9
User Name	Full Name	System Role	Job Title	Work Phone	Mobile Phone	Email
Administrator	Administrator					
DefaultAccount	DefaultAccount					
Guest	Guest					
Sarah	Sarah Smith			9874562165		sarah@aviation.lab
ben	Ben Jacobs			613258963		ben@aviation.lab
krbtgt	krbtgt					
mike	Mike Jones			6132232654		mike@aviation.lab
svcdap	LDAP Service Account		Windows Administrator			
tracey	Tracey Miller			2897564567		tracey@aviation.lab

- In the left navigation pane, click **OU=Service Accounts,DC=aviation,DC=lab**.
The **svcdap** account is an LDAP service account.
- In the left navigation pane, click **OU=VPN Users,DC=aviation,DC=lab**.
These are the users who belong to the VPN users group.

Create a VPN Pool

Now, you will create a VPN pool, where you will specify the IP range for the VPN network.

To create a VPN pool

- Continuing on the FortiSIEM management GUI, click **RESOURCES**.
- Click **Networks > VPN Pool**.
- Click **VPN Pool**.
- Click **New**.
- Configure the following values:

Field	Value
Name	SSL_VPN_Pool
Low	10.212.134.1
High	10.212.134.254
Mask	24

- Click **Save**.

To run a real-time search for the SSL tunnel

- Continuing on the FortiSIEM management GUI, click **ANALYTICS**.
- Click the **Edit Filters and Time Range** field.
- In the **Filter** section, select **Event Attribute**, and configure the following values:

Attribute	Operator	Value	Next
Reporting IP	=	10.0.3.254	AND
Event Type	=	FortiGate-ssl-vpn-session-tunnel-up	

4. In the **Time** section, select **Real Time**.

Your configuration should match the following example:

Filter

Load Save Clear All

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	=	10.0.3.254	+	AND	+
+	Event Type	=	Event Types: FortiGate-ssl-vpn-sess	+	AND	+

☐ CMDB Attribute

Time Range

☒ Real-time ☐ Relative

☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

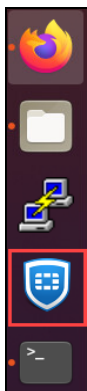
5. Click **Apply & Run**.

Connect to the SSL VPN

Now, you will establish an SSL VPN connection to FortiGate.

To connect to the SSL VPN

1. Go to the Local-Host VM
2. Open FortiClient from the task bar.





If the system prompts for password to run FortiClient then enter `password`.

3. Connect to the Aviation organization through SSL VPN with the following credentials:

Field	Value
VPN Name	SSL_VPN_Aviation
User	Sarah
Password	password

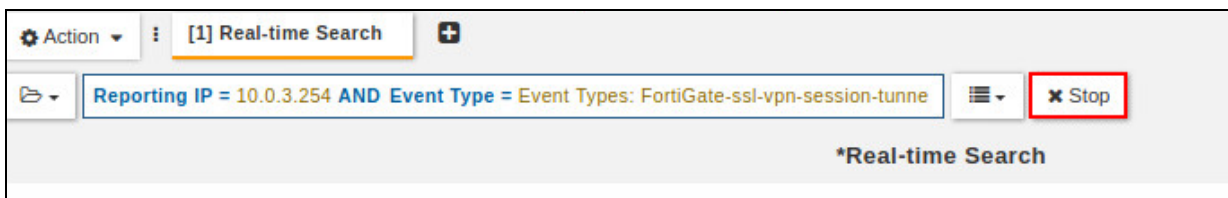
4. Click **Connect**.
5. Click **Continue**.

Analyze the SSL VPN Event

Now, you will analyze the SSL VPN event on FortiSIEM, and note the relevant attributes that will be used for constructing a subpattern.

To analyze the SSL VPN event

1. Return to the FortiSIEM management GUI, and on the **ANALYTICS** page, click **Stop**.



2. Select the event, and then click the arrow icon (🔍) in the **Raw Event Log** column.
The **Event Details** window opens.

Notice that the internal IP address assigned to the user is presented by the **Post-NAT Source IP** attribute.

Event Details

Search...

Lines: 37

Display	Filter	Item	Value
☐	☐	Log Level	Information
☐	☐	Member ID	0101039947
☐	☐	Organization ID	2007
☐	☐	Organization Name	Aviation
☐	☐	Post-NAT Source IP	10.212.134.200
☐	☐	Reason for Error	tunnel established
☐	☐	Relaying IP	10.0.3.254
☐	☐	Reporting Device	HOST-10.0.3.254
☒	☒	Reporting IP	10.0.3.254
☐	☐	Reporting Model	FortiOS
☐	☐	Reporting Vendor	Fortinet

OK

Close

Based on the observations that you made in this exercise, you will need the following attributes to build a template for the first rule subpattern to track a successful SSL VPN login:



Attribute	Value
Event Type	FortiGate-ssl-vpn-session-tunnel-up
User	Any
Post-NAT Source IP	Any

3. Close the **Event Details** dialog box.
4. Log out of the Supervisor FortiSIEM management GUI.



Do not disconnect the SSL VPN connection.

Exercise 2: Reviewing an RDP Event

In this exercise, you will review an RDP logon event.

Run a Real-Time Analytics Search

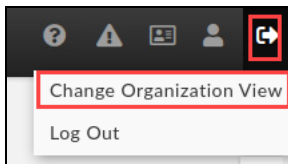
Now, you will run a real-time analytics search for Windows security events being reported by the Win-Agent Windows server. After that, you will establish an RDP connection to the Windows server, and that will generate a Windows logon security log, which will be forwarded to FortiSIEM by the Windows agent.

To run a real-time analytics search

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click the **Change Organization View** icon, and in the drop-down list, select **Change Organization View**.



5. Select **Switch to Organization**, and in the drop-down list, select **Aviation**.
6. Click **Change View**.
7. Click **ANALYTICS**.
8. Click the **Edit Filters and Time Range** field.
9. In the **Filter** section, select **Attribute**, and configure the following values:

Attribute	Operator	Value	Next
Reporting IP	=	10.0.3.10	AND
Event Type	=	Win-Security-4624	AND
Win Logon Type	=	10	

10. In the **Time** section, select **Real Time**.

Your configuration should match the following example:

Reporting IP = 10.0.3.254 AND Event Type = Event Types: FortiGate-ssl-vpn-session-tunnel-u

Filter

Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	=	10.0.3.10	+	AND	+
+	Event Type	-	Event Types: Win Security 4624	+	AND	+
+	Win Logon Type	=	10	+	AND	+

Time Range

☒ Real-time ☐ Relative

☐ Absolute

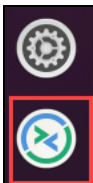
Trend Interval: Auto

Apply & Run Apply Cancel

11. Click **Apply & Run**.

To establish an RDP connection to Win-Agent

1. Go to the Local-Host VM.
2. Open Remmina from the task bar.



3. Double-click **Server_2016_Sarah**.
This is a bookmark for an RDP session for 10.0.3.10.
4. If the bookmark prompts for credentials then enter the following credentials:

Field	Value
User name	SARAH
Password	password
Domain	Aviation

5. Accept any certificate warnings.
The RDP connection to the Win-Agent VM opens.

6. Close the RDP session.

Analyze an RDP Event

Now, you will analyze the RDP event on FortiSIEM and note the relevant attributes that will be used for constructing a subpattern. After that, you will disconnect the VPN.

To analyze an RDP event

1. Return to the Supervisor FortiSIEM management GUI, and on the **ANALYTICS** page, click **Stop**.



2. Select and review the event that was received for a successful RDP logon.
3. Enable **Show Event Type**.
4. Select the **Win-Security-4624** event, and click the arrow icon (🔍) in the **Raw Event Log** column.

The **Event Details** window opens.

Notice this event contains the server IP address (**Destination IP**), the user who logged in (**User**), the source IP address of the user (**Source IP**), and the logon type code (**Win Logon Type**) which indicates that it is an RDP logon.

Based on the observations that you made in this exercise, you will need the following attributes to build a template for the second rule subpattern to track the RDP logon :



Attribute	Value
Event Type	Win-Security-4624
Destination IP	10.0.3.10
Win Logon Type	10

The user account **Sarah** is a member of the **VPN Users** group and the source IP address is from the **SSL_VPN_Pool** pool. These two conditions will be the factors that will trigger the rule. The rule will track users who are not supposed to access the server using RDP.

5. Close the **Event Details** window.
6. Log out of the Supervisor FortiSIEM management GUI.
7. Return to the Local-Host VM, and on the FortiClient SSLVPN client, click **Stop**.
8. Close FortiClient.
9. Close the Local-Host VM browser tab.

Exercise 3: emranBuilding a Multipattern Rule

In this exercise, you will build the rule using the two subpatterns that you analyzed in the previous two exercises.

Create a New Multipattern Rule

In the previous two exercises of this lab, you obtained relevant information for building a subpattern. Now, you will use that information to create a multipattern rule.

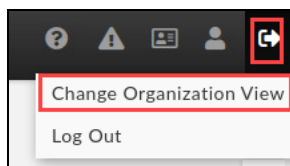
FortiSIEM supports rules with multiple subpatterns. These cover conditions where two patterns might need to occur within a specific time period, or one of a selection of patterns needs to occur to prove an incident condition exists.

To build a new multipattern rule

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click the **Change Organization View** icon, and in the drop-down list, select **Change Organization View**.



5. Select **Switch to Organization**, and in the drop-down list, select **Aviation**.
6. Click **Change View**.
7. Click **RESOURCES**.
8. In the left navigation pane, expand **Rules > Security**.
9. Click **New**.
10. In **Step 1: General**, enter the following values:

Field	Value
Rule Name	Successful RDP Logon from VPN Pool for Disallowed User
Description	Detects RDP Logon to AD Server from VPN Pool for Disallowed Users

11. Click **Step 2: Define Condition**.
12. In the time window field, type 3600.
13. Click the pencil icon (✎) to edit the **Subpattern**.
14. In the **Name** field, type `SSL_VPN_Logon`.
15. Configure the following **Filter**:

Attribute	Operator	Value	Next
Event Type	=	FortiGate-ssl-vpn-session-tunnel-up	AND

16. Configure the following **Aggregate** function:

Attribute	Operator	Value	Next
COUNT(Matched Events)	>=	1	AND

To configure **Aggregate** functions use the **Expression Builder**, available when you click on **Attribute** field for the **Aggregate** section.

1. Select **Function** from the drop-down list
2. Add **Function** to the expression
3. Select the **Event Attribute**
4. Add the **Event Attribute** to the expression
5. Click **Validate** and ensure the expression is valid
6. Finally click **OK** when the expression is ready



17. Add the following **Group By** attributes:

- **User**
- **Post-NAT Source IP**

Your configuration should match the following example:

Name:

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
+ -		Event Type	=	ortiGate-ssl-vpn-session-tunnel-up	+ -	AND	+ -

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
+ -		COUNT(Matched Events)	>=	1	+ -	AND	+ -

Group By:

Attribute	Row	Move
User	+ -	↑ ↓
Post-NAT Source IP	+ -	↑ ↓

18. Click **Save**.
19. In the **Next** column, in the drop-down list, select **FOLLOWED_BY**.
20. Click the add icon (+) to add a new subpattern.
21. In the **Name** field, type **RDP_Logon**.
22. Configure the following **Filters**:

Attribute	Operator	Value	Next
Event Type	=	Win-Security-4624	AND
Win Logon Type	=	10	AND
User	NOT IN	Select from CMDB Expand Users > DC=Aviation,DC=lab . Select OU=Service Accounts,DC=Aviation,DC=lab . Click the add folder icon (»), and then click OK .	AND
Destination IP	=	10.0.3.10	AND
Source IP	IN	Select from CMDB Expand Networks , and then select VPN Pool . Click the add folder icon (»), and then click OK .	AND

23. Enter the following **Aggregate** function:

Attribute	Operator	Value	Next
COUNT(Matched Events)	>=	1	AND

To configure **Aggregate** functions use the **Expression Builder**, available when you click on **Attribute** field for the **Aggregate** section.

1. Select **Function** from the drop-down list
2. Add **Function** to the expression
3. Select the **Event Attribute**
4. Add the **Event Attribute** to the expression
5. Click **Validate** and ensure the expression is valid
6. Finally click **OK** when the expression is ready



24. Add the following **Group By** attributes:

- **User**
- **Source IP**

Your configuration should match the following example:

Filters:						
Paren	Attribute	Operator	Value	Paren	Next	Row
+	Event Type	=	Win-Security-4624	+	AND	+
+	Win Logon Type	=	10	+	AND	+
+	User	NOT IN	Group: OU=Service Accounts,DC=	+	AND	+
+	Destination IP	=	10.0.3.10	+	AND	+
+	Source IP	IN	Group: VPN Pool	+	AND	+

Aggregate:						
Paren	Attribute	Operator	Value	Paren	Next	Row
+	COUNT(Matched Events)	>=	1	+	AND	+

Group By:				
Attribute	Row	Move		
User	+	-	↑	↓
Source IP	+	-	↑	↓

25. Click **Save**.

26. Configure the following subpattern relationships:

Subpattern	Attribute	Operator	Subpattern	Attribute
SSL_VPN_Logon	User	=	RDP_Logon	User
SSL_VPN_Logon	Post-NAT Source IP	=	RDP_Logon	Source IP

Your configuration should match the following example:

Condition: If this Pattern occurs within any 360 second time window

Paren	Subpattern	Operator	Subpattern	Attribute	Next	Row
+	SSL_VPN_Logon	=	RDP_Logon	User	FOLLOWED_BY	+
+	RDP_Logon	=	RDP_Logon	Source IP		+

Given these subpattern relationships:

Subpattern	Attribute	Operator	Subpattern	Attribute	Next	Row
SSL_VPN_Logon	User	=	RDP_Logon	User		+
SSL_VPN_Logon	Post-NAT Source IP	=	RDP_Logon	Source IP		+

27. Click **Step 3: Define Action**.
28. Configure the following values:

Field	Value
Severity	9-HIGH
Category	Security
Subcategory	Suspicious Activity
Technique	[T1564.002] Hide Artifacts: Hidden Users

29. Click the pencil icon (✎) to edit the **Action** setting.
30. Configure the following **Incident Attributes**:

Event Attribute	Subpattern	Filter Attribute
Source IP	SSL_VPN_Logon	Post-NAT Source IP
User	SSL_VPN_Logon	User

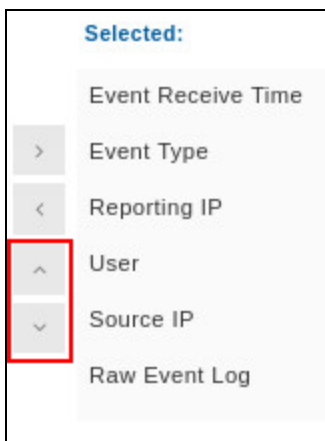


In this case, using either subpattern attributes will obtain the same result.

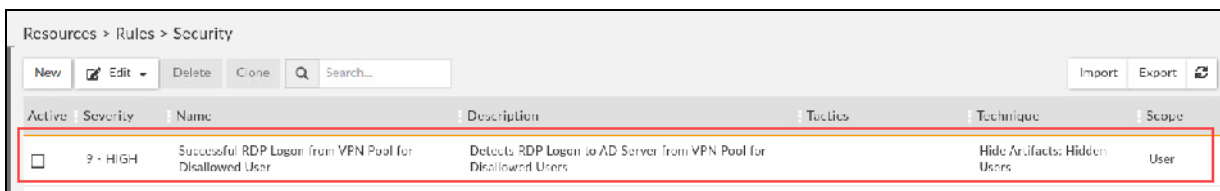
31. Add the following **Triggered Attributes**:

- User
- Source IP

32. Use the move icons (▲ or ▼) to rearrange the attributes to match the following example:



33. Click **Save**.
34. Click **Save**.
35. Click the checkbox to activate your custom rule.



36. Click **Continue**.

Establish an RDP Connection over SSL VPN

Now, you will establish an SSL VPN connection, and then connect over RDP to the Windows server, over the VPN tunnel.

To connect to SSL VPN

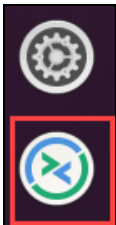
1. Go to the Local-Host VM.
2. Open FortiClient from the task bar.
3. Connect to the Aviation organization through SSL VPN with the following credentials:

Field	Value
VPN Name	SSL_VPN_Aviation
User	Sarah
Password	password

4. Click **Connect**.
5. Click **Continue**.

To establish an RDP connection to Win-Agent

1. Continuing on the Local-Host VM, open Remmina from the task bar.



2. Double-click **Server_2016_Sarah**.
This is a bookmark for an RDP session for 10.0.3.10.
3. If the bookmark prompts for credentials then enter the following credentials:

Field	Value
User name	SARAH
Password	password
Domain	Aviation

4. Accept any certificate warnings.
The RDP connection to the Win-Agent VM opens.
5. Close the RDP session, and then close Remmina.
6. Disconnect the VPN, and then close FortiClient.
7. Close the Local-Host VM browser tab.

Review the Incident

Now, you will review the incident that was generated by the rule you created to track successful RDP logons from the VPN pool for disallowed users.

To review the incident

1. Return to the Supervisor FortiSIEM management GUI, and click **Incidents**.
2. Find the **Security** widget, and then click **High**.
It may take a few minutes for the incident to show up.



3. Select the **Successful RDP Logon from VPN Pool for Disallowed Users** incident, and then click **Details**.
4. Click **Events**.
5. In the **Subpattern** drop-down list, select **SSL_VPN_Logon**.

Note the **Event Receive Time**.

Last Occurred

Incident

Jan 21 2020, 08:30:00 AM

Successful RDP Logon from VPN Pool for Disallowed User

Details

Events

Rule

Subpattern: SSL_VPN_Logon

Auto expand

Wrap Raw

Event Receive Time

Event Name

Reporting IP

Jan 21 2020, 08:28:30 AM

FortiGate ssl vpn session tunnel up

10.0.3.254

6. In the **Subpattern** drop-down list, select **RDP_Logon**.

Note the **Event Receive Time**.

Last Occurred

Incident

Jan 21 2020, 08:30:00 AM

Successful RDP Logon from VPN Pool for Disallowed User

Details

Events

Rule

Subpattern: RDP_Logon

☐ Auto expand

☐ Wrap Raw Eve

Event Receive Time

Jan 21 2020, 08:29:08 AM

Jan 21 2020, 08:29:08 AM

Event Name

Windows logon success

Windows logon success

Reporting IP

10.0.3.10

10.0.3.10



In the examples shown here, the event receive time for the SSL VPN tunnel occurred 38 seconds before the RDP logon event. This satisfies the followed by condition in the rule, which states that the VPN logon event must occur before the RDP logon event.

7. Log out of the Supervisor FortiSIEM management GUI.

Lab 8: Baseline Theory

In this lab, you will explore the baselining features on FortiSIEM, and create your own baseline profile.

Objectives

- Review baseline reports
- Review baseline rules
- Determine what you need to baseline
- Create a baseline with the BaselineMate script
- Verify that the baseline report has been applied
- View data in the daily DB and profile DB

Time to Complete

Estimated: 50 minutes

Exercise 1: Reviewing Baseline Reports and Rules

In this exercise, you will review the baseline reports and rules.

Review Baseline Reports

You will review the out-of-the-box baseline reports, and understand the anomaly detection baseline feature on those reports.

To review baseline reports

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **RESOURCES**.
5. In the left navigation pane, click **Reports > Baseline**.
6. Review the following anomaly detection baseline reports. Select each report, and then click **Edit**.
 - **Privileged Logon Profile**
 - **STM Response Time Profile**
 - **Failed User Logon Profile**
 - **Successful Device Logon Profile**
 - **Reported Error Log Profile**
 - **DNS Request Profile**

For each report, review the **Event Type** that it's referencing. Click **Cancel** after you're done.

7. In the left navigation pane, click **Event Status**.
8. Select **All FortiSIEM Non-reporting Modules**, and then click **Edit**.



Notice that the **Anomaly Detection Baseline** setting has been deselected for this report. This is a special flag to indicate to the system where the data will be queried from. This is the major difference between a baseline report and an ordinary report.

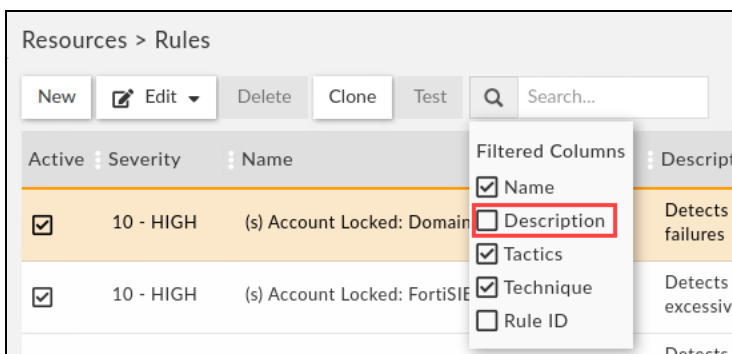
9. Click **Cancel**.

Review Baseline Rules

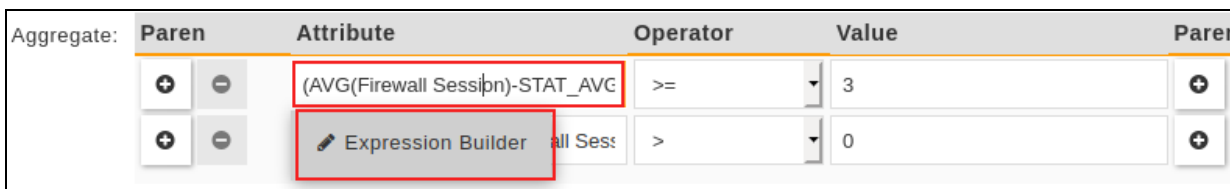
There are several out-of-the-box rules that refer to baseline data to compute aggregate conditions and generate incidents. The rule names start with the term **Sudden**. You will review one of these baseline rules.

To review baseline rules

1. Continuing on the **RESOURCE** tab, in the left navigation pane, expand **Rules**.
2. In the left pane, select and expand **Rules**.
3. Click the search icon (🔍), and in the drop-down list, deselect **Description**.

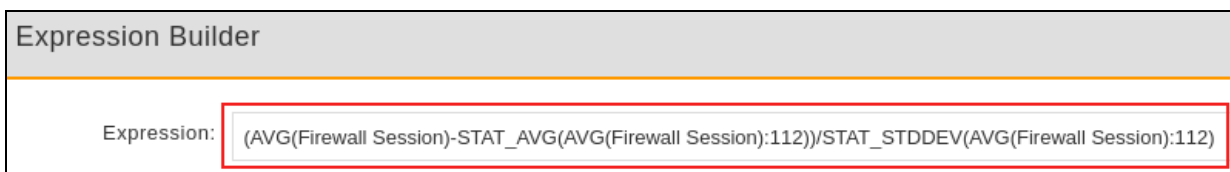


4. In the search field, type **sudden**.
Review the list of baseline rules that appear in the filtered list.
5. Select **Sudden Increase In Firewall Connections**, and then click **Edit**.
6. Click **Step 2: Define Condition**.
7. Click the pencil icon (✎) to edit the **Subpattern**.
Review the rule construction.
8. Click one of the **Aggregate** condition fields, and in the drop-down list, select **Expression Builder**.



The **Expression Builder** opens.

9. Review the full expression, and try to determine what it means.





The rule detects a sudden increase in permitted firewall connections when, over a 30 minute window, the number of current firewall connections is more than three standard deviations away from the mean.

For the statistical average and standard deviation rule functions, the format is the name, followed by the aggregation, attribute, and profile ID arguments.

The statistical average is the moving average value of **AVG(Firewall Session)** from profile 112 in the profile database.

10. Click **Cancel**.
11. Click **Cancel**.
12. Log out of the Supervisor FortiSIEM management GUI.

Exercise 2: Determining What to Baseline

In this exercise, you will determine the parameters required to baseline a profile.

Determine Parameters to Baseline

You will determine the parameters that require baseline, and run a script to generate USB write events.

To disable the Windows Server USB File Write rule

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **RESOURCES**.
5. In the left pane, expand **Rules**.
6. In the search field, type `Windows Server USB File Write`.
7. Deselect the **Active** checkbox.
The **Set Activation Scope** window opens.
8. Deselect **All Orgs**.
9. Deselect **Active**.

Set Activation Scope

Activation Status for New Org:

☐ Active

Activation Status for This Rule:

☐ All Orgs

☐ Super/Local

☐ Banking

☐ University

☐ Aviation

10. Click **Save**.

To run a script to replay USB events

1. Go to the Local-Host VM.
2. Open a terminal window (Ctrl + Alt + T).
3. Type the following command to change the working directory:

```
cd Desktop/Resource/Lab/lab8/8_2
```

4. Type the following command to start the script:

```
sudo ./runLab8_2.sh
```

```
student@linux: ~/Desktop/Resource/Lab/lab8/8_2
File Edit View Search Terminal Help

student@linux:~/Desktop/Resource/Lab/lab8/8_2$ ls
events runLab8_2.sh usb_report.xml
student@linux:~/Desktop/Resource/Lab/lab8/8_2$ sudo ./runLab8_2.sh
```

5. Type the password `password`.
6. Type `1`, and then press **Enter**.
Wait for the **All Done!** message.
7. Type `2`, and then press **Enter** to exit the script.
8. Close the terminal window.
9. Close the Local-Host VM browser tab.

To identify parameters for baseline

1. Return to the Supervisor FortiSIEM management GUI, and click **ANALYTICS**.
2. Click the **Edit Filters And Time Range** field.

