



FortiGate-6000 and FortiGate-7000 - Release Notes

Version 6.2.3 Build 6252

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



October 7, 2020

FortiGate-6000 and FortiGate-7000 6.2.3 Build 6252 Release Notes

01-623-583509-20201007

TABLE OF CONTENTS

Change log	5
FortiGate-6000 and FortiGate-7000 6.2.3 release notes	6
Supported FortiGate-6000 and 7000 models	6
What's new	7
Security Fabric and Split-Task VDOM support	7
Enabling Split-Task VDOM mode	8
Split-Task VDOM mode limitations and notes	9
Reverting to Multi VDOM mode	10
Multi VDOM mode and the Security Fabric	11
Virtual clustering	12
Limitations of FortiGate-6000 and 7000 virtual clustering	13
Virtual clustering VLAN/VDOM limitation	13
Virtual cluster configuration example	14
Configuration sync monitor	17
In-band management improvements	19
FortiGate-6000 management interface LAG and VLAN support	19
Management interface LAG limitations	20
ECMP support	20
VDOM-based session tables	20
Supported ECMP load balancing methods	21
Enabling auxiliary session support	21
FortiGate-6000 and 7000 HA options added to the GUI	21
HA heartbeat VLAN double-tagging	22
New protocol for handling HA chassis ID conflicts	22
execute factoryreset-shutdown command	22
Load balancing TCP and UDP sessions with fragmented packets	23
Special notices	24
SDN connector support	24
Before downgrading from FortiOS 6.2.3 remove virtual clustering	24
The Fortinet Security Fabric must be enabled	24
Adding a flow rule to support DHCP relay	25
Limitations of installing FortiGate-6000 firmware from the BIOS after a reboot	26
Limitations of installing FortiGate-7000 firmware from the BIOS after a reboot	26
Installing firmware on an individual FortiGate-6000 FPC	26
Installing firmware on an individual FortiGate-7000 FPM	27
SD-WAN is not supported	28
IPsec VPN features that are not supported	28
Quarantine to disk not supported	29
Local out traffic is not sent to IPsec VPN interfaces	29
Special configuration required for SSL VPN	29
If you change the SSL VPN server listening port	30
Adding the SSL VPN server IP address	30

Example FortiGate-6000 HA heartbeat switch configurations	30
Example triple-tagging compatible switch configuration	30
Example double-tagging compatible switch configuration	32
Example FortiGate-7000 HA heartbeat switch configuration	33
Example triple-tagging compatible switch configuration	33
Example double-tagging compatible switch configuration	34
Default FortiGate-6000 and 7000 configuration for traffic that cannot be load balanced	35
Managing individual FortiGate-6000 management boards and FPCs	41
Special management port numbers	41
HA mode special management port numbers	42
Connecting to individual FPC consoles	43
Connecting to individual FPC CLIs	44
Performing other operations on individual FPCs	44
Managing individual FortiGate-7000 FIMs and FPMs	45
Special management port numbers	45
HA mode special management port numbers	46
Managing individual FIMs and FPMs from the CLI	47
Connecting to individual FIM and FPM CLIs of the secondary FortiGate-7000 in an HA configuration	47
Upgrade information	48
HA graceful upgrade to FortiOS 6.2.3	48
About FortiGate-6000 firmware upgrades	48
About FortiGate-7000 firmware upgrades	49
Product integration and support	51
FortiGate-6000 6.2.3 special features and limitations	51
FortiGate-7000 6.2.3 special features and limitations	51
Maximum values	51
Resolved issues	52
Known issues	55

Change log

Date	Change description
October 7, 2020	Updated HA graceful upgrade to FortiOS 6.2.3 on page 48 to add FortiOS 6.0.9 and 6.0.10 to the upgrade path.
May 6, 2020	Changes to Multi VDOM mode and the Security Fabric on page 11 .
March 4, 2020	New section added: Load balancing TCP and UDP sessions with fragmented packets on page 23 .
March 2, 2020	Fixes to resolved issue descriptions.
February 28, 2019	Fixes to links and descriptions throughout the document.
February 27, 2020	Initial version.

FortiGate-6000 and FortiGate-7000 6.2.3 release notes

These platform specific release notes describe new features, special notices, upgrade information, product integration and support, resolved issues, and known issues for FortiGate-6000 and 7000 for 6.2.3 Build 6252. FortiGate-6000 and 7000 for 6.2.3 Build 6252 also includes the changes in default behavior, changes in CLI defaults, changes in default values, changes in table size, new features or enhancements, special notices, product integration and support, resolved issues, and known issues described in the [FortiOS 6.2.3 Release Notes](#).

For FortiGate-6000 documentation for this release, see the [FortiGate-6000 Handbook](#).

For FortiGate-7000 documentation for this release, see the [FortiGate-7000 Handbook](#).

Supported FortiGate-6000 and 7000 models

FortiGate-6000 and 7000 for FortiOS 6.2.3 Build 6252 supports the following models:

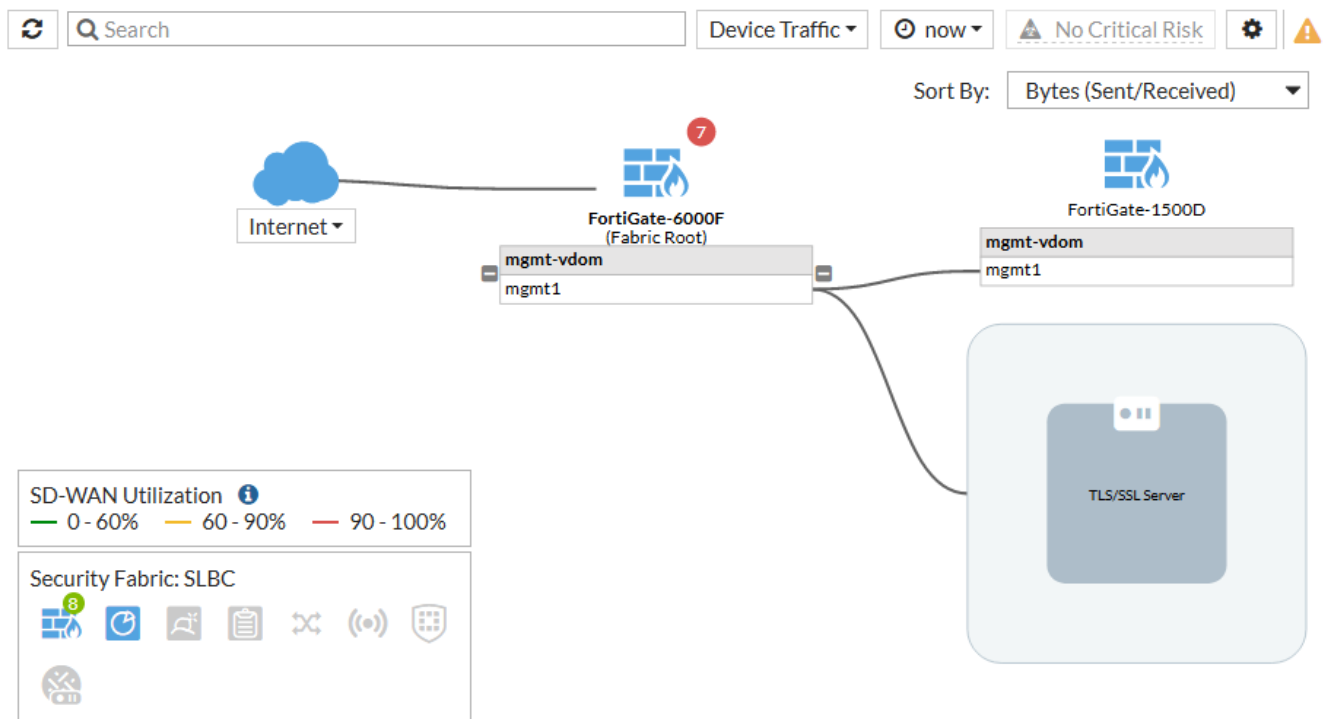
- FortiGate-6300F
- FortiGate-6301F
- FortiGate-6500F
- FortiGate-6501F
- FortiGate-7030E
- FortiGate-7040E
- FortiGate-7060E

What's new

The following new features have been added to FortiGate-6000 and 7000 for FortiOS 6.2.3 Build 6252. The changes in default behavior, CLI defaults, default values, changes in table size, and new features and enhancements described in the [FortiOS 6.2.3 release notes](#) also apply to FortiGate-6000 and 7000 FortiOS 6.2.3 Build 6252.

Security Fabric and Split-Task VDOM support

FortiGate-6000 and 7000 for FortiOS 6.2.3 supports the Fortinet Security Fabric and all Security Fabric related features including Security Rating. To fully support the Security Fabric, you must switch the FortiGate-6000 or 7000 to operate in Split-Task VDOM mode.



In both Multi VDOM mode and Split-Task VDOM mode, the Security Fabric widget and the Security Fabric topologies no longer show individual FortiGate-6000 FPCs or FortiGate-7000 FIMs and FPMs. You can now use the Configuration Sync Monitor to see the status of individual FortiGate-6000 or 7000 components. See [Configuration sync monitor on page 17](#).



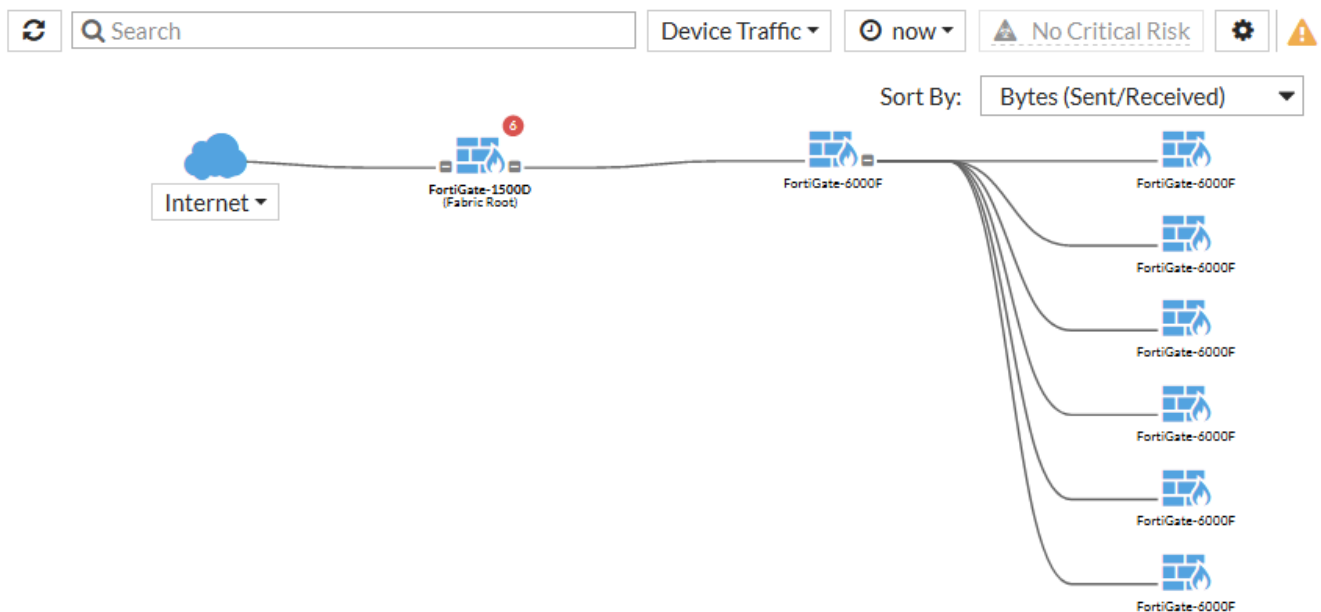
In both VDOM modes the Security Fabric must be enabled for normal SLBC operation. See [The Fortinet Security Fabric must be enabled on page 24](#) for details.

