Fortinet Security Fabric - Upgrade Guide

VERSION 5.6.0

Introduction

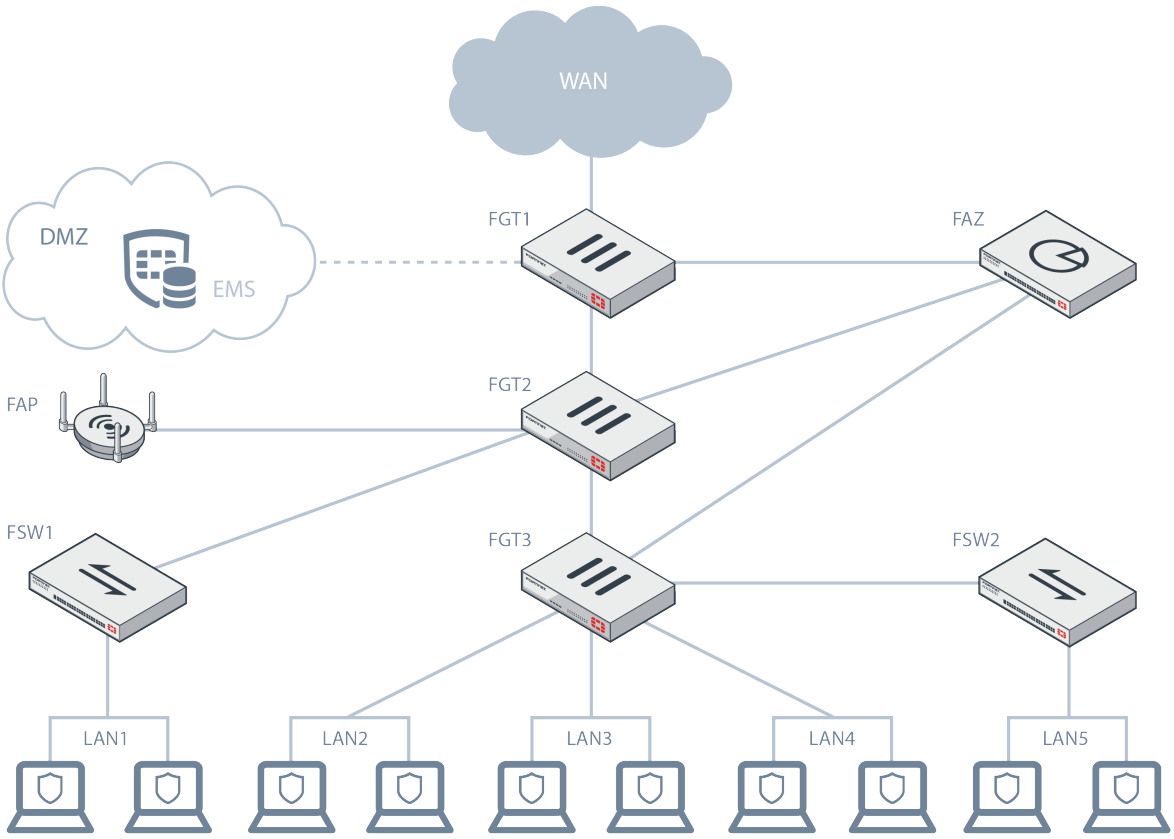
This guide describes how to upgrade Security Fabric. A Security Fabric spans across an entire network, using FortiTelemetry to link different security sensors and tools together to collect, coordinate, and respond to malicious behavior anywhere it occurs on your network in real time. A Security Fabric can be used to coordinate the behavior of different Fortinet products in your network, including FortiGate, FortiAnalyzer, FortiClient, FortiSandbox, FortiAP, FortiSwitch, and FortiClient Enterprise Management Server (EMS).

You should use this upgrade guide when you are using two or more products that are used for Security Fabric. This guide describes how to upgrade the products in the correct sequence. For details about upgrading each product, see the following documents:

- *FortiAnalyzer Release Notes*
- *FortiClient Release Notes*
- *FortiClient EMS Release Notes*
- *FortiSwitch Release Notes*
- *FortiGate Release Notes*
- *FortiAP Release Notes*

In FortiOS 5.6.0, the *Cooperative Security Fabric* feature was renamed to *Security Fabric*. In addition, the Security Fabric feature in FortiOS 5.6.0 requires that you have a FortiAnalyzer unit and enable logging to the FortiAnalyzer unit.

