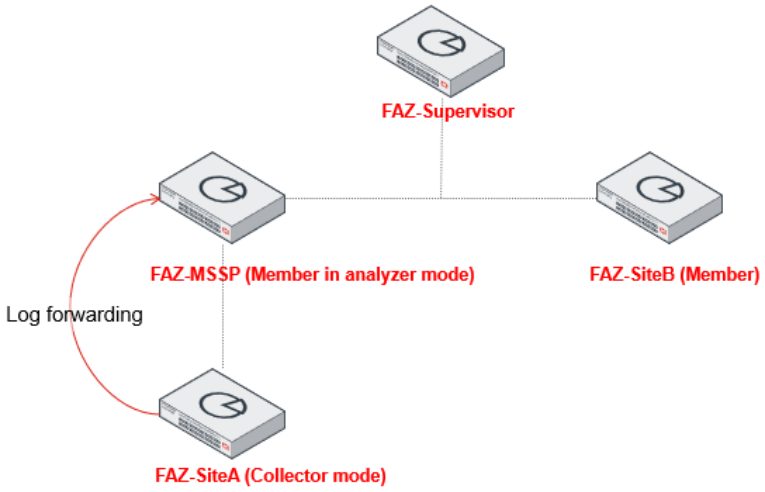
Exercise 2: Configuring the FortiAnalyzer Fabric

In this exercise, you will create a FortiAnalyzer Fabric made up of four FortiAnalyzer devices. FAZ-Supervisor will act as the Fabric supervisor. FAZ-MSSP and FAZ-SiteB will act as the Fabric members. FAZ-SiteA will act as a collector, which forwards logs to FAZ-MSSP. Then, you will confirm that logs from the downstream FortiAnalyzer devices are displayed on the supervisor.

Review the FortiAnalyzer Fabric Topology

The FortiAnalyzer Fabric enables the centralized viewing of devices, incidents and events, and reporting across the Fabric.



FAZ-MSSP has two ADOMs configured:

- **MSSP-Local (contains FortiGate-MSSP)**
- **SiteA (contains logs that FAZ-SiteA forwarded)**

For information about the IP addressing, see the Lab Network Topology on page 1.

Configure the FortiAnalyzer Fabric

First, you will configure the FortiAnalyzer Fabric supervisor, and then you will configure the Fabric members. Next, you will authorize the Fabric members.

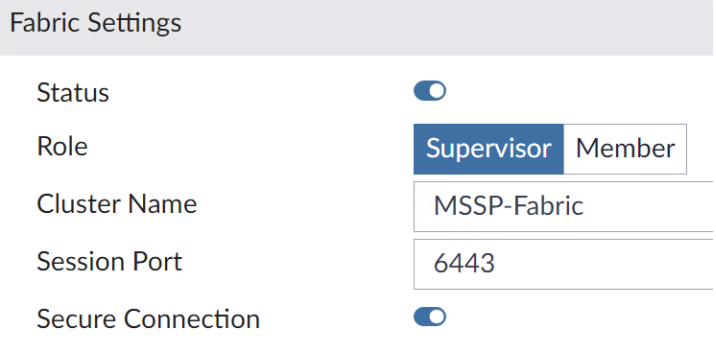
To configure the supervisor

1. On the bastion host, open Chrome, and then log in to the FAZ-Supervisor GUI (10.200.4.235) with the following credentials:

- Username: admin
- Password: Fortinet1!

2. Click **System Settings** > **Fabric Management** > **FortiAnalyzer Fabric**.
3. Configure the following settings:

Field	Value
Status	Enabled
Role	Supervisor
Cluster Name	MSSP-Fabric
Session Port	6443
Secure Connection	Enabled



4. Click **Apply**.

You will be logged out of the FAZ-Supervisor GUI.

5. Log in to the FAZ-Supervisor GUI again (10.200.4.235) with the following credentials:

- Username: admin
- Password: Fortinet1!

