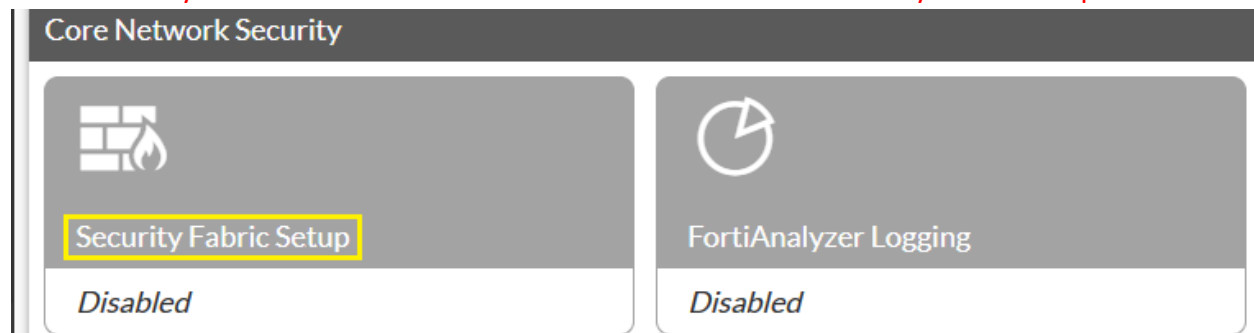


Deploying Downstream Security Fabric:

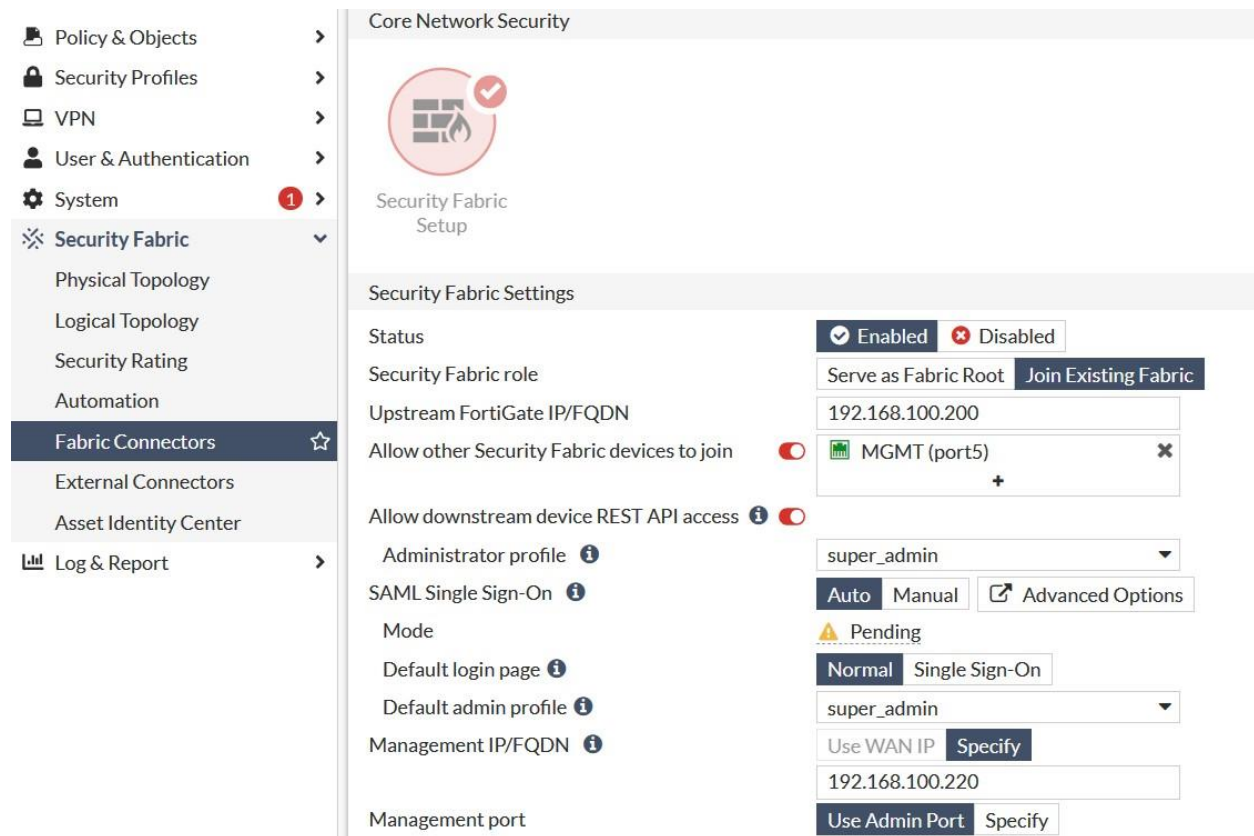
Downstream FortiGate units can be securely added to the Security Fabric without sharing the password of the root FortiGate. Downstream unit serial numbers can be authorized from the root FortiGate, or allowed to join by request.