3. In the **Filter** section, click **Event Attribute**.
4. Configure the following attributes:

Attribute	Operator	Value	Next
Reporting IP	IN	10.0.1.1,10.0.1.5,10.0.1.9	AND
Event Type	=	AO-WUA-RemovableMedia-AddFile	

5. Set the time to 40 minutes.
6. Click **Apply**.
7. Click the **Change Display Fields** icon (≡).
8. Configure the following **Group By and Display Fields**. Leave all **Order** and **Display As** fields empty:
 - Reporting IP
 - Reporting Device
 - Disk Name
 - Disk Model
 - User
 - COUNT (Matched Events)
 - COUNT DISTINCT (File Name)
9. Configure the following **Display Conditions**:
 - COUNT (Matched Events) >= 1
 - COUNT DISTINCT (File Name) >= 1

Your configuration should match the following example:

Group By and Display Fields
Load Save Clear All

Attribute	Order	Display As	Row	Move
Reporting IP	▼		+	+
Reporting Device	▼		+	+
Disk Name	▼		+	+
Disk Model	▼		+	+
User	▼		+	+
COUNT (Matched Events)	▼		+	+
COUNT DISTINCT (File Name)	▼		+	+

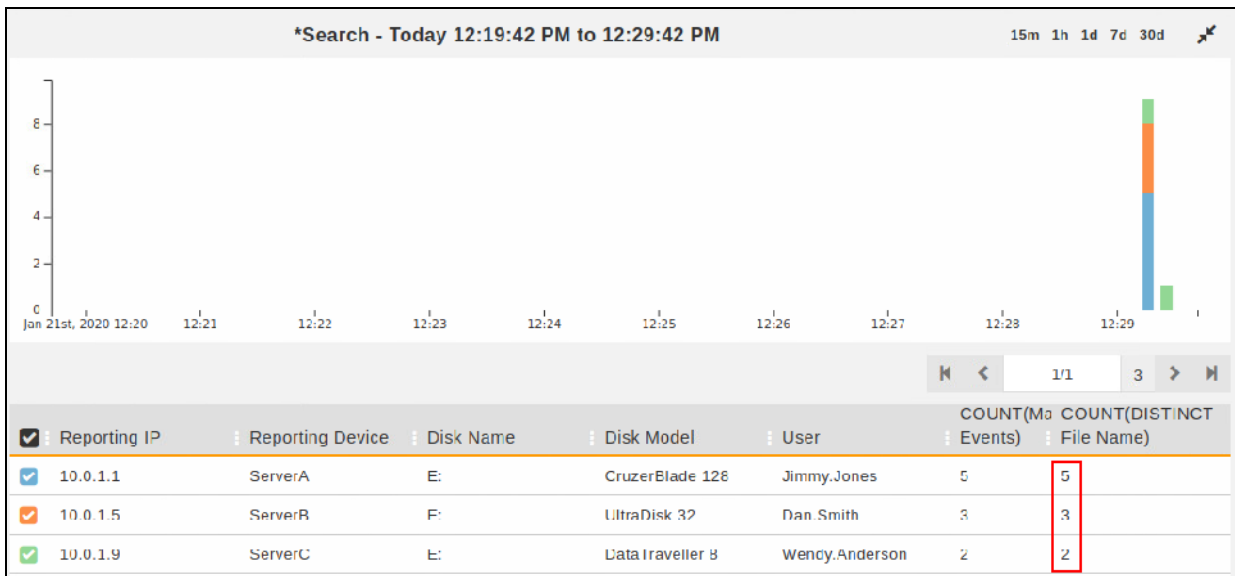
Display Conditions

Paren	Attribute	Operator	Value	Paren	Next	Row
+	COUNT (Matched Events)	>=	1	+	AND	+
+	COUNT DISTINCT (File Name)	>=	1	+	AND	+

Apply & Run Apply Cancel

9. Click **Apply & Run**.

Notice there are three servers that reported USB write events, with a total of 10 events. You should see that the results are ordered by the **COUNT DISTINCT(File Name)** values.



10. Log out of the Supervisor FortiSIEM management GUI.

Exercise 3: Creating a Baseline With the BaselineMate Script

In this exercise, you will create a baseline with the BaselineMate script.

Define an Event

When you create a new baseline for device logs, you must add a new event type to FortiSIEM so that the log events can be identified.

To define an event

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **ADMIN**.
5. Click **Device Support > Event Types**.
6. Click **New**.
7. Configure the following values:

Field	Value
Event Type	PH_PROF_ET_175_USB
Device Type	Fortinet FortiSIEM
Event Type Group	Info
Severity	1 - LOW

Your configuration should match the following example:

Event Definition

Event Type:PH_PROF_ET_175_USB

Device Type:Fortinet FortiSIEM

Event Type Group:Info

Availability

Performance

Change

Security

Regular Traffic

Fatal

Error

Warning

Info

Incidents

Ungrouped

Severity:1 - LOW

Event Name:

Save

Cancel

- Click **Save**.
- Select the event, and then click **Apply**.
- Click **Yes**, to save the changes.

Run the BaselineMate Script from Supervisor

Now, you will create a baseline profile report using a script. The script will also warn you about the missing event attributes that you will add using the GUI.

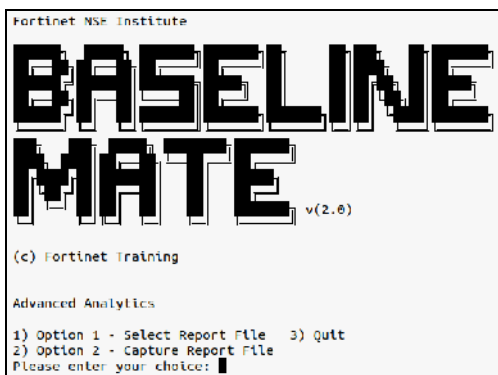
To run the BaselineMate script from Supervisor

- Go to the Local-Host VM.
- Open a terminal window (Ctrl + Alt + T).
- Type the following command to open an SSH connection to the FortiSIEM supervisor:

```
ssh root@10.0.1.130
```
- Type the password `Fortinet1!`.
- Type the following command to change the working directory:

```
cd Lab/lab8/8_3
```
- Type the following command to start the script:

```
./baselineMate.sh
```



7. Type 1, and then press Enter.
8. Type 2, and then press Enter.
9. Type 175 for the **Profile ID**, and then press Enter.
10. Type PH_PROF_ET_175_USB for the **Profile EventType**, and then press Enter.
11. Type yes, and then press Enter.
12. Type 1000 for the number of rows and then press Enter.

The **Profile Report** definition is displayed.

```
New Profile Report Definition Created.....

<DataRequest id="175" type="Report" profileId="PH_PROF_ET_175_USB" numRows="1000">
  <Name>Search</Name>
  <Description></Description>
  <CustomerScope groupByEachCustomer="true">
    <Include all="true"/>
  </Include>
  </CustomerScope>
  <SelectClause numEntries="All">
    <AttrList>reptDevIpAddr, reptDevName, diskName, hwdiskModel, user, COUNT(*), COUNT(DISTINCT fileName)</AttrList>
  </SelectClause>
  <OrderByClause>
    <AttrList>COUNT(DISTINCT fileName) DESC</AttrList>
  </OrderByClause>
  <ReportInterval><Window unit="Hourly" val="1"/></ReportInterval>
  <PatternClause window="3600">
    <SubPattern displayName="Filter_1" name="Filter_1">
      <SingleEvtConstr>eventType = "AO-WUA-RenovableMedia-AddFile" AND reptDevIpAddr IN (10.0.1.1,10.0.1.5,10.0.1.9)</SingleEvtConstr>
    </SubPattern>
    <GroupByAttr>reptDevIpAddr, reptDevName, diskName, hwdiskModel, user</GroupByAttr>
  </PatternClause>
</DataRequest>
</ProfileReports>
```

Review the definition and verify that **SelectClause**, **OrderByClause**, **SingleEvtConstr**, and **GroupByAttr** are listed.

13. Type y, and then press Enter.
- The script displays a three-step menu.

```
Look OK? (y/n):
y
1) Step A - Deploy New Profile Report AUTOMATICALLY
2) Step B - Determine Missing Attributes required for Baseline
3) Step C - Create Baseline Report
4) Quit
Please select the following options in Order: █
```

14. Type 1, and then press Enter to deploy the **New Profile Report**.
- The **phReportWorker** and **phReportMaster** processes are restarted.

```
Look OK? (y/n):
y
1) Step A - Deploy New Profile Report AUTOMATICALLY
2) Step B - Determine Missing Attributes required for Baseline
3) Step C - Create Baseline Report
4) Quit
Please select the following options in Order: 1

Killing backend Processes...
Waiting for Processes to Restart.....
Please select the following options in Order: 
```

15. Type 2 to initiate a check for required attributes.
A warning is displayed.

```
Please select the following options in Order: 2
Processing Profile_175 Schema..
WARNING: New Entry required for minDistinctFileName with a Value Type of UINT64
WARNING: New Entry required for maxDistinctFileName with a Value Type of UINT64
WARNING: New Entry required for avgDistinctFileName with a Value Type of double
WARNING: New Entry required for sdevDistinctFileName with a Value Type of double

All done, Schema Processing Complete!
```



Do not close the terminal window. Leave it running in the background, and you will come back to it later.

16. Return to the Supervisor FortiSIEM management GUI, and click **Event Attribute**.
17. Click **New**.
18. Configure the following attributes:

Name	Display Name	Value Type
minDistinctFileName	Min Distinct File Name	UINT64
maxDistinctFileName	Max Distinct File Name	UINT64
avgDistinctFileName	Avg Distinct File Name	DOUBLE
sdevDistinctFileName	Std Dev Distinct File Name	DOUBLE

Your configuration should match the following example:

Devices/Apps			
Event Attributes			
Event Types			
Parsers			
Monitoring			
Custom Properties			
SNMP SysObjectId			
Upload File			
New	Edit	Delete	Apply
Clone	Search...	Columns	
Name	Display Name	Value Type	Elasticsearch Value Type
sdevDistinctFileName	Std Dev Distinct File Name	DOUBLE	Double
avgDistinctFileName	Avg Distinct File Name	DOUBLE	Double
maxDistinctFileName	Max Distinct File Name	UINT64	Long
minDistinctFileName	Min Distinct File Name	UINT64	Long

19. Click **Apply**.

Device/App			
Event Attribute			
Event			
Parser			
Monitoring			
Custom Property			
SNMP SysObjectId			
Upload			
New	Edit	Delete	Apply
Clone	Search...	Columns	
Name	Display Name	Value Type	

20. Click **Yes**.

21. Return to the Local-Host VM, and in the terminal window, type `y` and press `Enter`.

22. Type `3` to create a baseline report.

23. For the profile name, type `USB Write Profile`, and then press `Enter`.

The baseline report is displayed.

```
<Reports>
  <Report group="PH_SYS_REPORT_Baseline" baseline="true" rsSync="">
    <Name>USB Write Profile</Name>
    <Description>Baseline Report for 1/5</Description>
    <CustomerScope groupByEachCustomer="true">
      <Include>1</Include>
      <Exclude/>
    </CustomerScope>
    <SelectClause>
      <AttrList>profDateType, hourOfDay, replDevIpAddr, replDevName, diskName, hwDiskModel, user, avgDistinctFileName, sdevDistinctFileName, a
    </SelectClause>
    <OrderByClause>
      <AttrList>profDateType ASC, hourOfDay ASC, COUNT(DISTINCT fileName) DESC</AttrList>
    </OrderByClause>
    <PatternClause window="3600">
      <SubPattern id="5107046" name="Filter_Baseline_175">
        <SingleEvtConstr>eventType = "PH_PROF_ET_175_USB"</SingleEvtConstr>
      </SubPattern>
    </PatternClause>
    <userRoles/>
    <SyncOrgs/>
  </Report>
</Reports>
```

24. Type `yes`, and then press `Enter`.

Wait for the upload to finish.

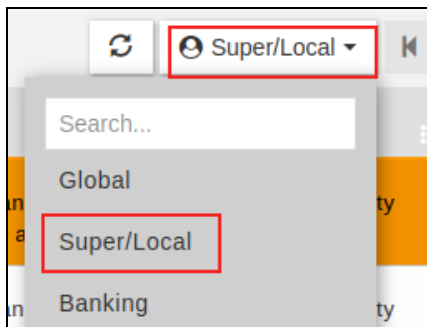
```
Upload Baseline Analytic Report to FortiSIEM GUI? (yes/no) : yes
Upload Complete! - Please check FortiSIEM GUI Resource/Reports/Baseline
[root@supervisor 8_3]#
```

25. Close the terminal window.

26. Close the Local-Host VM browser tab.

To view the baseline report

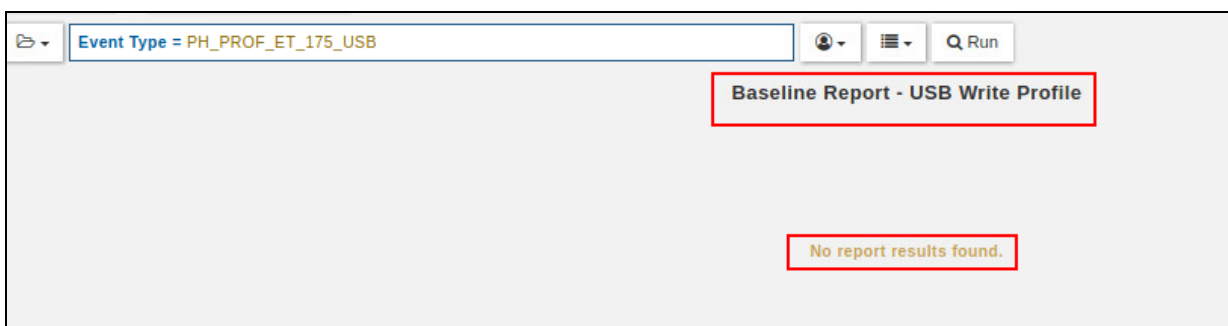
1. Return to the FortiSIEM GUI, and click **RESOURCES**.
2. In the left navigation pane, expand **Reports**, and then click **Baseline**.
3. In the **Global** drop-down list, select **Super/Local**.



The baseline report was created for the super organization. You can see this in the **customer ID**, which is set to 1. This means that this report is for those assets that belong to the super organization.

4. In the search field, type `USB Write Profile`.
5. Select **USB Write Profile**, and then click **Run**.

No report results found is displayed.



This is expected behavior since this baseline report reads from the profile DB, which only updates at midnight and currently contains no data.

6. Log out of the Supervisor FortiSIEM management GUI.

Exercise 4: Verifying the Baseline Report

In this exercise, you will verify the baseline report.

Verify the Baseline Report

Now, you will verify the baseline report that you created in the previous exercise. You will also view the profile table that was created in the daily DB.

To verify the baseline report

1. Go to the Local-Host VM.
2. Open a terminal window (Ctrl + Alt + T).
3. Type the following command to open an SSH connection to the FortiSIEM supervisor:
`ssh root@10.0.1.130`
4. Type the password `Fortinet1!`.
5. Type the following command:

```
cat /opt/phoenix/data-definition/profile/ProfileReports.xml
```

The new profile report is displayed.

```
<DataRequest id="175" type="Report" profileId="PH_PROF_ET_175_USB" numRows="1000">
  <Name>USB Lab - Writes By Critical Servers</Name>
  <Description></Description>
  <CustomerScope groupByEachCustomer="true">
    <Include all="true"/>
    <Exclude/>
  </CustomerScope>
  <SelectClause numRows="ALL">
    <AttrList>reptDevIpAddr, reptDevName, diskName, hwDiskModel, user, COUNT(*), COUNT(DISTINCT fileName)</AttrList>
  </SelectClause>
  <OrderByClause>
    <AttrList>COUNT(DISTINCT fileName) DESC</AttrList>
  </OrderByClause>
  <ReportInterval><Window unit="Hourly" val="1"/></ReportInterval>
  <PatternClause window="3600">
    <SubPattern displayName="Filter_1" name="Filter_1">
      <SingleEvtConstr>eventtype = "AD-WUA-RemovableMedia-AddFile" AND reptDevIpAddr IN (10.0.1.1,10.0.1.5,10.0.1.9)</SingleEvtConstr>
    </SubPattern>
    <GroupByAttr>reptDevIpAddr, reptDevName, diskName, hwDiskModel, user</GroupByAttr>
  </PatternClause>
</DataRequest>
```

6. Type the following commands to see the profile table that was created in the daily DB:

```
sqlite3 /opt/phoenix/cache/daily.db
.tables
```

You should see a profile table for `profile_175`.

```
[root@super 8_2]# sqlite3 /opt/phoenix/cache/daily.db
SQLite version 3.8.1 2013-10-17 12:57:35
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
profile_104  profile_109  profile_114  profile_119  profile_125  profile_130
profile_105  profile_110  profile_115  profile_120  profile_126  profile_175
profile_106  profile_111  profile_116  profile_121  profile_127
profile_107  profile_112  profile_117  profile_122  profile_128
profile_108  profile_113  profile_118  profile_123  profile_129
```

7. Type the following command to quit the SQLite prompt:

```
.quit
```

Leave the SSH session running in the background. You will return to it later.

Run the Script to Replay USB Events

Now, you will run the script to replay USB events.

To run the script to replay USB events

1. On the Local-Host VM, open another terminal window (Ctrl + Alt + T).
2. Type the following command to change the working directory:

```
cd Desktop/Resource/Lab/lab8/8_4
```

3. Type the following command to run the script:

```
sudo ./runLab8_4.sh
```

```
student@linux:~$ cd Desktop/Resource/Lab/lab8/
student@linux:~/Desktop/Resource/Lab/lab8$ ls
8_2  8_4
student@linux:~/Desktop/Resource/Lab/lab8$ cd 8_4
student@linux:~/Desktop/Resource/Lab/lab8/8_4$ ls
baselineDataTracker.sh  results.txt  sql  updateProfiledb.sh
events                  runLab8_4.sh  updateDailydb.sh
student@linux:~/Desktop/Resource/Lab/lab8/8_4$ sudo ./runLab8_4.sh
```

4. Type the password `password`.
Wait for the **All Done!** message.

Update the Daily and Profile Databases

The daily database values are populated in the profile database at midnight, and the daily database is purged to prepare for the next day's values. Since data is being written hourly, and then again at midnight, you need to simulate this data. You will simulate this process by running a script to inject data into the daily and profile databases.

To update the daily databases from Supervisor

1. Return to the terminal window connected to the FortiSIEM supervisor, and type the following command to change the working directory:

```
cd Lab/lab8/8_4
```

2. Type the following command to run the script:

```
./updateDailydb.sh
```

```
[root@supervisor 8_4]# pwd
/root/Lab/lab8/8_4
[root@supervisor 8_4]# ls
baselineDataTracker.sh  results.txt  sql  updateProfiledb.sh
events                  runLab8_4.sh  updateDailydb.sh
[root@supervisor 8_4]#
[root@supervisor 8_4]# ./updateDailydb.sh
```

Wait for the **All Done!** message.

3. Type the following commands to query the daily DB for stored data:

```
sqlite3 /opt/phoenix/cache/daily.db
.headers on
select * from profile_175;
```

The table data is displayed.

```
sqlite> .headers on
sqlite> select * from profile_175;
custId|profDateType|hourOfDay|replDevTpAddr|replDevName|diskName|hwDiskModel|user|minDistinctFileName|maxDistinctFileName|avgDistinctFileName|s
devDistinctFileName|minMatchedEvents|maxMatchedEvents|avgMatchedEvents|sdevMatchedEvents|minPoints
1|1|9|10.0.1.1|ServerA|E|CruzerBlade 128|Jimmy.Jones|5|5|0.0|9|9|0.0|1
1|1|11|10.0.1.1|ServerA|E|CruzerBlade 128|Jimmy.Jones|2|2|2.0|0.0|2|2|0.0|1
1|1|16|10.0.1.1|ServerA|E|CruzerBlade 128|Jimmy.Jones|3|3|3.0|0.0|4|4|0.0|1
1|1|12|10.0.1.1|ServerB|E|UltraDisk 32|Dan.Smith|3|3|0.0|3|3|0.0|1
1|1|17|10.0.1.1|ServerB|E|UltraDisk 32|Dusan.Nandos|1|1|1.0|0.0|1|1|0.0|1
1|1|8|10.0.1.9|ServerC|E|DataTraveller 8|Wendy.Anderson|2|2|2.0|0.0|2|2|0.0|1
1|1|19|10.0.1.9|ServerC|E|CruzerBlade 32|administrator|1|1|1.0|0.0|1|1|0.0|1
sqlite>
```

4. Review the data.
5. Type the following command to exit SQLite:

```
.quit
```

To update profile database from Supervisor

1. Continuing on the terminal window connected to the FortiSIEM supervisor, type the following commands:

```
./updateProfiledb.sh
```

```
[root@supervisor 8_4]# pwd
/root/Lab/lab8/8_4
[root@supervisor 8_4]# ls
baselineDataTracker.sh  results.txt  sql  updateProfiledb.sh
events                  runLab8_4.sh  updateDailydb.sh
[root@supervisor 8_4]#
[root@supervisor 8_4]# ./updateProfiledb.sh
```

This script simulates the daily DB data being merged at midnight with the profile DB. Wait for the **All Done!** message.

2. Type `exit` to quit the SSH session.
3. Close the terminal windows.
4. Close the Local-Host VM browser tab.

Run the Baseline Report

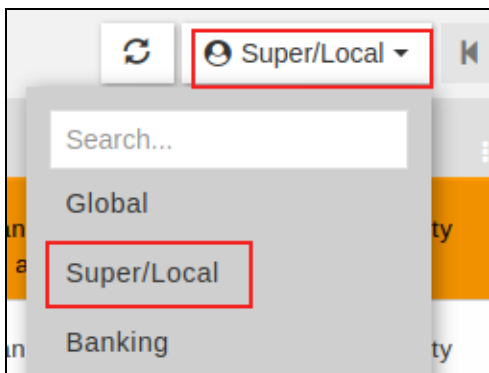
Now that the data is available in the profile database, you can run a baseline report to view the baseline data values that are calculated and stored in the profile database.

To run the baseline report

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **RESOURCES**.
4. In the **Global** drop-down list, select **Super/Local**.



5. In the left navigation pane, expand **Reports**, and then click **Baseline**.
6. Select the **USB Write Profile** report, and then click **Run**.

Your output should match the following example:

Baseline Report - USB Write Profile									
Profile Date Type	Hour Of Day	Reporting IP	Reporting Device	Disk Name	Disk Model	User	Avg Distinct File Name	Std Dev Distinct File Name	Std Dev Matched Events
1 (Week Day)	8	10.0.1.8	ServerA	E:	DATA/Model 0	Wendy Anderson	2	0	0
1 (Week Day)	9	10.0.1.1	ServerA	E:	CruzerBlade 128	Jimmy Jones	5	0	0
1 (Week Day)	11	10.0.1.1	ServerA	E:	CruzerBlade 128	Jimmy Jones	2	0	0
1 (Week Day)	12	10.0.1.5	ServerB	E:	UltraDisk 32	Dan Smith	3	0	0
1 (Week Day)	16	10.0.1.1	ServerA	E:	CruzerBlade 128	Jimmy Jones	3	0	4
1 (Week Day)	17	10.0.1.5	ServerB	E:	UltraDisk 32	Dan Smith	1	0	1
1 (Week Day)	19	10.0.1.9	ServerC	E:	CruzerBlade 32	administrator	1	0	1

7. Select one of the **ServerA** rows.
8. Click the down arrow icon (▼) in the **Reporting Device** column, and in the drop-down list, select **Add To Filter**.

9. Select =.

Reporting Device	Disk Name	Disk Model
ServerC	E:	DataTraveller 8
ServerA	E:	CruzerBlade 128
ServerA	E:	CruzerBlade 128
ServerB		
ServerA		
ServerB		
ServerC	E:	

10. Find the user **Jimmy.Jones**, click the down arrow icon (▼) in the **User** column, and in the drop-down list, select **Add To Filter**.

11. Select =.

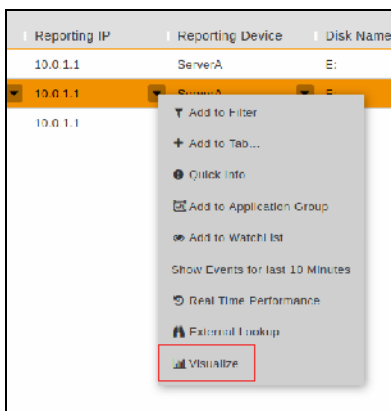
User	Avg Distinct File Name	Std Dev Distinct File Name
Wendy.Anderson	2	0
Jimmy.Jones	5	0
Jimmy.Jones		
Dan.Smith		
Jimmy.Jones		
Dusan.Nandos		
administrator		

12. Click **Run**.

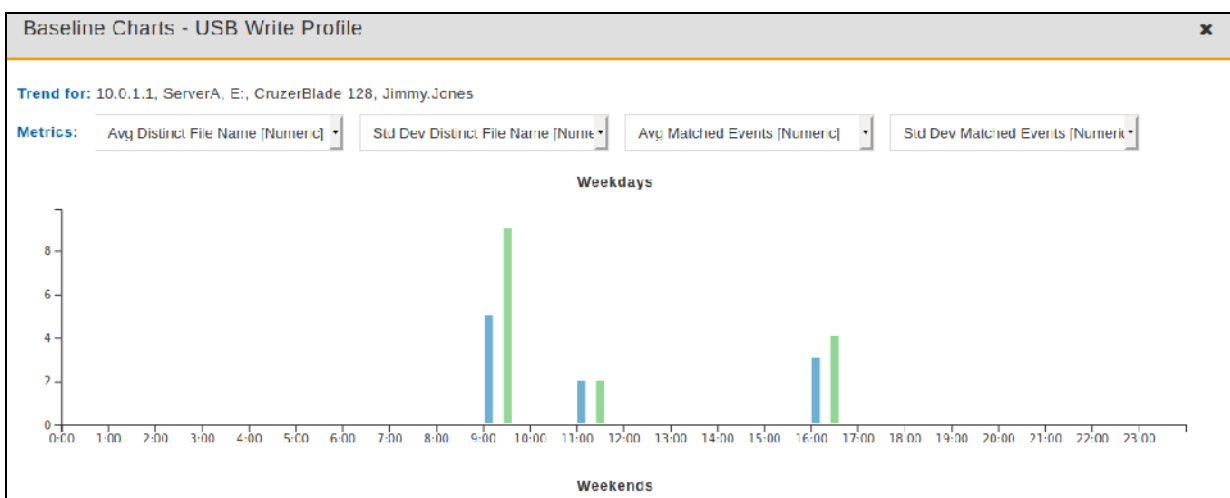
The filtered results are displayed.

*Baseline Report - USB Write Profile											
Profile Date	Type	Hour Of Day	Reporting IP	Reporting Device	Disk Name	Disk Model	User	Avg Distinct File Name	Std Dev Distinct File Name	Avg Matched Events	Std Dev Matched Events
1 (Work Day)		9	10.0.1.1	ServerA	E:	CruzerBlade 128	Jimmy.Jones	0	0	0	0
1 (Work Day)		11	10.0.1.1	ServerA	E:	CruzerBlade 128	Jimmy.Jones	2	0	2	0
1 (Work Day)		15	10.0.1.1	ServerA	E:	CruzerBlade 128	Jimmy.Jones	3	0	4	0

13. Select any of the **Reporting IP** addresses, click the down arrow icon (▼), and then select **Visualize**.



The baseline chart is displayed.