Security Fabric topology



Upgrade

This section describes how to upgrade the products used for Security Fabric in the correct order. It includes a summary of the procedure followed by a detailed procedure.

You should perform this upgrade procedure during a maintenance window because the procedure affects network traffic flow.

Summary

To upgrade Security Fabric (summary):

1. In FortiOS 5.4.2 or later, disable FortiClient enforcement (FortiTelemetry).
   FortiOS 5.6.0 either blocks network access for non-compliant endpoints or displays a warning portal for non-compliant endpoints. It is recommended to temporarily disable FortiClient enforcement to let you upgrade endpoints without losing network access.
2. Upgrade FortiClient EMS to 1.2.0 or later.
   FortiClient 5.6.0 requires FortiClient EMS 1.2.0 or later.
3. Upgrade all endpoints to FortiClient 5.6.0 or later.
   FortiClient enforcement in FortiOS 5.6.0 requires FortiClient 5.6.0 or later.
4. Upgrade the OS version for FortiSwitch in managed mode to 3.5.2 or later.
   It is recommended to upgrade to FortiSwitch 3.5.3 or later to access all of the new features.
5. Upgrade the OS version for the FortiAnalyzer units in the Security Fabric topology to FortiAnalyzer 5.6.0 or later.
   The Security Fabric feature in FortiOS 5.6.0 and later requires that you have a FortiAnalyzer unit and enable logging to the FortiAnalyzer unit. Whether logging to FortiAnalyzer is enabled in FortiOS before you upgrade affects how you upgrade the firmware for FortiAnalyzer units.

   If FortiOS 5.4.2 or later has logging to FortiAnalyzer enabled, upgrade the FortiAnalyzer units to 5.6.0 or later.

   If FortiOS 5.4.2 or later has logging to FortiAnalyzer disabled, disable Security Fabric on all FortiGate units in the Security Fabric group before you upgrade the firmware for FortiAnalyzer to 5.6.0 or later.
6. Upgrade firmware for all FortiGate units in the Security Fabric topology to FortiOS 5.6.0 or later.
   The Security Fabric feature in FortiOS 5.6.0 and later requires that you have a FortiAnalyzer unit and enable logging to the FortiAnalyzer unit. If FortiOS 5.4.2 or later has logging to FortiAnalyzer disabled, disable Security Fabric on all FortiGate units in the Security Fabric group before you upgrade the firmware to 5.6.0.
7. If logging to FortiAnalyzer was enabled in Security Fabric groups before the upgrade, you must complete the logging configuration for each Security Fabric group by registering all FortiGate units in each Security Fabric group with the primary FortiAnalyzer in each Security Fabric group and enabling communication between the units.
8. Upgrade the OS version for FortiAP to 5.6.0 or later.

FortiOS 5.6 supports FortiAP 5.4.x. However, it is recommended to upgrade to FortiAP 5.6.0 to access all of the new features.

9. Verify that the endpoints for which you want to enable enforcement have been upgraded to FortiClient 5.6.0 or later.
10. In FortiOS 5.6.0 or later, enable FortiClient enforcement (FortiTelemetry).

Detailed procedure

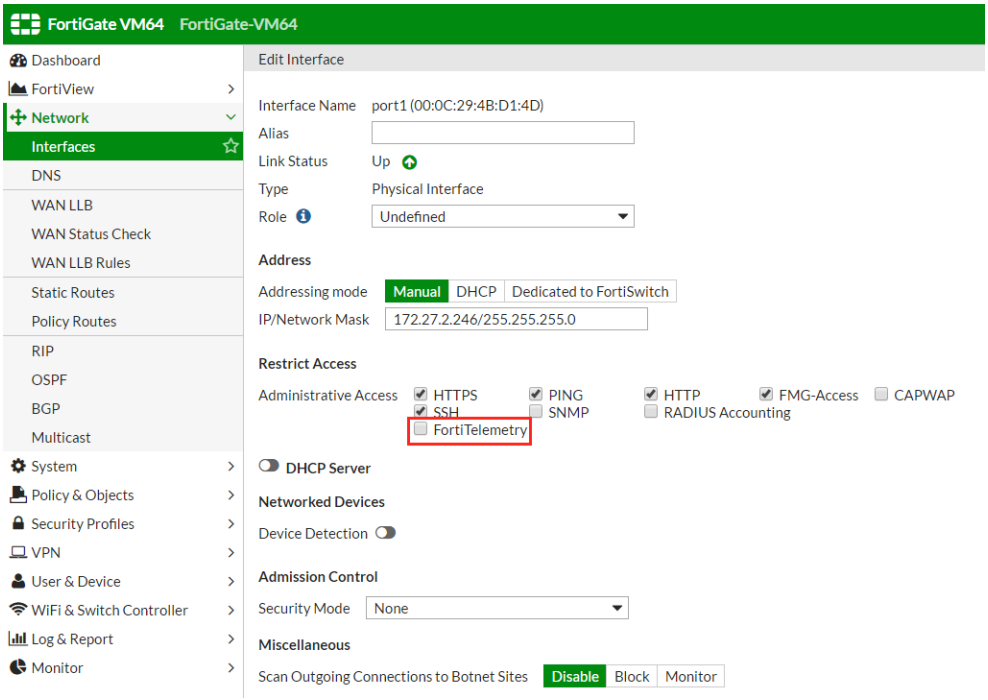
To upgrade Security Fabric (detailed procedure):

