

Exercise 1: Configuring Data Sources

In this exercise, you will determine which data sources in your lab environment are applicable in the context of detecting the Group ABC mapped behaviors. You will identify these data sources and configure them to forward the applicable logs to FortiAnalyzer.

Identify Data Sources in Context

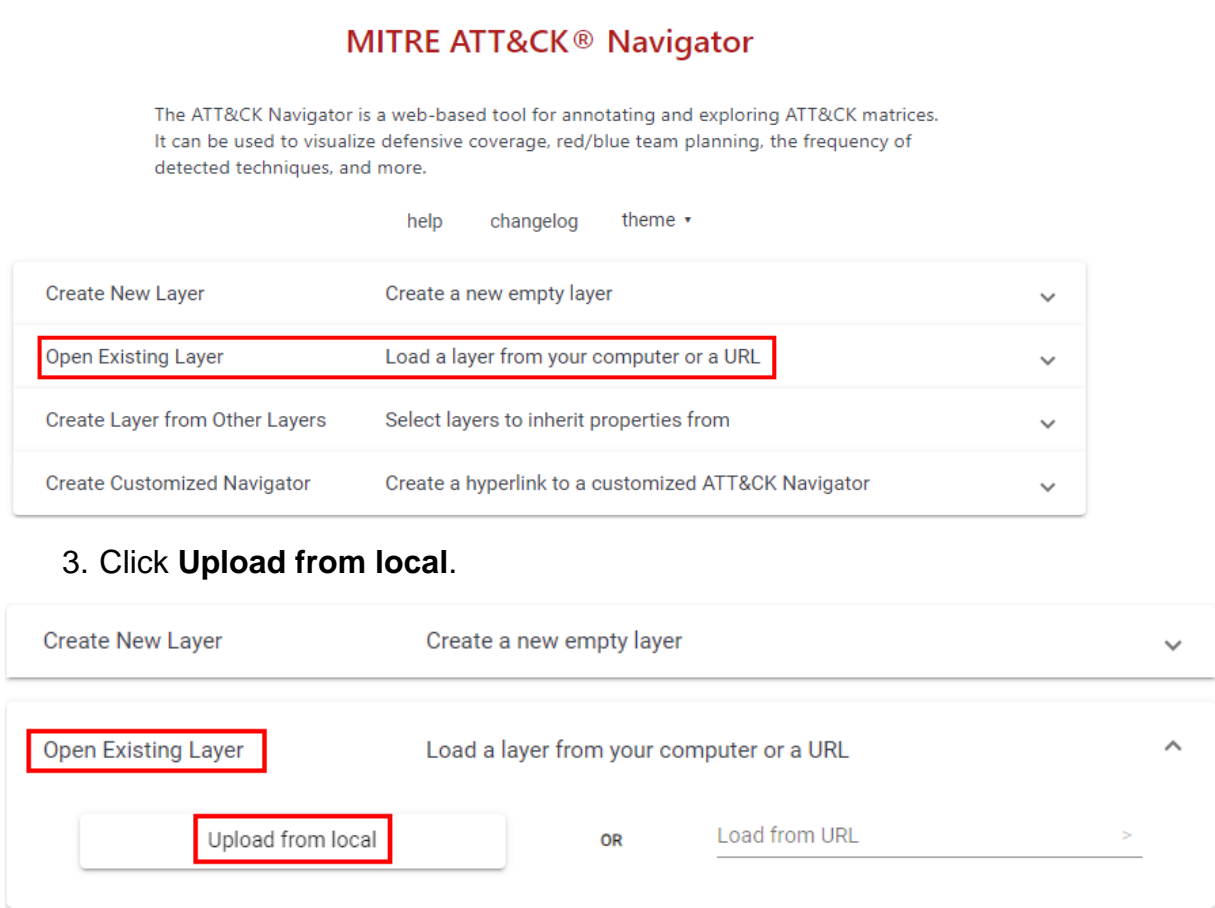
First, you will load the MITRE JSON attack file that you created in Lab 1, as a member of the purple team, into the ATT&CK Navigator. Next, you will analyze the ATT&CK technique and define the data sources.