Begin setting up the Security Fabric for your FortiGate-6000 or 7000 by going to **Security Fabric > Settings > FortiGate Telemetry > FortiAnalyzer Logging** and adding a FortiAnalyzer. Once the FortiAnalyzer is added, you can continue configuring the Security Fabric in the same way as any FortiGate device. The FortiGate-6000 or 7000 can serve as the Security Fabric root or join an existing fabric. For more information see [Fortinet Security Fabric](#).

When setting up a Security Fabric that includes FortiGate-6000s or 7000s:

- The root FortiGate must have a **Fabric name** (also called a group name). You can use the default Fabric name (SLBC) or change it to a custom name.
- A non-root FortiGate can have a different or blank Fabric name as long as the non-root FortiGate is authorized by the root FortiGate.
- If the Security Fabric is set up in legacy mode, then all of the FortiGates in the Security Fabric should have a matching Fabric name and Group password.
- When you add a FortiGate-6000 or 7000 to an existing fabric, the Security Fabric topologies show the FPCs, FIMs, and FPMs as individual components in the topology. On the root FortiGate you only need to authorize the FortiGate-6000 management board or FortiGate-7000 primary FIM. All of the FortiGate-6000 FPCs or FortiGate-7000 FIMs and FPMs are then automatically authorized.
- You can click on any FPC, FIM, or FPM and select **Login** to log into that component using the special management port number.
- When adding a FortiGate-6000 or 7000 to an existing security fabric, you must manually add a FortiAnalyzer to the FortiGate-6000 or 7000 configuration. This is required because the default FortiGate-6000 or 7000 security fabric configuration has `configuration-sync` set to `local`, so the FortiGate-6000 or 7000 doesn't receive security fabric configuration settings, such as the FortiAnalyzer configuration, from the root FortiGate.

FortiGate-6301F added to a Security Fabric with a FortiGate-1500D acting as the Fabric root



Enabling Split-Task VDOM mode

By default the FortiGate-6000 and 7000 operate in Multi VDOM mode. Use the following steps to convert a FortiGate-6000 or 7000 from Multi VDOM mode to Split-Task VDOM mode. Converting to Split-Task VDOM mode involves first

disabling VDOMs and then enabling Split-Task VDOM mode.

The following includes CLI steps, and where possible, GUI steps. All of these steps can be completed from the CLI. Some of these steps cannot be completed from the GUI. For example, you cannot use the GUI to turn off VDOMs from Multi VDOM mode.

1. If required, delete all VDOMs except for mgmt-vdom and root.
2. Log into the CLI and enter the following command to turn off VDOMs:

```
config global
  config system global
    set vdom-mode no-vdom
  end
```

You are logged out of the CLI.

3. Log into the GUI or CLI and switch to Split-Task VDOM mode:

- From the CLI, enter the following command:

```
config system global
  set vdom-mode split-vdom
end
```

You are logged out of the CLI.

- From the GUI go to **System > Settings > System Operation Settings**, enable **Virtual Domains**, select **Split-Task VDOM** and select **OK**.

You don't need to add any management interfaces to the management VDOM. The required management interfaces and HA interfaces are added to the management VDOM automatically.

You are logged out of the GUI.

4. Log back into the CLI or GUI.

The FortiGate-6000 or 7000 will be operating in Split-Task VDOM mode and FortiGate Telemetry will be enabled. In Split-Task VDOM mode, the following VDOMs are available:

VDOM	Description
FG-traffic	All data traffic must use the FG-traffic VDOM. By default, all data interfaces have been added to the root VDOM and you must move them to the FG-traffic VDOM to be able to process data traffic.
mgmt-vdom	The management VDOM. Just as in Multi VDOM mode, mgmt-vdom contains the management and HA interfaces. You can't add or remove interfaces from the mgmt-vdom.
root	The root VDOM cannot be used for management or data traffic. By default, all data interfaces are in the root VDOM and you must move interfaces to the FG-traffic VDOM to be able to use them for data traffic.

Split-Task VDOM mode limitations and notes

FortiGate-6000 and 7000 for FortiOS 6.2.3 Split-Task VDOM mode includes the following limitations:

- You cannot switch an HA cluster between VDOM modes. If you are operating an HA cluster in Multi VDOM mode, you must remove each FortiGate from the cluster, switch the FortiGates to running in Split-Task VDOM mode and then re-configure the cluster. The same applies for switching an HA cluster between Split-Task VDOM mode and Multi VDOM mode.

- Split-Task VDOM mode does not support virtual clustering. FGCP, FGSP, standalone configuration synchronization, and VRRP are supported in Split-Task VDOM mode.
- While switching between Multi VDOM mode and Split-Task VDOM mode, your FortiGate-6000 or 7000 goes through an intermediate step where it has no VDOMs. The FortiGate-6000 or 7000 cannot forward data traffic without VDOMs so you must switch to Split-Task VDOM mode to be able to use the FortiGate-6000 or 7000 to forward data.
- You can't switch to Multi VDOM mode if FortiGate Telemetry is enabled.

Reverting to Multi VDOM mode

If your FortiGate-6000 or 7000 is operating in Split-Task VDOM mode, you can use the information in this section to revert back to Multi VDOM mode.



You can revert to Multi VDOM mode by resetting your FortiGate-6000 or 7000 to factory default settings by entering the `execute factoryreset` command. You will lose all configuration settings by entering this command, including network settings. However, the FortiGate-6000 or 7000 will be in Multi VDOM mode.

You can revert to Multi VDOM mode from the CLI or the GUI. The CLI process is recommended because it involves fewer steps.

Reverting to Multi VDOM mode from the CLI (recommended)

The following steps show how to use the CLI to switch from Split-Task VDOM mode to Multi VDOM mode.

1. If required, use the following command to set the Security Fabric role to root by unsetting the upstream IP address:

```
config global
  config system csf
    unset upstream-ip
  end
```

2. If the Security Fabric group name is blank, use the following command to add a group name:

```
config global
  config system csf
    set group-name <name>
  end
```

The group name may be blank if the FortiGate-6000 or 7000 had joined a Security Fabric.

3. Enter the following command to switch to Multi VDOM mode:

```
config global
  config system global
    set vdom-mode multi-vdom
  end
```

You are logged out of the CLI.

4. Log into the GUI or CLI.

The FortiGate-6000 or 7000 will be operating in Multi VDOM mode. The FG-traffic VDOM will still be available. However, it will be empty and you can choose to delete if you do not need it.

Reverting to Multi VDOM mode from the GUI

The following steps show how to use the GUI to switch from Split-Task VDOM mode to Multi VDOM mode.

1. If required, set the Security Fabric role to root by going to **Security Fabric > Settings** and setting the **Security Fabric role** to **Serve as Fabric Root**, and select **Apply**.
2. Disable FortiGate Telemetry, go to **Security Fabric > Settings** and disable **FortiGate Telemetry** and select **Apply**.
3. Go to **System > Settings > System Operation Settings** and select **Multi VDOM** and select **OK**.
You are logged out of the GUI.
4. Log into the GUI.

The FortiGate-6000 or 7000 will be operating in Multi VDOM mode. The FG-traffic VDOM will still be available. However, it will be empty and you can choose to delete if you do not need it.

Also, Security Fabric will not be enabled and the **Security Fabric > Settings > FortiGate Telemetry** GUI page will be hidden.

5. Enable the Security Fabric from the CLI:

```
config system csf
    set status enable
    unset upstream-ip
    unset group-name
end
```

Multi VDOM mode and the Security Fabric

When operating in Multi VDOM mode, the FortiGate-6000 and 7000 use the Security Fabric for communication and synchronization between the management board and FPCs or between the FIMs and FPMs. By default Security Fabric Telemetry is enabled. You can verify this from the GUI by going to **Security Fabric > Settings** and verifying that **FortiGate Telemetry** is enabled.

In addition to FortiGate Telemetry being enabled, the default **Security Fabric role** is set to **Serve as Fabric Root** and the **Fabric name** is **SLBC**. In Multi VDOM mode, the role and fabric name must not be changed.

You can also verify the default Security Fabric configuration from the CLI:

```
config system csf
    set status enable
    set upstream-ip 0.0.0.0
    set upstream-port 8013
    set group-name "SLBC"
    set group-password <password>
    set configuration-sync local
    set management-ip <ip-address>
    set management-port 44300
end
```

Where **<ip-address>** is set to the IP address of the FortiGate-6000 mgmt1 or FortiGate-7000 mgmt interface.

While operating in Multi VDOM mode, you should not change the Security Fabric configuration from the CLI or the FortiGate Telemetry configuration from the GUI. And you cannot add the FortiGate-6000 or 7000 to a Security Fabric. Multi VDOM mode also does not support the Security Rating feature.



The Security Rating feature is available in Split-Task VDOM mode.

You can go to **Security Fabric > Settings > FortiGate Telemetry** to enable and configure **FortiAnalyzer Logging**.

Multi VDOM mode also supports all other configurations on the **Security Fabric > Settings** menu, including **Central Management**, **Sandbox Inspection**, **Fabric Devices**, and **FortiClient Endpoint Management System (EMS)**. You can also view the **Physical Topology** and **Local Topology** and configure **Automation** and **Fabric Connectors**.

Virtual clustering

FortiGate-6000 and 7000 for FortiOS 6.2.3 supports virtual clustering with two FortiGate-6000s or 7000s if the FortiGate-6000s or 7000s are operating in Multi VDOM mode.



Virtual clustering is not supported in Split-Task VDOM mode.

A virtual cluster consists of two FortiGates operating in active-passive HA mode with Multi VDOM mode enabled. Virtual clustering is an extension of FGCP HA that uses VDOM partitioning to send traffic for some VDOMs to the primary FortiGate and traffic for other VDOMs to the secondary FortiGate. Distributing traffic between the FortiGates in a virtual cluster is similar to load balancing and can potentially improve overall throughput. You can adjust VDOM partitioning at any time to optimize traffic distribution without interrupting traffic flow.

VDOM partitioning distributes VDOMs between two virtual clusters (virtual cluster 1 and virtual cluster 2). When configuring virtual clustering you would normally set the device priority of virtual cluster 1 higher for the primary FortiGate and the device priority of virtual cluster 2 higher for the secondary FortiGate. With this configuration, all traffic in the VDOMs in virtual cluster 1 is processed by the primary FortiGate and all traffic in the VDOMs in virtual cluster 2 is processed by the secondary FortiGate. The FGCP selects the primary and secondary FortiGates whenever the cluster negotiates. The primary FortiGate can dynamically change based on FGCP HA primary unit selection criteria.