Since there is only one data point so far, the standard deviation values are 0, so not all values are plotted. You can see only the **Average Distinct File Names** and **Average Matched Events** for each hour of the day for **ServerA** and the user **Jimmy.Jones**.

14. Click **Close**.
15. Log out of the Supervisor FortiSIEM management GUI.

Lab 9: Configuration of Baseline Rules

In this lab, you will create a baseline rule.

Objectives

- Prepare FortiSIEM for a baseline rule
- Build a baseline rule
- Trigger the new baseline rule

Time to Complete

Estimated: 30 minutes

Exercise 1: Building a Baseline Rule

In this exercise, you will build a new baseline rule to detect if there is an anomaly in the number of distinct filenames being written to USB by the same user.

Build a Baseline Rule

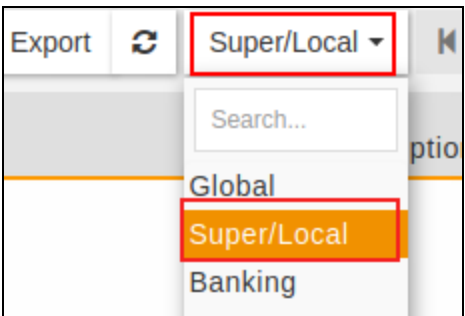
Now, you will create a new baseline rule to detect if there is an anomaly in the number of distinct filenames being written to USB by the same user. You will create aggregation conditions to analyze if a distinct filename is more than three standard deviations away from the mean for the current hour.

To build a baseline rule

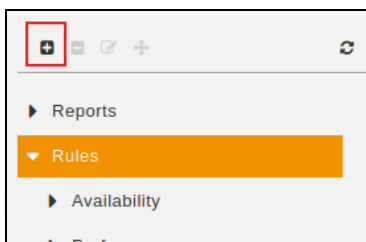
1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

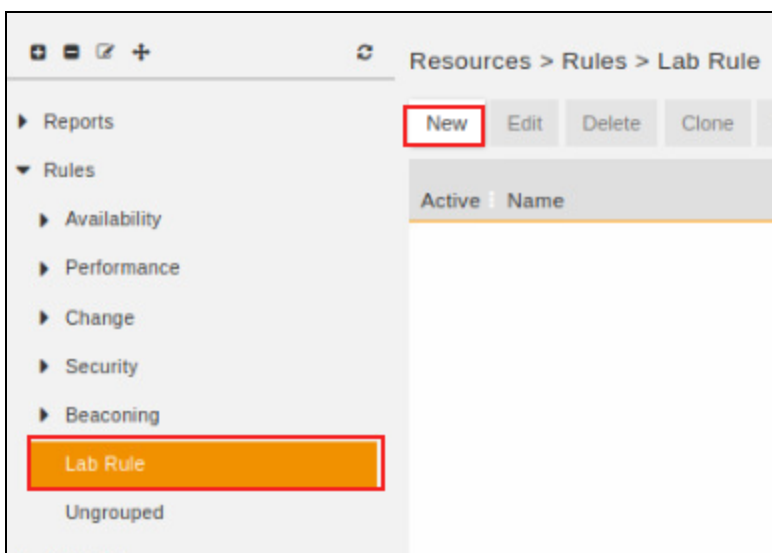
3. Click **LOGIN**.
4. Click **RESOURCES**.
5. In the **Global** drop-down list, select **Super/Local**.



6. In the left navigation pane, click **Rules**.
7. Click the plus icon (+) to add a new rules group.



8. In the **Group** field, type Lab Rule.
9. Click **Save**.
10. In the left navigation pane, expand **Rules**, and then click **Lab Rule**.
11. Click **New**.



12. In the **Rule Name** field, type Sudden Increase in File Transfers to USB.
13. In the **Description** field, type Detects an anomaly in the number of distinct filenames being written to USB by the same user if more than 3 standard deviations away from the mean for the current hour.
14. Click **Step 2: Define Condition**.
15. Click the pencil icon (✎) to edit the **Subpattern**.
16. Configure the following **Filters**:

Attribute	Operator	Value	Next
Event Type	=	AO-WUA-RemovableMedia-AddFile	AND
Reporting IP	IN	10.0.1.1,10.0.1.5,10.0.1.9	

17. Configure the following **Group By** attributes:
 - Reporting IP
 - Reporting Device
 - Disk Name

- Disk Model
- User

Leave the rule editor open,

- Go to the Local-Host VM.
- Open a terminal window (Ctrl + Alt + T).
- Type the following command to open an SSH connection to the FortiSIEM supervisor:

```
ssh root@10.0.1.130
```

- Type the password Fortinet1!.
- Type the following command to change the working directory:

```
cd /root/Lab/lab9/9_1
```

- Type the following commands

```
[root@supervisor 9_1]# pwd
/root/Lab/lab9/9_1
[root@supervisor 9_1]# ls
baselineRuleHelper.sh ruleUpload.sh usb rule.xml
[root@supervisor 9_1]# ./baselineRuleHelper.sh
```

- For the **profile ID**, type 175, and then press **Enter**.

```
*****
Rule Functions for COUNT(DISTINCT fileName)
*****
Statistical Average: STAT_AVG(COUNT(DISTINCT File Name):175)
Statistical Standard Deviation: STAT_STDDEV(COUNT(DISTINCT File Name):175)

Option 1 : 50% LESS than the Statistical Average for COUNT(DISTINCT fileName)
Attribute      Operator  Value      Next Op
COUNT(DISTINCT File Name) <= 0.5*STAT_AVG(COUNT(DISTINCT File Name):175)

Option 2 : 25% MORE than the Statistical Average for COUNT(DISTINCT fileName)
Attribute      Operator  Value      Next Op
COUNT(DISTINCT File Name) >= 1.25*STAT_AVG(COUNT(DISTINCT File Name):175)

Option 3 : 50% MORE than the Statistical Average for COUNT(DISTINCT fileName)
Attribute      Operator  Value      Next Op
COUNT(DISTINCT File Name) >= 1.5*STAT_AVG(COUNT(DISTINCT File Name):175)

Option 4 : 75% MORE than the Statistical Average for COUNT(DISTINCT fileName)
Attribute      Operator  Value      Next Op
COUNT(DISTINCT File Name) >= 1.75*STAT_AVG(COUNT(DISTINCT File Name):175)

Option 5 : Twice (ie:100% MORE than) the Statistical Average for COUNT(DISTINCT fileName)
Attribute      Operator  Value      Next Op
COUNT(DISTINCT File Name) >= 2*STAT_AVG(COUNT(DISTINCT File Name):175)

Option 6 : MORE than 3 standard Deviations Away from the Mean for COUNT(DISTINCT fileName)
Attribute      Operator  Value      Next Op
((COUNT(DISTINCT File Name)-STAT_AVG(COUNT(DISTINCT File Name):175))/STAT_STDDEV(COUNT(DISTINCT File Name):175) >= 3 AND
STAT_STDDEV(COUNT(DISTINCT File Name):175) > 0

Option 7 : LESS than 3 standard Deviations Away from the Mean for COUNT(DISTINCT fileName)
Attribute      Operator  Value      Next Op
((COUNT(DISTINCT File Name)-STAT_AVG(COUNT(DISTINCT File Name):175))/STAT_STDDEV(COUNT(DISTINCT File Name):175) <= -3 AND
STAT_STDDEV(COUNT(DISTINCT File Name):175) > 0

*****
All Done!
```

The script will examine the defined profile report and return options for each aggregated field that can be entered in the rule definition.

The **Option 6** section for the **COUNT(DISTINCT fileName)** rule functions provides the aggregation function for the rule you are building.

- Select and copy the first **COUNT(DISTINCT fileName) Option 6** aggregate function.

```
(COUNT(DISTINCT File Name)-STAT_AVG(COUNT(DISTINCT File Name):175))/STAT_STDDEV(COUNT(DISTINCT File Name):175)
```

26. Return to the Supervisor FortiSIEM management GUI, and in the **Aggregate** section, in the **Attribute** drop-down list, select **Expression Builder**.

The screenshot shows the 'Aggregate' section of the FortiSIEM management GUI. It features two tables: 'Filters' and 'Aggregate'. The 'Aggregate' table has columns for 'Paren', 'Attribute', 'Operator', 'Value', 'Paren', 'Next', and 'Row'. The 'Attribute' dropdown in the second row is highlighted with a red box, and the 'Expression Builder' option is selected.

27. In the **Expression** field, paste the copied function.
28. Click **Validate**.
An **Expression is valid** message is displayed.

The screenshot shows the 'Expression Builder' pop-up window. It has fields for 'Expression', 'Function', 'Event Attribute', and 'CMDB Attribute'. The 'Expression' field contains the function 'IT(DISTINCT File Name)-STAT_AVG(COUNT(DISTINCT File Name):175)/STAT_STDDEV(COUNT(DISTINCT File Name):175)'. The 'Validate' button is highlighted with a red box, and a yellow message box displays 'Expression is valid.'

29. Close the pop-up window.
30. Click **OK**.
31. In the **Operator** drop-down list, select **>=**.
32. In the **Value** field, type **3**.
33. Click the **Add New Row** (+) to add a second **Aggregate** condition.
34. Return to the terminal window, and copy the second **COUNT(DISTINCT fileName) Option 6** aggregate function.
`STAT_STDDEV(COUNT(DISTINCT File Name):175)`
35. Return to the Supervisor FortiSIEM management GUI, and in the **Aggregate** section, in the **Attribute** drop-down list, in the second row, select **Expression Builder**.
36. In the **Expression** field, paste the copied function.
37. Click **Validate**.
An **Expression is valid** message is displayed.
38. Close the pop-up window.
39. Click **OK**.
40. In the **Operator** drop-down list, in the second row, select **>**.
41. In the **Value** field of the second row, type **0**.

Your configuration should match the following example:

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
		Event Type	=	O-WUA-RemovableMedia-AddFile		AND	
		Reporting IP	IN	10.0.1.1, 10.0.1.5, 10.0.1.9		AND	

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
		(COUNT DISTINCT(File Name)-S1	>=	3		AND	
		STAT_STDDEV(COUNT DISTINC'	>	0		AND	

Group By:	Attribute	Row	Move
	Reporting IP		
	Reporting Device		
	Disk Name		
	Disk Model		
	User		

42. Click **Save**.
43. Click **Step 3: Define Action**.
44. Configure the following values:

Event attribute	Filter attribute
Category	Security
Subcategory	Behavioral Anomaly

45. Click the pencil icon () to edit the **Action** setting.
46. Configure the following **Incident Attributes**:

Event attribute	Subpattern	Filter attribute
Host IP	filter_0	Reporting IP
Host Name	filter_0	Reporting Device
Avg Distinct File Name	filter_0	STAT_AVG(COUNT(DISTINCT File Name):175)
Std Dev Distinct File Name	filter_0	STAT_STDDEV(COUNT(DISTINCT File Name):175)
Count	filter_0	COUNT(DISTINCT File Name)

47. Add the following **Triggered Attributes**:
 - **Reporting Device**
 - **Disk Name**
 - **Disk Model**
 - **User**
43. Remove the following **Triggered Attributes**:

- **Reporting IP**
 - **Raw Event Log**
44. Use the move icons (⤴ and ⤵) to rearrange the attributes to match the following order:
- **Event Receive Time**
 - **Event Type**
 - **Reporting Device**
 - **Disk Name**
 - **Disk Model**
 - **User**
45. Click **Save**.
46. Click **Save**.
47. Click the checkbox to activate your baseline rule.



48. Click **Continue**.
49. Log out of the Supervisor FortiSIEM management GUI.
50. Return to the Local-Host VM, and close the terminal window.
51. Close the Local-Host VM browser tab.

Exercise 2: Preparing FortiSIEM for a Baseline Rule

In this exercise, you will update the numpoints data in the profile database.

Update the Profile Database

The numpoints value in the profile database plays an important role when rules evaluate any attribute. The importance of the numpoint value is to avoid premature triggering of a rule before a baseline is set and becomes active. The rules engine will therefore only fetch values from the profile database that have a numpoints value equal to 2 or more.

You will run a script to manipulate the numpoint value so that you can use it in the baseline rule.

To update numpoint on Profile database

1. Go to the Local-Host VM.
2. Open a terminal window (Ctrl + Alt + T).
3. Type the following command to open an SSH connection to the FortiSIEM supervisor:

```
ssh root@10.0.1.130
```

4. Type the password Fortinet1!.
5. Type the following command to change your working directory:
6. Type the following command to run the script:

```
cd /root/Lab/lab9/9_2
```

```
./updateProfiledbRules.sh
```

```
[root@supervisor 9_2]# pwd
/root/Lab/lab9/9_2
[root@supervisor 9_2]# ls
sql updateProfiledbRules.sh
[root@supervisor 9_2]# ./updateProfiledbRules.sh
```

The script updates the profile DB with some up-to-date values, including updating the **numPoints** value to be greater than 2, so the data will be available for the rules engine.

7. Review the output on the screen.

```
Now displaying the updated contents of the Profile DB, for user Jimmy Jones

custId|profDateType|hourOfDay|reptDevIpAddr|reptDevName|diskName|hwDiskModel|user|minDistinctFileName
devDistinctFileName|minMatchedEvents|maxMatchedEvents|avgMatchedEvents|sdevMatchedEvents|numPoints
1|1|9|10.0.1.1|ServerA|E:|CruzerBlade 128|Jimmy.Jones|5|5|5.0|0.0|9|9|9.0|0.0|1
1|1|11|10.0.1.1|ServerA|E:|CruzerBlade 128|Jimmy.Jones|2|2|2.0|0.0|2|2|2.0|0.0|1
1|1|14|10.0.1.1|ServerA|E:|CruzerBlade 128|Jimmy.Jones|5|5|5.0|0.5|9|9|9.0|0.5|3
1|1|15|10.0.1.1|ServerA|E:|CruzerBlade 128|Jimmy.Jones|5|5|5.0|0.5|9|9|9.0|0.5|3
1|1|16|10.0.1.1|ServerA|E:|CruzerBlade 128|Jimmy.Jones|3|3|3.0|0.0|4|4|4.0|0.0|1

Killing backend Rule Processes...
Waiting for Processes to Restart.....

All Done!
```

From the profile DB output, you will see that for the current **Hour of Day**, for the user **Jimmy.Jones**, the **numPoints** value has been increased to **3**.



Do not close the SSH session to the supervisor. Continue to the next exercise.

Exercise 3: Triggering a Baseline Rule

In this exercise, you will trigger the new baseline rule that you created in the previous exercise.

Trigger a Baseline Rule

Now, you will set up the conditions to trigger the baseline rule that you created in the previous exercise. You will send 32 USB events to the supervisor node.

To restart the process on FortiSIEM

1. Go to the Local-Host VM.
2. Open a terminal window (Ctrl + Alt + T).
3. Type the following command to open an SSH connection to the FortiSIEM supervisor:
`ssh root@10.0.1.130`
4. Type the password `Fortinet1!`.
5. Type `phstatus`.
The FortiSIEM processes are displayed. Keep the terminal window open.
6. Open another terminal window (Ctrl + Alt + T), and then type the following command to open another SSH connection to the FortiSIEM supervisor:
`ssh root@10.0.1.130`
7. Type the password `Fortinet1!`.
8. Type the following command to change your working directory:
`cd /root/Lab/lab9/9_3`
9. Type the following command to run the script that will restart all supervisor processes:

```
./processrestart.sh  
[root@supervisor 9_3]# pwd  
/root/Lab/lab9/9_3  
[root@supervisor 9_3]# ls  
events processrestart.sh runLab9_3.sh verifyRuleData.sh  
[root@supervisor 9_3]# ./processrestart.sh
```

Wait for the **All Done!** message. You can monitor the process status in the previous terminal window.



Wait until all processes are started. Do not proceed to the next section before that.

To run the script to replay USB events

1. Continuing on the Local-Host VM, open another terminal window (Ctrl + Alt + T).
2. Type the following command to change your working directory:
`cd Desktop/Resource/Lab/lab9/9_3`
3. Type the following command to start the script:
`sudo ./runLab9_3.sh`

```
student@linux:~/Desktop/Resource/Lab/lab9/9_3$ ls
events runLab9_3.sh verifyRuleData.sh
student@linux:~/Desktop/Resource/Lab/lab9/9_3$ sudo ./runLab9_3.sh
```

4. Type the password `password`.
Wait for the **All Done!** message.

Verify the Incident on FortiSIEM

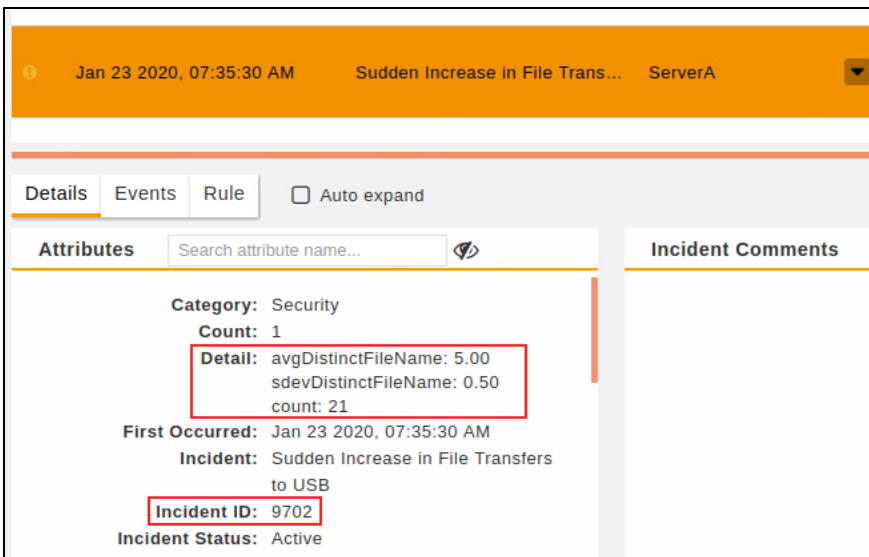
Now, you will verify the incident that was generated by the baseline rule. You will verify the incident on the GUI and CLI, using a script. The aggregation calculation is not shown in the incident details on the GUI—only the individual component scores are shown. The script displays the aggregation calculation in the CLI.

To verify the incident on the FortiSIEM GUI

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOG IN**.
4. Click **INCIDENT**.
5. In the **Top Incidents** section, click the **Sudden Increase in File Transfers to USB** widget.
6. Select the incident, and then click **Details**.
7. Review the incident details and triggering events, and then note the **Incident ID**.
In the following example, the **Incident ID** is 9702. Your **Incident ID** may be different.



To verify the incident on the FortiSIEM CLI

1. Return to the terminal window connected to the FortiSIEM supervisor, and type the following command to change your working directory:

```
cd /root/Lab/lab9/9_3
```

2. Type the following command to verify the incident:

```
./verifyRuleData.sh
```

```
[root@supervisor 9_3]# pwd
/root/Lab/lab9/9_3
[root@supervisor 9_3]# ls
events  processrestart.sh  runLab9 3.sh  verifyRuleData.sh
[root@supervisor 9_3]# ./verifyRuleData.sh
```

Enter your incident ID when prompted.

The script queries the incident details and returns exactly why the rule was triggered.

```
VERIFY  
RULE  
DATA  
(c) Fortinet Training 2019  
What is the Incident ID ? :  
9702  
Baseline Rule Aggregation Results.....  
Standard Deviations Away from the Mean is : 32.00  
Baseline Rule Data.....  
Actual Distinct File Names in the events that matched the rule subpattern filter, Count: 21  
-Statistical Average Distinct File Name for the Hour of Day 15 for device 10.0.0.1: 5.00  
Statistical Standard Deviation of Distinct File Names for the Hour of Day 15 : 0.50  
Calculated By.....  
Standard Deviations Away from the Mean (zScore) is : (Actual - Statistical Average)/Statistical Standard  
Deviation  
= (21 - 5.00) / 0.50 = 32.00  
Rule Triggers since the zScore is > 3  
All Done!
```

3. Close all terminal windows.
4. Close Firefox.

Lab 10: UEBA

In this lab, you will build an AI model on FortiSIEM and generate anomaly events to trigger UEBA rules. You will then analyze the UEBA incidents.

Objectives

- Build a UEBA AI model
- Generate a UEBA anomaly event
- Analyze a UEBA incident
- Analyze UEBA dashboards and widgets

Time to Complete

Estimated: 30 minutes

Exercise 1: Building a UEBA AI Model

In this exercise, you will build an AI model on FortiSIEM using a script.

Train the AI Engine

You will train the AI engine with simulated logs.



Do not run this script on a production machine or in a customer POC.

To replace the ai.properties file

1. On the Local-Host VM, open a terminal window (Ctrl+Alt+T).
2. Enter the following command to open an SSH connection to the FortiSIEM supervisor:
`ssh root@10.0.1.130`
3. Enter the password `Fortinet1!`.
4. Enter the following command to verify your working directory—it should be `/root`:
`pwd`
5. Enter the following command, and then verify that the highlighted file is available:
`ls -lrt`

```
[root@super ~]# ls -lrt
total 58628
drwxr-xr-x  2 root root      69 Feb 21  2020 fixes
drwxr-xr-x  8 root root     91 Feb 21  2020 incidentSimData
drwxr-xr-x  2 root root     68 Nov 22  2020 fsmUebaDemo
drwxrwxr-x  4 root root     30 May 28 14:34 Lab
-rw-----  1 root root    971 Jul  1 19:34 original-ks.cfg
-rw-----  1 root root   1610 Jul  1 19:34 anaconda-ks.cfg
-rw-r--r--  1 root root 59760640 Jul  1 19:34 VBoxGuestAdditions.iso
-rwxr-xr-x  1 root root    485 Jul  1 19:36 zerofill.sh
-rwxr-xr-x  1 root root   61454 Jul 13 20:48 fsmIncidentSimulator2_4.sh
-rw-r--r--  1 root root   91316 Jul 13 20:52 fsmIncidentSim.zip
-rw-r--r--  1 root root    7037 Jul 13 20:52 fsmUebaDemo.zip
-rw-r--r--  1 root root   58587 Jul 13 20:57 Lab.zip
-rw-r--r--  1 root root    840 Jul 14 10:04 security_incident
-rw-r--r--  1 root root    3460 Jul 14 10:04 security_sysmon_incident
-rw-r--r--  1 root root    1427 Jul 14 10:04 security_user_incident
-rw-r--r--  1 root root   16510 Jul 26 14:32 incidentSimLog.log
[root@super ~]#
```

6. Enter the following command to navigate to the `fsmUebaDemo` directory:
`cd fsmUebaDemo`
7. Enter the following command to replace the default `ai.properties` file with the included example:
`cp ai.properties /opt/fortiinsight-ai/bin/config/ai.properties`
8. Type `y` to confirm the overwrite.
9. Enter the following command to change the owner of the new `ai.properties` file:
`chown admin:admin /opt/fortiinsight-ai/bin/config/ai.properties`
10. Enter the following command to identify the `phFortiInsightAI` process ID (PID):

```
ps -edf | grep Insight
```

In the following example, the PID is 1096. The PID will be different in your environment.

```
[root@super fsmUebaDemo]# ps -edf | grep Insight
admin    1096      1  0 Jul14  ?        00:28:36 phFortiInsightAI -classpath /opt/fortiinsight-ai/lib/* -Xmx8192M com.zonefox.ai.AI
root     1642922 4036389  0 10:22 pts/1    00:00:00 grep --color=auto Insight
[root@super fsmUebaDemo]#
```

- Enter the following command to kill the process. Make sure you use the PID you retrieved in the previous step.

```
kill <PID>
```

The process restarts after a few minutes.

- After a few minutes, type the following command, and then verify that the `phFortiInsightAI` service has started again:

```
phstatus
```

```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime: 10:26:32 up 12 days, 23:45, 2 users, load average: 0.97, 1.39, 1.61
Tasks: 28 total, 0 running, 28 sleeping, 0 stopped, 0 zombie
Cpu(s): 4 cores, 1.7%us, 1.0%sy, 0.0%ni, 95.4%id, 0.0%wa, 1.7%hi, 0.2%si, 0.0%st
Mem: 16212212k total, 11576756k used, 731176k free, 5248k buffers
Swap: 26058744k total, 0k used, 26058744k free, 4600388k cached
```

PROCESS	UPTIME	CPU%	VIRT_MEM	RES_MEM
phParser	12-23:42:07	0	2305m	1006m
phQueryMaster	3-17:41:36	0	1103m	119m
phRuleMaster	3-17:41:21	0	1561m	656m
phRuleWorker	3-17:41:16	0	1559m	337m
phQueryWorker	3-17:41:36	0	1463m	174m
phDataManager	12-23:42:25	0	1519m	547m
phDiscover	12-23:42:25	0	569m	62m
phReportWorker	3-17:41:01	0	1456m	264m
phReportMaster	3-17:41:00	0	720m	61m
phIpIdentityWorker	12-23:42:25	0	1044m	275m
phIpIdentityMaster	12-23:42:25	0	515m	45m
phAgentManager	12-23:42:25	0	1537m	65m
phCheckpoint	12-23:42:24	0	309m	39m
phPerfMonitor	12-23:42:24	0	830m	85m
phReportLoader	12-23:42:25	0	815m	310m
phDataPurger	12-23:42:25	0	1151m	597m
phEventForwarder	12-23:42:25	0	537m	41m
phMonitor	4-22:51:18	0	1317m	127m
Apache	12-23:45:19	0	307m	17m
Rsyslogd	12-23:45:20	0	192m	5148k
Node.js-charting	12-23:45:13	0	613m	81m
Node.js-pm2	12-23:45:12	0	875m	63m
phFortiInsightAI	00:32	0	11926m	200m
AppSvr	12-23:45:09	0	9096m	4253m
DBSvr	12-23:45:21	0	425m	37m
phAnomaly	12-23:42:28	0	727m	61m
SVNLite	12-23:45:21	0	7532m	709m
Redis	12-23:45:13	0	209m	110m

- Type `Ctrl+C` to return to the command line.

To train the AI model

- Continuing on the SSH session, enter the following command to view the script run options:

```
./fsmUebaDemo.php
```

```
[root@super fsmUebaDemo]# ./fsmUebaDemo.php

Usage:
  -t Train the engine with simulated logs
  -m Monitor stats with 10s refresh
  -l Display AI engine logs
  -s Send demo events
  -a Toggle active or training mode
[root@super fsmUebaDemo]#
```

2. Type the following command to train the model:

```
./fsmUebaDemo.php -t
```



The process will take 10–20 minutes.