To load the MITRE JSON file into the ATT&CK Navigator

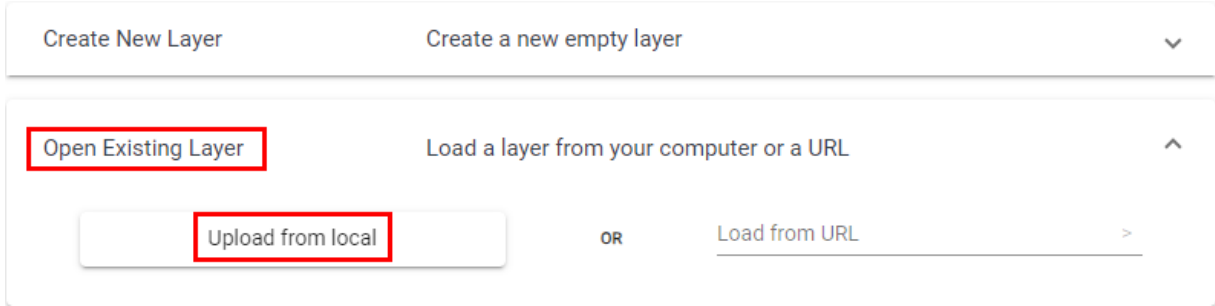
1. On the bastion host, in Google Chrome, return to the ATT&CK Navigator tab.

If you closed or navigated away from that tab, perform the following steps to retrieve your mapping:

1. On the bastion host, in Chrome, open a new tab, and then click the **ATT&CK Navigator** bookmark in the **SOC Analyst** folder.
2. Click **Open Existing Layer**.

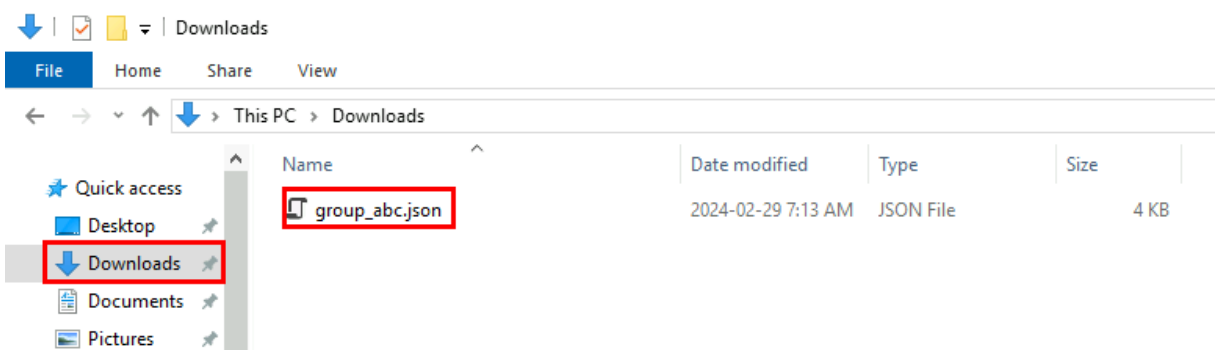


3. Click **Upload from local**.



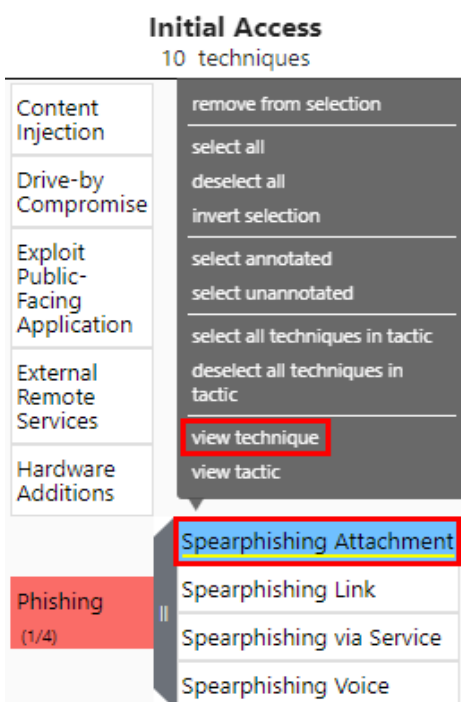
4. Locate the JSON file of your mapping that you downloaded in the previous lab, and then click **Open**.