If a failure occurs and only one FortiGate continues to operate, all traffic fails over to that FortiGate, similar to normal FGCP HA. When the failed FortiGate rejoins the cluster, the configured traffic distribution is restored.

For more information about virtual clustering see:

- [HA virtual cluster setup \(FortiOS 6.2.3\)](#)
 - [Virtual clustering \(FortiOS 6.0\)](#)
-



If you don't want active-passive virtual clustering to distribute traffic between FortiGates, you can configure VDOM partitioning to send traffic for all VDOMs to the primary FortiGate. The result is the same as standard active-passive FGCP HA, all traffic is processed by the primary FortiGate.

Virtual clustering creates a cluster between instances of each VDOM on the two FortiGates in the virtual cluster. All traffic to and from a given VDOM is sent to one of the FortiGates where it stays within its VDOM and is only processed

by that VDOM. One FortiGate is the primary FortiGate for each VDOM and one FortiGate is the secondary FortiGate for each VDOM. The primary FortiGate processes all traffic for its VDOMs. The secondary FortiGate processes all traffic for its VDOMs.

The HA heartbeat provides the same HA services in a virtual clustering configuration as in a standard HA configuration. One set of HA heartbeat interfaces provides HA heartbeat services for all of the VDOMs in the cluster. You do not have to add a heartbeat interface for each VDOM.

Limitations of FortiGate-6000 and 7000 virtual clustering

FortiGate-6000 and 7000 for FortiOS 6.2.3 virtual clustering includes the following limitations:

- Virtual clustering supports two FortiGates only.
- Active-passive HA mode is supported, active-active HA is not.
- The root and mgmt-vdom VDOMs must be in virtual cluster 1 (also called the primary virtual cluster).
- A VLAN must be in the same virtual cluster as the physical interface or LAG that the VLAN has been added to. The VLAN can be in the same VDOM as its physical interface or LAG or in a different VDOM, as long as both VDOMs are in the same virtual cluster.
- The interfaces that are created when you add an inter-VDOM link must be in the same virtual cluster as the inter-VDOM link. You can change the virtual cluster that an inter-VDOM link is in by editing the inter-VDOM link and changing the `vcluster` setting.
- Using HA reserved management interfaces to manage individual cluster units is not supported. You can use In-band management to manage and monitor VDOMs in virtual cluster 2 by enabling management access for one or more data interfaces in the VDOMs in virtual cluster 2 and then logging into the GUI or CLI using these interfaces. See [Using data interfaces for management traffic](#).

You can also use special management port numbers to connect to the secondary chassis FortiGate-6000 management board (see [HA mode special management port numbers on page 42](#)).

Virtual clustering VLAN/VDOM limitation

In a FortiGate-6000 virtual clustering configuration, a VLAN must be in the same virtual cluster as the physical interface, LAG, or redundant interface that the VLAN has been added to. The VLAN can be in the same VDOM as its physical interface, LAG, or redundant interface or in a different VDOM, as long as both VDOMs are in the same virtual cluster.

If virtual clustering has already been set up, when adding VLANs, GUI and CLI error checking prevents you from adding a VLAN to a VDOM that is in a different virtual cluster than the physical interface, LAG, or redundant interface that you are attempting to add the VLAN to. However, error checking can't prevent this problem if you configure the VLANs before setting up virtual clustering or if you move VDOMs to different virtual clusters after adding the VLANs.

A recommended strategy for preventing this problem could involve the following steps:

1. Start by setting up virtual clustering before creating new VDOMs.
2. Create a placeholder VDOM and add it to virtual cluster 2.
3. Separate traffic interfaces between the root VDOM in virtual cluster 1 and the placeholder VDOM in virtual cluster 2.

Based on network planning you can create an even distribution of planned traffic volume between the two virtual clusters.

4. Build up your configuration by adding more VDOMs, LAGs, redundant interfaces, and VLANs as required, making sure to keep VLANs in the same virtual cluster as their parent interfaces, LAGs, or redundant interfaces.

Example incorrect VLAN configuration

Consider the following FortiGate-6000 virtual clustering example, which shows how traffic can be blocked by this limitation:

- Three data traffic VDOMs: root, Engineering, and Marketing.
- One LAG interface: LAG1 in the root VDOM.
- Two VLAN interfaces added to LAG1: vlan11 and vlan12.
 - vlan11 is added to the Engineering VDOM.
 - vlan12 is added to the Marketing VDOM.
- The root and Engineering VDOMs are in virtual cluster 1.
- The Marketing VDOM is in virtual cluster 2.

As a result of this configuration:

- vlan11 is in the Engineering VDOM, which is in virtual cluster 1. vlan11 is also in LAG1, which is in the root VDOM, also in virtual cluster 1. vlan11 and its LAG are in the same virtual cluster. Traffic can pass through vlan11.
- vlan12 is in the Marketing VDOM, which is in virtual cluster 2. vlan12 is also in LAG1, which is in the root VDOM, in virtual cluster 1. vlan12 and its LAG are in different virtual clusters. Traffic cannot pass through vlan12.

Virtual cluster configuration example

Configuring virtual clustering is the same as configuring standard FCGP HA with the addition of VDOM partitioning. Using VDOM partitioning, you can control the distribution of VDOMs, and the traffic they process, between the FortiGates in the cluster.

VDOM partitioning can be thought of in two parts. First, there is configuring the distribution of VDOMs between two virtual clusters. By default, all VDOMs are in virtual cluster 1, virtual cluster 1 is associated with the primary FortiGate, and the primary FortiGate processes all traffic. If you want traffic to be processed by the secondary FortiGate, you need to enable virtual cluster 2, move some of the VDOMs to it, and associate virtual cluster 2 with the secondary FortiGate.

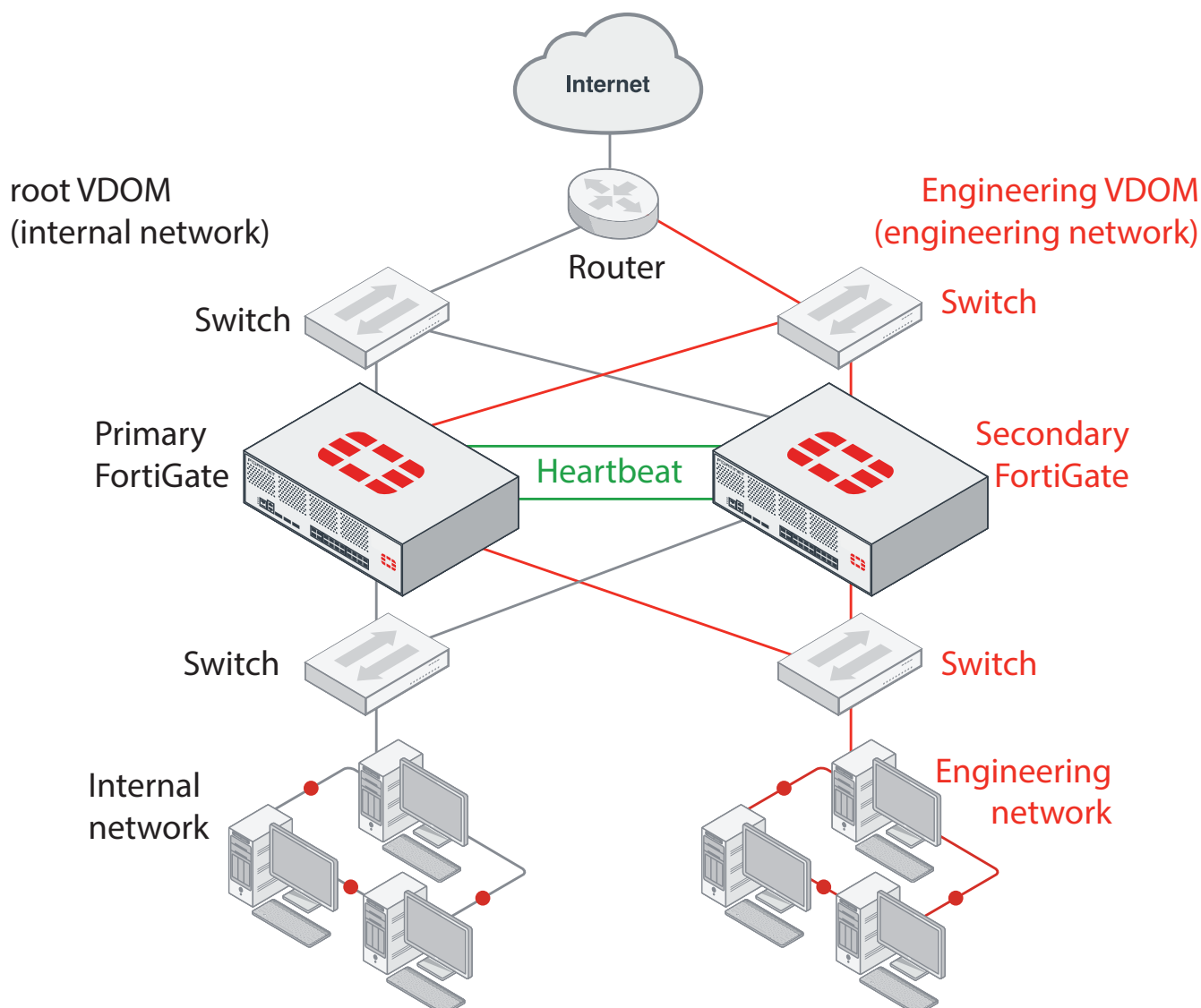
You associate a virtual cluster with a FortiGate using device priorities. The FortiGate with the highest device priority is associated with virtual cluster 1. To associate a FortiGate with virtual cluster 2, you must enable virtual cluster 2 and set virtual cluster 2 device priorities on each FortiGate. The FortiGate with the highest virtual cluster 2 device priority processes traffic for the VDOMs added to virtual cluster 2. (Reminder: device priorities are not synchronized.)

Normally, you would set the virtual cluster 1 device priority for the primary FortiGate and the virtual cluster 2 device priority higher for the secondary FortiGate. Then the primary FortiGate would process virtual cluster 1 traffic and the secondary FortiGate would process virtual cluster 2 traffic.

Enabling virtual cluster 2 also turns on HA override for virtual cluster 1 and 2. Enabling override is required for virtual clustering to function as configured. Enabling override causes the cluster to negotiate every time the cluster state changes. If override is not enabled, the cluster may not negotiate as often. While more frequent negotiation may cause more minor traffic disruptions, with virtual clustering its more important to negotiate after any state change to make sure the configured traffic flows are maintained.

The figure below shows a simple FortiGate virtual cluster that provides redundancy and failover for two networks. The configuration includes two VDOMs. The root VDOM handles internal network traffic and the Engineering VDOM handles Engineering network traffic. VDOM partitioning has been set up to send all root VDOM traffic to the primary FortiGate and all Engineering VDOM traffic to the secondary FortiGate.

