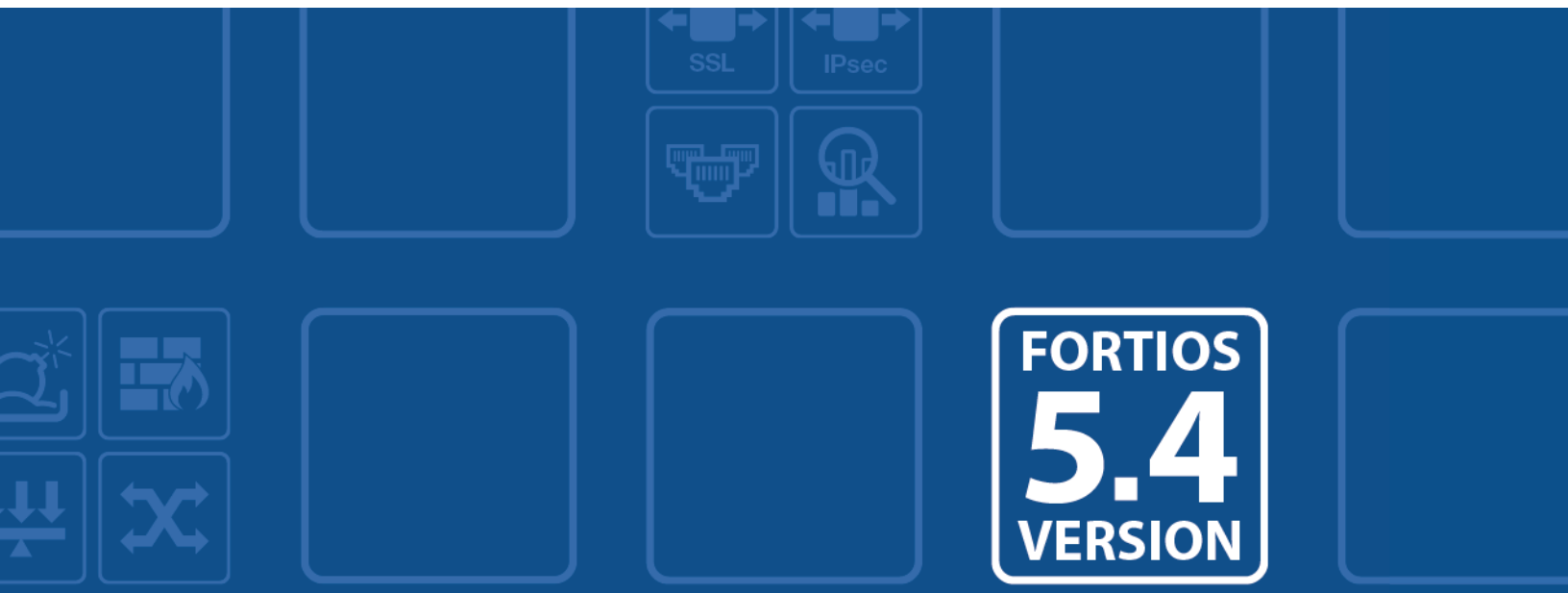
FORTINET
High Performance Network Security

Cooperative Security Fabric - Upgrade Guide

FORTIOS VERSION 5.4.5



FORTIOS 5.4 VERSION

Introduction

This guide describes how to upgrade Cooperative Security Fabric (CSF). A CSF 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 CSF can be used to coordinate the behavior of different Fortinet products in your network, including FortiGate, FortiClient, FortiSandbox, FortiAP, FortiSwitch, and FortiClient Enterprise Management Server (EMS).