6. Click the icon to open the FortiAnalyzer CLI.
7. Enter the following commands:

config system interface

edit port1

set allowaccess ping soc-fabric

end

It is important to note that the two protocols defined in the set allowaccess command will override existing access protocol settings. For example, if you have https and ssh enabled, after you enter end, only ping and soc-fabric will be allowed on the interface. If you must have https and ssh enabled, along with ping and soc-fabric, you must enter the following commands instead:

config system interface

edit port1

set allowaccess https ssh ping soc-fabric

end

In this lab environment, you are connecting to the network devices through the management network on the 10.200.4.0/24 subnet, which is on port2 for the FAZ-Supervisor VM. Therefore, you will not lose access.

However, you should pay special attention when you configure allowed protocols, especially if the port you are editing is used for administrative access.

8. Enter the following command to confirm that you entered the commands in the previous step correctly:

show system interface port1

```
FAZ-Supervisor # show system interface port1
config system interface
    edit "port1"
        set ip 10.0.1.235 255.255.255.0
        set allowaccess ping soc-fabric
        set type physical
    next
end
```

9. Close the CLI.

10. Keep the browser tab with the FAZ-Supervisor GUI open.

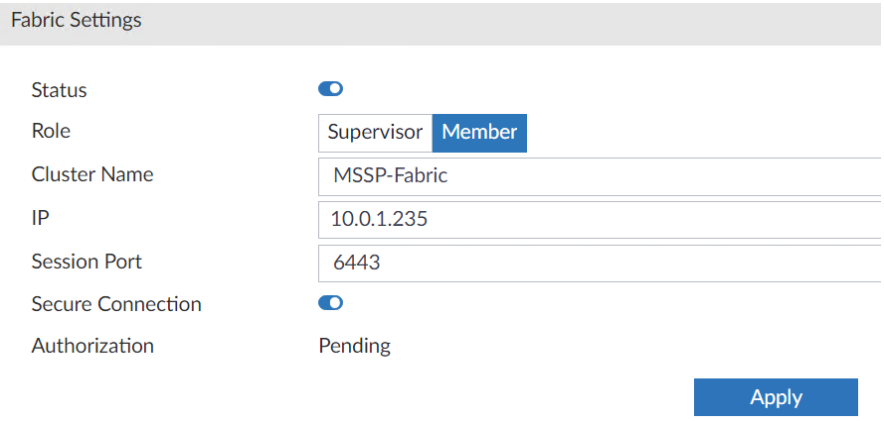
To configure the members

1. Continuing on the bastion host, in Chrome, log in to the FAZ-MSSP GUI (10.200.4.236) with the following credentials:

- Username: admin
- Password: Fortinet1!

2. Click **root**.
3. Click **System Settings** > **Fabric Management** > **FortiAnalyzer Fabric**.
4. Configure the following settings:

Field	Value
Status	Enabled
Role	Member
Cluster Name	MSSP-Fabric
IP	10.0.1.235
Session Port	6443
Secure Connection	Enabled



Depending on your environment, you may not see the **Pending** state. Proceed to the next step even if you do not see it.

5. Click **Apply**.
6. Click the icon to open the FortiAnalyzer CLI.
7. Enter the following commands:

```
config system interface
edit port1
set allowaccess ping soc-fabric
end
```

8. Enter the following command to confirm that you entered the commands in the previous step correctly:

```
show system interface port1
```

```
FAZ-MSSP # show system interface port1
config system interface
    edit "port1"
        set ip 10.0.1.236 255.255.255.0
        set allowaccess ping soc-fabric
        set type physical
    next
end
```