Security Fabric Configuration:

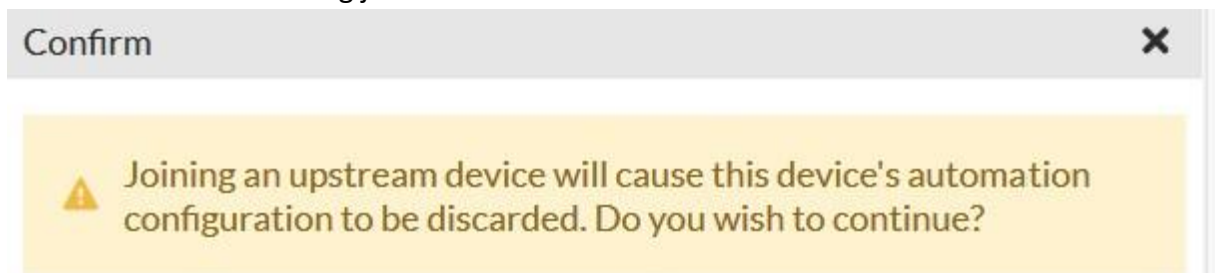
Go to **Security Fabric > Fabric Connectors** and double-click the **Security Fabric Setup** card.



For Status, select **Enabled**. Set the Security Fabric role to **Join Existing Fabric**. Enter the IP address of the root FortiGate in the Upstream FortiGate IP field in this case **192.168.100.200**. Select **OK**.



It will show below warning just click confirm.

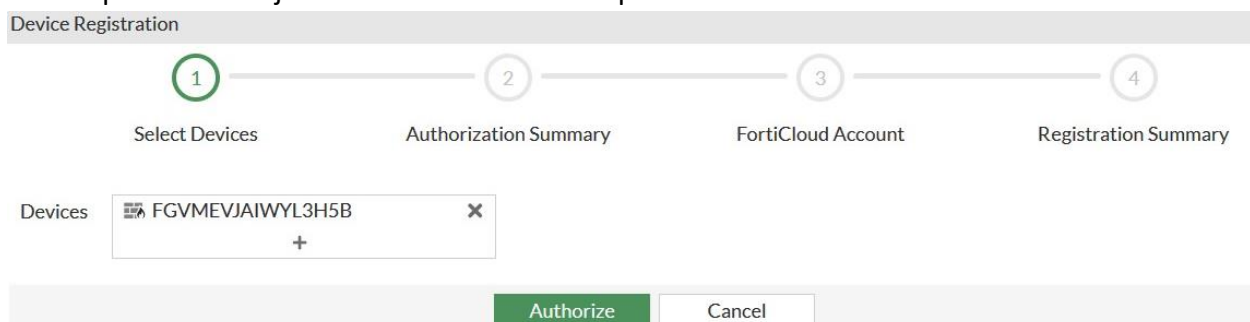


Root FortiGate Authorization:

Connect to the root FortiGate and go to **Security Fabric -> Fabric Connectors**. The new FortiGate appears in the topology tree as unauthorized. Select the unauthorized unit & select **Authorize**.