If you saved the JSON file in the default location, it is located in the **Downloads** folder.



To analyze the ATT&CK technique and define the data sources

1. In the **Initial Access** column, to the right of the **Phishing** technique, click || to expand the subtechniques.
2. Right-click the **Spearphishing Attachment** subtechnique, and then select **view technique**.



The **Spearphishing Attachment** subtechnique page opens in a new tab.

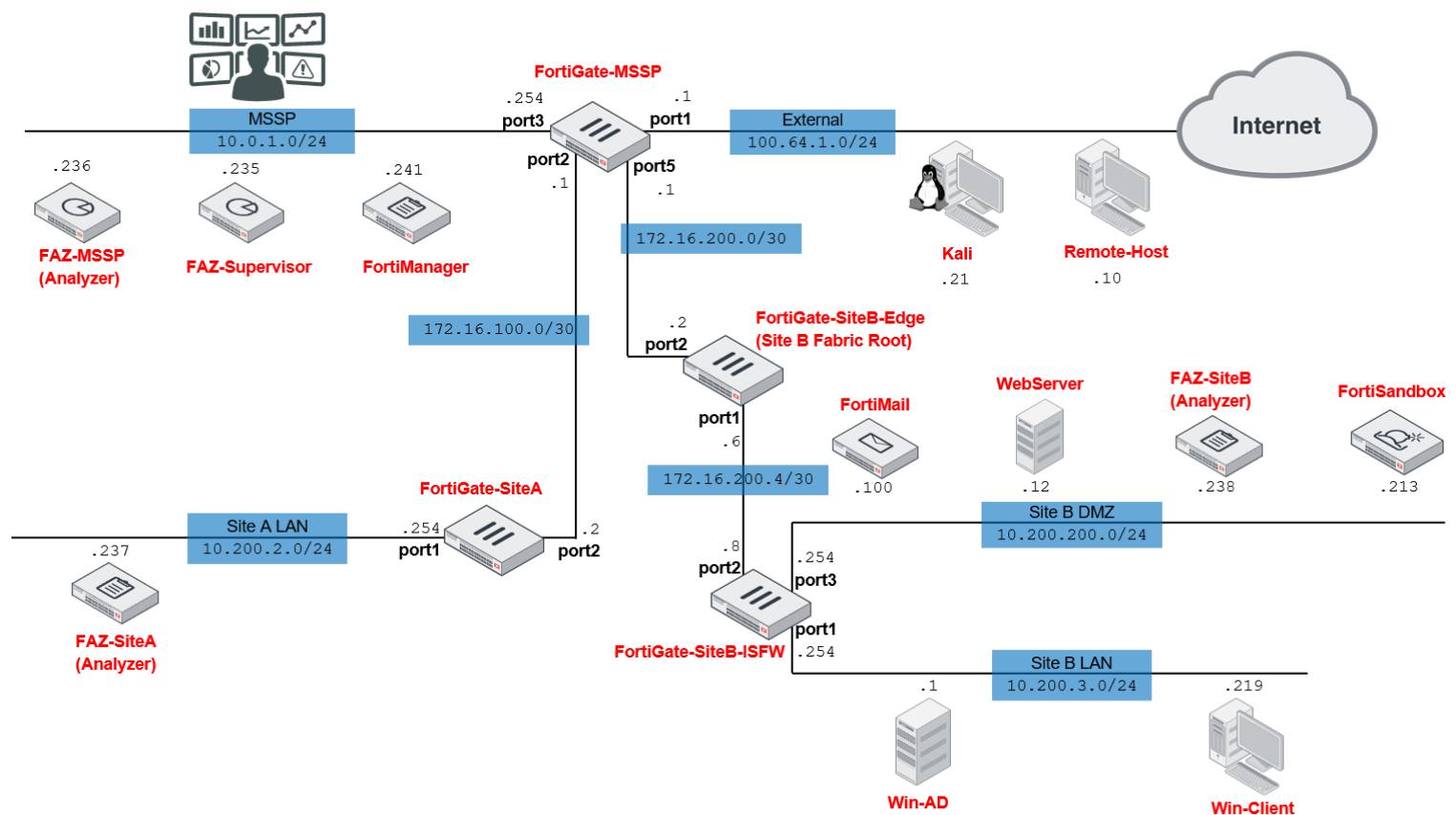


3. Scroll down, and then in the **Detection** section, review the information about how the applicable data sources can potentially detect the **Spearphishing Attachment** subtechnique.

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor for third-party application logging, messaging, and/or other artifacts that may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed. ^{[251][252]} Anti-virus can potentially detect malicious documents and attachments as they're scanned to be stored on the email server or on the user's computer. Monitor for suspicious descendant process spawning from Microsoft Office and other productivity software. ^[253]
DS0022	File	File Creation	Monitor for newly constructed files from a spearphishing emails with a malicious attachment in an attempt to gain access to victim systems.
DS0029	Network Traffic	Network Traffic Content	Monitor and analyze SSL/TLS traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed. ^{[251][252]}
		Network Traffic Flow	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

4. Review the following image of your lab environment topology:



Stop and think!

Based on the subtechnique details and your knowledge of Fortinet products, which solutions in your lab environment do you think are better equipped for detecting the **Spearphishing Attachment** subtechnique?

The product that is best suited for the purposes of this solution in this environment is FortiMail because of its secure email gateway capabilities, including antivirus. If it is integrated with FortiSandbox, FortiMail can cover most, if not all, of the details that are described in the **Detection** section of the **Spearphishing Attachment** subtechnique page.

You could also leverage FortiClient antivirus and FortiGate (Edge and ISFW) UTM capabilities in this case, but since the lab environment already contains FortiMail and FortiSandbox, you will focus on these two solutions in this lab.