3. Type 1 to change the AI engine to Active Detection mode:

```
== Training completed on 50000 events ==

Time                Status      Events  Users  Mem Total  Mem Free  Warn
=====
14:40:34 2021-07-27  training  49782   201     487587840  212640312

== Old AI Engine State ==
Status: training

[1] Change to Active Detection Mode
[2] Change to Training Mode
Any other key to quit

Enter Option: 1

== Current AI Engine State ==
Status: ad
```

4. Close the SSH session browser tab.

Exercise 2: Running the UEBA Demo

In this exercise, you will trigger anomalies based on previous pattern behavior by sending events that the AI engine has not seen before.

Run the UEBA Demo

You will send 50 regular logs to FortiSIEM. In the 50 log set, there are a few logs that will trigger anomalies.

To run the demo

1. On the Local-Host VM, open a terminal window (Ctrl+Alt+T).
2. Enter the following command to open an SSH connection to the FortiSIEM supervisor:
`ssh root@10.0.1.130`
3. Enter the password `Fortinet1!`.
4. Enter the following command to navigate to the `fsmUebaDemo` directory:
`cd fsmUebaDemo`
5. Enter the following command to send the logs:
`./fsmUebaDemo.php -s`

```
[root@super fsmUebaDemo]# ls
ai.properties fsmUebaDemo.php readmc.txt userDB.json
[root@super fsmUebaDemo]# ./fsmUebaDemo.php

Usage:
  -t Train the engine with simulated logs
  -m Monitor stats with 10s refresh
  -l Display AI engine logs
  -s Send demo events
  -a Toggle active or training mode
[root@super fsmUebaDemo]# ./fsmUebaDemo.php -s

== Sent 50 normal logs ==
Sent 50 logs based on previous user activity. File upload logs should be the only trigger due to the random upload destination

== New Process Usage ==
Sending previously unseen process nc.exe to user fortipoc__tp3281 on machine corp-np-19

== Unusual Machine Login ==
User fortipoc__vw2113 logs in to host corp-mo-51 which is not their regular machine

== Unusual File Upload ==
User fortipoc__vw2113 uploads unusual file c:\\unusualFiles614\\0777d94e.csv to 68.196.96.176

== Unusual Time of Day ==
Sending regular process nspaint.exe to user fortipoc__xd2226 on machine corp-on-63 at 02.30am

== Power User Processes Used by Regular User ==
Sent power user process events for this regular user:
  User : fortipoc__jy2796
  Host : corp-fg-25
These processes have not been previously seen for this user
```

6. Close the SSH session browser tab.

Exercise 3: Reviewing UEBA Incidents

In this exercise, you will review the UEBA incidents generated by the UEBA rules.

Review the UEBA Incidents

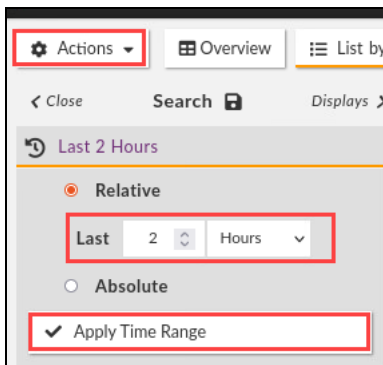
You will review the incidents generated by the AI engine.

To review the UEBA incidents

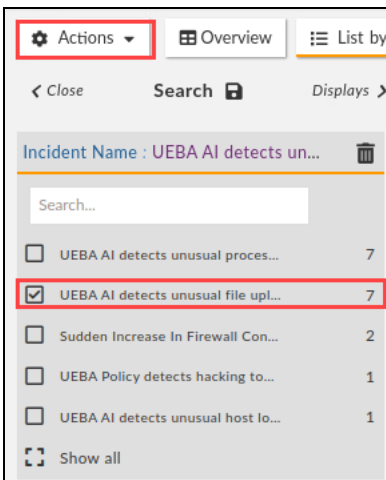
1. On the supervisor FortiSIEM GUI, log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

2. Click **LOG IN**.
3. Click **INCIDENTS**.
4. Select **List by Time**.
5. In the left navigation pane, click **Actions > Search**.
6. Search for all incidents for the last 2 hours, and then click **Apply Time Range**.



7. Filter the results by **Incident Name**, using the string **UEBA AI detects unusual file upload**.



Do not close the **Action** menu. You will search through different UEBA AI incidents in this exercise.

8. Review the UEBA AI detects unusual file upload incident.

Severity Category	Last Occurred	Incident	Detail	Target
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual file upload	Process Name: explorer.exe Activity Name: file_uploaded Resource Name: c:\files\d1030ba9.txt -> https://132.127.26.48	corp-ks-62 Domain: fortipoc User: j37149
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual file upload	Process Name: explorer.exe Activity Name: file_uploaded Resource Name: c:\files\d80621dc.txt -> https://13.75.167.205	corp-gm-96 Domain: fortipoc User: xu7321
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual file upload	Process Name: explorer.exe Activity Name: file_uploaded Resource Name: c:\files\9c1234a5.txt -> https://10.11.20.213	corp-sb-15 Domain: fortipoc User: gf7461
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual file upload	Process Name: explorer.exe Activity Name: file_uploaded Resource Name: c:\unusualFiles614\0777d94e.csv -> https://68...	corp-mo-62 Domain: fortipoc User: vw2113
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual file upload	Process Name: explorer.exe Activity Name: file_uploaded Resource Name: c:\files\bc0d9a99.txt -> https://144.41.166.65	corp-zy-29 Domain: fortipoc User: zk3731
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual file upload	Process Name: explorer.exe Activity Name: file_uploaded Resource Name: c:\files\fa1b263a.txt -> https://27.155.11.121	corp-zz-61 Domain: fortipoc User: gl4789
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual file upload	Process Name: explorer.exe Activity Name: file_uploaded Resource Name: c:\files\6b53c1d2.txt -> https://18.13.165.95	corp-nu-68 Domain: fortipoc User: rh5349

Seven different incidents were triggered for the same rule. Different types of unusual files were uploaded by different users.

9. In the filter section, clear the **UEBA AI detects unusual file upload** checkbox.
10. In the filter section, select the **UEBA AI detects unusual process created** checkbox.
11. Review the **UEBA AI detects unusual process created** incident.

SHBOARD ANALYTICS INCIDENTS CASES CMD3 RESOURCES TASKS ADMIN				
Time	Risk	Let Explorer	UEBA	MITRE ATT&CKR
All Incidents. Filters Applied				
Severity Category	Last Occurred	Incident	Detail	Target
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual process created	Process Name: dns.exe Activity Name: new process created Resource Name: c:\windows\system32\dns.exe	corp-fg-25 Domain: fortipoc User: j2796
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual process created	Process Name: powershell.exe Activity Name: new process created Resource Name: c:\windows\system32\windowspowershell\v1.0\...	corp-fg-25 Domain: fortipoc User: j2796
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual process created	Process Name: msaccess.exe Activity Name: new process created Resource Name: c:\program files\microsoft office\root\office16\...	corp-fg-25 Domain: fortipoc User: j2796
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual process created	Process Name: perlmon.exe Activity Name: new process created Resource Name: c:\windows\system32\perlmon.exe	corp-fg-25 Domain: fortipoc User: j2796
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual process created	Process Name: nc.exe Tag Name: hack_tool Activity Name: new process created	corp-np-19 Domain: fortipoc User: tp3281
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual process created	Process Name: pscp.exe Activity Name: new process created Resource Name: c:\program files\putty\pscp.exe	corp-fg-25 Domain: fortipoc User: j2796
MEDIUM	Jul 27 2021, 11:03:30 AM	UEBA AI detects unusual process created	Process Name: notepad++.exe Activity Name: new process created Resource Name: c:\program files\notepad++\notepad++.exe	corp-fg-25 Domain: fortipoc User: j2796

Seven different incidents were triggered for the same rule. Different types of unusual processes were created by different users.

12. In the filter section, clear the **UEBA AI detects unusual process created** checkbox.
13. In the filter section, select the **UEBA Policy detects hacking tool usage** and **UEBA AI detects unusual host logon** checkboxes.

All Incidents. Filters Applied				
Severity Category	Last Occurred	Incident	Detail	Target
MEDIUM	Jul 27 2021, 11:01:00 AM	UEBA AI detects unusual host logon	Activity Name: user logged on	corp-mo-51 Domain: fortipoc User: vv2113
MEDIUM	Jul 27 2021, 11:01:00 AM	UEBA Policy detects hacking tool usage	Process Name: nc.exe Activity Name: new process created Resource Name: c:\program files\netcat\nc.exe	corp-np-19 Domain: fortipoc User: tp3201

One incident was generated because UEBA AI detected an unusual host logon activity. Another incident was generated because UEBA detected a user using a hacking tool.

14. Close the **Action** menu.

Review the UEBA Rules

There are several out-of-the-box UEBA rules that refer to AI data to compute an anomaly and generate incidents. The rule names start with the term **UEBA**. You will review the four UEBA rules that were triggered in this lab.

To review the UEBA AI detects unusual file upload rule

1. Continuing on the FortiSIEM GUI, click **RESOURCE**.
2. In the left pane, select and expand **Rules**.
3. Select and expand **Security**.
4. Click **UEBA**.

There are 50 built-in UEBA rules. By default, a few rules are not active. If you need those rules in your environment, you must activate them manually.

5. Search for the **UEBA AI detects unusual file upload** rule that triggered several incidents in this lab.
6. Select this rule, and then click **Edit**.
7. Click **Selected Rule**.
8. Click **Step 2: Define Condition**.
9. Edit the **UEBA** subpattern.

Edit SubPattern

Name: UEBA

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row			
+	-	Event Type	=	FortiInsight-AiAlert-fileuploaded	+	-	AND	+	-

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row			
+	-	COUNT(Matched Events)	>=	1	+	-	AND	+	-

Group By:

Attribute	Row	Move		
Host Name	+	-	↑	↓
Domain	+	-	↑	↓
User	+	-	↑	↓
Process Name	+	-	↑	↓
Tag Name	+	-	↑	↓
Activity Name	+	-	↑	↓
Resource Name	+	-	↑	↓

Save Save as Report Run as Query Cancel

This rule is tracking the **Event Type** that has the value **FortiInsight-AiAlert-fileuploaded**. A single such event triggers an incident. This occurs only if there is an anomaly event that deviates from the AI model.

10. Click **Cancel**.
11. Click **Cancel** again.

To review the UEBA Policy detects hacking tool usage rule

1. Continuing on the UEBA rules page, search for the **UEBA Policy detects hacking tool usage** rule.
2. Select the rule, and then click **Edit**.
3. Click **Selected Rule**.
4. Click **Step 2: Define Condition**.
5. Edit the **UEBA** subpattern.

Edit SubPattern

Name: UEBA

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Event Type	=	FINS-Windows-new-process-created	+	AND	+
+	Process Name	IN	wireshark.exe, zenmap, zenmap.exe	+	AND	+

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	COUNT(Matched Events)	>=	1	+	AND	+

Group By:

Attribute	Row	Move
Host Name	+	↑ ↓
Domain	+	↑ ↓
User	+	↑ ↓
Process Name	+	↑ ↓
Activity Name	+	↑ ↓
Resource Name	+	↑ ↓

Save Save as Report Run as Query Cancel

This rule is tracking the **Event Type** that has the value **FINS-Windows-new-process-created**. This rule is also tracking the following processes:

- metasploit
- metasploit.exe
- mimikatz.exe
- nc
- nc.exe
- ncat
- nmap
- nmap.exe
- oclhashcat
- psexec.exe
- psexecsvc.exe
- runas.exe
- tor browser
- tor browser.exe

- tor
- tor.exe
- tor.real
- wireshark
- wireshark.exe
- zenmap
- zenmap.exe

If an anomaly event matches the event type defined and that event contains one or more of the processes defined, it triggers an incident.

6. Click **Cancel**.
7. Click **Cancel** again.

To review the UEBA AI detects unusual process created rule

1. Continuing on the UEBA rules page, search for the **UEBA AI detects unusual process created** rule.
2. Select the rule, and then click **Edit**.
3. Click **Selected Rule**.
4. Click **Step 2: Define Condition**.
5. Edit the **UEBA** subpattern.

Edit SubPattern

Name: UEBA

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	-	Event Type	=	Fortinsight-AiAlert-newprocesscre	+	-
						AND	

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	-	COUNT(Matched Events)	>=	1	+	-
						AND	
	+	-	AVG(Confidence)	>	0	+	-
						AND	

Group By:

Attribute	Row	Move
Host Name	+	-
Domain	+	-
User	+	-
Process Name	+	-
Tag Name	+	-
Activity Name	+	-
Resource Name	+	-

Save Save as Report Run as Query Cancel

This rule is tracking the **Event Type** that has the value **Fortinsight-AiAlert-newprocesscreated**. A single such event triggers an incident. This occurs only if there is an anomaly event that deviates from the AI model. The event must also have an average confidence value greater than 0.

6. Click **Cancel**.
7. Click **Cancel** again.

To review the UEBA AI detects unusual host logon rule

1. Continuing on the UEBA rules page, search for the **UEBA AI detects unusual host logon** rule.
2. Select the rule, and then click **Edit**.
3. Click **Selected Rule**.
4. Click **Step 2: Define Condition**.
5. Edit the **UEBA** subpattern.

Edit SubPattern

Name: UEBA

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Event Type	=	Fortiinsight-AiAlert-userloggedon	+	AND	+

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	COUNT(Matched Events)	>=	1	+	AND	+

Group By:

Attribute	Row	Move
Host Name	+	↑ ↓
Domain	+	↑ ↓
User	+	↑ ↓
Process Name	+	↑ ↓
Tag Name	+	↑ ↓
Activity Name	+	↑ ↓
Resource Name	+	↑ ↓

Save Save as Report Run as Query Cancel

This rule is tracking the **Event Type** that has the value **Fortiinsight-AiAlert-userloggedon**. A single such event triggers an incident. This occurs only if there is an anomaly event that deviates from the AI model.

6. Click **Cancel**.
7. Click **Cancel** again.
8. Log out of the supervisor FortiSIEM GUI.

Exercise 4: Reviewing the UEBA Dashboard

In this exercise, you will review the UEBA alerts and events dashboard.

Review the UEBA Dashboards

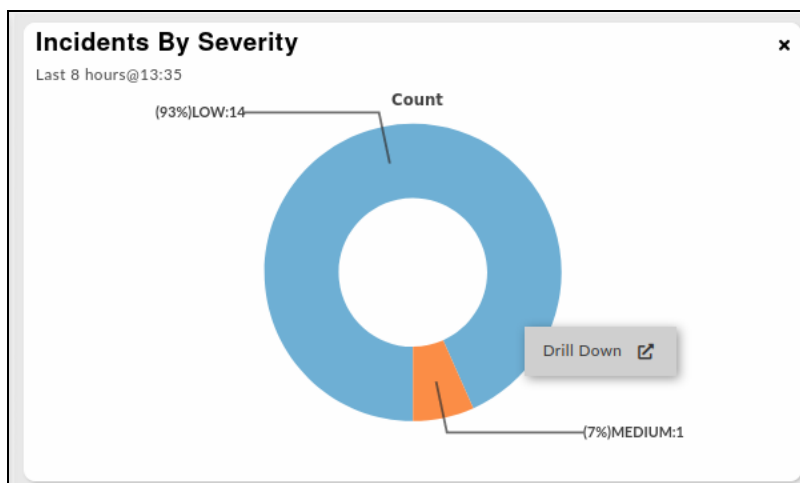
You will review the UEBA dashboards.

To review the UEBA alerts dashboard

1. On the supervisor FortiSIEM GUI, log in to the super organization with the following credentials:

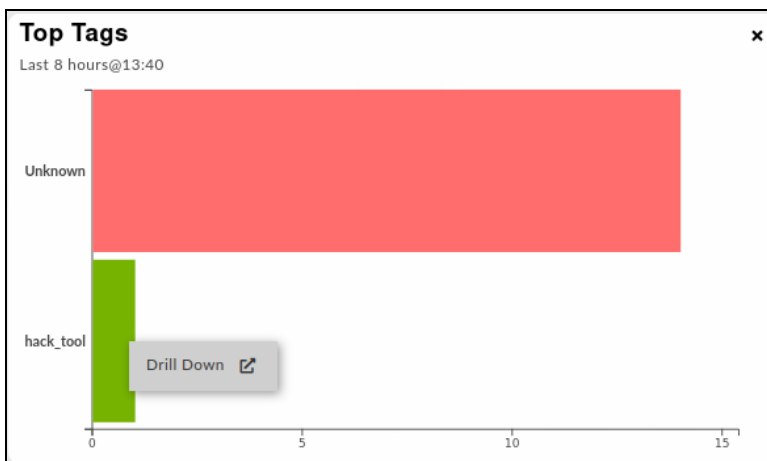
Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

2. Click **LOG IN**.
3. Click **DASHBOARD**.
4. Click **UEBA Alerts**.
5. Review the **Incidents By Severity** widget.

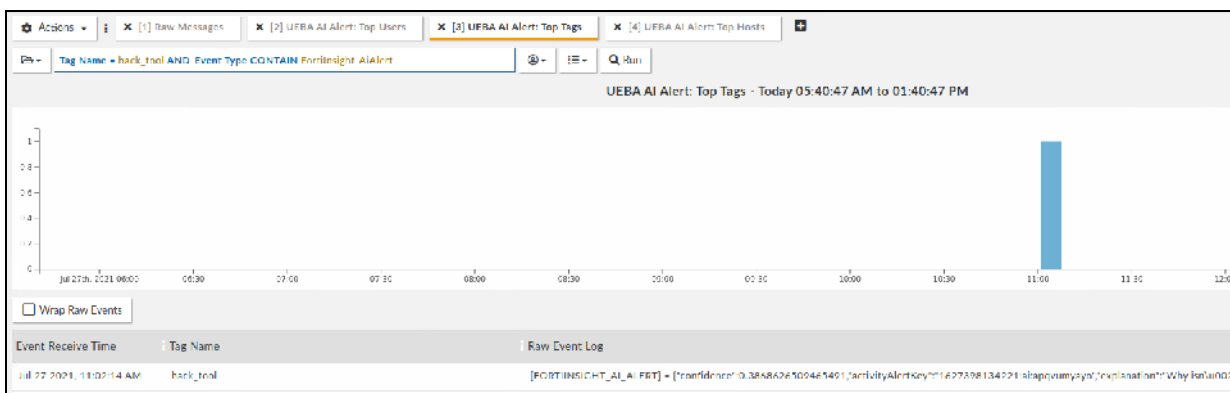


You can drill down to **Analytics** to see more details about the incidents.

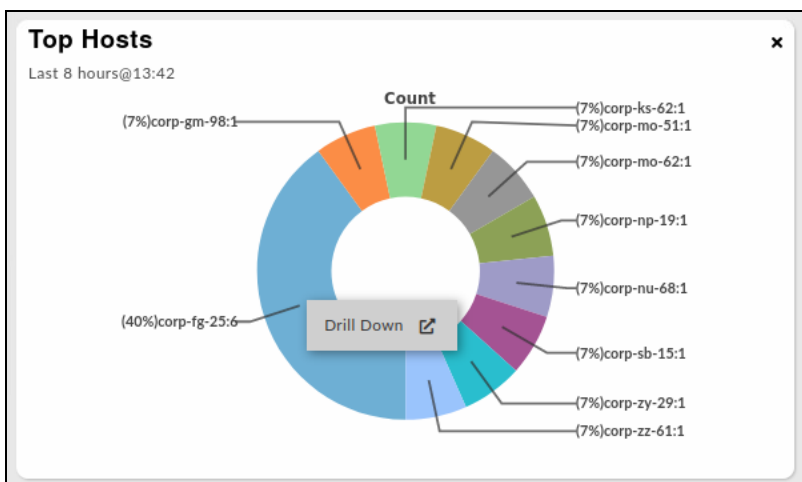




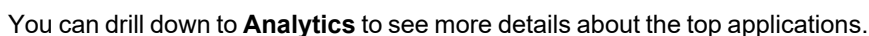
You can drill down to **Analytics** to see more details about the top tags.



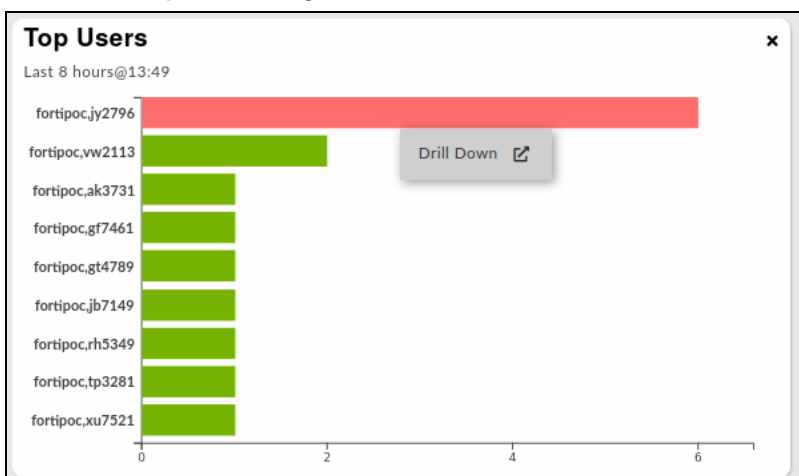
8. Review the Top Hosts widget.



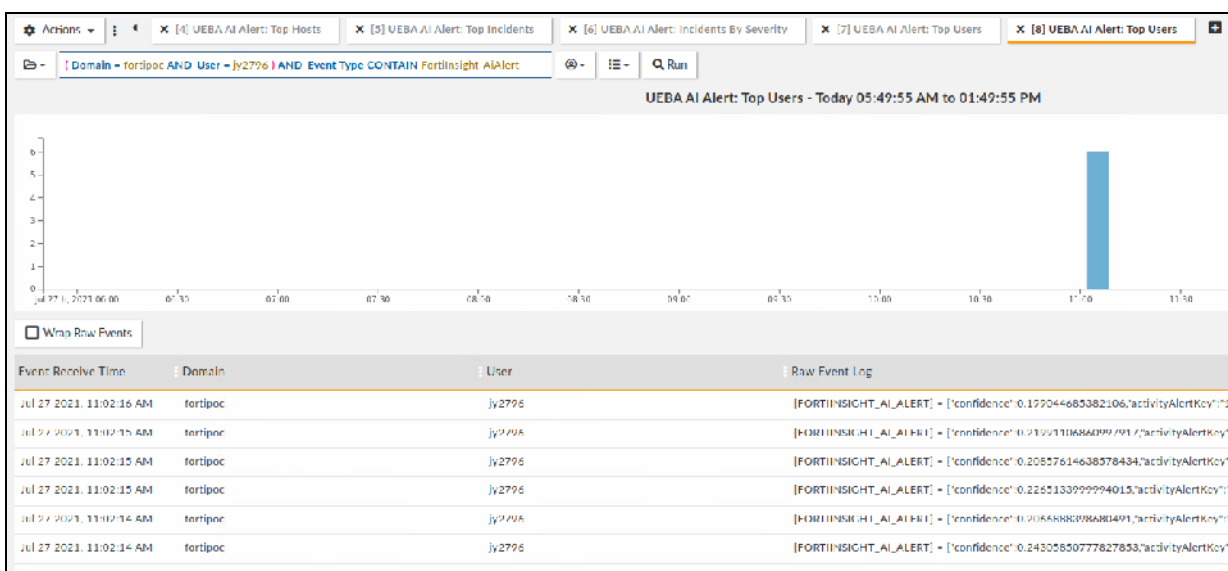
You can drill down to **Analytics** to see more details about the top hosts.



10. Review the Top Users widget.



You can drill down to **Analytics** to see more details about the top users.