Example virtual clustering configuration



Primary FortiGate configuration

The primary FortiGate configuration:

- Sets the primary FortiGate to be chassis 1.
- Enables virtual cluster 2 (`vcluster2`) to enable virtual clustering.
- Enables override for virtual cluster 1.
- Sets the virtual cluster 1 device priority to 200.
- Enables override for virtual cluster 2 (`secondary-vcluster`).
- Sets the virtual cluster 2 device priority to 50.
- Adds the Engineering VDOM to virtual cluster 2 (all VDOMs remain in virtual cluster 1 unless you add them to virtual cluster 2).

```
config system ha
```

```
set group-id 6
set group-name <name>
set mode a-p
set password <password>
set hbdev "ha1" 50 "ha2" 50
set chassis-id 1
set vcluster2 enable
set override enable
set priority 200
config secondary-vcluster
    set override enable
    set priority 50
    set vdom Engineering
end
```

Secondary FortiGate configuration

The secondary FortiGate configuration:

- Sets the secondary FortiGate to be chassis 2.
- Enables virtual cluster 2 (`vcluster2`) to enable virtual clustering.
- Enables override for virtual cluster 1.
- Sets the device priority of virtual cluster 1 to 50.
- Enables override for virtual cluster 2 (`secondary-vcluster`).
- Sets the virtual cluster 2 device priority to 200.
- You do not need to add the Engineering VDOM to virtual cluster 2, the configuration of the VDOMs in virtual cluster 2 is synchronized from the primary FortiGate.

```
config system ha
    set group-id 6
    set group-name <name>
    set mode a-p
    set password <password>
    set hbdev "ha1" 50 "ha2" 50
    set chassis-id 2
    set vcluster2 enable
    set override enable
    set priority 50
    config secondary-vcluster
        set override enable
        set priority 200
        set vdom Engineering
    end
```








Since the primary FortiGate has the highest device priority, it processes all traffic for the VDOMs in virtual cluster 1. Since the secondary FortiGate has the highest virtual cluster 2 device priority, it processes all traffic for the VDOM in virtual cluster 2. The primary FortiGate configuration adds the VDOMs to virtual cluster 2. All you have to configure on the secondary FortiGate for virtual cluster 2 is the virtual cluster 2 (or `secondary-vcluster`) device priority.

Virtual cluster GUI configuration


From the GUI, you configure virtual clustering from the **Global** menu by going to **System > HA**, configuring HA settings and VDOM Partitioning.

Primary FortiGate VDOM partitioning

☒ VDOM Partitioning






Virtual cluster 1	<div><div> mgmt-vdom</div><div> root</div><div>+</div><div></div></div>
Virtual cluster 2	<div><div> Engineering</div><div>+</div><div></div></div>

Secondary Cluster Settings


Device priority 

Secondary FortiGate VDOM partitioning

☒ VDOM Partitioning

Virtual cluster 1	<div><div> mgmt-vdom</div><div> root</div><div>+</div><div></div></div>
Virtual cluster 2	<div><div> Engineering</div><div>+</div><div></div></div>

Secondary Cluster Settings

Device priority 

Configuration sync monitor

From the Global GUI you can now go to **Monitor > Configuration Sync Monitor** to view the configuration synchronization status of your FortiGate-6000 or 7000 and its individual FPCs, FIMs, or FPMs.



From the menu bar at the top of the FortiGate-6000 and 7000 GUI, you can click on the host name and pull down a list of the FPCs or FIMs and FPMs in the current device. From the list you can see the status of each component, change the host name, or log into the GUI using the special management port number.

The Configuration Sync monitor shows information for the FortiGate-6000 or 7000 component that you have logged into. For example:

- If you log into a FortiGate-6000 management board, you can view the configuration status of the management board and all of the FPCs in the FortiGate-6000.
- If you log into an FPC, you can see the configuration status of that FPC and the management board.
- If you log into the management board of a FortiGate-6000 HA cluster you will see the configuration status of the management board that you have logged into. The display does not contain HA-specific information or information about the other FortiGate-6000 in the HA cluster.




Synchronization information includes the configuration status, role, up time, and time since the last heartbeat was received from the component. If a component has failed, it will be removed from the list. If a component is out of synchronization this will be reflected on the Configuration Status list.

If you are logged into the primary unit in an HA configuration, the configuration sync monitor also shows the status of the secondary FortiGate-6000 management board or FortiGate-7000 primary FIM.

Search	Q	F6KF31T018900143			
Serial	Slot ID	Configuration Status	Role	Up Time	Last Heartbeat
F6KF31T018900143	0	In Sync	Master	1h 35m	
FPC6KFT018901327	1	In Sync	Slave	1h 33m	25 seconds ago
FPC6KFT018901372	2	In Sync	Slave	1h 33m	⌚ Every 10 minutes
FPC6KFT018901346	3	In Sync	Slave	1h 33m	⌚ Every 5 minutes
FPC6KFT018901574	4	In Sync	Slave	1h 33m	⌚ Every 2 minutes
FPC6KFT018901345	5	In Sync	Slave	1h 33m	⌚ Every 1 minute
FPC6KFT018901556	6	In Sync	Slave	53m	⌚ Every 30 seconds
					⌚ Now
				7	Updated: 08:35:24

You can hover your mouse cursor over any of the components and view more detailed information about the component including the hostname, serial number, firmware version, management IP address, special management port number, CPU usage, memory usage, and session count.

From the pop up you can also select **Login** to log into the component using its management IP address and special port number. You can also select **Configure** to change the component's host name.

FortiGate	 FPC6KFT018901327
Hostname	F6KF31T018900143
Serial Number	FPC6KFT018901327
Model	FortiGate 6301F
Version	v6.2.3 build1066
Management IP/FQDN	172.25.176.31
Management Port	44301
CPU Usage	<div><div>0%</div></div>
Memory Usage	<div><div>14%</div></div>
Session Count	36
<div><div> Login</div><div> Configure</div></div>	

In-band management improvements

The following improvements have been made to in-band management for FortiOS 6.2.3:

- FortiGate-6000 for FortiOS 6.2.3 supports in-band management with IPv6 addresses.
- In-band management connections to the IP address of a VDOM link interface are now supported.
- Large (or jumbo) packets from in-band management sessions are no longer fragmented by the FPCs or FPMs before they are forwarded to the management board or primary FIM.

For more information about in-band management and its limitations, see [Using data interfaces for management traffic](#).

FortiGate-6000 management interface LAG and VLAN support

FortiGate-6000 supports adding the mgmt1 and mgmt2 interfaces to an LACP link aggregation group (LAG). You can also add VLAN interfaces to the mgmt1, mgmt2, and mgmt3 interfaces or to a LAG that includes mgmt1 and mgmt2.

You can use the following configuration to create a management interface LAG that includes the mgmt1 and mgmt2 interfaces.

```
config system interface
  edit "lacp_mgmt"
    set vdom mgmt-vdom
    set type aggregate
    set member mgmt1 mgmt2
  end
```



To be able to add an interface to a LAG you must remove all references to that interface (including static routes) and unset the IP address of the interface.

The management interface LAG fully supports LACP and supports other standard interface features. The management interface LAG as well as any VLAN interfaces added to the mgmt1, mgmt2, or mgmt3 interfaces or to the management interface LAG must remain in the mgmt-vdom VDOM.

Management interface LAG limitations

Management interface LAG support has the following limitations:

- You cannot set a management interface LAG to be the SLBC management interface by adding it to the `config load-balance setting slbc-mgmt-intf` option. This means that you cannot use the management interface LAG IP address with special port numbers to access the management board or individual FPCs as described in [Special management port numbers on page 41](#).
After creating a management interface LAG, if you still want to be able to use special port numbers to log into the management board or individual FPCs, you can use the mgmt3 interface for this access by setting `slbc-mgmt-intf` to `mgmt3` and connecting MGMT3 to the management network.
- FPCs and the management board assign different MAC addresses to the management interface LAG. The management board uses the MAC address of the second interface in the member list while the FPCs use the MAC address of the first interface in the member list.
- You can add the mgmt3 interface to the same LAG as mgmt1 and mgmt2. This configuration is not recommended, since LACP may not work as expected if the LACP group contains interfaces with different speeds. Adding mgmt3 might work in some configurations.
- You can add mgmt1, mgmt2, or mgmt3 to a LAG even if the management interface is configured as the SLBC management interface.
- If mgmt1, mgmt2, or mgmt3 are HA monitored interfaces they cannot be added to a management interface LAG.

ECMP support

FortiOS 6.2.3 for FortiGate-6000 and 7000 now includes support for most FortiOS IPv4 ECMP functionality. (IPv6 ECMP is not supported.) Before setting up an ECMP configuration you need to use the following command to configure the DP processor to operate with VDOM-based session tables:

```
config load-balance setting
    set dp-session-table-type vdom-based
end
```

Once you have enabled VDOM-based session tables, you can enable and configure ECMP as you would for any FortiGate.

VDOM-based session tables

In an ECMP configuration, because of load balancing return traffic could enter through a different interface than the one it exited from. If this happens, the DP processor operating with default interface-based session tables may not be able

to send the return traffic to the FPC or FPM that processed the incoming session, causing the return traffic to be dropped. Operating with VDOM-based session tables solves this problem, allowing traffic received on a different interface to be properly identified and sent to the correct FPC or FPM.

Enabling VDOM session tables can reduce connections per second (CPS) performance so it should only be enabled if needed to support ECMP. This performance reduction can be more noticeable if the FortiGate-6000 or 7000 is processing many firewall only sessions. If the FortiGate-6000 or 7000 is performing content inspection where CPS performance is less important, the performance reduction resulting from enabling VDOM-based session tables may be less noticeable.

Supported ECMP load balancing methods

You can use the following command to configure the ECMP load balancing method for a VDOM:

```
config system settings
  set v4-ecmp-mode {source-ip-based | weight-based | source-dest-ip-based | usage-based}
end
```

With VDOM-based session tables enabled, the FortiGate-6000 and 7000 support all ECMP load balancing methods except `usage-based`. If you select `usage-based`, all traffic uses the first ECMP route instead of being load balanced among all ECMP routes. All other ECMP load balancing methods are supported.

Enabling auxiliary session support

When ECMP is enabled, TCP traffic for the same session can exit and enter the FortiGate on different interfaces. To allow this traffic to pass through, FortiOS creates auxiliary sessions. Allowing the creation of auxiliary sessions is handed by the following command:

```
config system settings
  set auxiliary-sessions {disable | enable}
end
```

By default, for FortiOS 6.2.3 the `auxiliary-session` option is disabled. This can block some TCP traffic when ECMP is enabled. If this occurs, enabling `auxiliary-session` may solve the problem. For more information, see [Technical Tip: Enabling auxiliary session with ECMP or SD-WAN](#).

FortiGate-6000 and 7000 HA options added to the GUI

FortiGate-6000 and 7000 for FortiOS 6.2.3 adds more FortiGate-6000 and 7000 specific settings to the HA GUI page:

- The Chassis Identifier (`chassis-id`)
- Synchronize management VDOM

HA heartbeat VLAN double-tagging

To support the different types of VLAN tagging modes supported by third-party switches used to connect FortiGate-6000 and 7000 HA heartbeat interfaces, FortiOS 6.2.3 now supports double VLAN tagging and changing the outer TPID.