The Fortinet solutions considered above can also work as mitigations. Because, in this lab, you want the attack to succeed in order to detect all phases, these solutions will operate with a configuration that will only detect the attack activity, not provide actual protection. This applies to all solutions in the lab that are capable of mitigation.



Because of time constraints, you are not going to review all of the Group ABC TTPs. You will also use a subset of all potential detection capabilities that the lab environment can provide. To reduce the number of configuration items for you to have to work on, there are additional detection capabilities used in later exercises that are preconfigured for you.

The goal of this lab is for you to understand the concepts of this methodological approach in building detection capabilities, while also identifying the potential of Fortinet solutions to work in such a capacity.

5. Repeat steps 1–3 for the following subtechnique:

- **Email Addresses** subtechnique (in the **Reconnaissance** column, under the **Gather Victim Identity Information** technique)

To summarize, you will use the following data sources to build detection capabilities for each of the following Group ABC TTPs:

Technique or Subtechnique	Tactic/Technique	Data Sources
Email Addresses	Reconnaissance > Gather Victim Identity Information	FortiMail (as email server) FortiMail
Spearfishing Attachment	Initial Access > Phishing	FortiSandbox
Create a Windows Service	Persistence > Create or Modify System Process: Windows	Windows Security Audit Logs (using Syslog Forwarder)
Clear Windows Event Logs	Defense Evasion > Indicator Removal on Host	Windows Security Audit Logs (using Syslog Forwarder)
Configure Data Source	Log Forwarding	

You will configure FortiSandbox, FortiMail, and FortiClient EMS to forward logs to FortiAnalyzer.

For this course, the lab environment has been preconfigured with fundamental integration between the Fortinet solutions, including the Fortinet Security Fabric. The labs in this course build on these integrations, and you will work specifically on configuring log forwarding, and detection and response capabilities.



If you want to learn how to complete these initial configurations, visit the Fortinet Training Institute to see available training options. The requirements and recommended certification and training for this course are a good starting point.