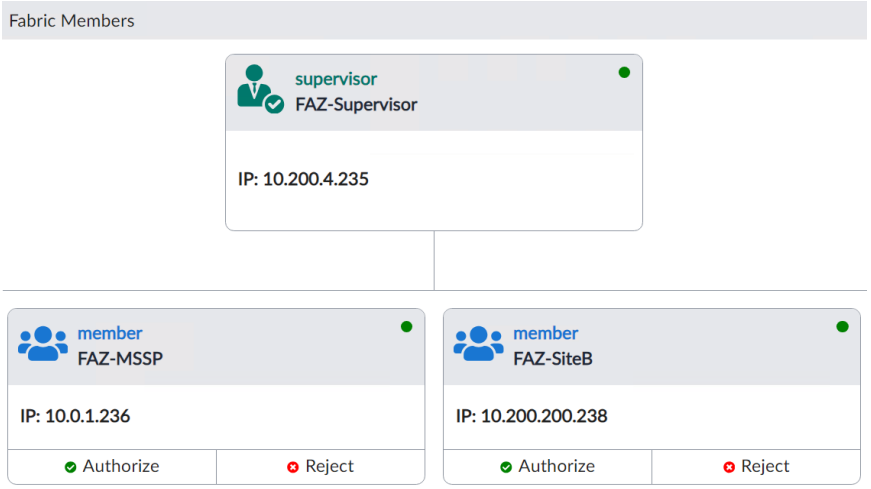
9. Close the CLI.
10. On FAZ-SiteB (10.200.4.238), repeat steps 3–5.

Do *not* modify port1 on FAZ-SiteB.

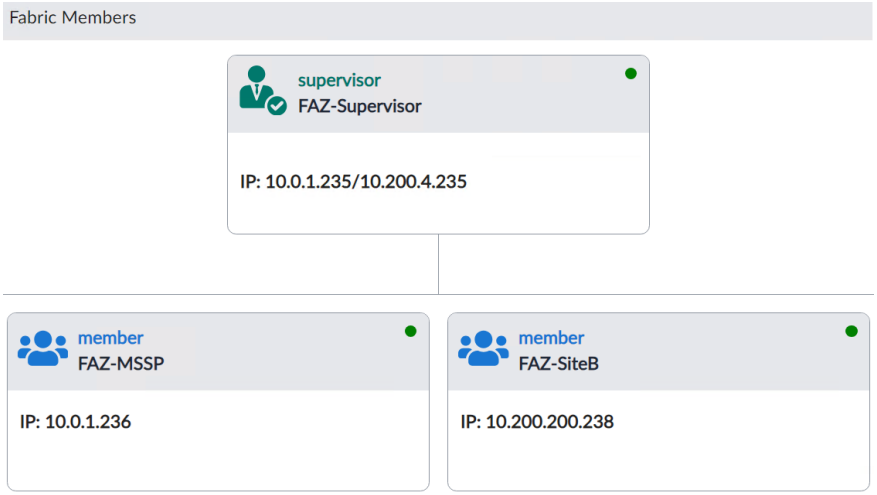
Port1 on FAZ-SiteB is preconfigured for you. In addition to ping and soc-fabric, it also has https enabled for a later exercise.

To accept the connections on the supervisor

1. Continuing on the FAZ-Supervisor GUI, click **System Settings** > **Fabric Management** > **FortiAnalyzer Fabric**.
2. Scroll to the bottom of the page, and then confirm that you can see two FortiAnalyzer members pending authorization.



3. For one member, click **Authorize**.
4. In the **Confirm Operation** window, click **OK**.
5. For the other member, click **Authorize**.
6. In the **Confirm Operation** window, click **OK**.
7. Wait a few minutes, refresh the page, and then confirm that the Fabric is established.



8. Click **Device Manager**.
9. Confirm that **FAZ-MSSP** and its two ADOMs—**SiteA** and **MSSP-Local**—appear in the list.

You may need to wait a few minutes for the devices to appear.

10. Confirm that **FAZ-SiteB** and its Security Fabric—**Site-B-Fabric**—appear in the list.

You may need to wait a few minutes for the devices to appear.

Collapse All | Expand All | Show Charts | Search...