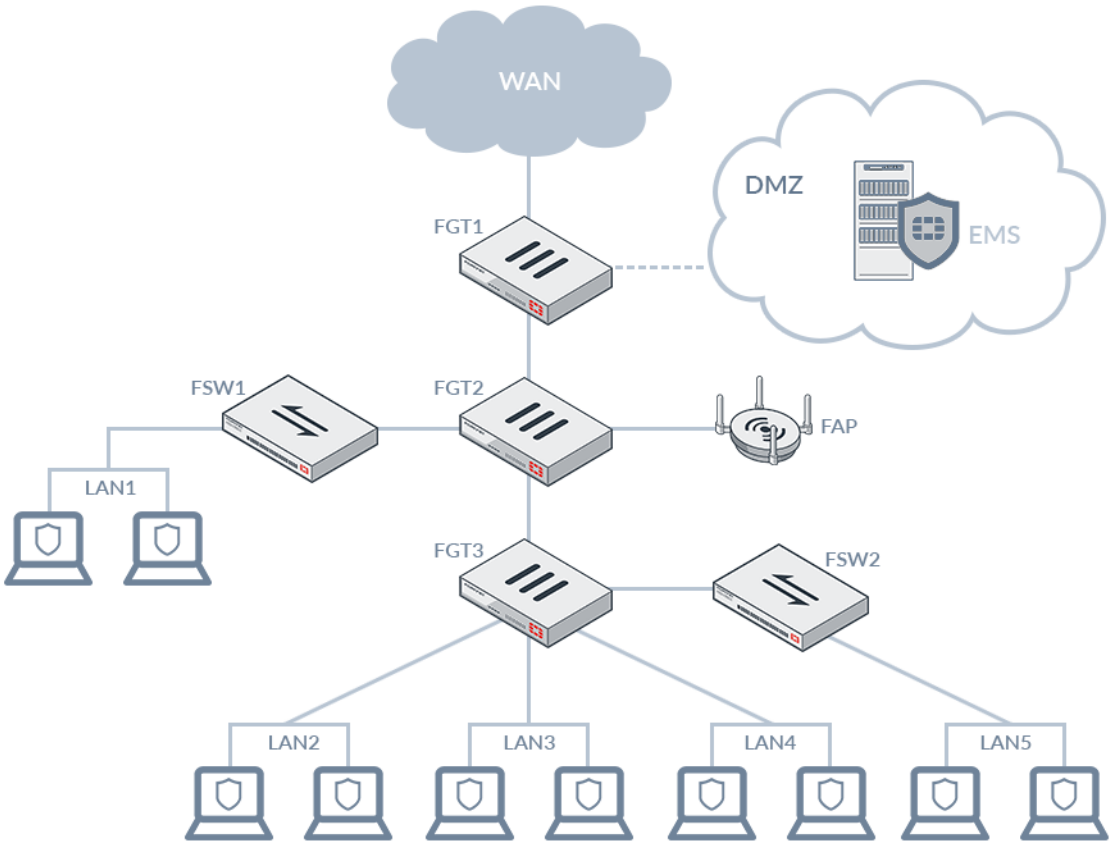
You should use this upgrade guide when you are using two or more products that are used for CSF. This guide describes how to upgrade the products in the correct sequence. For details about upgrading each product, see the following documents:

- *FortiClient Release Notes*

You should pay special attention to the section in this guide about FortiClient. See Prepare Endpoints for Upgrade and Migration to EMS on page 4.

- *FortiClient EMS Release Notes*
- *FortiOS 5.4.x Upgrade Guide for Managed FortiSwitch Devices*
- *FortiGate Release Notes*
- *FortiAP Release Notes*

CSF topology



Prepare Endpoints for Upgrade and Migration to EMS

If you do not use advanced FortiClient profiles (XML configuration) in FortiOS to configure endpoints, you can skip this section.

If you use advanced FortiClient profiles in FortiOS to configure endpoints, you should review this procedure. FortiOS 5.4.1 and later no longer supports advanced FortiClient profiles. If you want to continue managing and provisioning FortiClient configurations by using advanced profiles, you should migrate to using FortiClient EMS.

FortiClient EMS is an application that runs on your Windows Server for management of endpoints. It requires an annual subscription. For more information, see the *FortiClient EMS Administration Guide*.