To configure FortiSandbox to forward logs to FortiAnalyzer

1. On the bastion host, in Chrome, log in to the FortiSandbox GUI (10.200.4.213) with the following credentials:
 - Username: admin
 - Password: Fortinet1!
2. Click **Log & Report > Log Servers**.
3. Click **Create New**.

+ Create New

 **Edit**

 **Delete**

Name

Server Type

Server Address

Port

Status

4. On the **New Remote Log Server** page, configure the following settings:

Field

Value

Name	FortiAnalyzer
Type	Syslog UDP
Log Server Address	10.200.200.23
Address	8
Status	Enable

5. Select all of the checkboxes.

New Remote Log Server

Name:

FortiAnalyzer

Letters, digits and ./_ only.

Type:

Syslog UDP

Log Server Address:

10.200.200.238

Port:

514

Status:

☒ Enable ☐ Disable

☒ Alert Logs

☒ Include Jobs with Clean Rating

☒ Critical Logs

☒ Error Logs

☒ Warning Logs

☒ Information Logs

☒ Debug Logs

OK

Cancel



This configuration ensures that FortiSandbox forwards all types of logs, not only alert logs, to FortiAnalyzer. Just like in a production environment, you must select all available logging options so that you can correctly monitor FortiSandbox logs from a central location, such as FortiAnalyzer.

6. Click **OK**.





To configure FortiMail to forward logs to FortiAnalyzer

1. Continuing on the bastion host, in Chrome, log in to the FortiMail GUI (10.200.4.243/admin) with the following credentials:

- Username: admin
- Password: Fortinet1!

2. Click **Log & Report > Log Setting**.

3. Click the **Remote** tab, and then click **New**.

  New...  Edit...  Delete

Total: 0

Stat...	Name	Server	Port	Protocol ...	Level	Facility ...	

4. Configure the following settings:

Field	Value
Status	Enabled
Name	FortiAnalyzer
Server	10.200.200.23
name/IP	8
Server port	514
Protocol	Syslog
Mode	UDP
Level	Information
Facility	kern
CSV format	Disabled

Log to Remote Host

Status	<input checked="" type="checkbox"/>
Name	<input type="text" value="FortiAnalyzer"/>
Server name/IP	<input type="text" value="10.200.200.238"/>
Server port	<input type="text" value="514"/>
Protocol	<input type="text" value="Syslog"/>
Mode	<input type="text" value="UDP"/>
Level	<input type="text" value="Information"/>
Facility	<input type="text" value="kern"/>
CSV format	<input type="checkbox"/>
Comment	<input type="text"/>

5. Expand **Logging Policy Configuration**, expand **System Event** and **Mail Event**, and then enable all settings.

☒ Logging Policy Configuration

☒ System Event

☒ Configuration change

☒ Admin activity

☒ System activity

☒ HA

☒ Update

☒ DNS

☒ Mail Event

☒ Webmail

☒ POP3

☒ IMAP

☒ SMTP

☒ History

☒ AntiVirus

☒ AntiSpam

☒ Encryption

This configuration ensures that FortiMail forwards all logs to FortiAnalyzer.

6. Click **Create** to save the configuration.

The following table summarizes the logging configuration in your lab, in the context of these lab exercises:

Log source	Log destination	Protocol
FortiMail	FortiAnalyzer	syslog
FortiSandbox	FortiAnalyzer	syslog
Windows client syslog forwarder	FortiAnalyzer	syslog

To configure FortiMail to send suspicious files to FortiSandbox

1. Continuing on the FortiMail GUI, click **System > FortiSandbox**.
2. In the **Server name/IP** field, type 10.200.200.213.
3. In the **File patterns** field, type *.odt, and then click **+**.
4. In the **URL Scan Setting** section, ensure that the **Email selection** field is set to **All email**.

FortiSandbox

FortiSandbox Inspection

Statistics...