Name	IP Address	Platform	Logs
FAZ-MSSP	10.0.1.236	FortiAnalyzer-VM64	
SiteA			
FortiGate-SiteA	10.200.2.254	FortiGate-VM64	Real Time
root		vdom	Real Time
MSSP-Local			
FortiGate-MSSP	10.0.1.254	FortiGate-VM64	Real Time
root		vdom	Real Time
FAZ-SiteB	10.200.200.238	FortiAnalyzer-VM64	
root			
Site-B-Fabric			
FortiGate-SiteB-Edge	172.16.200.5	FortiGate-VM64	Real Time
root		vdom	Real Time
FortiGate-SiteB-ISFW	10.200.200.254	FortiGate-VM64	Real Time
root		vdom	Real Time

Validate the FortiAnalyzer Fabric

You will verify that the FortiAnalyzer Fabric is functioning correctly by running a diagnostic command. You will also create test logs on different FortiGate devices, and separate incidents on Fabric members. Then, you will verify that you can see the logs and incidents on the supervisor.

To confirm the Fabric sync status

1. Open the FAZ-Supervisor CLI, and then enter the following command:

diagnose test application fabricsyncd 3

2. Confirm that the Fabric members appear as auth: Accepted and status: up.

```
FAZ-Supervisor # diagnose test application fabricsyncd 3
  fabricsync members: total=2, schedule_len=2, n_launch_max=5
    1. FAZ-VMTM24000905 auth: Accepted   status: up    notice_ver: 592/592  last-sync: 244 sec ago (OK)
    2. FAZ-VMTM24000908 auth: Accepted   status: up    notice_ver: 846/846  last-sync: 2424 sec ago (OK)
```

To generate test logs

1. On the bastion host, in Chrome, log in to the FortiGate-SiteA GUI (10.200.4.250) with the following credentials:

- Username: admin
- Password: Fortinet1!

2. Click the icon to open the FortiGate CLI.
3. Make a note of your current time, and then enter the following command:

diagnose log test

4. Close the CLI.
5. On FortiGate-SiteB-ISFW (10.200.4.234), repeat steps 1–4.

To create test incidents

1. On the bastion host, in Chrome, return to the FAZ-MSSP GUI (10.200.4.236), and then log in with the following credentials:

- Username: admin
- Password: Fortinet1!