FortiGate-6000 and 7000 now support two tagging methods for HA control packets:

- Triple tagging (called proprietary mode) has the following structure:

```
TPID 0x8100 VLAN <vlan-id> (by default 999) + TPID 0x88a8 VLAN 10/30 + TPID 0x8100 VLAN 10/30 + ethernet packet
```

- The new double-tagging mode has the following structure:

```
TPID 0x8100 VLAN <vlan-id> (by default 999) + TPID 0x8100 VLAN 10/30 + ethernet packet
```

You can use the following command to change the HA VLAN tagging mode and customize the outer TPID. Both FortiGates in the cluster must have the same VLAN tagging configuration.

```
config system ha
  set ha-port-dtag-mode {proprietary | double-tagging}
  set ha-port-outer-tpid {0x8100 | 0x9100 | 0x88a8}
end
```

The default outer TPID is 0x8100. The default outer TPID is compatible with FortiSwitch and most third-party switches.

For a FortiGate-6000 double-tagging example, see [Example double-tagging compatible switch configuration on page 1](#).

For a FortiGate-7000 double-tagging example, see [Example double-tagging compatible switch configuration on page 1](#).

New protocol for handling HA chassis ID conflicts

If both FortiGate-6000s or 7000s in a cluster are configured with the same chassis ID, both chassis begin operating in HA mode without forming a cluster. A message similar to the following is displayed on the CLI console of both devices:

```
HA cannot be formed because this box's chassis-id 1 is the same from the HA peer
'F76E9D3E17000001' chassis-id 1.
```

As well, a log message similar to the following is created:

```
Jan 29 16:29:46 10.160.45.70 date=2020-01-29 time=16:29:51 devname="CH-02" devid="F76E9D3E17000001" slot=1 logid="0108037904" type="event" subtype="ha" level="error" vd="mgmt-vdom" eventtime=1580344192162305962 tz="-0800" logdesc="Device set as HA master" msg-g="HA group detected chassis-id conflict" ha_group=7 sn="F76E9DT018900001 chassis-id=1"
```

You can resolve this issue by logging into one of the FortiGates and changing its Chassis ID to 2. When this happens, the two chassis will form a cluster.

execute factoryreset-shutdown command

You can use this command to reset the configuration of the FortiGate-6000 or 7000 and shut the system down.

On a FortiGate-6000 the command resets and shuts down the FortiGate-6000 management board and all of the FPCs.

On a FortiGate-7000 the command resets and shuts down all of the FIMs and FPMs.

This command replaces the `execute factoryreset3` command.

Load balancing TCP and UDP sessions with fragmented packets

FortiGate-6000 and 7000 for FortiOS 6.2.3 supports load balancing TCP and UDP sessions with fragmented packets.

Previous versions supported load balancing ICMP sessions with fragmented packets by enabling the `dp-fragment-session` load balancing setting. FortiOS 6.2.3 adds the new `sw-load-distribution-method` option that you can configure to support load balancing TCP and UDP sessions with fragmented packets.

To load balance TCP, UDP, and ICMP sessions with fragmented packets, use the following configuration:

```
config load-balance setting
    set dp-fragment-session enable
    set sw-load-distribution-method src-dst-ip
end
```

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for FortiGate-6000 and FortiGate-7000 6.2.3 Build 6252. The [Special notices](#) described in the [FortiOS 6.2.3 release notes](#) also apply to FortiGate-6000 and 7000 FortiOS 6.2.3 Build 6252.

SDN connector support

FortiGate-6000 and 7000 for FortiOS 6.2.3 supports the following SDN connectors:

- Cisco Application Centric Infrastructure (ACI)
- Amazon Web Services (AWS)
- Microsoft Azure
- VMware NSX

These SDN connectors communicate with their public or private clouds through the root VDOM and may require routing in this VDOM to support this communication. Also, in some scenarios, these SDN connectors may not be able to correctly retrieve dynamic firewall addresses.

The following SDN connectors are not yet supported:

- Kubernetes
- Oracle Cloud Infrastructure (OCI)
- OpenStack (Horizon)

Before downgrading from FortiOS 6.2.3 remove virtual clustering

If you are operating a FortiGate-6000 or 7000 system running FortiOS 6.2.3 with virtual clustering enabled, and decide to downgrade to FortiOS 6.0.x or earlier, you must remove all VDOMs from virtual cluster 2 and disable VDOM partitioning before performing the firmware downgrade.

If there are VDOMs in virtual cluster 2 when you perform the firmware downgrade, the FortiGate-6000 FPCs or FortiGate-7000 FIMs and FPMs may not be able to start up after the previous firmware version is installed. If this happens you may have to reset the configurations of all components to factory defaults.

The Fortinet Security Fabric must be enabled

FortiGate-6000 and 7000 Session-Aware Load Balancing (SLBC) uses the Fortinet Security Fabric for internal communication and synchronization.

In both Split-Task and Multi VDOM modes you can enable Fortinet Telemetry from the GUI by going to **Security Fabric > Settings** and enabling and configuring **FortiGate Telemetry**.

In either VDOM mode, you can also enable the Security Fabric from the CLI using the following command:

```
config system global
  cong system csf
    set status enable
  end
```

For more information about the Security Fabric and Multi VDOM mode, see [Multi VDOM mode and the Security Fabric on page 11](#).

Adding a flow rule to support DHCP relay

The FortiGate-6000 and FortiGate-7000 default flow rules may not handle DHCP relay traffic correctly.

The default configuration includes the following flow rules for DHCP traffic:

```
config load-balance flow-rule
  edit 7
    set status enable
    set vlan 0
    set ether-type ipv4
    set src-addr-ipv4 0.0.0.0 0.0.0.0
    set dst-addr-ipv4 0.0.0.0 0.0.0.0
    set protocol udp
    set src-l4port 67-67
    set dst-l4port 68-68
    set action forward
    set forward-slot master
    set priority 5
    set comment "dhcpv4 server to client"
  next
  edit 8
    set status enable
    set vlan 0
    set ether-type ipv4
    set src-addr-ipv4 0.0.0.0 0.0.0.0
    set dst-addr-ipv4 0.0.0.0 0.0.0.0
    set protocol udp
    set src-l4port 68-68
    set dst-l4port 67-67
    set action forward
    set forward-slot master
    set priority 5
    set comment "dhcpv4 client to server"
  end
```

These flow rules handle traffic when the DHCP client sends requests to a DHCP server using port 68 and the DHCP server responds using port 67. However, if DHCP relay is involved, requests from the DHCP relay to the DHCP server and replies from the DHCP server to the DHCP relay both use port 67. If this DHCP relay traffic passes through the FortiGate-6000 or 7000 you must add a flow rule similar to the following to support port 67 DHCP traffic in both directions:

```
config load-balance flow-rule
```

```
edit 8
  set status enable
  set vlan 0
  set ether-type ipv4
  set src-addr-ipv4 0.0.0.0 0.0.0.0
  set dst-addr-ipv4 0.0.0.0 0.0.0.0
  set protocol udp
  set src-l4port 67-67
  set dst-l4port 67-67
  set action forward
  set forward-slot master
  set priority 5
  set comment "dhcpv4 relay"
next
```

Limitations of installing FortiGate-6000 firmware from the BIOS after a reboot

Installing or upgrading FortiGate-6000 firmware from the BIOS installs firmware on and resets the configuration of the management board only. The FPCs will continue to operate with their current configuration and firmware build. The FortiGate-6000 system does not synchronize firmware upgrades performed from the BIOS.

See [Installing FortiGate-6000 firmware from the BIOS after a reboot](#) for detailed procedures for upgrading FortiGate-6000 firmware from the BIOS.

Limitations of installing FortiGate-7000 firmware from the BIOS after a reboot

Installing or upgrading FortiGate-7000 firmware from the BIOS installs firmware on and resets the configuration of the primary FIM only. The other FIM and the FPMs will continue to operate with their current configuration and firmware build. The FortiGate-7000 system does not synchronize firmware upgrades performed from the BIOS.

See [Installing FIM firmware from the BIOS after a reboot](#) and [Installing FPM firmware from the BIOS after a reboot](#) for detailed procedures for upgrading FortiGate-6000 firmware from the BIOS.

Installing firmware on an individual FortiGate-6000 FPC

You may want to install firmware on an individual FPC to resolve a software-related problem with the FPC or if the FPC is not running the same firmware version as the management board. The following procedure describes how to transfer a new firmware image file to the FortiGate-6000 internal TFTP server and then install the firmware on an FPC.

1. Copy the firmware image file to a TFTP server, FTP server, or USB key.
2. To upload the firmware image file onto the FortiGate-6000 internal TFTP server, from the management board CLI, enter one of the following commands.

- To upload the firmware image file from an FTP server:

```
execute upload image ftp <image-file-and-path> <comment> <ftp-server-address>
<username> <password>
```

- To upload the firmware image file from a TFTP server:

```
execute upload image tftp <image-file> <comment> <tftp-server-address>
```

- To upload the firmware image file from a USB key:

```
execute upload image usb <image-file-and-path> <comment>
```

3. Enter the following command to install the firmware image file on to an FPC:

```
execute load-balance update image <slot-number>
```

where <slot-number> is the FPC slot number.

This command uploads the firmware image to the FPC and the FPC restarts. When the FPC starts up, the configuration is reset to factory default settings and then synchronized by the management board. The FPC restarts again, rejoins the cluster, and is ready to process traffic.

4. To verify that the configuration of the FPC has been synchronized, enter the `diagnose sys confsync status | grep in_sy` command. The command output below shows an example of the synchronization status of some of the FPCs in an HA cluster of two FortiGate-6301F devices. The field `in_sync=1` indicates that the configuration of the FPC is synchronized.

```
FPC6KFT018901327, Slave, uptime=615368.33, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=1
F6KF31T018900143, Master, uptime=615425.84, priority=1, slot_id=1:0, idx=0, flag=0x10, in_sync=1
FPC6KFT018901372, Slave, uptime=615319.63, priority=20, slot_id=1:2, idx=1, flag=0x4, in_sync=1
F6KF31T018900143, Master, uptime=615425.84, priority=1, slot_id=1:0, idx=0, flag=0x10, in_sync=1
FPC6KFT018901346, Slave, uptime=423.91, priority=21, slot_id=1:3, idx=1, flag=0x4, in_sync=1
```

FPCs that are missing or that show `in_sync=0` are not synchronized. To synchronize an FPC that is not synchronized, log into the CLI of the FPC and restart it using the `execute reboot` command. If this does not solve the problem, contact Fortinet Support at <https://support.fortinet.com>.

The example output also shows that the uptime of the FPC in slot 3 is lower than the uptime of the other FPCs, indicating that the FPC in slot 3 has recently restarted.

If you enter the `diagnose sys confsync status | grep in_sy` command before an FPC has completely restarted, it will not appear in the output. Also, the Configuration Sync Monitor will temporarily show that it is not synchronized.

Installing firmware on an individual FortiGate-7000 FPM

Use the following procedure to upgrade the firmware running on an individual FPM. To perform the upgrade, you must enter a command from the primary FIM CLI to allow ELBC communication with the FPM. Then you can just log in to the FPM GUI or CLI and perform the firmware upgrade.