FortiSandbox type

Appliance

Cloud

Enhanced Cloud

Server name/IP

10.200.200.213

Test Connection

Notification email

Statistics interval

5

(minutes)

Scan timeout

30

(minutes)

Scan result expires in

60

(minutes)

File Scan Setting

File types

Windows executable

PDF

JavaScript

HTML

Microsoft Office document

Adobe flash

Jar

Archive

File patterns

*.odt

File size

Maximum file size to upload

1024

(KB)

URL Scan Setting

Email selection

All email

Suspicious email

URL selection

unrated

+

Upload URL on rating error

Bypass one-time URL

Number of URLs per email

3

5. Click **Apply**.
6. Click **Test Connection**.

Stop and think!

Why does the test fail? The answer is provided in the error. You must authorize FortiMail on FortiSandbox to send the suspicious files.

To authorize devices on FortiSandbox

1. Continuing on the bastion host, in Chrome, click the **FortiSandbox** tab.
2. Click **Security Fabric > Device**.
3. In the **FortiMail** row, click the edit icon.

	Filter ...
Device Name	Serial
FortiWeb	FVVM01TM22000081
WIN-AD	FCTEMS8823000389
FortiGate-SiteB-Edge	FGVMSLTM24000455
FortiGate-SiteB-ISFW	FGVMSLTM24000847
FortiMail	FEVMSLTM22000111

4. In the **Permissions & Policy** section, in the **Authorized** field, select the checkbox.

Device Status	
Serial Number:	FEVMSLTM22000111
Hostname:	FortiMail
IP:	10.200.200.100
Status:	
Last Modified:	2024-02-13 15:52:51
Last Seen:	2024-02-13 18:12:25
Permissions & Policy	
Authorized:	<input checked="" type="checkbox"/> Last Changed 2024-02-13 15:52:51
New VDOMs/Domains Inherit Authorization:	<input checked="" type="checkbox"/>
Email Settings	
Administrator Email:	Please input valid email address to enable below checkbox.
Send Notifications:	<input checked="" type="checkbox"/>
Send PDF Reports:	<input checked="" type="checkbox"/>

5. Click **OK**.
6. Click **OK**.

FortiMail is now authorized to send suspicious files to FortiSandbox.

Filter ...

Device Name	Serial	Malicious	High	Medium	Low	Clean	Others	Mal Pkg	URL Pkg	Auth	Limit	Status	
<div><div></div>FortiMail</div>	FEVMSLTM22000111	0	0	0	0	0	0	N/A	N/A	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>



If you don't see the status turn green, go back to the FortiMail browser tab, and then perform another connection test to FortiSandbox. This time, you should see a **Connected Successfully** message. Then, return to the FortiSandbox browser tab and confirm that the status is now green.

7. The following devices have been preconfigured and preauthorized on FortiSandbox:
 - FortiGate-SiteB-Edge
 - FortiGate-SiteB-ISFW
 - FortiWeb (not used)

- WIN-AD

All the devices in the Security Fabric are now authorized on FortiSandbox.

Filter ...													
Device Name	Serial	Malicious	High	Medium	Low	Clean	Others	Mal Pkg	URL Pkg	Auth	Limit	Status	
<input checked="" type="checkbox"/> WIN-AD	FCTEMS8823000389	0	0	0	0	0	0	N/A	N/A		<input type="checkbox"/>		
<input checked="" type="checkbox"/> FortiGate-SiteB-Edge:root	FGVMSLTM24000455	0	0	0	0	0	0	4.102	4.100		<input type="checkbox"/>		
<input checked="" type="checkbox"/> FortiGate-SiteB-ISFW:root	FGVMSLTM24000847	0	0	0	0	0	0	4.102	4.100		<input type="checkbox"/>		
<input checked="" type="checkbox"/> FortiGate-SiteB-ISFW	FGVMSLTM24000847	0	0	0	0	0	0	4.102	4.100		<input type="checkbox"/>		
<input checked="" type="checkbox"/> FortiGate-SiteB-Edge	FGVMSLTM24000455	0	0	0	0	0	0	4.102	4.100		<input type="checkbox"/>		
<input checked="" type="checkbox"/> FortiMail	FEVMSLTM22000111	0	0	0	0	0	0	N/A	N/A		<input type="checkbox"/>		
<input checked="" type="checkbox"/> FortiWeb	FVVM01TM22000081	0	0	0	0	0	0	N/A	N/A		<input type="checkbox"/>		

To authorize devices on FortiAnalyzer

1. Log in to the FAZ-SiteB GUI (10.200.4.238) with the following credentials:
 - Username: admin
 - Password: Fortinet1!
2. Click **Device Manager**.
3. Click **Unauthorized Devices**.
4. Select the checkboxes for all three devices, and then click **Authorize**.