You should perform these steps by using FortiOS 5.4.0 before you upgrade to FortiOS 5.4.1 or later, FortiClient 5.4.1 or later, and FortiClient EMS 1.0.1 or later.

The *forticlient-advanced-cfg* command has been removed from FortiOS 5.4.1 and later. The following example shows that the *forticlient-advanced-cfg* command has been removed from FortiOS 5.4.1:

```
config endpoint-control profile
   edit "default"
      config forticlient-winmac-settings
         set forticlient-advanced-cfg enable <<<<< Removed in FortiOS 5.4.1.
      end
   next
end
```

Without the *forticlient-advanced-cfg* command, you cannot use advanced FortiClient profiles with FortiOS 5.4.1 and later to delegate all managed endpoints to FortiClient EMS. Instead, you must use FortiOS 5.4.0 and an advanced FortiClient profile to delegate all managed endpoints to FortiClient EMS before you upgrade to FortiOS 5.4.1 and later. This section describes how to use FortiOS 5.4.0 and an advanced FortiClient profile to delegate all managed endpoints to FortiClient EMS.

In FortiOS 5.4.1 and later, you can use only basic FortiClient profiles to manage endpoints.

To prepare endpoints for upgrade and migration to EMS:

1. In FortiOS 5.4.0, use an advanced FortiClient profile (XML configuration) to push a secondary IP address for FortiClient EMS to all endpoints, which will allow endpoints to register to FortiClient EMS when FortiGate is temporarily unreachable during the upgrade.
   a. In FortiOS 5.4.0, go to *Dashboard* > *CLI Console*.
   b. Enter: `set forticlient-advanced-cfg enable`
   c. Go to *Security Profiles* > *FortiClient Profiles* > *Advanced XML*, and input the following text:

```
<endpoint_control>
...
      <fortigates>
         <fortigate>
            <serial_number />
```

```
            <name />
            <registration_password />
            <addresses>{FortiGate IP}:8013;{EMS Server IP}:8013</addresses>
         </fortigate>
      </fortigates>
```

You can use a partial or full XML configuration. For more information about XML configurations, see the *FortiClient XML Reference*.

2. Confirm that endpoints received the IP address for FortiClient EMS.
   a. In FortiClient console for one endpoint, back up the configuration by selecting *File* > *Settings* > *Backup*.
   b. Open the configuration file in a text editor, and confirm the IP address entries.
3. For the Active Directory server, ensure that GPO is correctly set up, which will allow FortiClient EMS to correctly manage endpoints.

   For information about the correct GPO setup, see the "Deploy FortiClient using Microsoft Active Directory server" section in the *FortiClient Administration Guide*.

   Later in the upgrade procedure, when you disable the *FortiHeartBeat* option on the FortiGate 5.4.0 interfaces, endpoints will be temporarily unable to connect to FortiGate and will connect to FortiClient EMS by using the secondary IP address for FortiClient EMS.
4. In FortiClient EMS, confirm that all endpoints are registered to FortiClient EMS.
5. If you are using FortiClient enforcement in FortiOS 5.4.1 and later, ensure that the *Non-compliance action* option in the FortiClient Profile is set to either *Block* or *Warning*. When set to *Auto-update*, FortiGate pushes its configuration to the endpoints, which may have an undesired effect.

If a FortiClient endpoint that is managed by FortiClient EMS is not registering to the FortiGate for FortiClient compliance, trigger the FortiClient to re-register by using the Endpoints page in FortiClient EMS.

Upgrade

This section describes how to upgrade the products used for CSF 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.

To upgrade CSF (summary):

1. If you use advanced FortiClient profiles (XML configuration) and plan to migrate to FortiClient EMS, prepare endpoints for the upgrade by using FortiOS 5.4.0 and advanced FortiClient profiles to delegate all managed endpoints to FortiClient EMS.

   If you do not use advanced FortiClient profiles and do not plan to migrate to FortiClient EMS, you can skip this step.
2. In FortiOS 5.4.0, disable FortiClient enforcement (FortiHeartBeat).