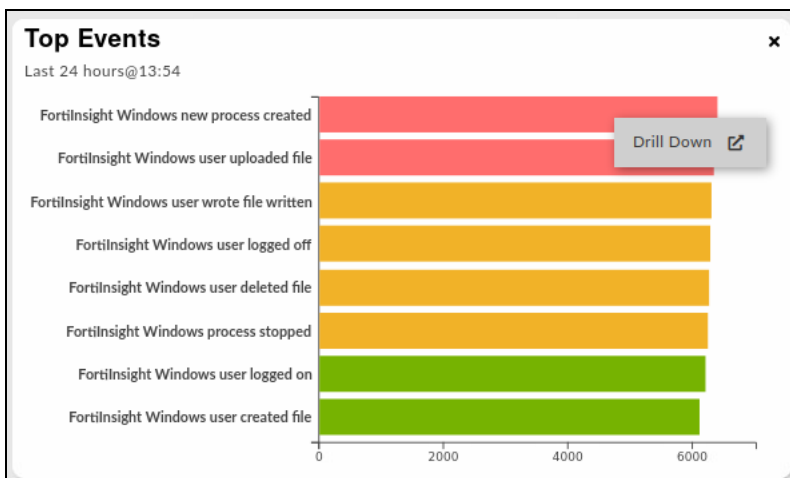


11. Review the All Incidents widget.

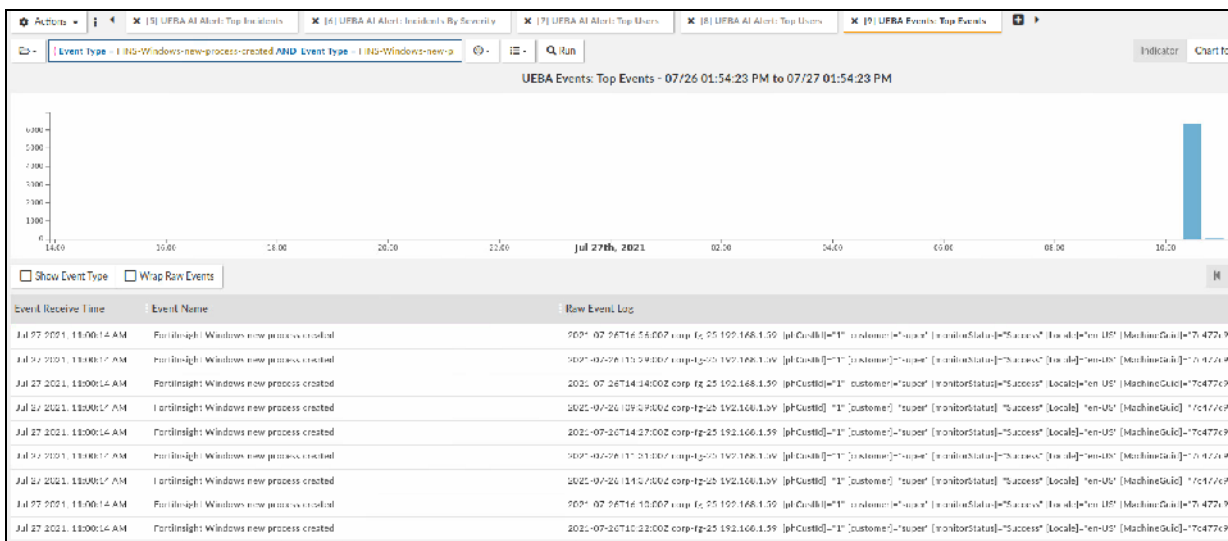
All Incidents									
Last 24 hours@13:51									
Event Receive Time	Event Name	Event Severity	Inc Name	Confidence	Host Name	Domain	User	Process Name	Resource Name
Jul 27 2021, 11:02:16 AM	AI Alert is triggered by unusual new process created	1		19	comp-10-21	fortipoc	jv2796	cmd.exe	c:\windows\system32\cmd
Jul 27 2021, 11:02:15 AM	AI Alert is triggered by unusual new process created	1		21	comp-10-21	fortipoc	jv2796	notepad++.exe	c:\program files\notep
Jul 27 2021, 11:02:15 AM	AI Alert is triggered by unusual new process created	1		20	comp-10-21	fortipoc	jv2796	cmd.exe	c:\windows\system32\cmd
Jul 27 2021, 11:02:15 AM	AI Alert is triggered by unusual new process created	1		22	comp-10-21	fortipoc	jv2796	cmd.exe	c:\program files\cmd
Jul 27 2021, 11:02:14 AM	AI Alert is triggered by unusual new process created	1		10	comp-10-21	fortipoc	jv2796	cmd.exe	c:\program files\cmd
Jul 27 2021, 11:02:14 AM	AI Alert is triggered by unusual new process created	1		24	comp-10-21	fortipoc	jv2796	cmd.exe	c:\windows\system32\cmd
Jul 27 2021, 11:02:14 AM	AI Alert is triggered by unusual new process created	1	hacker tool	24	comp-10-21	fortipoc	jv2796	cmd.exe	c:\program files\cmd
Jul 27 2021, 11:02:14 AM	AI Alert is triggered by unusual file accessed	1		10	comp-10-21	fortipoc	jv2796	cmd.exe	c:\windows\system32\cmd
Jul 27 2021, 11:02:14 AM	AI Alert is triggered by unusual user logged on	1		14	comp-10-21	fortipoc	jv2796	cmd.exe	c:\windows\system32\cmd
Jul 27 2021, 11:02:13 AM	AI Alert is triggered by unusual file accessed	1		20	comp-10-21	fortipoc	jv2796	cmd.exe	c:\windows\system32\cmd

To review the UEBA events dashboard

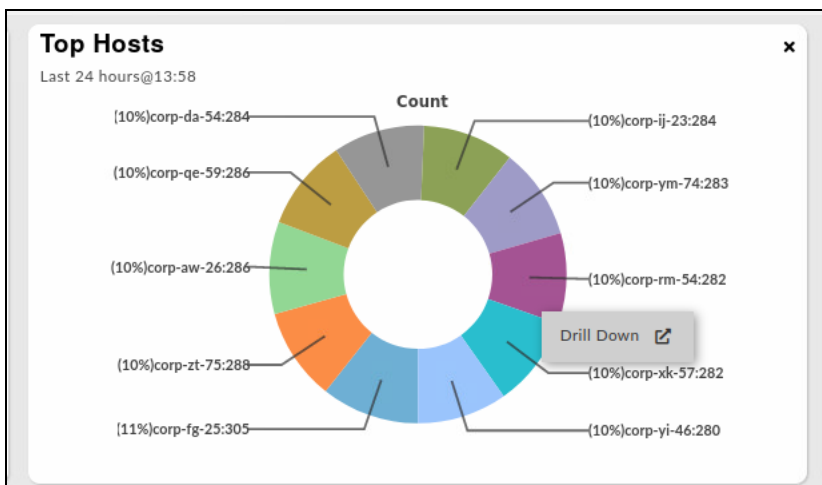
- Continuing on the **DASHBOARD** page, click **UEBA Events**.
- Review the **Top Events** widget.



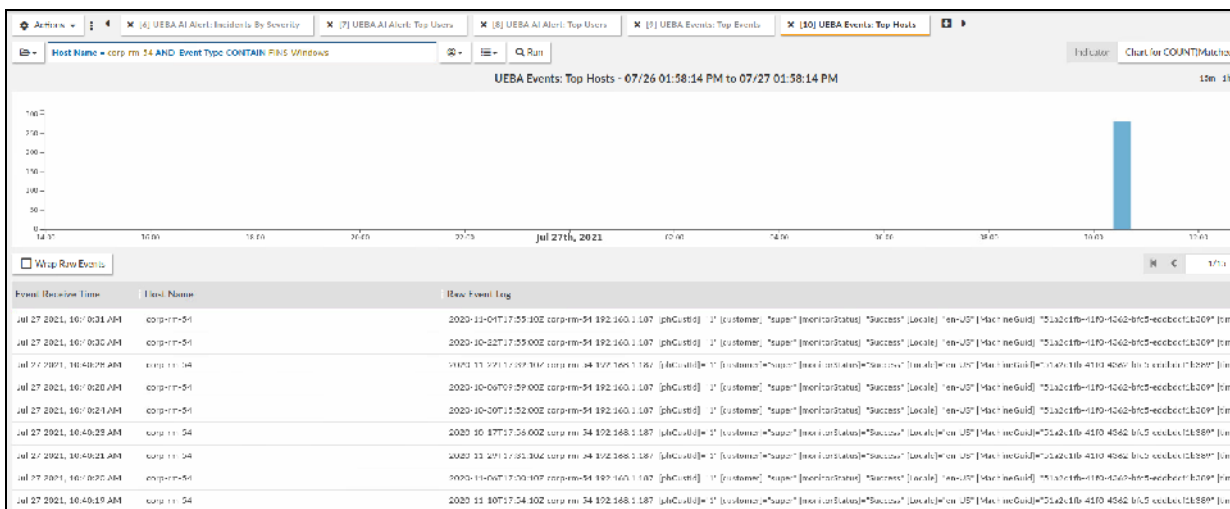
You can drill down to **Analytics** to see more details.



3. Review the Top Hosts widget.



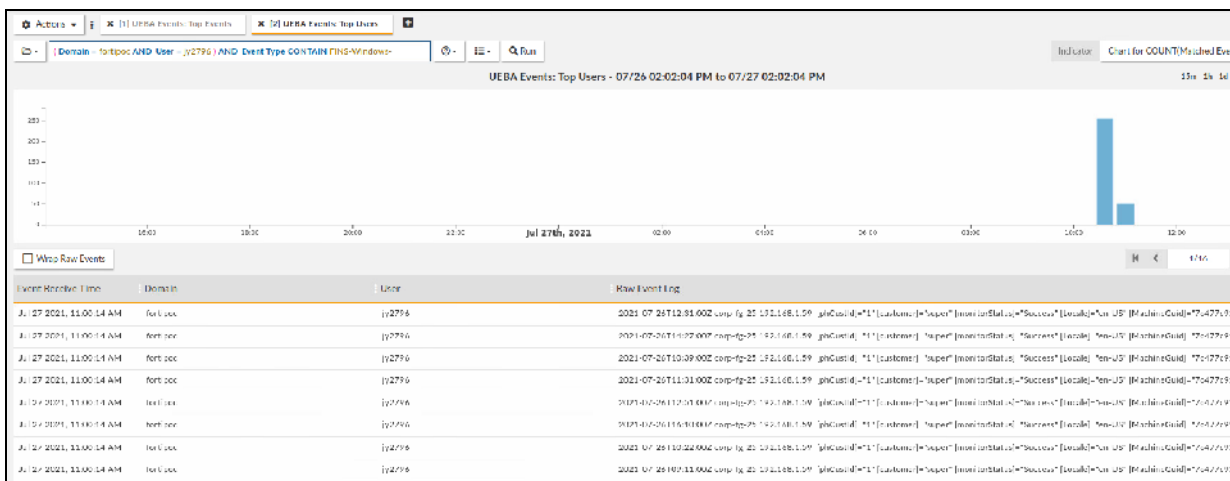
You can drill down to **Analytics** to see more details.



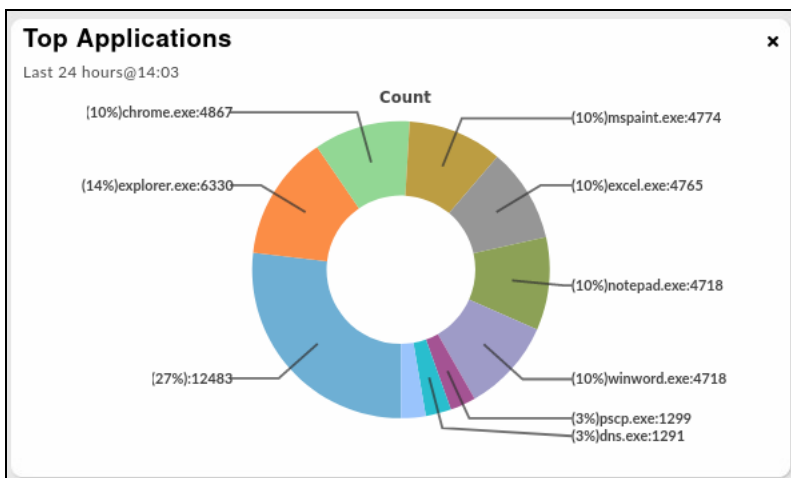
4. Review the Top Users widget.



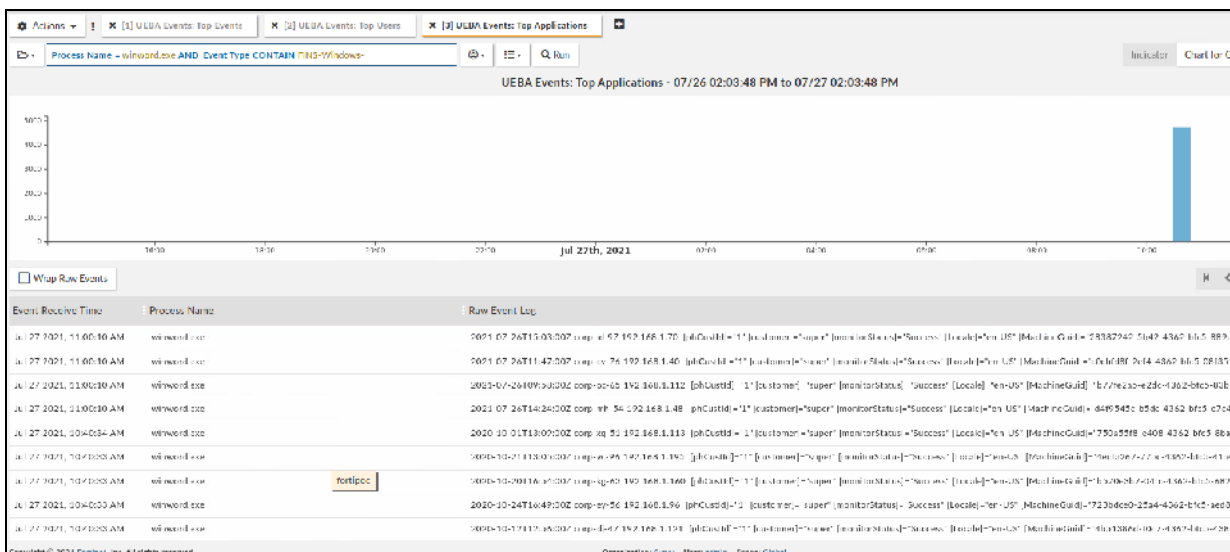
You can drill down to **Analytics** to see more details.



5. Review the Top Applications widget.



You can drill down to **Analytics** to see more details.



6. Log out of the supervisor FortiSIEM GUI.

Lab 11: MITRE ATT&CK Framework

In this lab, you will generate several security incidents and analyze them through the MITRE ATT&CK framework on FortiSIEM and FortiSOAR.

Objectives

- Analyze incidents on FortiSIEM with the MITRE ATT&CK framework
- Map FortiSIEM incident MITRE techniques to FortiSOAR
- Analyze alerts on FortiSOAR with the MITRE ATT&CK framework

Time to Complete

Estimated: 30 minutes

Exercise 1: Creating Tags on FortiSIEM

In this exercise, you will create a few tags on FortiSIEM and associate one of the tags with a rule. This makes it easier for you to search for incidents that the rule detects using the tag name. You can also map the tags on FortiSOAR.

Create Tags on FortiSIEM

You will create a few tags on FortiSIEM and associate one of the tags with a specific rule.

To create tags on FortiSIEM

1. On the supervisor FortiSIEM GUI, log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

2. Click **ADMIN**.
3. Click **Settings**.
4. Click **Tags**.
5. Click **New**.
6. Configure the following tags:

Tag	Color
phishing	red
ransomware	red
code execution	red
powershell	yellow

To add tags to incidents

1. Continuing on the FortiSIEM GUI, click **RESOURCES**.
2. In the left navigation pane, expand **Rules**.
3. Search for the **Windows: WannaCry Ransomware** rule name.
4. Select the rule, and then click **Edit**.
5. Click **Selected Rule**.

6. Click **Step3: Define Action**.
7. Click **Tag**, and then select **ransomware** in the drop-down list.

Windows: WannaCry Ransomware - Edit Details

Step 1: General > Step 2: Define Condition > **Step 3: Define Action**

Severity: 9 - HIGH

Category: Security

Subcategory: Defense Evasion

Technique: 5 Selected

Tactics: Discovery, Lateral Movement, Defense Evasion, Impact

Action: Defined

Exception: Undefined

Tag: ransomware

8. Click **Save**.
9. Log out of the supervisor FortiSIEM GUI.

Exercise 2: Generating Incidents on FortiSIEM

In this exercise, you will generate several different types of incidents on FortiSIEM using an incident generator script.

Generate Incidents on FortiSIEM

You will generate Windows security incidents through the incident generator script.

To generate incidents

1. On the Local-Host VM, open a terminal window (Ctrl+Alt+T).
2. Enter the following command to open an SSH connection to the FortiSIEM supervisor:
`ssh root@10.0.1.130`
3. Enter the password `Fortinet1!`.
4. Enter the following command to verify your working directory—it should be `/root`:
`pwd`
5. Enter the following command, and then verify that the highlighted files are available:

```
ls -lrt
[roo@super ~]# ls -lrt
total 58628
drwxr-xr-x 2 root root      69 Feb 21  2020 fixes
drwxr-xr-x 8 root root      91 Feb 21  2020 incidentSimData
drwxr-xr-x 2 root root      68 Nov 22  2020 fsmUebaDemo
drwxrwxr-x 4 root root      30 May 28 14:34 Lab
-rw----- 1 root root      971 Jul  1 19:34 original-ks.cfg
-rw----- 1 root root     1610 Jul  1 19:34 anaconda-ks.cfg
-rw-r--r-- 1 root root 59760640 Jul  1 19:34 VBoxGuestAdditions.iso
-rwxr-xr-x 1 root root      485 Jul  1 19:36 zerofill.sh
-rwxr-xr-x 1 root root     61454 Jul 13 20:48 fsmIncidentSimulator2_4.sh
-rw-r--r-- 1 root root     91316 Jul 13 20:52 fsmIncidentsSim.zip
-rw-r--r-- 1 root root      7037 Jul 13 20:52 fsmUebaDemo.zip
-rw-r--r-- 1 root root     58587 Jul 13 20:57 Lab.zip
-rw-r--r-- 1 root root       840 Jul 14 10:04 security_incident
-rw-r--r-- 1 root root      3460 Jul 14 10:04 security_sysmon_incident
-rw-r--r-- 1 root root      1427 Jul 14 10:04 security_user_incident
-rw-r--r-- 1 root root     16510 Jul 15 12:47 incidentSimLog.log
```

6. Enter the following command to run the script to generate security incidents:
`./fsmIncidentSimulator2_4.sh security_incident`
7. Once the script is complete, type the following command to generate user security incidents:
`./fsmIncidentSimulator2_4.sh security_user_incident`
8. Once the scripts are complete, type the following command to generate sysmon incidents:
`./fsmIncidentSimulator2_4.sh security_sysmon_incident`
9. Close the SSH session browser tab.

Exercise 3: Reviewing the MITRE ATT&CK Framework Support on FortiSIEM

In this exercise, you will review the baseline reports and rules.

Review the MITRE ATT&CK Incident Dashboard

You will review the MITRE ATT&CK incident dashboard.

To review the MITRE rule coverage

1. On the supervisor FortiSIEM GUI, log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

2. Click **LOG IN**.
3. Click **INCIDENTS**.
4. In the **MITRE ATT&CK** drop-down list, select **Rule Coverage**.

The FortiSIEM rule coverage of the MITRE framework is displayed.

965 Rules - 72% Coverage											
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
12	0	43	113	152	132	292	121	63	37	38	58
10 tech, 32 sub-tech	2 tech, 20 sub-tech	9 tech, 16 sub-tech	17 tech, 29 sub-tech	19 tech, 47 sub-tech	13 tech, 89 sub-tech	30 tech, 129 sub-tech	35 tech, 68 sub-tech	12 tech, 34 sub-tech	9 tech, 18 sub-tech	12 tech, 24 sub-tech	15 tech, 30 sub-tech
Gather Victim Identity Information	Compromise Infrastructure	Phishing (7)	Deploy Contingency	Scheduled Task/Job (12)	Process Injection (14)	Process Injection (14)	OS Credential Dumping (44)	Container and Resource Discovery	Software Deployment Tools	Archive Collected Data (6)	Multi-Stage Channels (1)
Gather Victim Host Information (1)	Establish Accounts	External Remote Services (4)	Native API (1)	Modify Authentication Process	Escape to Host	Modify Authentication Process	Brute Force (16)	Browser Bookmark Discovery	Use Persistent Authentication Material (7)	Data from Information Repository	Data Obfuscation (9)
Search Open Websites/Domains	Stage Canonical Init	Replication Through Removable Media (1)	Inter-Process Communication (2)	Inter-Signaling	Scheduled Task/Job (12)	Hide Artifacts (6)	Steal or Forge Cookies/Tickets (6)	Cloud Infrastructure Discovery (2)	Lateral Tool Transfer	Monitor the Middle (7)	Web Services
Gather Victim Org Information	Acquire Infrastructure	Supply Chain Compromise (1)	Container Administration Command	Hijack Execution Flow (17)	Domain Policy Modification (1)	Impair Defenses (49)	Man-in-the-Middle (7)	Domain Trust Discovery (3)	Exploitation of Remote Services (4)	Data from Configuration Repository (1)	Ingress Tool Transfer (14)
Gather Victim Network Information (7)	Obtain Capabilities	Hardware Additions (1)	Scheduled Task/Job (19)	Pre-OS Boot (1)	Exploitation for Privilege Escalation (4)	Indicator Removal and List (7)	Forge Web Credentials	System Network Configuration Discovery (1)	Remote Services (23)	Audio Capture (3)	New Application Layer Protocol (1)
Phishing for Information (1)	Develop Capabilities	Invested Relationship (1)	User Location (16)	Import Internal Image	Hijack Execution Flow (17)	Hijack Execution Flow (17)	Exploitation for Credential Access	Peripheral Device Discovery	Traversal Through Removable Media	Video Capture (1)	Communication Through C2 Channel (18)

To review the MITRE incident coverage

1. Continuing on the FortiSIEM GUI, in the **MITRE ATT&CK** drop-down list, select **Incident Coverage**.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
0	0	2	7	5	0	2	9	1	3	3	2	1
30 Tech, 82 Sub-Tech	7 Tech, 31 Sub-Tech	9 Tech, 16 Sub-Tech	10 Tech, 29 Sub-Tech	19 Tech, 91 Sub-Tech	15 Tech, 84 Sub-Tech	39 Tech, 120 Sub-Tech	12 Tech, 46 Sub-Tech	27 Tech, 84 Sub-Tech	9 Tech, 18 Sub-Tech	17 Tech, 28 Sub-Tech	14 Tech, 50 Sub-Tech	9 Tech, 12 Sub-Tech
Gather Victim Identity Information	Compromise Infrastructure	Phishing	Deploy Container	Scheduled Task/Job	Process Injection	Process Injection	OS Credential Dumping [1]	Enumerate and Resource Discovery	Software Deployment Tools	Archive Collected Data	Multi-Stage Channels	Exfiltration Over Alternative Protocol [2]
Gather Victim Email Information	Establish Accounts	External Remote Services [2]	Native API	Modify Authentication Process	Escalate to Host	Modify Authentication Process	Brute Force [2]	Browser Link/Bookmark Discovery	Use Alternate Authentication Material	Data from Information Repositories	Data Obfuscation	Transfer Data to Cloud Account
Search Open Websites/Domains	Stage Capabilities	Replication Through Removable Media	Inter-Process Communication	Intrusive Signaling	Scheduled Task/Job	Hide Artifacts	Steal or Forge Kerberos Tickets	Cloud Infrastructure Discovery	Lateral Tool Transfer	Main-in-the-Middle	Web Service	Exfiltration Over Physical Media
Gather Victim Org Information	Acquire Infrastructure	Supply Chain Compromise	Container Administration Command	Hidden Execution Flow	Domain Policy Modification	Impair Defenses	Main-in-the-Middle	Domain Trust Discovery	Exploitation of Remote Services [1]	Data from Configuration Repository	Impress Tool Transfer	Data Transfer to Limits
Gather Victim Network Information	Obtain Capabilities	Hardware Additions	Scheduled Task/Job	Pre-OS Boot	Exploitation for Privilege Escalation	Indicator Removal on Host [1]	Image Web Credentials	System Network Configuration Discovery	Remote Services [2]	Audio Capture	Non-Application Layer Protocol	Scheduled Transfer
Phishing for Information	Develop Capabilities	Trusted Relationship	User Execution [1]	Implant Internal Image	Hijack Execution Flow	Hijack Execution Flow	Exploitation for Credential Access	Peripheral Device Discovery	Exploitation Through Removable Media	Video Capture	Communication Through Removable Media	Exfiltration Over C2 Channel

In this view, incidents generated on FortiSIEM are mapped to the MITRE framework.

2. In the **Execution** tactic column, select **Command and Scripting Interpreter**.
3. Click **Show Incidents**.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
2	7	5	0	2	
Trusted Relationship	User Execution [1]	Implant Internal Image	Hijack Execution Flow	Hijack Execution Flow	Exploitation of Credentials
Exploit Public-Facing Application	Command and Scripting Interpreter [1]	Valid Accounts	Valid Accounts	Modify Cloud Compute Infrastructure	Automated Collection
Device Inventory	Show Incidents	Configure	Event Triggered		

All incidents related to the **Command and Scripting Interpreter** technique are displayed.

Severity Category	Last Occurred	Incident	Tactics	Technique	Target	Detail
High (3)	Jul 26 2021, 02:34:00 PM	Windows: Non-Interactive PowerShell	Execution	Command and Scripting Interpreter...	Device: 172.16.8.94	Parent Process Name: C:\Windows\System32\cmd.exe
High (3)	Jul 26 2021, 02:34:00 PM	Windows: Non-Interactive PowerShell	Execution	Command and Scripting Interpreter...	Device: 172.16.8.93	Parent Process Name: C:\Windows\System32\cmd.exe
High (3)	Jul 26 2021, 02:34:00 PM	Windows: Download via PowerShell URI	Execution	Command and Scripting Interpreter...	Device: 172.16.8.94	Command: new-object system.net.webclient;download;http://...

To review the MITRE incident explorer

1. Continuing on the FortiSIEM GUI, in the **MITRE ATT&CK** drop-down list, select **Incident Explorer**.

Device	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
8.8.8.8			1		1			1		1		1		
Device_172_16_8_83			1		1					1		1		
Device_172_16_8_94			1		1					1		1		
device_172_16_8_98							1		1	1				1
51.103.242.26								1						
5.100.203.129			1		1					1		1		
device_172_16_8_91				1										
device_172_16_9_3					1						1			

In this view, incidents generated on FortiSIEM based on target device are mapped to the MITRE framework.

- Continuing on the **MITRE ATT&CK Incident Explorer** page, click **Tactics:All**.
- Select **Defense Evasion**.

Tactics: All	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation
All						
Initial Access						
Execution			1		1	
Persistence			1		1	
Defense Evasion			1		1	
Credential Access						
Discovery						
Lateral Movement						
Collection				1		1
Command And Control					3	
Exfiltration						2
Impact						

- Select the **device_172_16_8_98** device.
- Click the **Windows: WannaCry Ransomware** incident.
Review the incidents details, such as **Tactics** and **Technique**.

MITRE ATT&CK Incident Explorer

Defense Evasion incidents for device_172.16.8.98

Severity Category	Last Occurred	Incident	Tactics	Technique	Source	Target	Detail
HIGH	Jul 26 2021, 02:34:00 PM	Windows: WannaCry Ransomware	Impact, Lateral Move...	File and Directory P...		Device_172.16.8.98	Command: C:\Windows\System32\cmd.exe

Triggering Events

Subpattern: Filter ☐ Wrap Raw Events ☐ Show Raw Event Only

Event Receive Time	Host Name	Command	Raw Event Log
Jul 26 2021, 02:32:41 PM	Device_172.16.8.98	C:\Windows\System32\cmd.exe group	2017-08-14T18:41:51Z Device: 172.16.8.98 AccelOps: WUA WinLog: Microsoft UtcTime: 2017-08-14 16:41:50.651 ProcessGuid: {000181CC-396E-56CB-0C00-0010FC59D600} ProcessId: 2123A Image: C:\Windows\System32\ProgramData\tasksche.exe CommandLine: C:\Windows\System32\cmd.exe group CurrentDirectory: C:\Windows\System32\HealthServiceStall\ User: EXAMPLE_DOMAIN\Administrator LogonGuid: {000181CC-396E-56CB-0C00-0010FC59D600} LogonId: Da18F08 TerminalSessionId: 2

The incident was tagged with the **ransomware** tag that you created and applied to the rule in a previous exercise.

HIGH Jul 26 2021, 02:34:00 PM Windows: WannaCry Ransomware Impact, Lateral Move...

Details Events Rule ☐ Auto expand

Attributes Search attribute name...

Reporting IP: 172.16.8.98
Severity Category: HIGH
Tactics: Impact, Lateral Movement, Defense Evasion, Discovery
Tag: ransomware
Technique: File and Directory Permissions Modification: Windows File and Directory Permissions Modification, Exploitation of Remote Services, File and Directory Discovery, Data

Incident Comments
Add comments to Incident...