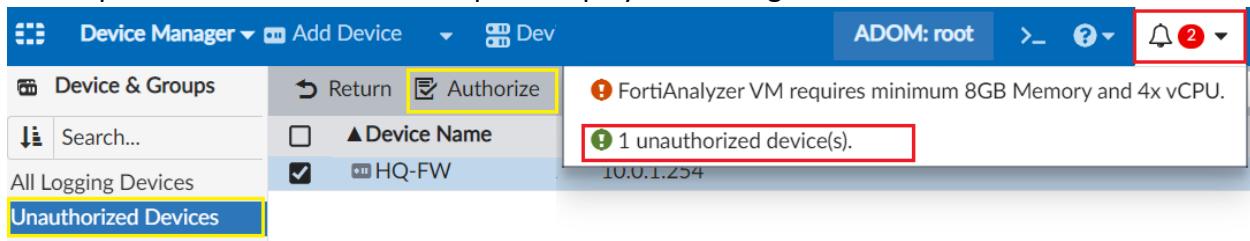
It will open a wizard just click Authorize to complete.



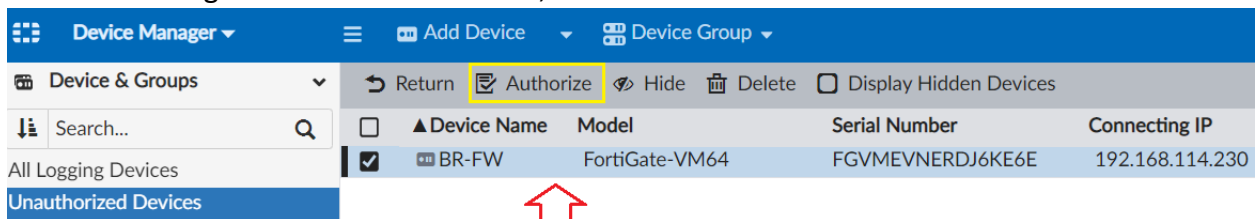
Device Registration					
<div> <div>✓</div> <div>2</div> <div>3</div> <div>4</div> </div>					
Select Devices		Authorization Summary		FortiCloud Account	
				Registration Summary	
Name	Model	Type	Status	Registration	FortiCloud Account
FGVMEVJAIWYL3H5B	FGVMEV		✖ Offline	✓ Registered	bijayswain@gmail.com

FortiAnalyzer Authorization:

Login to FortiAnalyzer in the root ADOM, go to **Device Manager** and click **Unregistered Devices** in the quick status bar. The content pane displays the unregistered devices.



Select the unregistered device or devices, then click **Authorize**.



Select the ADOM in the **Add the following device(s) to ADOM** list. Click **OK** to register the device or devices. The device or devices are added and FortiAnalyzer can start receiving logs from the device or devices.

Authorize Device

Add the following device(s) to ADOM: FG-7-0-9 (FortiGate 7.2)

Device Name	Assign New Device Name
DC-FW	DC-FW

➡
OK
Cancel

The device is successfully authorized click **Closed**.

Authorize Device



Device Authorization

100%

[View Details](#)

Double click or select Edit type the Admin User and Password in this case **admin/123**

Admin User	<input type="text" value="admin"/>
Password	<input type="password" value="•••••"/>

Verification:

Finally, FortiAnalyzer Logging and Security Fabric Setup has been completed. Make sure FortiAnalyzer Logging is green up arrow.

- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- System
- Security Fabric**
- Physical Topology
- Logical Topology
- Security Rating
- Automation
- Fabric Connectors

Core Network Security

Security Fabric Setup

MY-SF

FortiAnalyzer Logging

192.168.100.215

Cloud Logging

Disabled

Cloud Sandbox

Disabled

To verify navigate to **Dashboard>Status** Security Fabric Widget.

Dashboard

Status

Security

Network

Users & Devices

+

FortiView Sources

FortiView Destinations

FortiView Applications

+ Add Widget

Security Fabric: MY-SF

HQ-FW (Fabric Root)

DC-FW