   FortiClient enforcement in FortiOS 5.4.1 and later requires FortiClient 5.4.1 or later and blocks network access for non-compliant endpoints. Temporarily disabling FortiClient enforcement allows you to upgrade endpoints without losing network access.
3. Upgrade FortiClient EMS to 1.0.1 or later.
4. Upgrade all endpoints to FortiClient 5.4.1 or later.
5. Upgrade the OS version for FortiSwitch in managed mode to 3.4.2 or later.

   See the *FortiOS 5.4.x Upgrade Guide For Managed FortiSwitch Devices*.
6. Upgrade firmware for the FortiGate devices in the CSF topology to FortiOS 5.4.1 or later.
7. Upgrade the OS version for FortiAP to 5.4.1 or later.
8. Verify that the endpoints for which you want to enable enforcement have been upgraded to FortiClient 5.4.1 or later.
9. In FortiOS 5.4.1 or later, enable FortiClient enforcement (FortiTelemetry).

To upgrade CSF (detailed procedure):

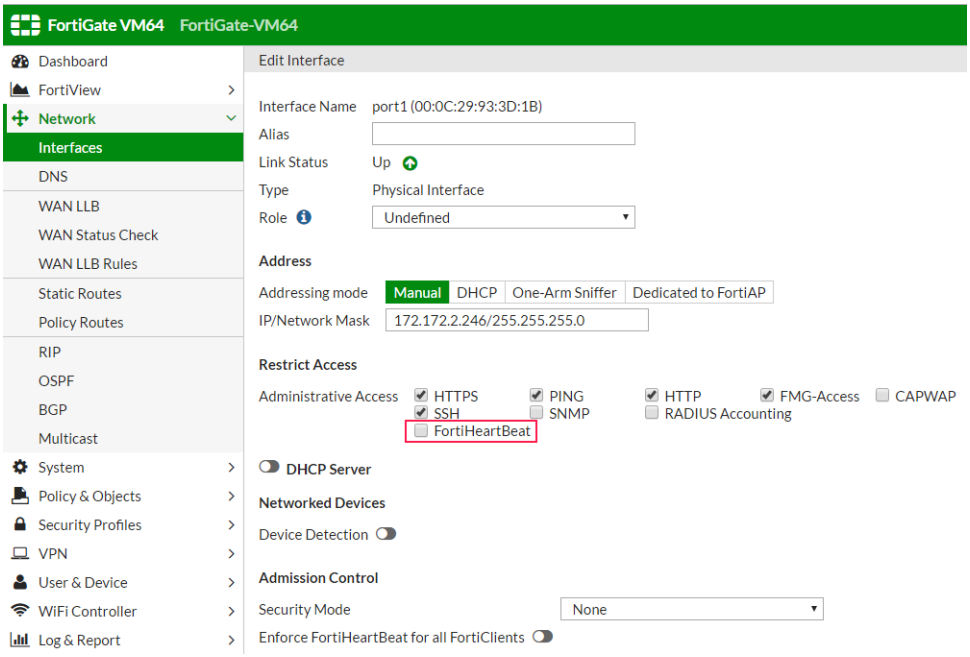
1. If you use advanced FortiClient profiles (XML configuration) and plan to migrate to FortiClient EMS, prepare endpoints for the upgrade. See Prepare Endpoints for Upgrade and Migration to EMS on page 4.

   If you do not use advanced FortiClient profiles and do not plan to migrate to FortiClient EMS, you can skip this step.
2. In FortiOS 5.4.0, temporarily disable FortiClient enforcement (FortiHeartBeat).

   FortiClient enforcement in FortiOS 5.4.1 and later requires FortiClient 5.4.1 or later and blocks network access for non-compliant endpoints. Temporarily disabling FortiClient enforcement allows you to 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 *Administrative Control* area, disable *FortiHeartBeat*.
c. Click *OK*.