1. In FortiOS 5.4.2 or later, temporarily disable FortiClient enforcement (FortiTelemetry).

   FortiOS 5.6.0 either blocks network access for non-compliant endpoints or displays a warning portal for non-compliant endpoints. It is recommended to temporarily disable FortiClient enforcement to let you upgrade endpoints without losing network access.

   You will enable FortiClient enforcement again at the end of the upgrade procedure.

   a. Go to *Network* > *Interfaces*, and edit the interface used for FortiClient enforcement.
   b. In the *Restrict Access* area, disable *FortiTelemetry*.
   c. Click *OK*.



2. Upgrade FortiClient EMS to FortiClient EMS 1.2 or later by running the installer file for FortiClient EMS 1.2 or later.

   For details, see the *FortiClient EMS Release Notes*.

3. Upgrade all endpoints to FortiClient 5.6.0 or later.

You can upgrade FortiClient by using FortiClient EMS, an Active Directory server, or another method, such as having endpoint users download and install the new version of FortiClient. For information about installing FortiClient, see the *FortiClient Administration Guide*.

The upgrade requires the endpoint users to reboot their computers. No other input is needed from endpoint users for the FortiClient upgrade.

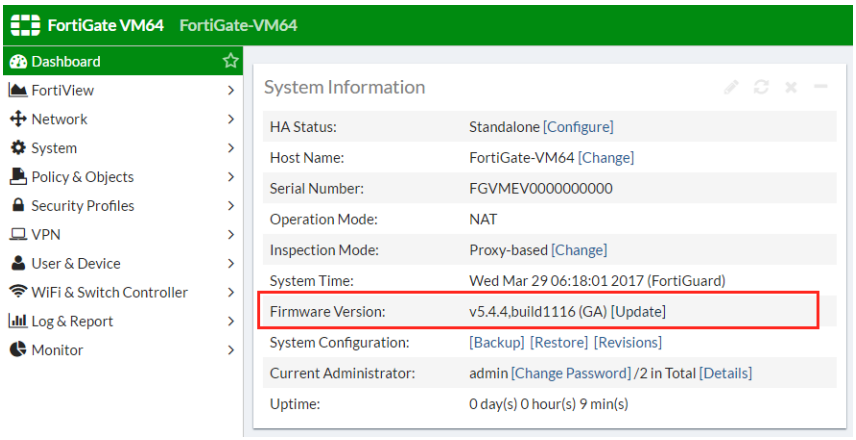
If you're using FortiClient EMS to upgrade FortiClient, you can add a FortiClient installer to EMS, and then select the FortiClient installer in the profile that is assigned to the endpoints. The FortiClient installer is downloaded to the endpoints with the next FortiTelemetry communication. It is recommended to install FortiClient to one group of endpoint users at a time. For details, see the *FortiClient EMS Administration Guide*.

4. Upgrade the OS version for FortiSwitch in managed mode to 3.5.2 or later.
   It is recommended to upgrade to FortiSwitch 3.5.3 or later to access all of the new features.
   a. Go to *WiFi & Switch Controller* > *Managed FortiSwitch*, and click *Upgrade* beside *FortiSwitch OS Version*.
5. Upgrade the OS version for the FortiAnalyzer units in the Security Fabric topology to FortiAnalyzer 5.6.0 or later.
   The Security Fabric feature in FortiOS 5.6.0 and later requires that you have a FortiAnalyzer unit and enable logging to the FortiAnalyzer unit. Whether logging to FortiAnalyzer is enabled in FortiOS before you upgrade affects how you upgrade the firmware for FortiAnalyzer units.