During this procedure, the FPM will not be able to process traffic. However, the other FPMs and the FIMs should continue to operate normally.

After verifying that the FPM is running the right firmware, you must log back into the primary FIM CLI and return the FPM to normal operation.

1. Log in to the primary FIM CLI and enter the following command:

```
diagnose load-balance switch set-compatible <slot> enable elbc
```

Where <slot> is the number of the FortiGate-7000 slot containing the FPM to be upgraded.

2. Log in to the FPM GUI or CLI using its special port number (for example, for the FPM in slot 3, browse to <https://192.168.1.99:44303> to connect to the GUI) and perform a normal firmware upgrade of the FPM.
3. After the FPM restarts, verify that the new firmware has been installed.
You can do this from the FPM GUI dashboard or from the FPM CLI using the `get system status` command.
4. Verify that the configuration has been synchronized. The following command output shows the sync status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=1
```

FIMs and FPMs that are missing or that show `in_sync=0` are not synchronized. To synchronize an FIM or FPM that is not synchronized, log into the CLI of the FIM or FPM and restart it using the `execute reboot` command. If this does not solve the problem, contact Fortinet Support at <https://support.fortinet.com>.

The command output also shows that the uptime of the FPM in slot 4 is lower than the uptime of the other modules, indicating that the FPM in slot 4 has recently restarted.

If you enter the `diagnose sys confsync status | grep in_sy` command before the FIM has completely restarted, it will not appear in the command output. As well, the Configuration Sync Monitor will temporarily show that it is not synchronized.

5. Once the FPM is operating normally, log back in to the primary FIM CLI and enter the following command to reset the FPM to normal operation:

```
diagnose load-balance switch set-compatible <slot> disable
```

Configuration synchronization errors will occur if you do not reset the FPM to normal operation.

SD-WAN is not supported

FortiGate-6000 and FortiGate-7000 Version 6.2.3 does not support SD-WAN because of the following known issues:

- 510522, when a link in an SD-WAN goes down and comes up, duplicate default routes are created on the management board.
- 510818, traffic from internal hosts is forwarded to destination servers even if SD-WAN health-checking determines that the server is down.
- 510389, SD-WAN usage is not updated on the management board GUI.
- 494019, SD-WAN monitor statistics are not updated on the management board GUI.
- 511091, SD-WAN load balancing rules based on packet loss, jitter, or latency do not work correctly.

IPsec VPN features that are not supported

FortiOS 6.2.3 for FortiGate-6000 and FortiGate-7000 does not support the following IPsec VPN features:

- Policy-based IPsec VPN is not supported. Only tunnel or interface mode IPsec VPN is supported.
- Policy routes cannot be used for communication over IPsec VPN tunnels.
- VRF routes cannot be used for communication over IPsec VPN tunnels.
- Remote networks with 0- to 15-bit netmasks are not supported. Remote networks with 16- to 32-bit netmasks are supported.
- IPv6 clear-text traffic (IPv6 over IPv4 or IPv6 over IPv6) is not supported.
- The FortiGate-7000 does not support load-balancing IPsec VPN tunnels to multiple FPMs. The FortiGate-6000 does support load balancing IPsec VPN tunnels to multiple FPCs as long as only static routes are used over the IPsec VPN tunnel and the configuration doesn't send traffic between IPsec VPN tunnels.
- IPsec SA synchronization between HA peers is not supported. After an HA failover, IPsec VPN tunnels have to be re-initialized.

Quarantine to disk not supported

The FortiGate-6000 platform, including the FortiGate-6301F and the FortiGate-6501F, and the FortiGate-7000 platform does not support quarantining files to the internal hard disks. Instead you must set the quarantine function to quarantine files to FortiAnalyzer.

Local out traffic is not sent to IPsec VPN interfaces

On most FortiGate platforms, an administrator can test an IPsec tunnel by opening the FortiGate CLI and pinging a remote host on the network at the other end of the IPsec VPN tunnel. This is not currently supported by the FortiGate-6000 and 7000.

Special configuration required for SSL VPN

Using a FortiGate-6000 or 7000 as an SSL VPN server requires you to manually add an SSL VPN load balance flow rule to configure the FortiGate-6000 or 7000 to send all SSL VPN sessions to the primary (master) FPC (FortiGate-6000) or the primary (master) FPM (FortiGate-7000). To match with the SSL VPN server traffic, the rule should include a destination port that matches the destination port of the SSL VPN server. A basic rule to allow SSL VPN traffic could be:

```
config load-balance flow-rule
  edit 0
    set status enable
    set ether-type ipv4
    set protocol tcp
    set dst-l4port 443-443
    set forward-slot master
    set comment "ssl vpn server to primary worker"
  next
end
```

This flow rule matches all sessions sent to port 443 (the default SSL VPN server listening port) and sends these sessions to the primary FPC. This should match all of your SSL VPN traffic if you are using the default SSL VPN server listening

port (443). This flow rule also matches all other sessions using 443 as the destination port so all of this traffic is also sent to the primary FPC.

If you change the SSL VPN server listening port

If you have changed the SSL VPN server listening port to 10443, you can change the SSL VPN flow rule as follows. This example also sets the source interface to port12, which is the SSL VPN server interface, instead of adding the IP address of port12 to the configuration:

```
config load-balance flow-rule
  edit 26
    set status enable
    set ether-type ipv4
    set protocol tcp
    set src-interface port12
    set dst-l4port 10443-10443
    set forward-slot master
    set comment "ssl vpn server to primary worker"
  end
```

Adding the SSL VPN server IP address

You can add the IP address of the FortiGate-6000 or 7000 interface that receives SSL VPN traffic to the SSL VPN flow rule to make sure that the flow rule only matches the traffic of SSL VPN clients connecting to the SSL VPN server. For example, if the IP address of the interface is 172.25.176.32 and the SSL VPN flow rule ID is 26:

```
config load-balance flow-rule
  edit 26
    set status enable
    set ether-type ipv4
    set protocol tcp
    set dst-addr-ipv4 172.25.176.32 255.255.255.255
    set dst-l4port 10443-10443
    set forward-slot master
    set comment "ssl vpn server to primary worker"
  end
```

This flow rule will now only match SSL VPN sessions with 172.25.176.32 as the destination address and send all of these sessions to the primary FPC or FPM.

Example FortiGate-6000 HA heartbeat switch configurations

FortiGate-6000 for FortiOS 6.2.3 allows you use proprietary triple-tagging or double-tagging for HA heartbeat packets.

Example triple-tagging compatible switch configuration

The switch that you use for connecting HA heartbeat interfaces does not have to support IEEE 802.1ad (also known as Q-in-Q, double-tagging). But the switch should be able to forward the double-tagged frames. Some switches will strip

out the inner tag and Fortinet recommends avoiding these switches. FortiSwitch D and E series can correctly forward double-tagged frames.



This configuration is not required for FortiGate-6000 HA configurations if you have set up direct connections between the HA heartbeat interfaces.

This example shows how to configure a FortiGate-6000 to use different VLAN IDs for the HA1 and HA2 HA heartbeat interfaces and then how to configure two interfaces on a Cisco switch to allow HA heartbeat packets.



This example sets the native VLAN ID for both switch ports to 777. You can use any VLAN ID as the native VLAN ID as long as the native VLAN ID is not the same as the allowed VLAN ID.

1. On both FortiGate-6000s, enter the following command to use different VLAN IDs for the HA1 and HA2 interfaces. The command sets the ha1 VLAN ID to 4091 and the ha2 VLAN ID to 4092:

```
config system ha
    set ha-port-dtag-mode proprietary
    set hbdev ha1 50 ha2 100
    set hbdev-vlan-id 4091
    set hbdev-second-vlan-id 4092
end
```

2. Use the `get system ha` or `get system ha status` command to confirm the VLAN IDs.

```
get system ha status
...
HBDEV stats:
F6KF51T018900026(updated 4 seconds ago):
    ha1: physical/10000full, up, rx-bytes/packets/dropped/errors=54995955/230020/0/0,
tx=63988049/225267/0/0, vlan-id=4091
    ha2: physical/10000full, up, rx-bytes/packets/dropped/errors=54995955/230020/0/0,
tx=63988021/225267/0/0, vlan-id=4092
F6KF51T018900022(updated 3 seconds ago):
    ha1: physical/10000full, up, rx-bytes/packets/dropped/errors=61237440/230023/0/0,
tx=57746989/225271/0/0, vlan-id=4091
    ha2: physical/10000full, up, rx-bytes/packets/dropped/errors=61238907/230023/0/0,
tx=57746989/225271/0/0, vlan-id=4092
...
```

3. Configure the Cisco switch interface that connects the HA1 interfaces to allow packets with a VLAN ID of 4091:

```
interface <name>
switchport mode trunk
switchport trunk native vlan 777
switchport trunk allowed vlan 4091
```

4. Configure the Cisco switch port that connects the HA2 interfaces to allow packets with a VLAN ID of 4092:

```
interface <name>
switchport mode trunk
switchport trunk native vlan 777
switchport trunk allowed vlan 4092
```

Example double-tagging compatible switch configuration

The following switch configuration is compatible with FortiGate-6000 HA heartbeat double tagging and with the default TPID of 0x8100.

The FortiGate-6000 HA heartbeat configuration is.

```
config system ha
    set ha-port-dtag-mode double-tagging
    set hbdev ha1 50 ha2 50
    set hbdev-vlan-id 4091
    set hbdev-second-vlan-id 4092
end
```

Example third-party switch configuration:

Switch interfaces 37 and 38 connect to the HA1 interfaces of both FortiGate-6000s.

```
interface Ethernet37
description **** FGT-6000F HA1 HA HB ****
speed forced 10000full
switchport access vlan 660
switchport trunk native vlan 4091
switchport mode dot1q-tunnel
!
interface Ethernet38
description **** FGT-6000F HA1 HA HB ****
speed forced 10000full
switchport access vlan 660
switchport trunk native vlan 4091
switchport mode dot1q-tunnel
!
```

Switch interfaces 39 and 40 connect to the HA2 interfaces of both FortiGate-6000s.