3. Upgrade FortiClient EMS to FortiClient EMS 1.0.1 or later by running the installer file for FortiClient EMS 1.0.1 or later.

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

4. Upgrade all endpoints to FortiClient 5.4.1 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 FortiHeartBeat. It is recommended to install FortiClient to one group of endpoint users at a time. For details, see the *FortiClient EMS Administration Guide*.

5. Upgrade the OS version for FortiSwitch to 3.4.2 or later by using FortiOS and the *FortiOS 5.4.x Upgrade Guide For Managed FortiSwitch Devices* document.

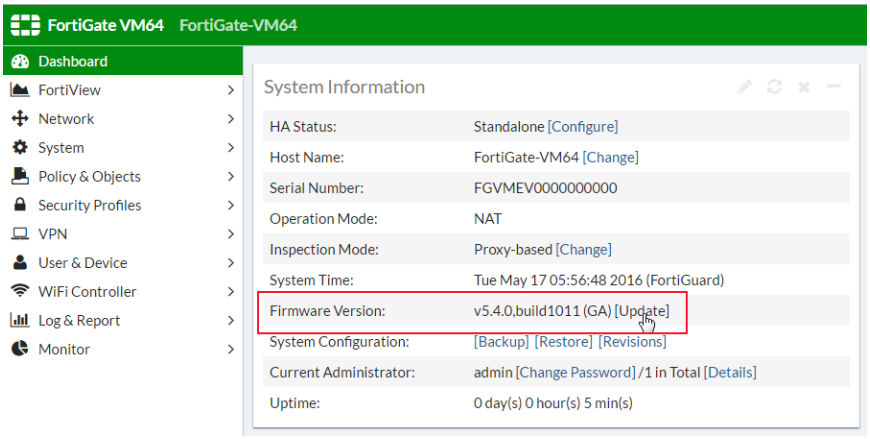
Managed FortiSwitch configurations have changed between FortiOS 5.4.0 and FortiOS 5.4.1. You must read the *FortiOS 5.4.x Upgrade Guide For Managed FortiSwitch Devices* to perform the necessary changes on the Managed FortiSwitch device after you complete the upgrade, such as reauthorizing FortiSwitch and reassigning VLANs to FortiSwitch ports.

6. Upgrade firmware for the FortiGate devices in the CSF topology to FortiOS 5.4.1 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.

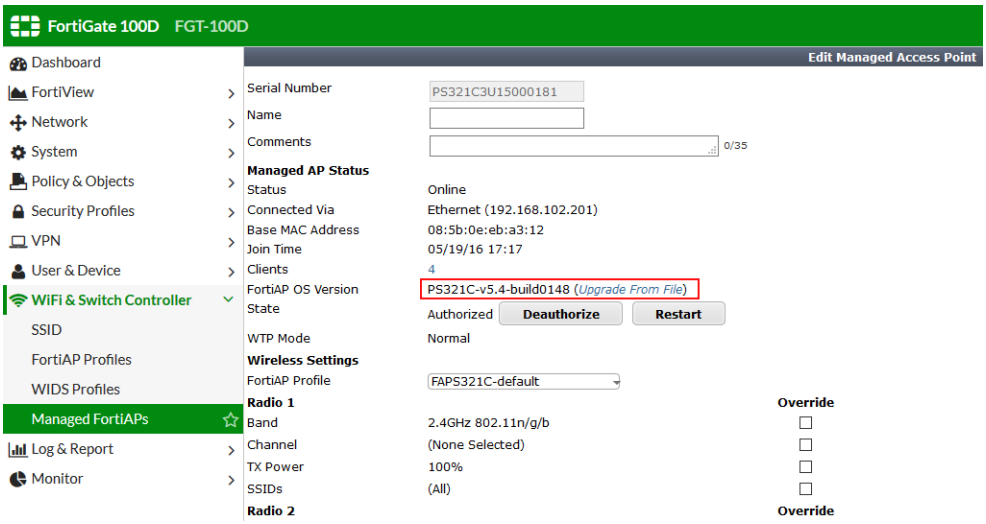
For details, see the *FortiGate Release Notes*.