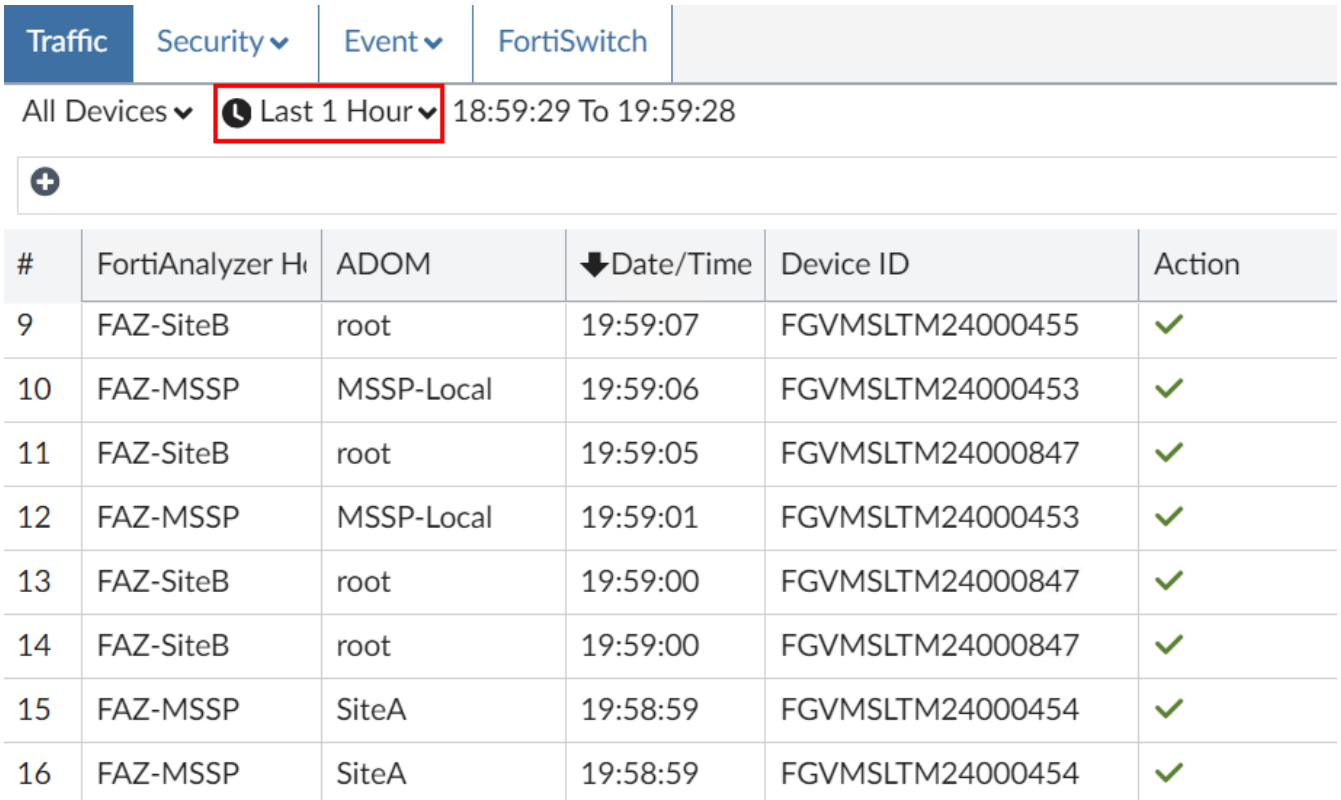
2. Select the **SiteA** ADOM.
3. Click **Incidents & Events** > **Incidents**.
4. Click **Create New**.
5. In the **Description** field, type Test Incident.
6. Click **OK**.
7. On FAZ-SiteB (10.200.4.238), repeat steps 1 and 3–6.

You do not perform step 2 because FAZ-SiteB does not have ADOMs enabled.