```
interface Ethernet39
description **** FGT-6000F HA2 HA HB ****
mtu 9214
speed forced 10000full
no error-correction encoding
switchport access vlan 770
switchport trunk native vlan 4092
switchport mode dot1q-tunnel
!
interface Ethernet42
description **** FGT-6000F HA2 HA HB ****
mtu 9214
speed forced 10000full
no error-correction encoding
switchport access vlan 770
switchport trunk native vlan 4092
switchport mode dot1q-tunnel
!
```


Example FortiGate-7000 HA heartbeat switch configuration

FortiGate-7000 for FortiOS 6.2.3 allows you use proprietary triple-tagging or double-tagging for HA heartbeat packets.

Example triple-tagging compatible switch configuration

The switch that you use for connecting HA heartbeat interfaces does not have to support IEEE 802.1ad (also known as Q-in-Q, double-tagging), but the switch should be able to forward the double-tagged frames. Fortinet recommends avoiding switches that strip out the inner tag. FortiSwitch D and E series can correctly forward double-tagged frames.



This configuration is not required for FortiGate-7030E HA configurations if you have set up direct connections between the HA heartbeat interfaces.

This example shows how to configure a FortiGate-7000 to use different VLAN IDs for the M1 and M2 HA heartbeat interfaces and then how to configure two ports on a Cisco switch to allow HA heartbeat packets.



This example sets the native VLAN ID for both switch ports to 777. You can use any VLAN ID as the native VLAN ID as long as the native VLAN ID is not the same as the allowed VLAN ID.

1. On both FortiGate-7000s in the HA configuration, enter the following command to use different VLAN IDs for the M1 and M2 interfaces. The command sets the M1 VLAN ID to 4086 and the M2 VLAN ID to 4087:

```
config system ha
    set ha-port-dtag-mode proprietary
    set hbdev "1-M1" 50 "2-M1" 50 "1-M2" 50 "2-M2" 50
    set hbdev-vlan-id 4086
    set hbdev-second-vlan-id 4087
end
```

2. Use the `get system ha` or `get system ha status` command to confirm the VLAN IDs.

```
get system ha status
...
HBDEV stats:
FG74E83E16000015(updated 1 seconds ago):
    1-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=579602089/2290683/0/0,
tx=215982465/761929/0/0, vlan-id=4086
    2-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=577890866/2285570/0/0,
tx=215966839/761871/0/0, vlan-id=4086
    1-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=579601846/2290682/0/0,
tx=215982465/761929/0/0, vlan-id=4087
    2-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=577890651/2285569/0/0,
tx=215966811/761871/0/0, vlan-id=4087
FG74E83E16000016(updated 1 seconds ago):
    1-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=598602425/2290687/0/0,
tx=196974887/761899/0/0, vlan-id=4086
    2-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=596895956/2285588/0/0,
tx=196965052/761864/0/0, vlan-id=4086
    1-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=598602154/2290686/0/0,
```

```
tx=196974915/761899/0/0, vlan-id=4087
  2-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=596895685/2285587/0/0,
tx=196965080/761864/0/0, vlan-id=4087
...
```

3. Configure the Cisco switch port that connects the M1 interfaces to allow packets with a VLAN ID of 4086:

```
interface <name>
switchport mode trunk
switchport trunk native vlan 777
switchport trunk allowed vlan 4086
```

4. Configure the Cisco switch port that connects the M2 interfaces to allow packets with a VLAN ID of 4087:

```
interface <name>
switchport mode trunk
switchport trunk native vlan 777
switchport trunk allowed vlan 4087
```

Example double-tagging compatible switch configuration

The following switch configuration is compatible with FortiGate-7040E HA heartbeat double tagging and with the default TPID of 0x8100.

The FortiGate-7040E HA heartbeat configuration is.

```
config system ha
  set ha-port-dtag-mode double-tagging
  set hbdev "1-M1" 50 "2-M1" 50 "1-M2" 50 "2-M2" 50
  set hbdev-vlan-id 4086
  set hbdev-second-vlan-id 4087
end
```

Example third-party switch configuration:

Switch interfaces 37 to 40 connect to the M1 interfaces of the FIMs in both FortiGate-7040E chassis.

```
interface Ethernet37
description **** FGT-7000E M1 HA HB ****
speed forced 10000full
switchport access vlan 660
switchport trunk native vlan 4086
switchport mode dot1q-tunnel
!
interface Ethernet38
description **** FGT-7000E M1 HA HB ****
speed forced 10000full
switchport access vlan 660
switchport trunk native vlan 4086
switchport mode dot1q-tunnel
!
interface Ethernet39
description **** FGT-7000E M1 HA HB ****
speed forced 10000full
switchport access vlan 660
switchport trunk native vlan 4086
switchport mode dot1q-tunnel
!
interface Ethernet40
```

```
description **** FGT-7000E M1 HA HB ****
speed forced 10000full
switchport access vlan 660
switchport trunk native vlan 4086
switchport mode dot1q-tunnel
!
```

Switch interfaces 41 to 44 connect to the M2 interfaces of the FIMs in both FortiGate-7040E chassis.

```
interface Ethernet41
description **** FGT-7000E M2 HA HB ****
mtu 9214
speed forced 10000full
no error-correction encoding
switchport access vlan 770
switchport trunk native vlan 4087
switchport mode dot1q-tunnel
!
interface Ethernet42
description **** FGT-7000E M2 HA HB ****
mtu 9214
speed forced 10000full
no error-correction encoding
switchport access vlan 770
switchport trunk native vlan 4087
switchport mode dot1q-tunnel
!
interface Ethernet43
description **** FGT-7000E M2 HA HB ****
mtu 9214
speed forced 10000full
no error-correction encoding
switchport access vlan 770
switchport trunk native vlan 4087
switchport mode dot1q-tunnel
!
interface Ethernet44
description **** FGT-7000E M2 HA HB ****
mtu 9214
speed forced 10000full
no error-correction encoding
switchport access vlan 770
switchport trunk native vlan 4087
switchport mode dot1q-tunnel
```

Default FortiGate-6000 and 7000 configuration for traffic that cannot be load balanced

The default `configure load-balance flow-rule` command contains the recommended default flow rules that control how the FortiGate-6000 or 7000 handles traffic types that cannot be load balanced. Most of the flow rules in the

default configuration are enabled and are intended to send common traffic types that cannot be load balanced to the primary FPC or FPM. FortiGate-6000 and 7000 for FortiOS 6.2.3 have the same default flow rules.

All of the default flow rules identify the traffic type using the options available in the command and direct matching traffic to the primary (or master) FPC or FPM (`action` set to `forward` and `forward-slot` set to `master`). The default flow rules also include a comment that identifies the traffic type.

The default configuration also includes disabled flow rules for Kerberos and PPTP traffic. Normally, you would only need to enable these flow rules if you know that your FortiGate will be handling these types of traffic.

The CLI syntax below was created with the `show full configuration` command.

```
config load-balance flow-rule
  edit 1
    set status disable
    set vlan 0
    set ether-type ip
    set protocol udp
    set src-l4port 88-88
    set dst-l4port 0-0
    set action forward
    set forward-slot master
    set priority 5
    set comment "kerberos src"
  next
  edit 2
    set status disable
    set vlan 0
    set ether-type ip
    set protocol udp
    set src-l4port 0-0
    set dst-l4port 88-88
    set action forward
    set forward-slot master
    set priority 5
    set comment "kerberos dst"
  next
  edit 3
    set status enable
    set vlan 0
    set ether-type ip
    set protocol tcp
    set src-l4port 179-179
    set dst-l4port 0-0
    set tcp-flag any
    set action forward
    set forward-slot master
    set priority 5
    set comment "bgp src"
  next
  edit 4
    set status enable
    set vlan 0
    set ether-type ip
    set protocol tcp
    set src-l4port 0-0
    set dst-l4port 179-179
```

```
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp dst"
    next
    edit 5
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 520-520
        set dst-l4port 520-520
        set action forward
        set forward-slot master
        set priority 5
        set comment "rip"
    next
    edit 6
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 521-521
        set dst-l4port 521-521
        set action forward
        set forward-slot master
        set priority 5
        set comment "ripng"
    next
    edit 7
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 67-67
        set dst-l4port 68-68
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 server to client"
    next
    edit 8
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 68-68
        set dst-l4port 67-67
        set action forward
```

```
        set forward-slot master
        set priority 5
        set comment "dhcpv4 client to server"
next
edit 9
    set status disable
    set vlan 0
    set ether-type ip
    set protocol tcp
    set src-l4port 1723-1723
    set dst-l4port 0-0
    set tcp-flag any
    set action forward
    set forward-slot master
    set priority 5
    set comment "pptp src"
next
edit 10
    set status disable
    set vlan 0
    set ether-type ip
    set protocol tcp
    set src-l4port 0-0
    set dst-l4port 1723-1723
    set tcp-flag any
    set action forward
    set forward-slot master
    set priority 5
    set comment "pptp dst"
next
edit 11
    set status enable
    set vlan 0
    set ether-type ip
    set protocol udp
    set src-l4port 0-0
    set dst-l4port 3784-3784
    set action forward
    set forward-slot master
    set priority 5
    set comment "bfd control"
next
edit 12
    set status enable
    set vlan 0
    set ether-type ip
    set protocol udp
    set src-l4port 0-0
    set dst-l4port 3785-3785
    set action forward
    set forward-slot master
    set priority 5
    set comment "bfd echo"
next
edit 13
    set status enable
```

```
set vlan 0
set ether-type ipv6
set src-addr-ipv6 ::/0
set dst-addr-ipv6 ::/0
set protocol udp
set src-l4port 547-547
set dst-l4port 546-546
set action forward
set forward-slot master
set priority 5
set comment "dhcpv6 server to client"
next
edit 14
set status enable
set vlan 0
set ether-type ipv6
set src-addr-ipv6 ::/0
set dst-addr-ipv6 ::/0
set protocol udp
set src-l4port 546-546
set dst-l4port 547-547
set action forward
set forward-slot master
set priority 5
set comment "dhcpv6 client to server"
next
edit 15
set status enable
set vlan 0
set ether-type ipv4
set src-addr-ipv4 0.0.0.0 0.0.0.0
set dst-addr-ipv4 224.0.0.0 240.0.0.0
set protocol any
set action forward
set forward-slot master
set priority 5
set comment "ipv4 multicast"
next
edit 16
set status enable
set vlan 0
set ether-type ipv6
set src-addr-ipv6 ::/0
set dst-addr-ipv6 ff00::/8
set protocol any
set action forward
set forward-slot master
set priority 5
set comment "ipv6 multicast"
next
edit 17
set status disable
set vlan 0
set ether-type ipv4
set src-addr-ipv4 0.0.0.0 0.0.0.0
set dst-addr-ipv4 0.0.0.0 0.0.0.0
```

```
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 2123-2123
        set action forward
        set forward-slot master
        set priority 5
        set comment "gtp-c to master blade"
    next
    edit 18
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1000-1000
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "authd http to master blade"
    next
    edit 19
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1003-1003
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "authd https to master blade"
    next
    edit 20
        set status enable
        set vlan 0
        set ether-type ip
        set protocol vrrp
        set action forward
        set forward-slot all
        set priority 6
        set comment "vrrp to all blades"
    next
end
```


Managing individual FortiGate-6000 management boards and FPCs

You can manage individual FPCs using special management port numbers, FPC consoles, or the `execute load-balance slot manage` command. You can also use the `execute ha manage` command to log in to the other FortiGate-6000 in an HA configuration.

Special management port numbers

You may want to connect to individual FPCs to view status information or perform a maintenance task, such as installing firmware or performing a restart. You can connect to the GUI or CLI of individual FPCs (or the management board) using the MGMT1 interface IP address with a special port number.



You can use the `config load-balance setting slbc-mgmt-intf` command to change the management interface used. The default is `mgmt1` and it can be changed to `mgmt2`, or `mgmt3`.

To enable using the special management port numbers to connect to individual FPCs, set `slbc-mgmt-intf` to an interface that is connected to a network, has a valid IP address, and has management or administrative access enabled. To block access to the special management port numbers you can set `slbc-mgmt-intf` to an interface that is not connected to a network, does not have a valid IP address, or has management or administrative access disabled.

For example, if the MGMT1 interface IP address is 192.168.1.99 you can connect to the GUI of the first FPC (the FPC in slot 1) by browsing to :