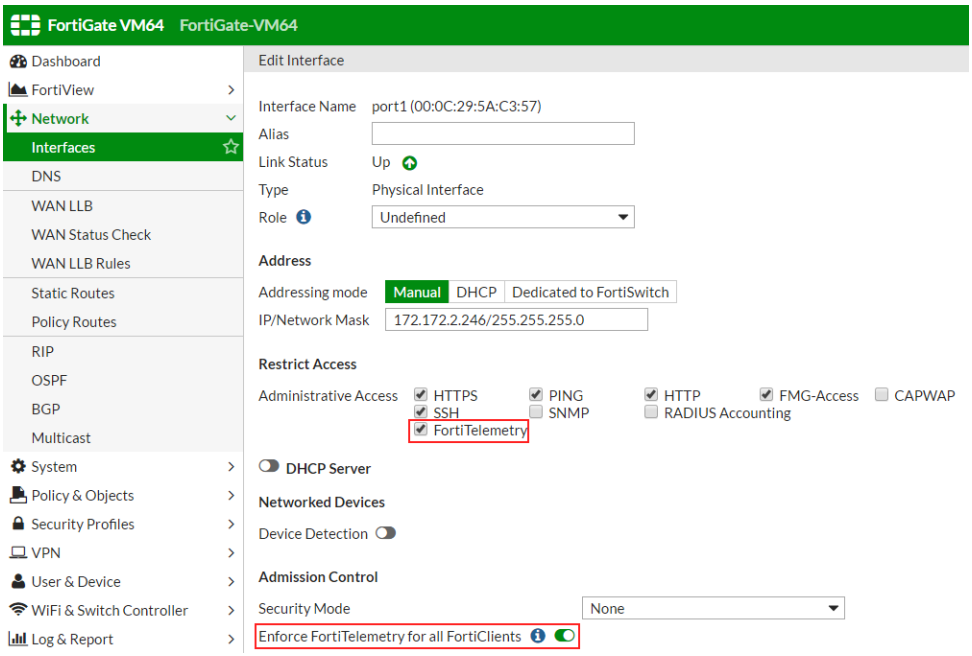
7. Upgrade the OS version for FortiAP to 5.4.1 or later by using FortiOS.
   a. Go to *WiFi & Switch Controller* > *Managed FortiAPs*, and click *Upgrade From File* beside *FortiAP OS Version*.

   You might need to physically unplug the link, and then plug the link back in again for FortiAP to appear.

   For details, see the *FortiAP Release Notes*.



8. In FortiOS 5.4.1 and later, use the FortiClient Monitor to verify that the endpoints for which you want to enable enforcement have been upgraded to FortiClient 5.4.1 or later.
9. In FortiOS 5.4.1 and later, enable FortiClient enforcement (FortiTelemetry).
   a. Go to *Network* > *Interfaces*, and edit the interface(s) used for FortiClient enforcement.
   b. In the *Admission Control* area, enable *FortiTelemetry* and *Enforce FortiTelemetry for All FortiClients*.
   c. Click *OK*.


FortiGate VM64 FortiGate-VM64
Dashboard
FortiView
Network
Interfaces
DNS
WAN LLB
WAN Status Check
WAN LLB Rules
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report
Edit Interface
Interface Name port1 (00:0C:29:5A:C3:57)
Alias
Link Status Up
Type Physical Interface
Role Undefined
Address
Addressing mode Manual DHCP Dedicated to FortiSwitch
IP/Network Mask 172.172.2.246/255.255.255.0
Restrict Access
Administrative Access HTTPS PING HTTP FMG-Access CAPWAP SSH SNMP RADIUS Accounting FortiTelemetry
DHCP Server
Networked Devices
Device Detection
Admission Control
Security Mode None
Enforce FortiTelemetry for all FortiClients

FORTINET®

High Performance Network Security