   If FortiOS 5.4.2 or later has logging to FortiAnalyzer enabled, upgrade the firmware for FortiAnalyzer units to 5.6.0 or later.

   If FortiOS 5.4.2 or later has logging to FortiAnalyzer disabled:
   a. Disable Security Fabric on all FortiGate units in the Security Fabric group by using FortiOS.
   b. Upgrade the firmware for FortiAnalyzer units to 5.6.0 or later.
6. Upgrade firmware for all FortiGate units in the Security Fabric topology to FortiOS 5.6.0 or later.
   The Security Fabric feature in FortiOS 5.6.0 and later requires that you have a FortiAnalyzer unit and enable logging to the FortiAnalyzer unit. If FortiOS 5.4.2 or later has logging to FortiAnalyzer disabled, disable Security Fabric on all FortiGate units in the Security Fabric group before you upgrade the firmware to 5.6.0 or later.

   It is recommended to upgrade the root FortiGate before upgrading the FortiGate devices that are connected to the root FortiGate.
   a. Go to *Dashboard*, and click *Update* beside *Firmware Version* in the *System Information* widget.
      For details, see the *FortiGate Release Notes*.



7. If logging to FortiAnalyzer was enabled in Security Fabric groups before the upgrade, you must complete the logging configuration for each Security Fabric group by registering all FortiGate units in each Security Fabric group with the primary FortiAnalyzer in each Security Fabric group and enabling communication between the units.

   After both FortiAnalyzer and FortiOS are upgraded to 5.6.0, all FortiGate units in each Security Fabric group must send logs to the primary FortiAnalyzer unit in the Security Fabric group. The primary FortiAnalyzer unit is defined as the unit to which the root FortiGate unit is sending logs. The primary FortiAnalyzer unit displays all FortiGate units in the Security Fabric group in Device Manager. Any previously registered FortiGate units display as registered devices in the FortiAnalyzer Device Manager. Any additional FortiGate units from the Security Fabric group display as unregistered devices in the FortiAnalyzer Device Manager. Complete the following steps to register all devices and enable communication.

   a. In FortiAnalyzer Device Manager, add all unregistered FortiGate units to the topology by selecting each an unregistered device and clicking the *Add Device* button.
   b. In FortiAnalyzer Device Manager, edit each newly registered FortiGate unit to add the username and password for the FortiGate unit. This enables communication of Security Fabric information between the FortiGate units and the FortiAnalyzer unit.
   c. Remove any disconnected FortiAnalyzer units from the Security Fabric group.

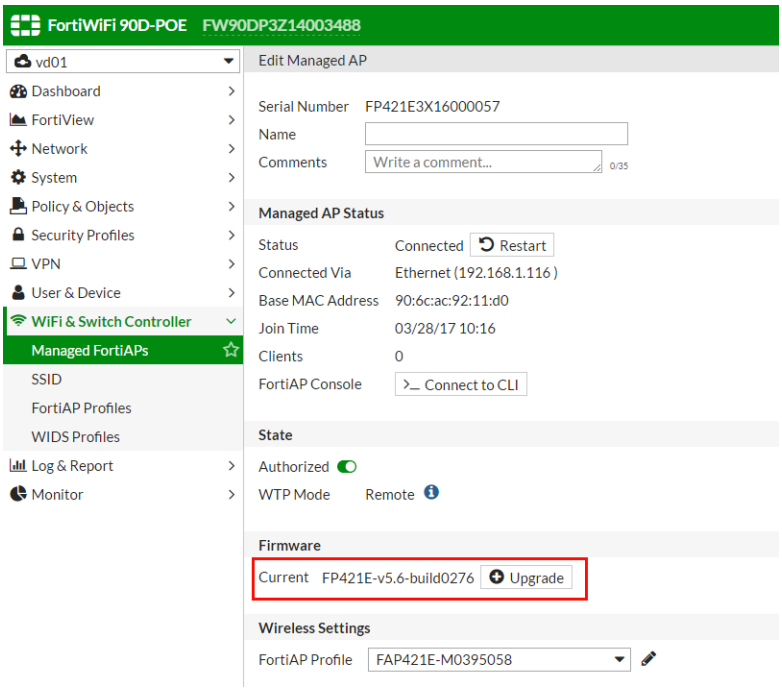
      Logs from disconnected FortiAnalyzer units are not automatically moved to the primary FortiAnalyzer unit in the Security Fabric group.