6. Log out of the supervisor FortiSIEM GUI.

Exercise 4: Reviewing the MITRE ATT&CK Framework Support on FortiSOAR

In this exercise, you will review the MITRE ATT&CK framework on FortiSOAR.

Review the MITRE ATT&CK Framework on FortiSOAR

You will review the incidents that were generated on FortiSIEM on FortiSOAR. FortiSOAR is preconfigured to ingest incidents from FortiSIEM.

To review the MITRE ATT&CK framework on FortiSOAR

- 1. On the FortiSOAR GUI, log in with the following credentials:

Field	Value
Username	csadmin
Password	Fortinet1!

- 2. Click Incident Response > MITRE ATT&CK Techniques.

MITRE ATT&CK Techniques



© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

525 Items

Add

	Tactics	Technique	Technique ID
	Search	Search	Search
>	☐ Collection	Data Staged	T1074
>	☐ Collection	Data from Cloud Storage Object	T1530
>	☐ Collection	Audio Capture	T1123
>	☐ Collection	Clipboard Data	T1115
>	☐ Collection	Data from Removable Media	T1025
>	☐ Collection	Data from Network Shared Drive	T1039

The module contains details about all of the 525 MITRE ATT&CK techniques. You can manually link alerts and incidents to various techniques or you can use a playbook to automate the process.

- 3. Continuing on the **Incident Response** module, click **Alerts**.
- 4. Open an alert in the list that is marked with the **Credential Access** MITRE technique.

Alerts

Assigned To: [Me](#) | [All](#)

Assigned To: [Me](#) | [All](#)

36 Items [+ Add](#) [▶ Down 10 Recently](#) [▶ Display Scenarios](#) [+ Favorite](#)

☐	ID	Priority Weight	Severity	Assigned To	Name	Source	Type	Status	Created On	Resolved	MITRE Technique	Tenant
	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search
☐	21	1	High	CS Admin	Virus found in mail-PH_RULE_MAIL_VIRUS	Fortinet Forti...			07/26/2021 ...		Collection	Self
☐	33	1	Medium	CS Admin	No logs from a device-PH_RULE_NO_LOG...	Fortinet Forti...			07/26/2021 ...			Self
☐	19	1	Medium	CS Admin	Successful VPN Logon From Outside My ...	Fortinet Forti...			07/26/2021 ...		Credential Access	Self
☐	30	1	Low	CS Admin	Multiple Logon Failures: VPN-PH_RULE_F...	Fortinet Forti...			07/26/2021 ...		Credential Access	Self
☐	10	1	Medium	CS Admin	Linux: Creation of an Archive with Comm...	Fortinet Forti...			07/26/2021 ...			Banking

- 5. Scroll down, and then click **Correlations**.
- 6. Click **ATT&CK Techniques**.

Alert: Successful VPN Logon From Outside My Coun...

Medium Alert-19 Successful VPN Logon From Outside My Country-PH_RULE_VPN_LOGON_SUCCESS_OUTSID...

Last Modified: 07/22/2023 02:52 PM by: dylbuck

Add Tag

BARONAS LIST

Select Date

Type Details

Type Select

MITRE Technique Credential Access

MITRE ATT&CK ID T1110.001

Indicators

Correlations

Tasks

Source Data

External Communications

Access Control

ATT&CK Technique

Enrich

Users

Incidents

Alerts

Assets

Attachments

Campaigns

Hosts

WinRM

1 Items

+ Add

Link

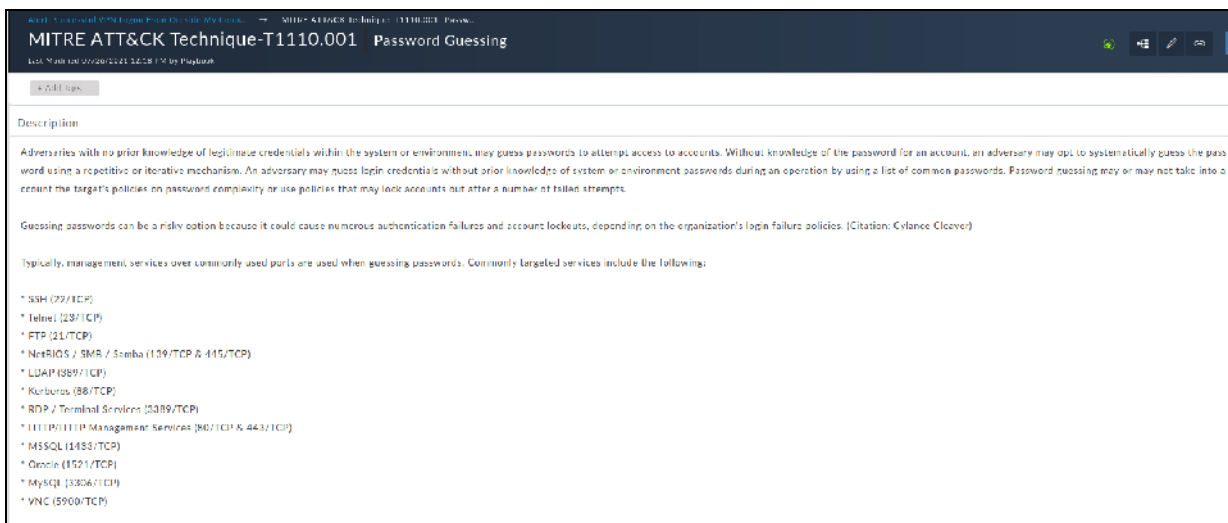
Technique ID	Technique	Rating	ID	Source	Source Weight	Source Weight ID
T1110.001	Password Guessing	Credential Access	478	Self	478	

< 1 of 1 >

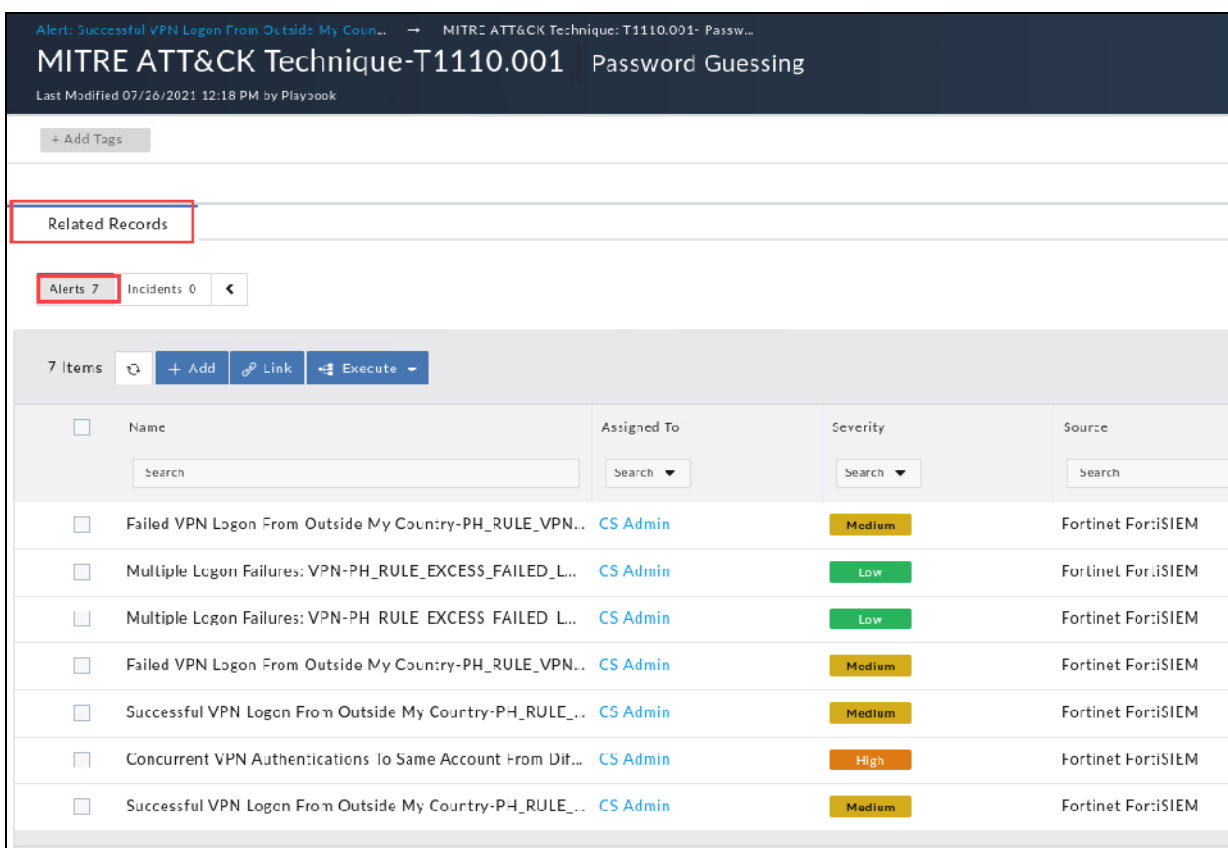
Items Per Page: 30

The technique is listed as **Password Guessing** and the **Technique ID** is **T1110.001**.

- 7. Click **T1110.001**.
Review the technique details.



8. Scroll down to the bottom, and in the **Related Records** section, click **Alerts**.



There are seven other alerts that are associated with the same technique on FortiSOAR. Analysts can quickly navigate to other alerts and remediate those alerts based on the mitigation action defined for the technique.

9. Log out of the FortiSOAR GUI.

Lab 12: Clear Conditions

In this lab, you will explore how clear conditions are applied to rules and how they are triggered.

Objectives

- Review time-based clear conditions
- Add a pattern-based clear condition to a rule

Time to Complete

Estimated: 30 minutes

Exercise 1: Reviewing Time-Based Clear Conditions

In this exercise, you will review time-based clear conditions.

Review Rules With Clear Conditions

Clear conditions specify conditions in which incidents will have their status changed from active to cleared. You can set the time period that must elapse for the clear condition to occur, and then set the conditions based on the triggering of the original rule, or on a subpattern based on the incident attributes.

A few out-of-the-box rules have clear conditions predefined. You will review those.

To run a CMDB report for rules with clear conditions

- 1. Go to the Supervisor FortiSIEM management GUI.
- 2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

- 3. Click **LOGIN**.
- 4. Click **CMDB**.
- 5. In the left navigation pane, click **CMDB Reports**.
- 6. In the search field, type `clear`.
- 7. Select **Rules with Clear Conditions**, and then click **Run**.

CMDB > CMDB Reports

NewEditDeleteClone

clear

RunScheduleResultsImportExportRefreshSystem

Name	Description	Scope
Rules with Clear Conditions	This report captures rules with clear conditions	System

- 8. Verify that **All Organizations** is selected, and then click **Run**.
Notice that for each rule with a clear condition, FortiSIEM reports whether it is **timebased** or **patternbased** on the GUI.

Rule Name	Clear Condition Constraints	Clear Condition Option
High Process Memory: Network Device		timebased
Windows Disk controller problem		timebased
Manual Service Started	PH_RULE_MANUAL_SRVC_START.hostIpAddr = PH_RULE_MANUAL_SRVC_START_CLEAR.hostIpAddr, PH_RULE_MANUAL_SRVC_START.hostName = PH_RULE_MANUAL_SRVC_START_CLEAR.hostName, PH_RULE_MANUAL_SRVC_START.serviceName = PH_RULE_MANUAL_SRVC_START_CLEAR.serviceName, PH_RULE_MANUAL_SRVC_START.servicePath = PH_RULE_MANUAL_SRVC_START_CLEAR.servicePath	patternbased
Cisco ACI Node Health Critical		timebased
No Events Reported From External Devices In Last Hour	PH_RULE_SYS_DEVICE_NO_EVENTS.srcIpAddr = PH_RULE_SYS_DEVICE_NO_EVENTS_CLEAR.srcIpAddr	patternbased
Oracle DB Low Library Cache Hit Ratio		timebased
ESX Network I/O Warning		timebased
Cisco Unity Connection Failback Failed	PH_RULE_CCM_UNITY_FAILBACK_FAILED.hostName = PH_RULE_CCM_UNITY_FAILBACK_FAILED_CLEAR.hostName	patternbased
Exchange Server Mailbox Queue high		timebased
Server Intf Error Critical		timebased

Review a Time-Based Clear Condition

Now, you will review a time-based clear condition rule. Specifying the time means that the original rule will not trigger again for a specified period of time, which can be in seconds, minutes, or hours.

To review a time-based clear condition

- Continuing on the FortiSIEM GUI, click **RESOURCES**.
- In the left navigation pane, click **Rules**.
- In the search field, type `High Process Memory`.
- Select the **High Process Memory: Network Device** rule, and then click **Edit > Selected Rule**.
- Click **Step 3: Define Action**.
- Click the pencil icon (✎) to edit the **Clear** settings.

Edit Rule Clear Conditions

Clear if Within:

20

Minutes

☒ the original rule does not trigger
 ☐ the following conditions are met

Clear Condition: If this Pattern occurs

Paren	Subpattern	Paren	Next	Row
+	-		+	-

This is a time-based clear condition. FortiSIEM will simply clear the incident after 20 minutes if the original rule does not trigger again.

- Click **Cancel**.
- Click **Cancel**.
- Log out of the Supervisor FortiSIEM management GUI.

Exercise 2: Configuring a Pattern-Based Clear Condition

In this exercise, you will configure a pattern-based clear condition.

Define a Pattern-Based Clear Condition

With a pattern-based clear condition, a subpattern must be defined which can be a single pattern or multiple patterns. Usually, it is almost an exact mirror of the original pattern in the rule but with a different aggregation calculation.

You will clone an existing rule and define a pattern-based clear condition for that rule.

To clone a rule

1. Go to the Supervisor FortiSIEM management GUI.
2. Log in to the super organization with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

3. Click **LOGIN**.
4. Click **RESOURCES**.
5. In the left navigation pane, click **Rules**.
6. In the search field, type `SNMP Service Unavailable`.
7. Deselect the checkbox in the **Active** column.
8. Deselect **Active**.
9. Deselect **All Orgs**.
10. Click **Save**.
11. Select the rule again, and then click **Clone**.
12. In the **Save As** field, type `SNMP Service Unavailable Kali`.
13. Click **Save**.
14. Select the **SNMP Service Unavailable Kali** rule, and select the checkbox to activate it.
15. Click **Active**.
16. Click **University**.
17. Click **Save**.

To define a pattern-based clear condition

- Continuing on the FortiSIEM GUI, select the **SNMP Service Unavailable Kali** rule, and then click **Edit**.
- Click **Step 2: Define Condition**.
- Click the pencil icon (✎) to edit the **SnmptDown** subpattern.
- In the **Value** field, for the **AVG(Packet Loss Pct)** attribute, type 5.
By reducing the packet loss percentage value, you can trigger the rule quickly. In a real-world environment, it is recommended to keep the value at 100.
- In the **Operator** drop-down list, for the **AVG(Packet Loss Pct)** attribute, select **>=**.
- Click **Save**.
- Click **Step 3: Define Action**.
- Click the pencil icon (✎) to edit the **Clear** settings.
- Verify that **the following conditions are met** is selected.
- Click the pencil icon (✎) to edit the **SnmptDown_CLEAR** subpattern.
Review the **Value** field for the **AVG(Packet Loss Pct)** attribute.

Name: SnmptDown_CLEAR									
Filters:									
Paren	Attribute	Operator	Value	Paren	Next	Row			
+	-	Event Type	=	PH_DEV_MON_SNMP_PING_STA	+	-	AND	+	-
Aggregate:									
Paren	Attribute	Operator	Value	Paren	Next	Row			
+	-	AVG(Packet Loss Pct)	<	10	+	-	AND	+	-
+	-	COUNT(Matched Events)	>=	1	+	-	AND	+	-

If the packet loss percentage is less than 10%, the incident will be cleared.

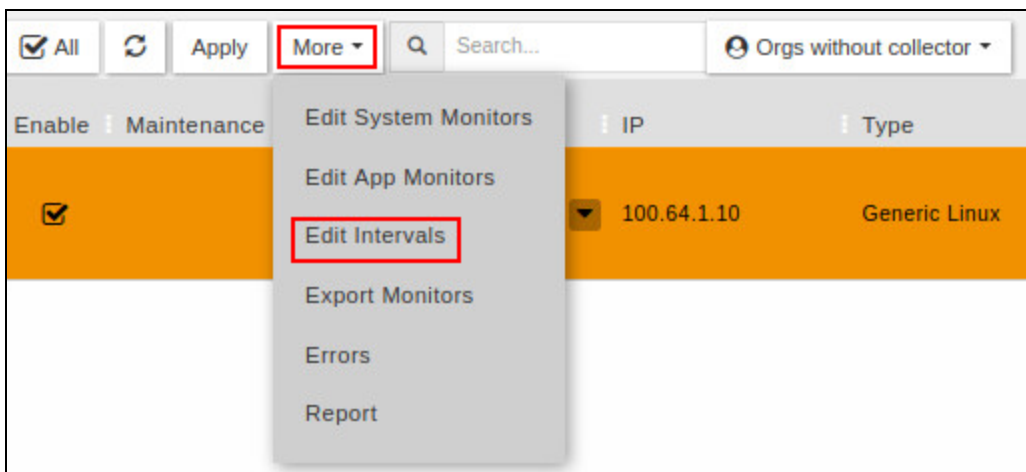
- Click **Cancel**.
- Click **Cancel**.
- Click **Save**.
- Click **OK**.

Modify the SNMP Ping Interval

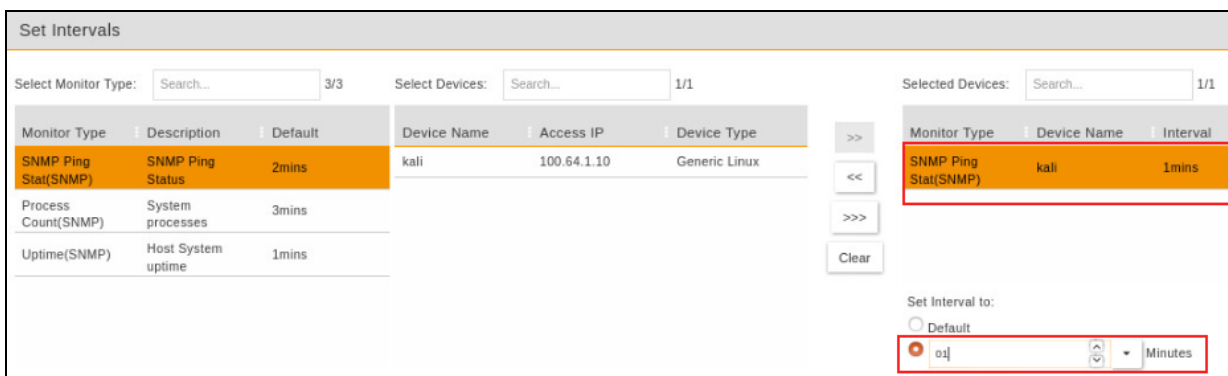
The default **SNMP Ping Stat** interval is two minutes. For this lab, you will reduce that interval to one minute so that the rule triggers sooner.

To reduce the SNMP Ping Stat interval

- Continuing on the FortiSIEM GUI, click **ADMIN**.
- Click **Monitor Performance**.
- Click **kali**, and then in the **More** drop-down list, select **Edit Intervals**.



4. Select **SNMP Ping Stat(SNMP)**, and then click >>>.
5. Set the interval to 01.



6. Click **Save**.

Disable the SNMP Service

To trigger the rule and generate an incident, you will now disable the SNMP service on Kali.

To disable the SNMP service on Kali

1. Go to the Kali VM.
2. Open a terminal window.
3. Type the following command to stop the SNMP service:


```
service snmpd stop
```
4. Type the following command to verify that the SNMP service has stopped:


```
service snmpd status
```

```
root@kali:~# service snmpd stop
root@kali:~# service snmpd status
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; disabled; vendor preset:
   Active: inactive (dead)
root@kali:~#
```

5. Press Q.

Run the Rule as a Query

You will run the **SNMP Service Unavailable** rule as a query, and monitor the packet loss percentages. An incident will be triggered only if the packet loss percentage value is more than 5%.

To run the rule as a query

1. Return to the FortiSIEM GUI, click **RESOURCES**.
2. In the left navigation pane, click **Rules**.
3. Select the **SNMP Service Unavailable Kali** rule, and then click **Edit**.
4. Click **Step 2: Define Condition**.
5. Click the pencil icon (✎) to edit the **SnmppDown** subpattern.
6. Click **Run as Query**.

Edit SubPattern

Name: SnmppDown

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Event Type	=	PH_DEV_MON_SNMP_PING_ST/	⊕ ⊖	AND	⊕ ⊖

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	AVG(Packet Loss Pct)	>=	5	⊕ ⊖	AND	⊕ ⊖
⊕ ⊖	COUNT(Matched Events)	>=	1	⊕ ⊖	AND	⊕ ⊖

Group By:

Attribute	Row	Move
Host Name	⊕ ⊖	⬆ ⬇
Host IP	⊕ ⊖	⬆ ⬇

Save Save as Report **Run as Query** Cancel

7. Deselect all organizations except **University**.
8. Set the **Time Range** to 4 minutes.

Edit SubPattern > Run as Query

Run Report For:

☐ All Orgs Search...

☐ Super/Local

☐ Banking

☐ Aviation

☒ University

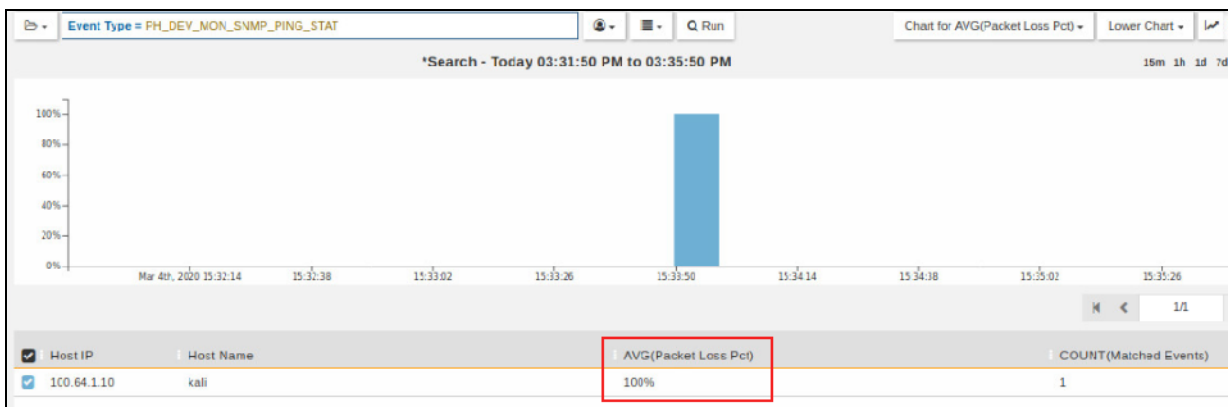
Time Range

☒ Relative ☐ Absolute

Last 4 Minute

9. Click **Run**.

The query results are displayed on a new browser tab.



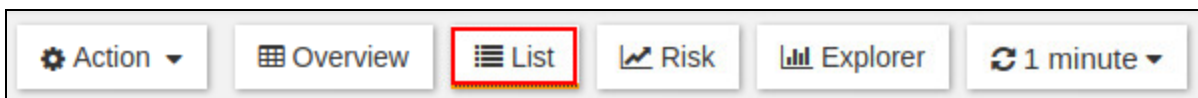
Review the **AVG(Packet Loss Pct)** column. The average packet loss percentage must be greater than 5% for the rule to trigger an incident. Run the query again after a few minutes if the average packet loss percentage is not above 5%.

Verify the Incident

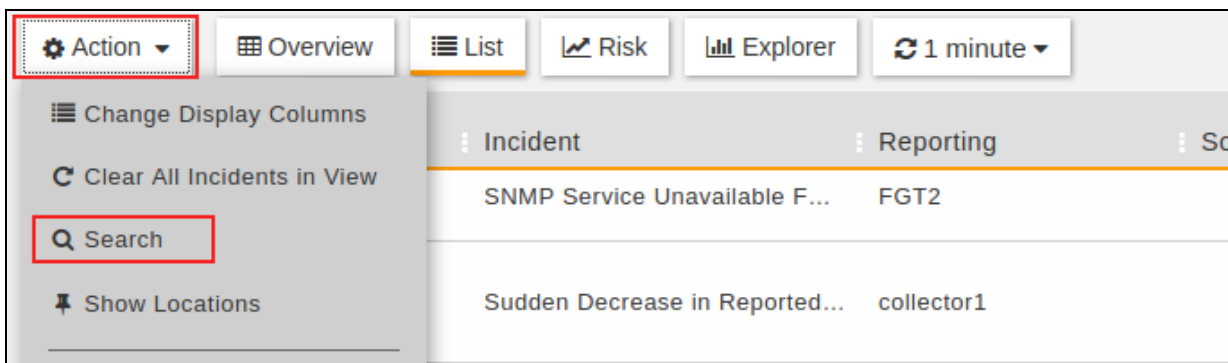
Now, you will verify the incident that was created because the SNMP service was down. You will notice that the incident status is **Active**.