<input checked="" type="checkbox"/>	Authorize	Hide	Delete	<input type="checkbox"/> Display Hidden Devices									
<input checked="" type="checkbox"/>	Device Name	Platform	Serial Number	IP Address	Firmware Version	Management Mode							
<input checked="" type="checkbox"/>	FCTEMS8823000389	FortiClient-EMS	FCTEMS8823000389	0.0.0.0	FortiClient 0.0	Logging Only							
<input checked="" type="checkbox"/>	FEVMSLTM22000111	FortiMail-VM	FEVMSLTM22000111	10.200.200.100	FortiMail 7.4	Logging Only							
<input checked="" type="checkbox"/>	FortiSandbox	FortiSandbox-VM	FSAVM0TM2200035	10.200.200.213	FortiSandbox 4.4	Logging Only							

5. In the **Authorize Device** window, configure the following settings:

Name	Assigned New Device Name
FCTEMS8823000389	FortiClient_EMS
FortiSandbox	FortiSandbox
FEVMSLTM22000111	FortiMail

6. Click **OK**.

Authorize Device

Add the following device(s) to ADOM:

root (Fabric 7.4)

Search...

Name	Assign New Device Name	
FCTEMS8823000389	FortiClient_EMS	
FortiSandbox	FortiSandbox	
FEVMSLTM22000111	FortiMail	

3

OK

Cancel

All three devices are authorized on FAZ-SiteB.

7. Click **Close**.
8. Click **All Logging Devices**.

<div><div><div>Edit</div><div>Delete</div><div>Table View</div><div>More</div></div><div><div>Show Charts</div><div>Search...</div></div></div>								
<input type="checkbox"/>	Device Name	IP Address	Platform	HA Status	Description	Firmware Version	Serial Number	Last Log Time
<input type="checkbox"/>	FortiClient_EMS	0.0.0.0	FortiClient-EMS			FortiClient 0.0	FCTEM58823000385	2/23/2024, 8:09:54 AM PST (
<input type="checkbox"/>	default [NAT]							2/23/2024, 8:09:54 AM PST (
<input type="checkbox"/>	FortiMail	10.200.200.100	FortiMail-VM			FortiMail 7.4	FEVMSLTM22000111	N/A
<input type="checkbox"/>	FortiSandbox	10.200.200.213	FortiSandbox-VM			FortiSandbox 4.4	FSAVM0TM2200035	2/23/2024, 8:13:52 AM PST (
<input type="checkbox"/>	SYSLOG-0AC80303	10.200.3.3	Syslog-Device			Standard	SYSLOG-0AC80303	2/23/2024, 7:39:47 AM PST (
<input type="checkbox"/>	Site-B-Fabric							
<input type="checkbox"/>	FortiGate-SiteB-Edge	172.16.200.5	FortiGate-VM64			FortiGate 7.4.2,build2571 (GA)	FGVMSLTM2400045	2/23/2024, 8:15:15 AM PST (
<input type="checkbox"/>	FortiGate-SiteB-ISFW	10.200.200.254	FortiGate-VM64			FortiGate 7.4.2,build2571 (GA)	FGVMSLTM2400084	2/23/2024, 8:15:17 AM PST (

There are six devices logging to FAZ-SiteB: FortiClient EMS, FortiMail, FortiSandbox, SYSLOG, FortiGate-SiteB-Edge, and FortiGate-SiteB-ISFW.

LAB-3 > Configuring Data Sources

Outline

preview

-