8. Upgrade the OS version for FortiAP, FortiAP-S, and FortiAP-W2 units to 5.6.0 or later by using FortiOS.

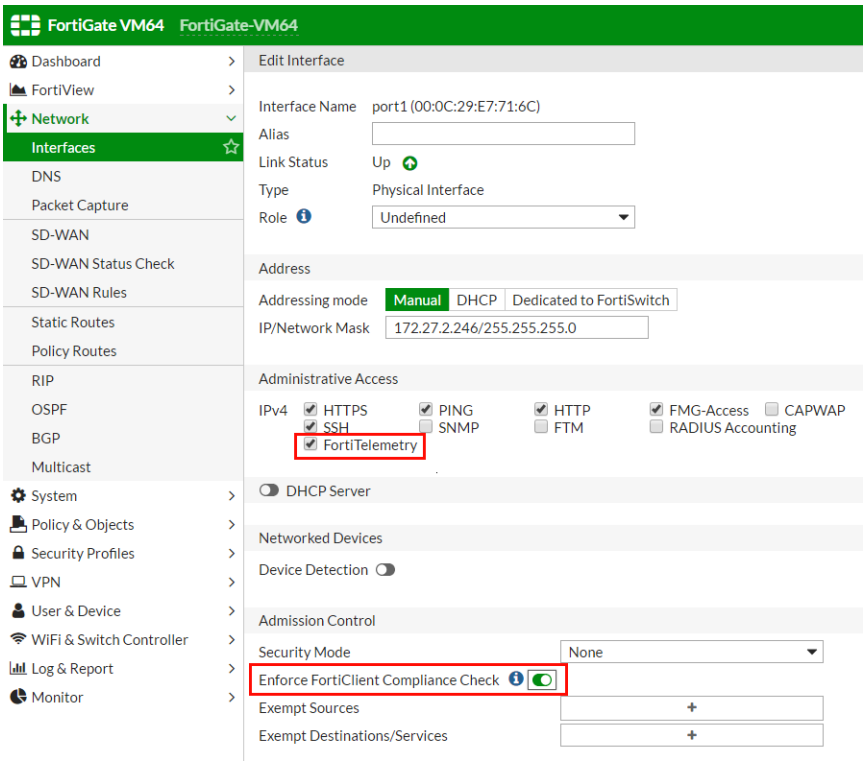
   FortiOS 5.6.0 supports FortiAP 5.4.x. However, it is recommended to upgrade to FortiAP 5.6.0 or later to access all of the new features.

   a. In FortiOS, ensure that all FortiAP units have reconnected after the FortiOS upgrade and have an *Online* status.
   b. Go to *WiFi & Switch Controller* > *Managed FortiAPs* > *Firmware*, and click *Upgrade*.

      For details, see the *FortiAP Release Notes*.



9. In FortiOS 5.6.0 or later, use the FortiClient Monitor to verify that the endpoints for which you want to enable enforcement have been upgraded to FortiClient 5.6.0 or later.
10. In FortiOS 5.6.0 or later, enable FortiClient enforcement (FortiTelemetry).
    a. Go to *Network* > *Interfaces*, and edit the interface(s) used for FortiClient enforcement.
    b. In the *Administrative Access* area, enable *FortiTelemetry*.
    c. In the *Admission Control* area, enable *Enforce FortiClient Compliance Check*.
    d. Click *OK*.


FortiGate VM64 FortiGate-VM64
Dashboard
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
SD-WAN Status Check
SD-WAN Rules
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report
Monitor
Edit Interface
Interface Name port1 (00:0C:29:E7:71:6C)
Alias
Link Status Up
Type Physical Interface
Role Undefined
Address
Addressing mode Manual DHCP Dedicated to FortiSwitch
IP/Network Mask 172.27.2.246/255.255.255.0
Administrative Access
IPv4 HTTPS PING HTTP FMG-Access CAPWAP
SSH SNMP FTM RADIUS Accounting
FortiTelemetry
DHCP Server
Networked Devices
Device Detection
Admission Control
Security Mode None
Enforce FortiClient Compliance Check
Exempt Sources
Exempt Destinations/Services