To verify the incident

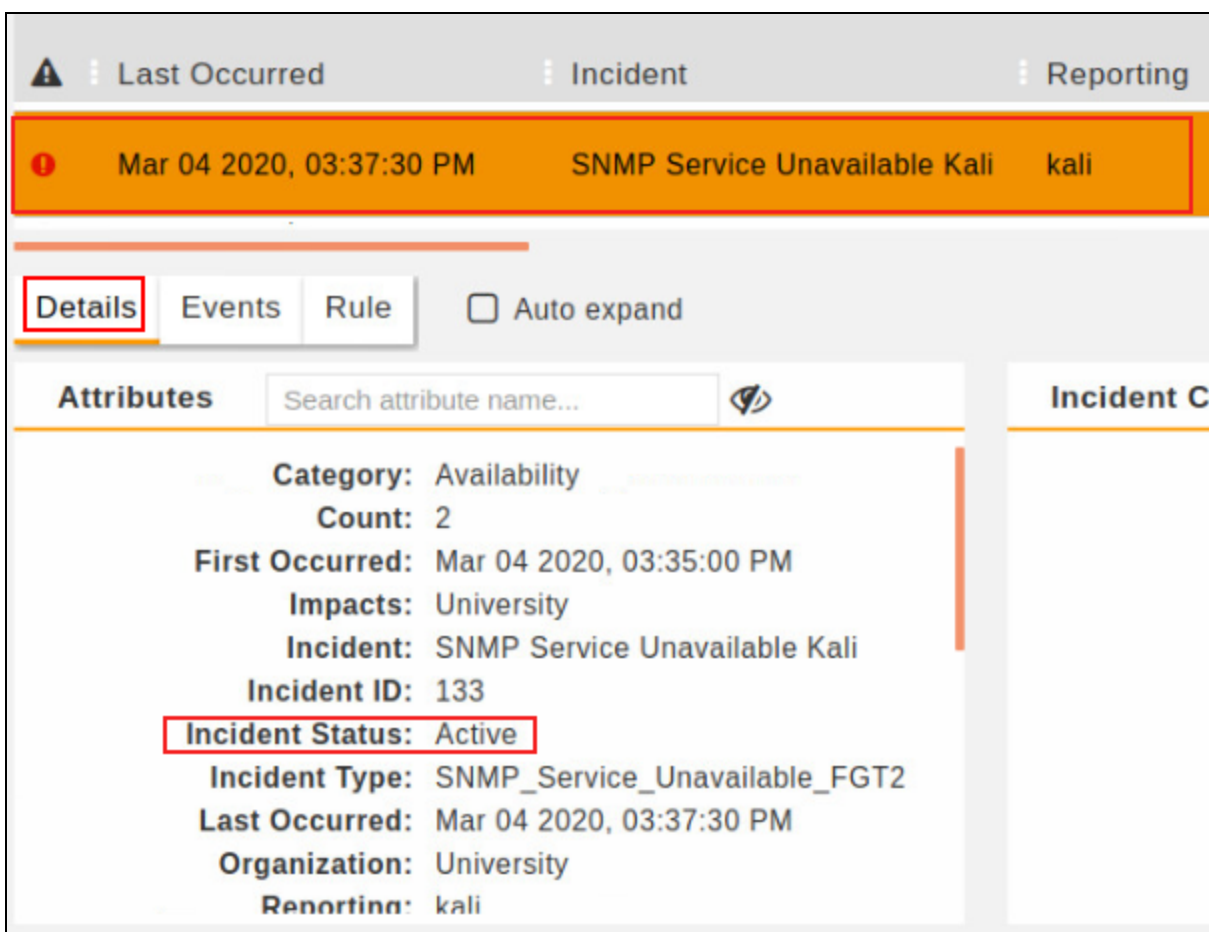
- Continuing on the FortiSIEM GUI, click the **INCIDENTS** icon (🔔).
- Click **List** and from the drop-down select **List by Time**.



3. In the **Action** drop-down list, select **Search**.



4. In the left pane, click **Incident Status**, and deselect **Active**.
This sets the **Incident Status** setting to **All**.
5. Find and select the **SNMP Service Unavailable Kali** incident.
6. Click **Details**.
Review the incident and the current status.



Enable the SNMP Service

Now, you will enable the SNMP service so that you can observe the incident status automatically change to an automatically cleared status.

To enable the SNMP service on Kali

1. Return to the Kali VM, and in the terminal window, type the following command to start the SNMP service:

```
service snmpd start
```

2. Type the following command to verify that the SNMP service has started:

```
service snmpd status
```

```
root@kali:~# service snmpd status
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Wed 2021-04-28 06:16:09 EDT; 25s ago
     Process: 1842 ExecStartPre=/bin/mkdir -p /var/run/agentx (code=exited, status=0/SUCCESS)
    Main PID: 1843 (snmpd)
      Tasks: 1 (limit: 2349)
     Memory: 9.5M
    CGroup: /system.slice/snmpd.service
            └─1843 /usr/sbin/snmpd -LOW -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f -p /run/snmpd.pid
```

3. Close the terminal window.
4. Close the Kali VM browser tab.

Run the Rule as a Query

You will run the **SNMP Service Unavailable** rule as a query again, and monitor the packet loss percentage. The incident will automatically clear if the packet loss percentage value is less than 10%.

To run the rule as a query

1. Return to the Supervisor FortiSIEM management GUI.
2. On the **Edit SubPattern** page, click **Run as Query**.
3. Deselect all organizations except **University**.
4. Set the **Time Range** to 4 minutes.
5. Click **Run**.

You will notice that the packet loss percentage value will continue to decrease. The system will automatically clear the incident when the packet loss percentage value is less than 10%.

Depending on network latency, the **SNMP Ping Stat** round trip value could be slower than usual.

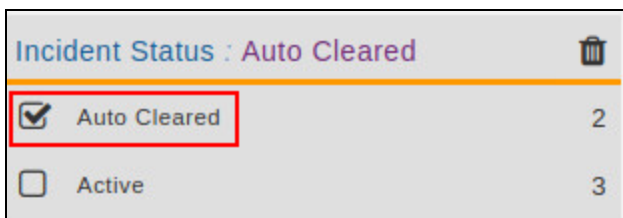
Verify the Incident Status

Now, you will verify the incident and observe the status of the incident change to automatically clear.

To verify the automatically cleared status for the SNMP service incident

1. Return to the **INCIDENTS** page of the FortiSIEM GUI.
2. In the left pane, click **Incident Status**.

3. Select **Auto Cleared**.

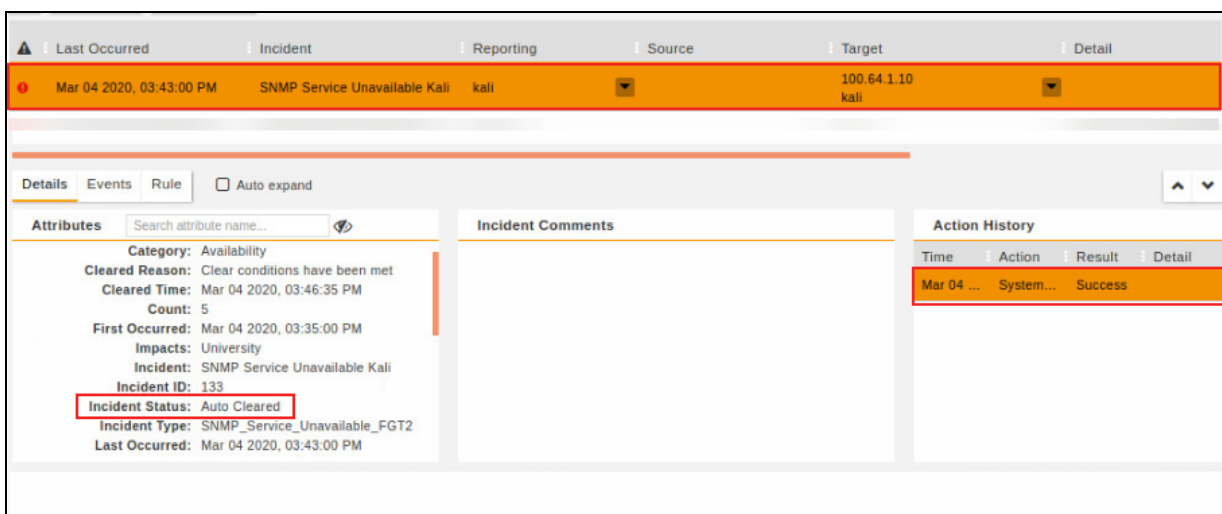


If you don't see the **Auto Cleared** option on your GUI, it means the incident has not automatically cleared yet. Wait a few more minutes.

4. Find and select the **SNMP Service Unavailable Kali** incident.

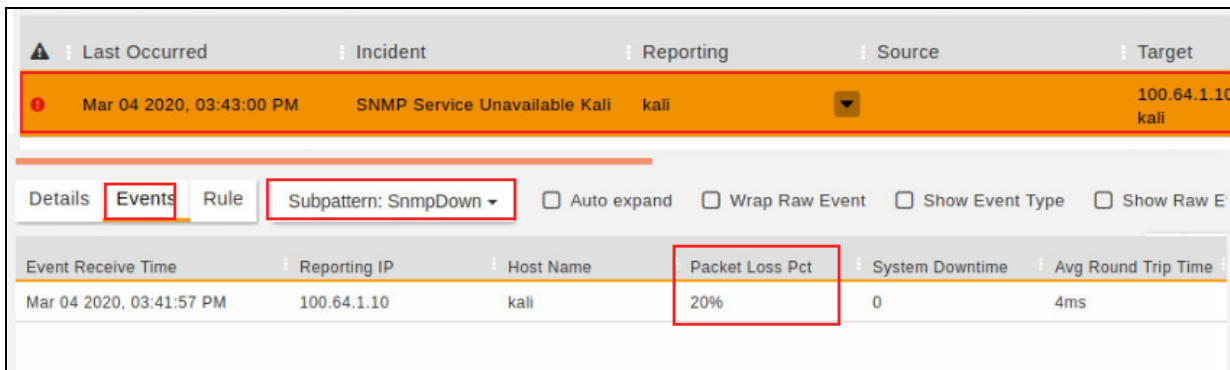
5. Click **Details**.

Review the incident and the current status.



The **Action History** section displays the reason the incident was cleared. In this case, it was cleared by the system since it met the clear conditions that were defined in the rule.

6. Click **Events**.



Review the packet loss percentage. In this example, the packet loss was 20% and this is the reason why the incident was triggered. In the rule, you defined 5% as the threshold and any packet loss above 5% should trigger an incident.

From the incident, you will not be able to view the event that caused the incident to clear. You can see only the events related to the subpattern that triggered the incident. In this case, the subpattern was **SnmpDown**.

7. Log out of the Supervisor FortiSIEM management GUI.

Lab 13: Remediation

In this lab, you will remediate incidents manually from FortiSIEM. You will also configure the REST API on FortiGate so that you can connect FortiSOAR to FortiGate. Then, you will perform mitigation of malicious indicators of compromise (IOCs) from FortiSOAR and block them on FortiGate.

You will perform other FortiSOAR actions, such as extracting and enriching indicators.

Objectives

- Run a remediation script on an incident to block an IP address on FortiGate
- Configure the REST API on FortiGate
- Configure the FortiGate connector on FortiSOAR
- Extract, enrich, and mitigate IOCs

Time to Complete

Estimated: 30 minutes

Exercise 1: Remediating an Incident

FortiSIEM can perform remediation after an incident is detected. The remediation can be performed either automatically, using notification policies, or manually. In this exercise, you will learn how to remediate an incident from FortiGate manually from FortiSIEM.

Execute the Remediation

On FortiSIEM, you will find several existing remediation scripts, including scripts for FortiGate devices. You will remediate an incident that was generated by FGT_Aviation. You will block the offending IP address on FortiGate by running a remediation action from FortiSIEM.

When an incident that affects a FortiGate device occurs, you can execute the remediation automatically using a notification policy. However, in this task, you will execute the remediation manually from FortiSIEM.

To execute the remediation script

1. On the supervisor FortiSIEM GUI, log in to the super organization with the following credentials:

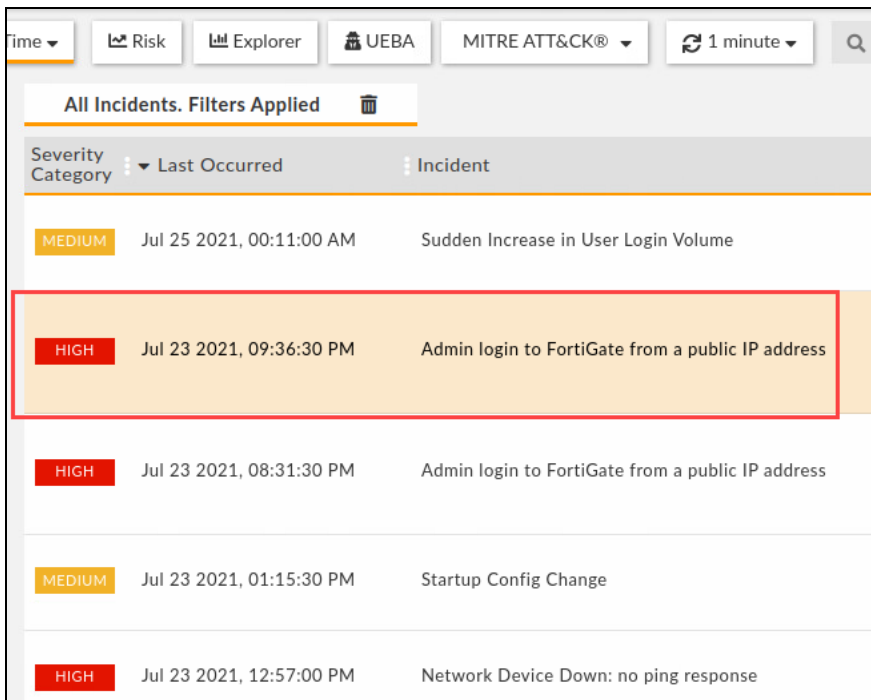
Field	Value
User ID	admin
Password	Fortinet1!
Cust/Org Id	super
Domain	LOCAL

2. Click **INCIDENT**.
3. Click **List**.
4. In the **Action** drop-down list, select **Search**.
5. Click **Last 2 Hours**, and then set it to **3 days**.
6. Click **Apply Time Range**.
7. Verify that **Incident Status** is set to **Active**.
8. In the search results, find an incident that has a **Target** of **fgt_aviation**.



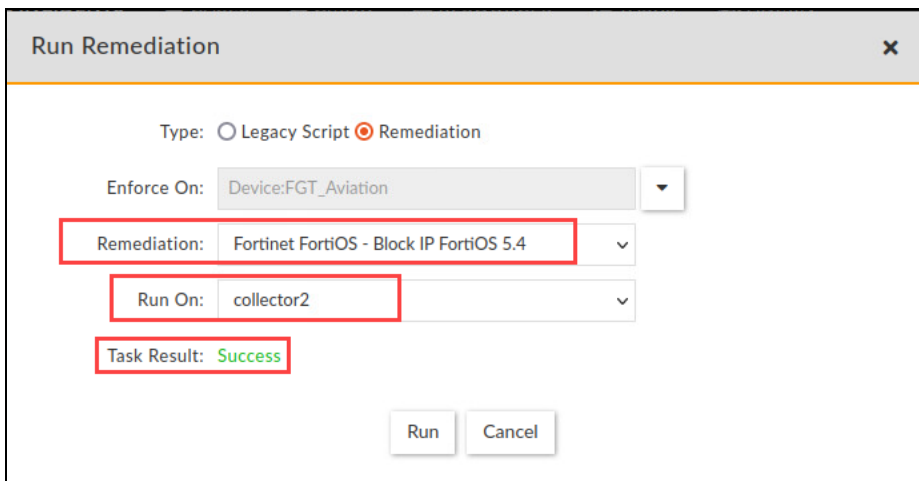
9. Identify and select the **Admin login to FortiGate from a public IP address** incident that has a **Source** of 100.64.1.10.

If you don't see any incidents on the first page, go to the next incident page.



10. Select the incident, and then in the **Action** drop-down list, select **Remediate Incident**.
11. In the **Type** field, select **Remediation**.
12. In the **Remediation** field, select **Fortinet FortiOS - Block IP FortiOS 5.4**.
13. In the **Run On** field, select **collector 2**.
14. Click **Run**.

Wait for the script to execute. The **Task Result** field displays **Success**.



The 'Run Remediation' dialog box shows the following configuration:

- Type: ☒ Remediation
- Enforce On: Device:FGT_Aviation
- Remediation: Fortinet FortiOS - Block IP FortiOS 5.4
- Run On: collector2
- Task Result: Success

Buttons: Run, Cancel

15. Close the **Run Remediation** window.
16. Click the **Details** tab to open details about the incident.

Review the **Action History** for the incident.

Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target
High	Jul 23 2021, 08:31:30 PM	Admin login to FortiGate from a public IP address	Initial Access	Exploit: Public Fac...	FGT_Aviation	100.64.1.10	10.0.3.254 FGT_Aviation User: admin

Details	Events	Rule	☐ Auto expand
---------	--------	------	--------------------------------------

Attributes

Event Type: Admin login to FortiGate from a public IP address

First Occurred: Jul 23 2021, 12:59:00 PM

Incident ID: 47

Incident Title: 100.64.1.10 attempted to log into FortiGate 10.0.3.254 from a public IP address

Incident Comments

Add comments to Incident...

Clear Save

Action History ☐ Wrap Content

Time	Action	Result
Jul 23 2021, 08:48:24 PM	User admin Remediation triggered	Success

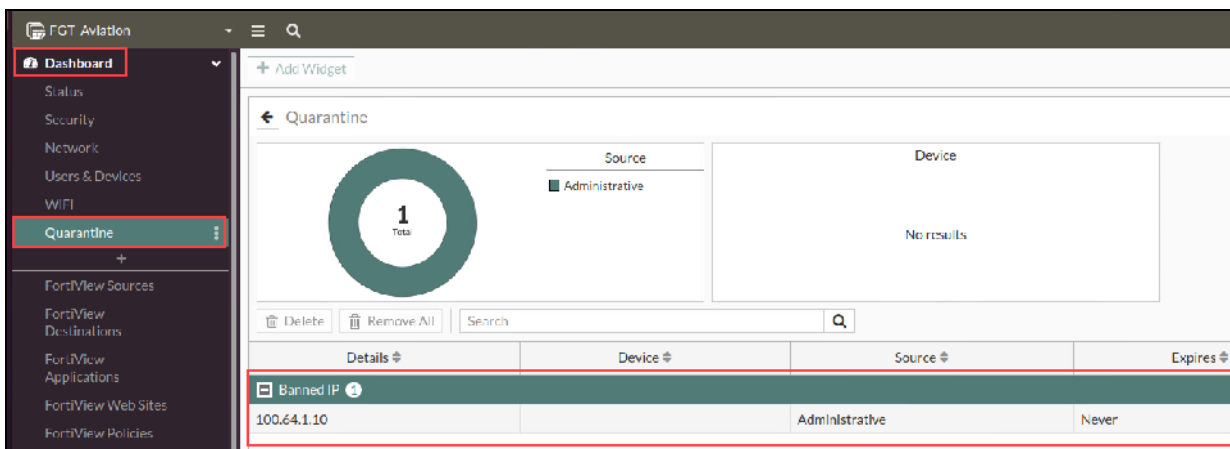
Analyze the Remediation Result

After the remediation is completed, the offending IP address is blocked on FGT_Aviation. Now, you will verify the blocked IP address on FGT_Aviation.

To analyze the remediation result

1. On the FGT_Aviation FortiGate GUI, log in with the username `admin` and password `password`.
2. Expand **Dashboard**.
3. Select **Quarantine**.
4. Review the **Banned IP** entry.

The IP address 100.64.1.10 was blocked by FortiSIEM because that is the source public IP address that logged in to the FGT_Aviation firewall.



5. Log out of the FortiGate GUI.

Exercise 2: Configuring the REST API on FortiGate

In this exercise, you will configure the REST API on FGT_Aviation.

Configure the REST API on FortiGate

You will create a new administrator profile and a REST API administrator account, and then generate an API key on FortiGate.

To configure a REST API administrator profile

1. On the FGT_Aviation FortiGate GUI, log in with the username `admin` and password `password`.
2. Click **System > Admin Profiles**.
3. Click **Create New**.
4. In the **Name** field, type `FortiSOAR_API`.
5. In the **Permissions** drop-down list, select **Read/Write**.

New Admin Profile

Name: FortiSOAR_API

Comments: 0/255

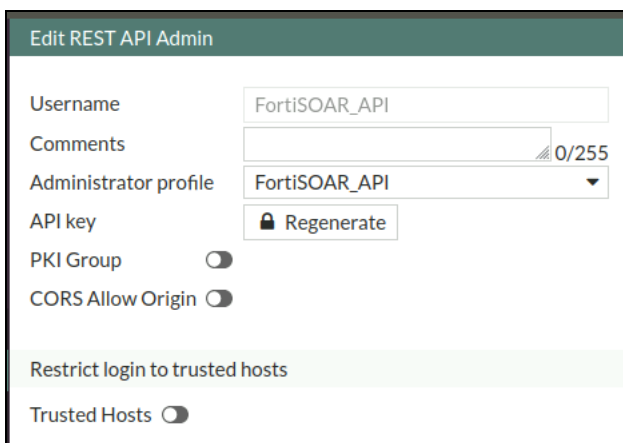
Access Permissions

Access Control	Permissions	Set All
Security Fabric	☐ None ☒ Read ☒ Read/Write	
FortiView	☐ None ☒ Read ☒ Read/Write	
User & Device	☐ None ☒ Read ☒ Read/Write	
Firewall	☐ None ☒ Read ☒ Read/Write	☒ Custom
Log & Report	☐ None ☒ Read ☒ Read/Write	☒ Custom
Network	☐ None ☒ Read ☒ Read/Write	☒ Custom
System	☐ None ☒ Read ☒ Read/Write	☒ Custom
Security Profile	☐ None ☒ Read ☒ Read/Write	☒ Custom
VPN	☐ None ☒ Read ☒ Read/Write	
WAN Opt & Cache	☐ None ☒ Read ☒ Read/Write	

6. Click **OK**.

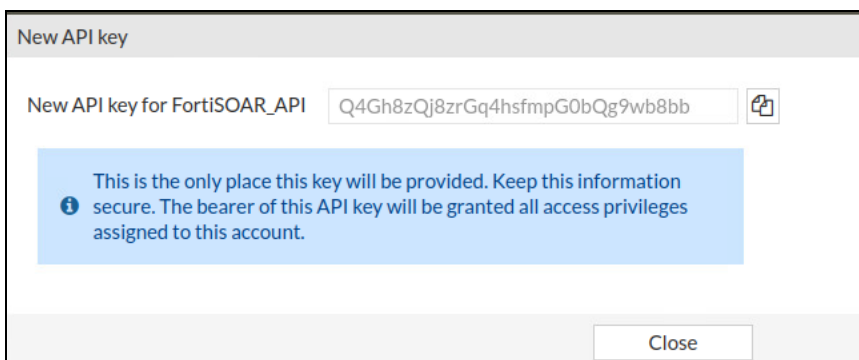
To configure an API administrator account

1. Continuing on the FGT_Aviation GUI, click **System > Administrators**.
2. In the **Create New** drop-down list, select **REST API Admin**.
3. In the **Username** field, type `FortiSOAR_API`.
4. In the **Administrator profile** drop-down list, select **FortiSOAR_API**.
5. Disable **PKI Group**.
6. Disable **Trusted Hosts**.



7. Click **OK**.

The API key is displayed. This is the key that is used to authenticate FortiSOAR on FortiGate.



It is important to save this API key because you will need it later when you configure the FortiGate connector on FortiSOAR. If you close the **New API key** window, you cannot access this same key again. If you lose the key or forget to save it, you can generate a new key by clicking **Regenerate** on the **Administrator** configuration page.

8. Click **Close**.
9. Click **OK**.

Configure a New Web Filter Profile

You will configure a new web filter profile that FortiSOAR modifies to block URLs.

To configure a new web filter profile

1. Continuing on the FortiGate GUI, click **Security Profiles > Web Filter**.
2. Click **Create New**.
3. In the **Name** field, type `FortiSOAR_URL_Block`.
4. Disable **FortiGuard category based filter**.
5. Enable **URL Filter**.
6. Click **Create New**.
7. Configure the following settings:

Field	Value
URL	fortinet.com
Type	Simple
Action	Exempt
Status	Enable

8. Click **OK**.

Your configuration should match the following example:

Edit Web Filter Profile

Name: FortiSOAR_URL_Block

Comments: Write a comment... 0/255

Feature set: Flow-based Proxy-based

☐ FortiGuard Category Based Filter

☐ Allow users to override blocked categories

☒ Static URL Filter

Block invalid URLs: ☐

URL Filter: ☒

[+ Create New](#) [Edit](#) [Delete](#)

URL	Type	Action	Status
fortinet.com	Simple	Exempt	Enable

☐ Block malicious URLs discovered by FortiSandbox

Content Filter: ☐

9. Click **OK**.
10. Log out of the FortiGate GUI.

Exercise 3: Configuring the FortiGate Connector

In this exercise, you will configure the FortiGate connector on FortiSOAR.

Configure the FortiGate Connector

The FortiGate connector allows FortiSOAR to query and make changes to a FortiGate configuration. Some sample actions include blocking URLs, domains, applications, and IP addresses. For this task, you need the REST API key you generated and saved in the previous exercise.

To configure the FortiGate connector

1. On the FortiSOAR GUI, log in with the username `csadmin` and password `Fortinet1!`.
2. Click **Automation > Connectors**.
3. Click **Installed**.
4. Click **Fortinet FortiGate**.
5. In the **Configuration Name** field, type `FGT_Aviation`.
6. Enable **Mark As Default Configuration**.
7. In the **Hostname** field, type `https://10.0.3.254`.
8. In the **API Key** field, paste the REST API key that you generated in the previous exercise.
9. Leave the **Port** number at the default value, which is `443`.
10. In the **Web Filter Profile Name** field, type `FortiSOAR_URL_Block`.
This is the name of the web filter profile that you created on FortiGate in the previous exercise, which FortiSOAR accesses using the REST API to apply URL and domain blocks.
11. Disable **Verify SSL**.
The SSL certificate that FortiGate uses in this lab environment uses a self-issued certificate that FortiSOAR cannot independently validate.
12. Click **Save**.
The value of the **CONFIGURATION** field is **COMPLETED**, and the value of the **HEALTH CHECK** field is **AVAILABLE**.

Fortinet FortiGate
Connector Version 5.0.0
Certified: Yes
Publisher: Fortinet

Fortinet FortiGate enterprise firewall provide high performance, consolidated advanced security and granular visibility for broad protection across the entire digital attack surface.

Active Deactivate Connector ✓ Compatible with your integration

Configurations **1** Actions **11** Playbooks **1** Agents **0**

FGT_Aviation Target ⓘ Self Agent

⚙ CONFIGURATION: COMPLETED 🔍 HEALTH CHECK: AVAILABLE ⓘ

Configuration Name *
FGT_Aviation

☒ Mark As Default Configuration Visibility ⓘ Public Private

Hostname: * ⓘ
https://10.0.3.254

API Key: *
Set API Key
.....

API Key fields are write-only. If you do not change this field, your API Key will not be overwritten.

Port: *
443

Web Filter Profile Name: ⓘ
FortiSOAR_URL_Block

✓ Save ✕ Cancel 🗑 Uninstall

13. Close the connector configuration page.

Configure a Playbook to Use the FortiGate Connector

You will review the **Mitigate Malicious URL** playbook that uses the FortiGate connector.