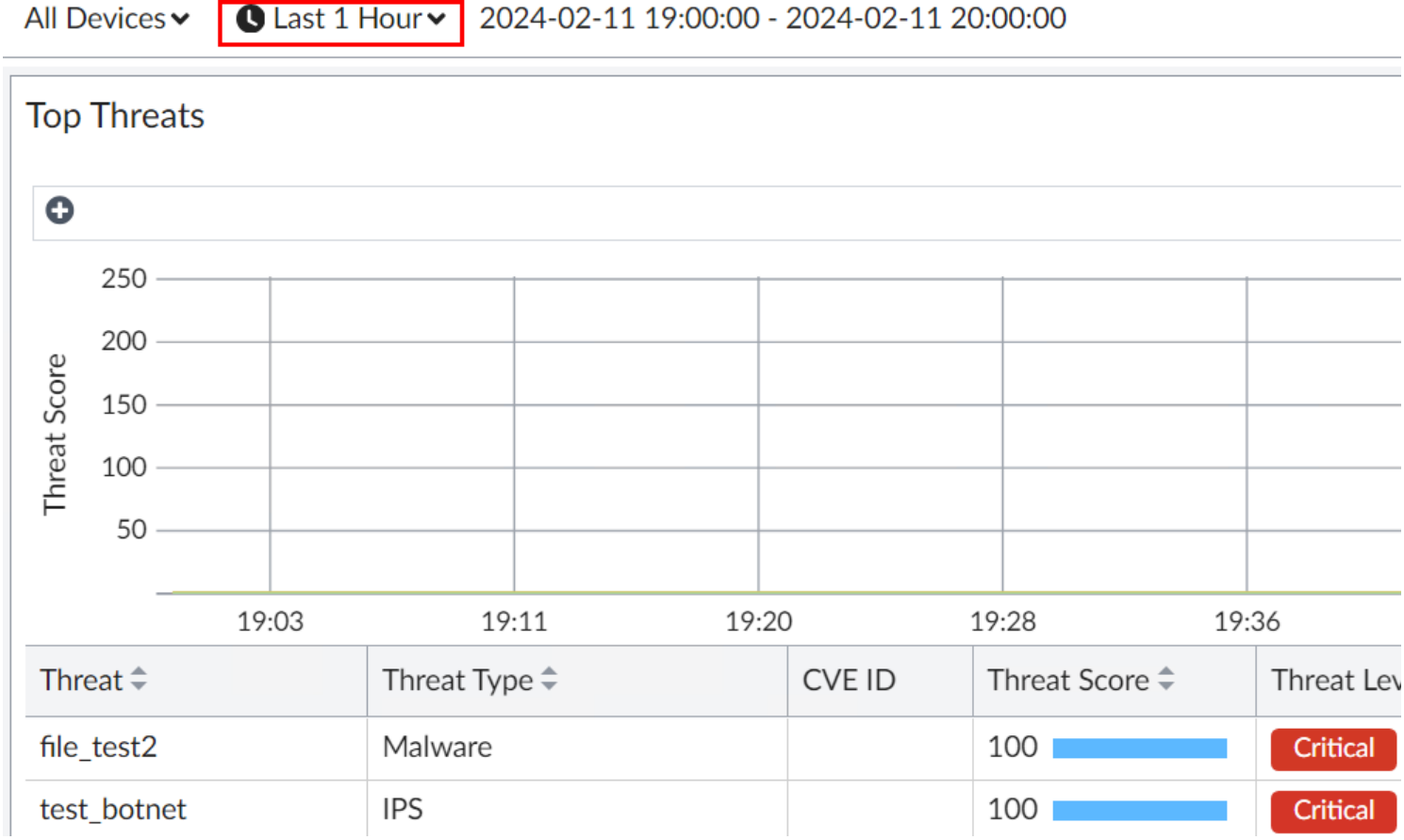
To view logs and incidents on the supervisor

1. Return to the FAZ-Supervisor GUI, and then click **Log View** > **FortiGate**.
2. Confirm that the logs from the time you entered the diagnose log test command are displayed.

You may need to adjust the log time period filter (**Last 1 Hour** in the following image), depending on how long ago you entered the command.

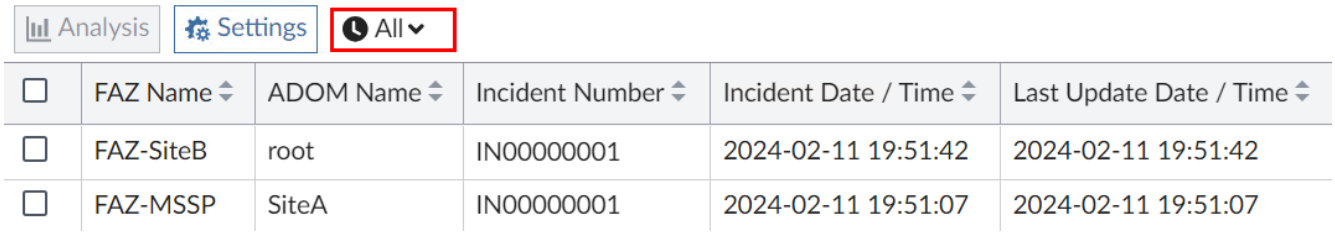


3. Click **FortiView** > **Threats**.
4. Confirm that security threats are displayed—if necessary, adjust the log time period filter.



5. Click **Incidents & Events** > **Incidents**.
6. Confirm that both incidents that you created are displayed—if necessary, adjust the log time period filter.

Your incident numbers may be different from those in the following image:



LAB-2 > Configuring the FortiAnalyzer Fabric