To configure a playbook to use the FortiGate connector

1. Continuing on the FortiSOAR GUI, click **Automation > Playbooks**.
2. Click **00-LAB 13**.
3. Open the **Mitigate Malicious URL custom** playbook.
4. Double-click the **Block URL** step.

Review the playbook step and verify that the **Configuration** field is set to **FGT_Aviation**. If it is not, select **FGT_Aviation** in the drop-down list.

The screenshot shows the configuration window for the Fortinet FortiGate connector. The window title is "Fortinet FortiGate 5.0.0". Inside, there's a "PROLOGUE" section with a description field. Below that, the connector details are shown: "Fortinet FortiGate", "Connector Version 5.0.0", "Certified: Yes", and "Publisher: Fortinet". A "DOCUMENTATION" link is present. The "Target" is set to "Self". The "Configuration:" dropdown is set to "FGT_Aviation" and is highlighted with a red box. The "Action:" dropdown is set to "Block URL". Below the action, there's a descriptive text: "Blocks URLs on Fortinet FortiGate using the Web Filter Profile Name Policy that you have specified while configuring Fortinet FortiGate. For more information see the 'Blocking or Unblocking IP addresses, URLs, or applications in Fortinet FortiGate' section." The "Inputs" section shows "URL:" with a value of "{{vars.input.records[0].value}}" and "VDOM:" which is empty. At the bottom, there are buttons for "+ Variables", "+ Loop", "+ Condition", "+ Message", "+ Mock Output", "Ignore Error", and "No". At the very bottom, there are "Save", "Cancel", and "Delete Step" buttons.

5. Click **Save**.
6. Click **Save Playbook**.
7. Log out of the FortiSOAR GUI.

Exercise 4: Mitigating Malicious IOCs

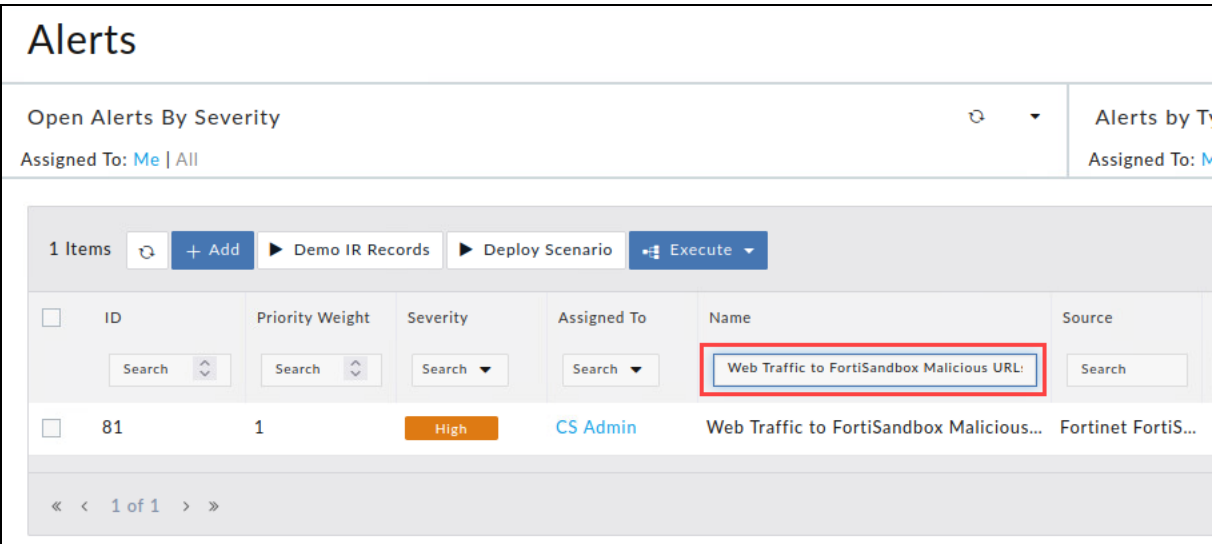
In this exercise, you will execute three different types of playbooks. The first playbook will extract indicators from an alert that was ingested from FortiSOAR. The second playbook will enrich indicators that were extracted from the alert. The third playbook will block malicious URLs on the FGT_Aviation FortiGate.

Extract Indicators

On FortiSOAR, there are a few built-in playbooks that you can use to extract indicators from phishing emails and so on. You will use a custom playbook designed to extract indicators from a FortiSIEM incident that was ingested to FortiSOAR.

To extract indicators

1. On the FortiSOAR GUI, log in with the username `csadmin` and password `Fortinet1!`.
2. Click **Incident Response > Alerts**.
3. Search for the **Web Traffic to FortiSandbox Malicious URLs** alert.



4. Select and open this alert.
5. Scroll down to the **Indicators** tab.
The indicator list is empty because no indicators were extracted.

Alert: Web Traffic to FortiSandbox Malicious URLs-P...

High Alert-81 Web Traffic to FortiSandbox Malicious URLs-PH_RULE_WEB_FORTISANDBOX_MALWARE_URL

Last Modified: 12/28/2021 01:56 PM by klaybook

+ Add Tags

Assigned To: CS Admin

Status: Select

Source: Fortinet FortiSIEM

Source ID: 158

Escalated: --

Type Details

Type: Select

MITRE Technique: Exfiltration

MITRE ATT&CK ID: T1041

Indicators Correlations Tasks Source Data External Communications Access Control

0 Items + Add Link Execute

Last Seen	First Seen	Status	Type	Sources	Value	File
No Results						

6. Scroll to the bottom of the record, and in the **Execute** drop-down list, select **Extract Indicators from FortiSIEM Incident custom**.

Indicators Correlations Tasks Source Data External Communications Access Control

0 Items + Add Link Execute

Search Playbooks

Add a user as record's owners

Extract Indicators from FortiSIEM Incident custom

Investigate Malicious Indicators

Pause SLA

Escalate Resolve Send Email Execute Actions

The playbook executes and the following indicators are populated.

Alert: Web Traffic to FortiSandbox Malicious URLs PH...
High Alert-81 Web Traffic to FortiSandbox Malicious URLs-PH_RULE_WEB_FORTISANDBOX_MALWARE_URL
Last Modified: 07/28/2021, 01:56 PM by SteveCock

+ Add Tags

Indicators Correlations Tasks Source Data External Communications Access Control

10 Items + Add Link Execute

	Last Seen	First Seen	Status	Type	Source	Value	File	Reputation
	Select	Select	Search	Search	Search	Search		Search
	07/28/2021 ...	07/28/2021 0...	TBD	Email Address		Ted.Jones@example.com		Good
	07/28/2021 ...	07/26/2021 0...	TBD	Email Address		admin@example.com		Good
	07/28/2021 ...	07/26/2021 0...	TBD	FileHash MD5		9ebab67ed5e3d66c5e253a407fa2f156		
	07/28/2021 ...	07/27/2021 0...	TBD	URL		https://upload.gumblar.cn		
	07/28/2021 ...	07/28/2021 0...	TBD	FileHash MD5		C4C4F56CF7B04762B053F8F88B8FCF47		
	07/28/2021 ...	07/27/2021 0...	TBD	IP Address		172.16.1.9		No Reputation Av
	07/28/2021 ...	07/26/2021 0...	TBD	Host		example.com		No Reputation Av
	07/28/2021 ...	07/28/2021 0...	TBD	File		firefox.exe		
	07/28/2021 ...	07/27/2021 0...	TBD	IP Address		172.16.0.100		No Reputation Av
	07/28/2021 ...	07/27/2021 0...	TBD	Host		upload.gumblar.cn		No Reputation Av

Escalate Resolve Send Email Execute Actions

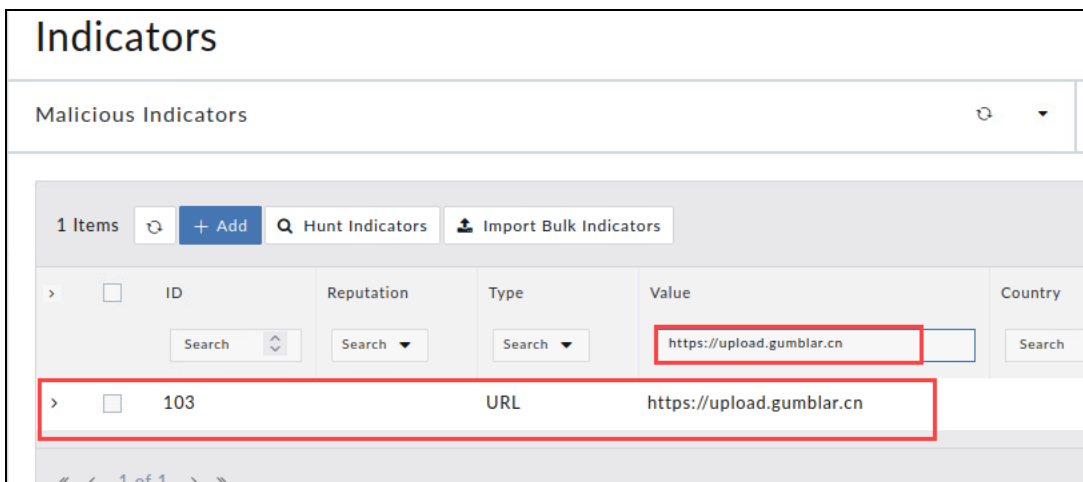
7. Close the record.

Enrich Malicious Indicators

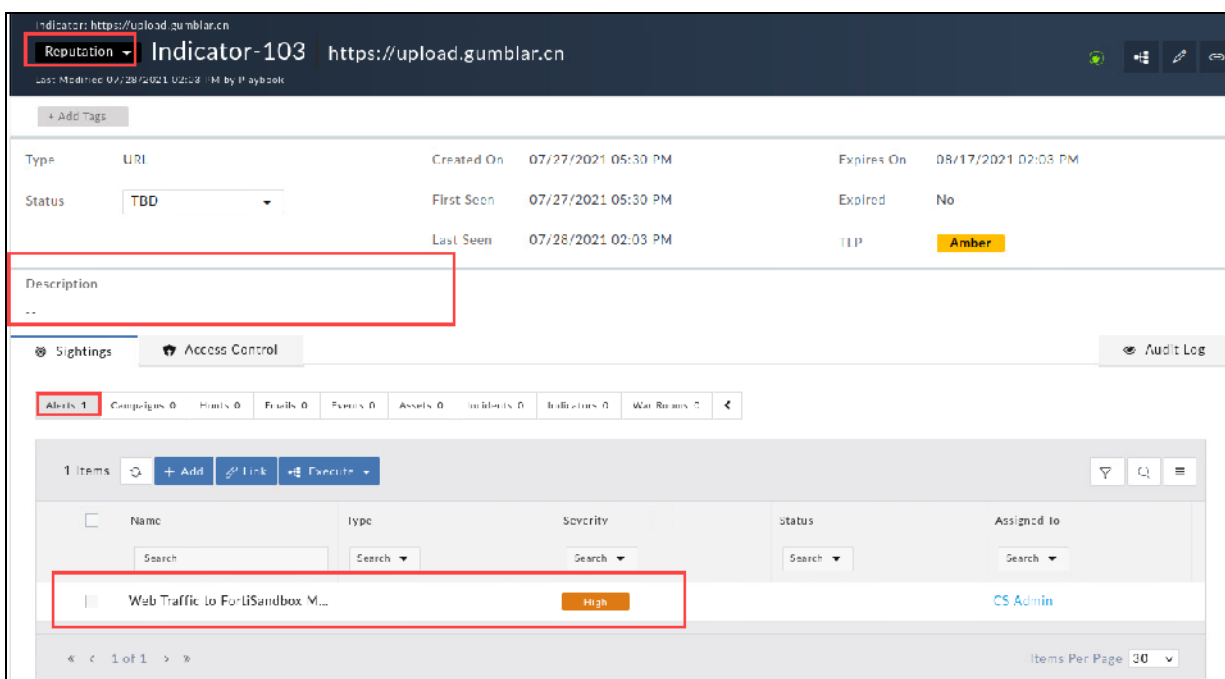
On FortiSOAR, there are a few built-in playbooks that you can use to enrich indicators from phishing emails and so on. You will use a custom playbook designed to enrich an indicator that was extracted from a FortiSIEM incident.

To enrich indicators

1. Continuing on the FortiSOAR GUI, click **Threat Intelligence > Indicators**.
2. Search for the **https://upload.gumblar.cn** indicator.

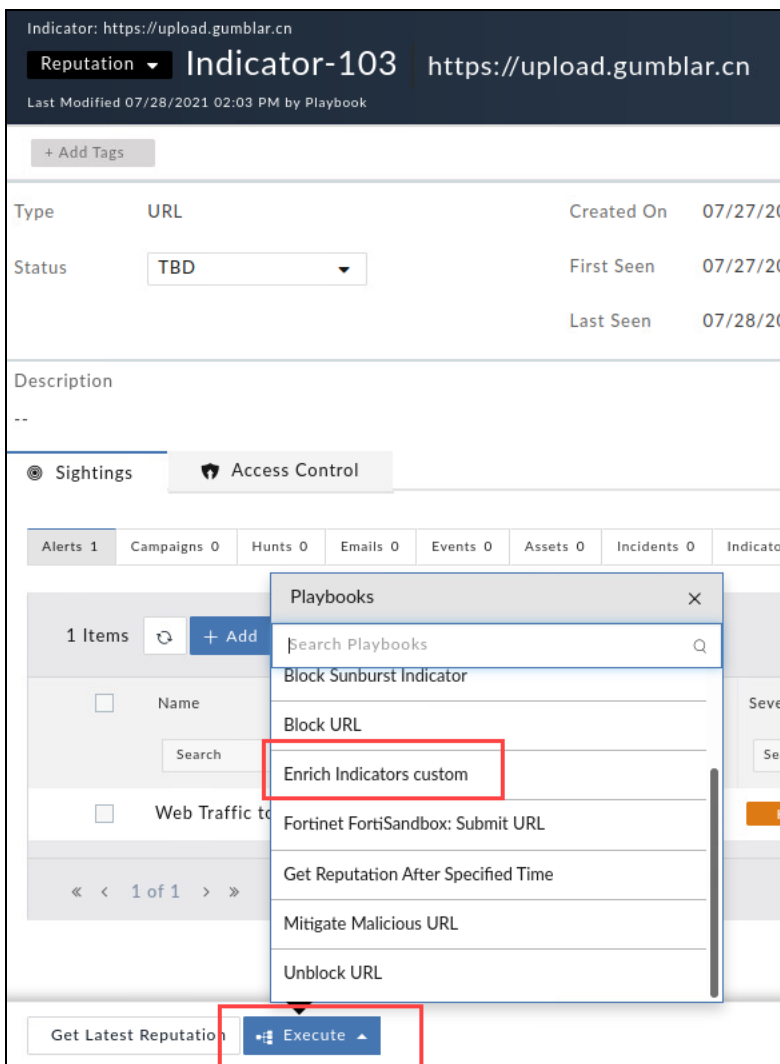


3. Select and open the indicator.
4. Review the indicator.

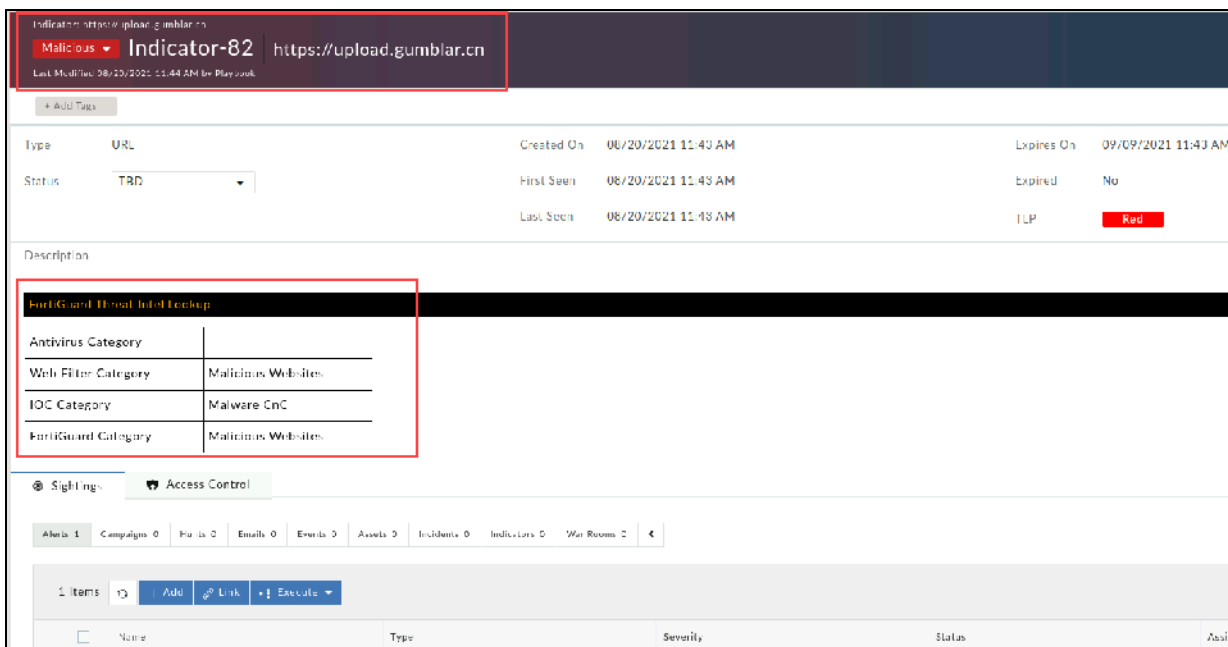


The **Reputation** for the indicator is unknown, and there is no description. The indicator is linked to the **Web Traffic to FortiSandbox Malicious URLs** alert.

5. Scroll to the bottom of the record, and then in the **Execute** drop-down list, select **Enrich Indicators custom**.



The playbook executes. The **Reputation** and **Description** of the indicator is updated and the **TLP** is updated to **Red**.



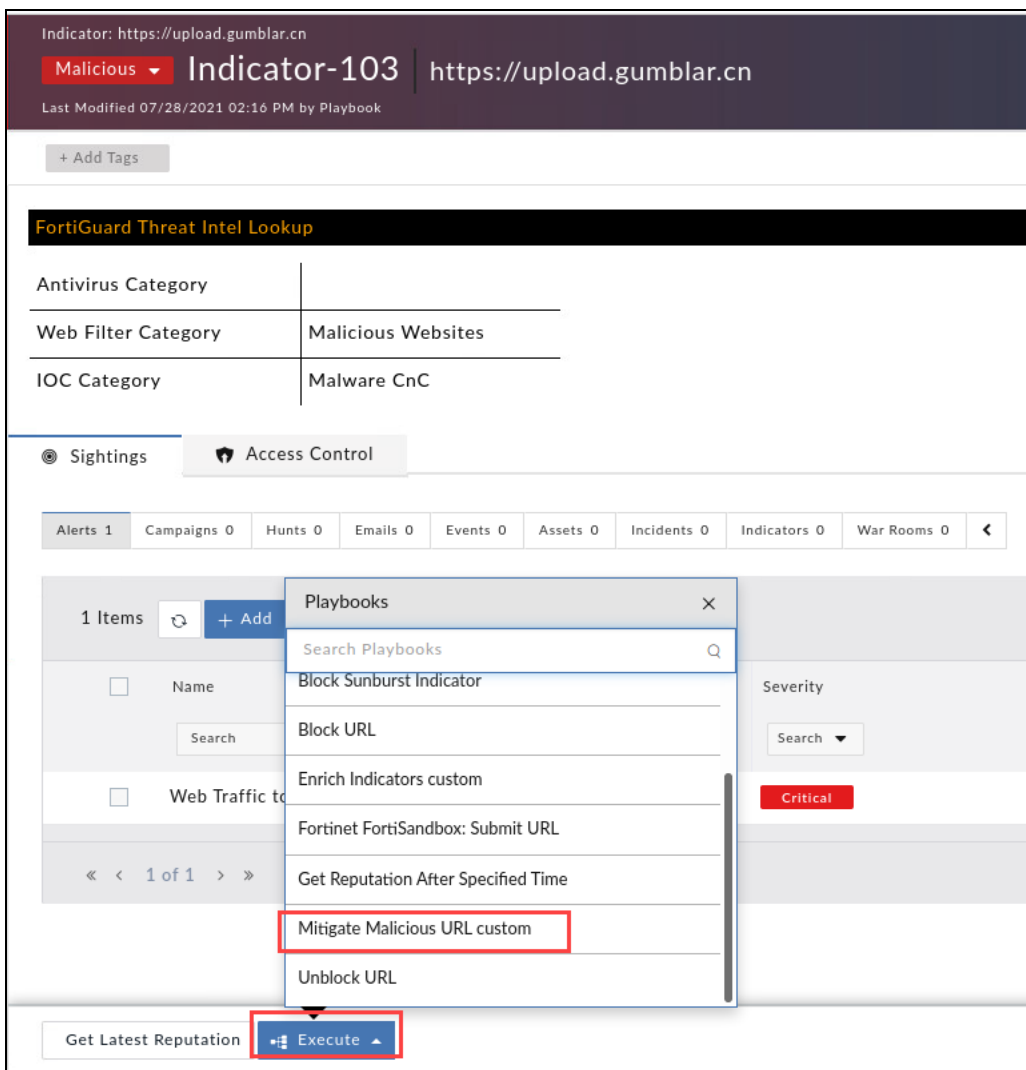
6. Close the record.

Block Malicious Indicators

You will block the malicious indicator on the FGT_Aviation firewall.

To block indicators on the firewall

1. Continuing on the FortiSOAR GUI, click **Threat Intelligence > Indicators**.
2. Search for the **https://upload.gumblar.cn** indicator.
3. Select and open the indicator.
4. Scroll to the bottom of the record, and then in the **Execute** drop-down list, select **Mitigate Malicious URL custom**.



Wait a minute for the playbook to finish executing.

5. Close the record.
6. Log out of the FortiSOAR GUI.

To verify the URL block on FortiGate

1. On the FGT_Aviation GUI, log in with the username `admin` and password `password`.
2. Click **Security Profiles > Web Filter**.
3. Double-click **FortiSOAR_URL_Block**.

Verify that the URL is added to the URL filter with a **Block** action.

Edit Web Filter Profile

Name: FortiSOAR_URL_Block

Comments: Write a comment... 0/255

Feature set: Flow-based Proxy-based

☐ FortiGuard Category Based Filter

☐ Allow users to override blocked categories

☒ Static URL Filter

Block invalid URLs ☐

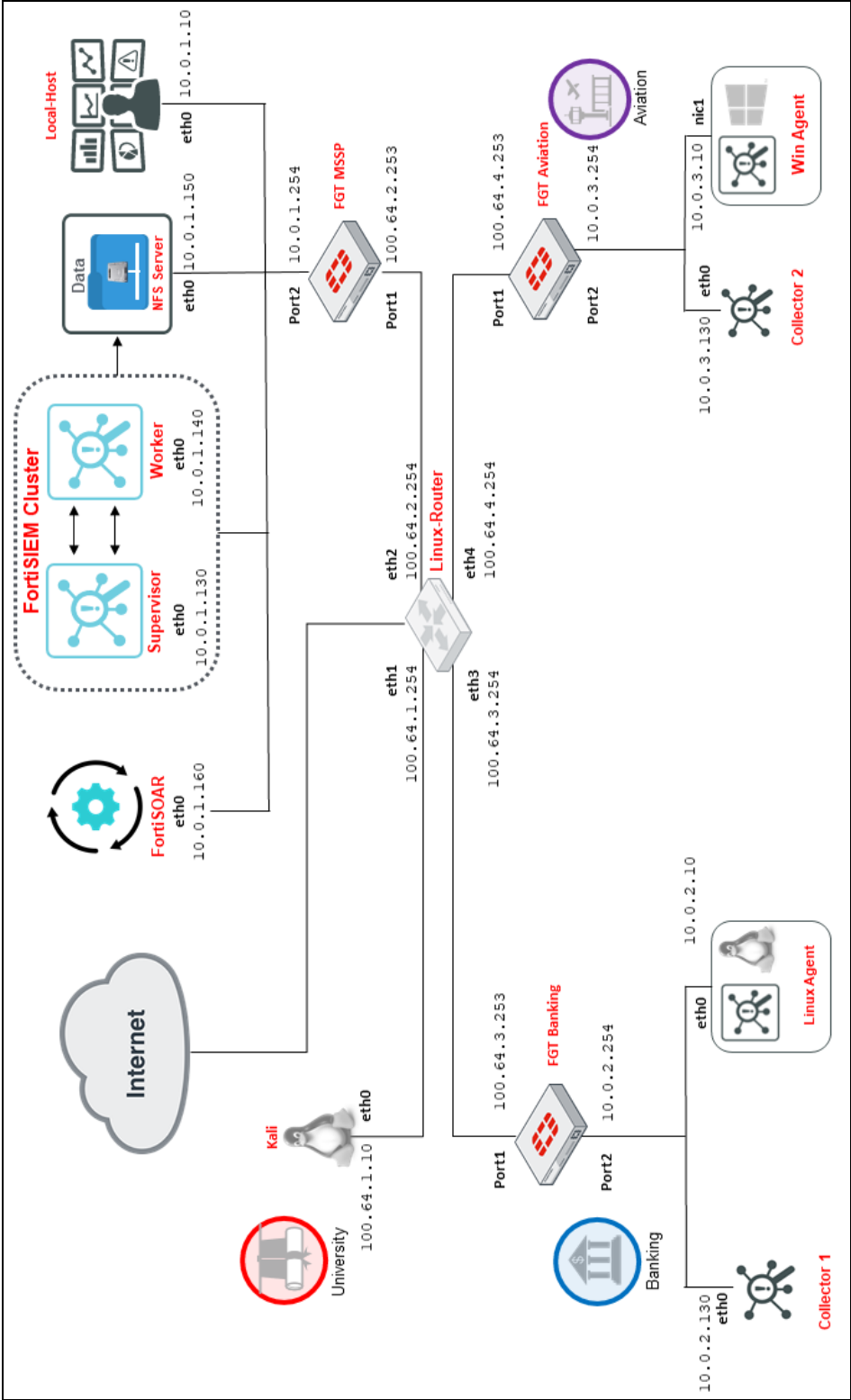
URL Filter ☒

URL	Type	Action	Status
fortinet.com	Simple	Exempt	Enable
tanerm.ug/~zadmin/lmark/frg1/link.php	Simple	Block	Enable
upload.gumblar.cn	Simple	Block	Enable

Block malicious URLs discovered by FortiSandbox ☐

4. Log out of the FGT_Aviation GUI.

Appendix A





FORTINET®



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2021 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.