```
https://192.168.1.99:44301
```

The special port number (in this case, 44301) is a combination of the service port (for HTTPS, the service port is 443) and the FPC slot number (in this example, 01).

You can view the special HTTPS management port number for and log in to the GUI of an FPC from the Configuration Sync Monitor.

The following table lists the special ports you can use to connect to individual FPCs or the management board using common management protocols. The FortiGate-6300F and 6301F have 7 slots (0 to 6) and the FortiGate-6500F and 6501F have 11 slots (0 to 10). Slot 0 is the management board (MBD) slot. Slots 1 to 10 are FPC slots.



You can't change the special management port numbers. Changing configurable management port numbers, for example the HTTPS management port number (which you might change to support SSL VPN), does not affect the special management port numbers.

FortiGate-6000 special management port numbers

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 0, (MBD)	8000	44300	2300	2200	16100
Slot 1 (FPC01)	8001	44301	2301	2201	16101
Slot 2 (FPC02)	8002	44302	2302	2202	16102
Slot 3 (FPC03)	8003	44303	2303	2203	16103
Slot 4 (FPC04)	8004	44304	2304	2204	16104
Slot 5 (FPC05)	8005	44305	2305	2205	16105
Slot 6 (FPC06)	8006	44306	2306	2206	16106
Slot 7 (FPC07)	8007	44307	2307	2207	16107
Slot 8 (FPC08)	8008	44308	2308	2208	16108
Slot 9 (FPC09)	8009	44309	2309	2209	16109
Slot 10 (FPC10)	8010	44310	2310	2210	16110

For example, to connect to the CLI of the FPC in slot 3 using SSH, you would connect to `ssh://192.168.1.99:2203`.

To verify which slot you have logged into, the GUI header banner and the CLI prompt shows the current hostname. The CLI prompt also shows slot address in the format `<hostname> [<slot address>] #`.

Logging in to different FPCs allows you to use the FortiView or Monitor GUI pages to view the activity on that FPC. You can also restart the FPC from its GUI or CLI. Even though you can log in to different FPCs, you can only make configuration changes from the management board.

HA mode special management port numbers

In an HA configuration consisting of two FortiGate-6000s in an HA cluster, you can connect to individual FPCs or to the management board in chassis 1 (chassis ID = 1) using the same special port numbers as for a standalone FortiGate-6000.

You use different special port numbers to connect to individual FPCs or the management board in the FortiGate-6000 with chassis ID 2 (chassis ID = 2).

FortiGate-6000 special management port numbers (chassis ID = 2)

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 0, (MBD)	8020	44320	2320	2220	16120
Slot 1 (FPC01)	8021	44321	2321	2221	16121
Slot 2 (FPC02)	8022	44322	2322	2222	16122

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 3 (FPC03)	8023	44323	2323	2223	16123
Slot 4 (FPC04)	8024	44324	2324	2224	16124
Slot 5 (FPC05)	8025	44325	2325	2225	16125
Slot 6 (FPC06)	8026	44326	2326	2226	16126
Slot 7 (FPC07)	8027	44327	2327	2227	16127
Slot 8 (FPC08)	8028	44328	2328	2228	16128
Slot 9 (FPC09)	8029	44329	2329	2229	16129
Slot 10 (FPC10)	8030	44330	2330	2230	16130

Connecting to individual FPC consoles

From the management board CLI, you can use the `execute system console-server` command to access individual FPC consoles. Console access can be useful for troubleshooting. For example, if an FPC does not boot properly, you can use console access to view the state of the FPC and enter commands to fix the problem or restart the FPC.

From the console, you can also perform BIOS-related operations, such as rebooting the FPC, interrupting the boot process, and installing new firmware.

For example, from the management board CLI, use the following command to log in to the console of the FPC in slot 3:

```
execute system console-server connect 3
```

Authenticate to log in to the console and use CLI commands to view information, make changes, or restart the FPC. When you are done, use **Ctrl-X** to exit from the console back to the management board CLI. Using **Ctrl-X** may not work if you are accessing the CLI console from the GUI. Instead you may need to log out of the GUI and then log in again.

Also, from the management board CLI you can use the `execute system console-server showline` command to list any active console server sessions. Only one console session can be active for each FPC, so before you connect to an FPC console, you can use the following command to verify whether or not there is an active console session. The following command output shows an active console session with the FPC in slot 4:

```
execute system console-server showline
MB console line connected - 1
Telnet-to-console line connected - 4
```

To clear an active console session, use the `execute system console-server clearline` command. For example, to clear an active console session with the FPC in slot 4, enter:

```
execute system console-server clearline 4
```



In an HA configuration, the `execute system console-server` commands only allow access to FPCs in the FortiGate-6000 that you are logged into. You can't use this command to access FPCs in the other FortiGate-6000 in an HA cluster

Connecting to individual FPC CLIs

From the management board CLI you can use the following command to log into the CLI of individual FPCs:

```
execute load-balance slot manage <slot-number>
```

Where:

<slot> is the slot number of the component that you want to log in to. The management board is in slot 0 and the FPC slot numbers start at 1.

When connected to the CLI of a FPC, you can view information about the status or configuration of the FPC, restart the FPC, or perform other operations. You should not change the configuration of individual FPCs because this can cause configuration synchronization errors.

Performing other operations on individual FPCs

You can use the following commands to restart, power off, power on, or perform an NMI reset on individual FPCs while logged into the management board CLI:

```
execute load-balance slot {nmi-reset | power-off | power on | reboot} <slots>
```

Where <slots> can be one or more slot numbers or slot number ranges separated by commas. Do not include spaces.

For example, to shut down the FPCs in slots 2, and 4 to 6 enter:

```
execute load-balance slot power-off 2,4-6
```

Managing individual FortiGate-7000 FIMs and FPMs

You can manage individual FIMs and FPMs using special port numbers or the `execute load-balance slot manage` command. You can also use the `execute ha manage` command to log in to the other FortiGate-7000 in an HA configuration.

Special management port numbers

In some cases you may want to connect to individual FIMs or FPMs to view status information or perform a maintenance task such as installing firmware or performing a restart. You can connect to the GUI or CLI of individual FIMs or FPMs in a FortiGate-7000 using the mgmt interface IP address with a special port number.



To enable using the special management port numbers to connect to individual FIMs and FPMs, the mgmt interface must be connected to a network, have a valid IP address, and have management or administrative access enabled. To block access to the special management port numbers, disconnect the mgmt interface from a network, configure the mgmt interface with an invalid IP address, or disable management or administrative access for the mgmt interface.

For example, if the mgmt interface IP address is 192.168.1.99, you can connect to the GUI of the FPM in slot 3 using the mgmt interface IP address followed by the special port number, for example:

```
https://192.168.1.99:44303
```

The special port number (in this case 44303) is a combination of the service port (for HTTPS, the service port is 443) and the slot number (in this example, 03).

You can view the special HTTPS management port number for and log in to the GUI of an FIM or FPM from the Configuration Sync Monitor.

The following table lists the special port numbers to use to connect to each FortiGate-7000 slot using common management protocols.



You can't change the special management port numbers. Changing configurable management port numbers, for example the HTTPS management port (which you might change to support SSL VPN), does not affect the special management port numbers.

FortiGate-7000 special management port numbers

Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
5	FPM05	8005	44305	2305	2205	16105

Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
3	FPM03	8003	44303	2303	2203	16103
1	FIM01	8001	44301	2301	2201	16101
2	FIM02	8002	44302	2302	2202	16102
4	FPM04	8004	44304	2304	2204	16104
6	FPM06	8006	44306	2306	2206	16106

For example, to connect to the GUI of the FIM in slot 2 using HTTPS you would browse to <https://192.168.1.99:44302>.

To verify which module you have logged into, the GUI header banner and the CLI prompt shows its hostname. The CLI prompt also shows slot address in the format `<hostname> [<slot address>] #`.

Logging in to different modules allows you to use FortiView or Monitor GUI pages to view the activity of that module. Even though you can log in to different modules, you can only make configuration changes from the primary FIM; which is usually the FIM in slot 1.

HA mode special management port numbers

In HA mode, you use the same special port numbers to connect to FIMs and FPMs in chassis 1 (chassis ID = 1) and different special port numbers to connect to FIMs and FPMs in chassis 2 (chassis ID = 2):

FortiGate-7000 HA special management port numbers

Chassis and Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Ch1 slot 5	FPM05	8005	44305	2305	2205	16105
Ch1 slot 3	FPM03	8005	44303	2303	2203	16103
Ch1 slot 1	FIM01	8003	44301	2301	2201	16101
Ch1 slot 2	FIM02	8002	44302	2302	2202	16102
Ch1 slot 4	FPM04	8004	44304	2304	2204	16104
Ch1 slot 6	FPM06	8006	44306	2306	2206	16106
Ch2 slot 5	FPM05	8005	44325	2325	2225	16125
Ch2 slot 3	FPM03	8005	44323	2323	2223	16123
Ch2 slot 1	FIM01	8003	44321	2321	2221	16121
Ch2 slot 2	FIM02	8002	44322	2322	2222	16122
Ch2 slot 4	FPM04	8004	44324	2324	2224	16124
Ch2 slot 6	FPM06	8006	44326	2326	2226	16126

Managing individual FIMs and FPMs from the CLI

From any CLI, you can use the `execute load-balance slot manage <slot>` command to log into the CLI of different FIMs and FPMs. You can use this command to view the status or configuration of the module, restart the module, or perform other operations. You should not change the configuration of individual FIMs or FPMs because this can cause configuration synchronization errors.

`<slot>` is the slot number of the slot that you want to log in to.

After you log in to a different module in this way, you can't use the `execute load-balance slot manage` command to log in to another module. Instead you must use the `exit` command to revert back to the CLI of the component that you originally logged in to. Then you can use the `execute load-balance slot manage` command to log into another module.

Connecting to individual FIM and FPM CLIs of the secondary FortiGate-7000 in an HA configuration

From the primary FIM of the primary FortiGate-7000 in an HA configuration, you can use the following command to log in to the primary FIM of the secondary FortiGate-7000:

```
execute ha manage <id>
```

Where `<id>` is the ID of the other FortiGate-7000 in the cluster. From the primary FortiGate-7000, use an ID of 0 to log into the secondary FortiGate-7000. From the secondary FortiGate-7000, use an ID of 1 to log into the primary FortiGate-7000. You can enter the `?` to see the list of IDs that you can connect to.

After you have logged in, you can manage the secondary FortiGate-7000 from the primary FIM or you can use the `execute-load-balance slot manage` command to connect to the CLIs of the other FIM and the FPMs in the secondary FortiGate-7000.

Upgrade information

Use the graceful upgrade information or other firmware upgrade information in these release notes to upgrade your FortiGate-6000 or 7000 system to the latest firmware version with only minimal traffic disruption and to maintain your configuration.

You can also refer to the Upgrade Path Tool (<https://docs.fortinet.com/upgrade-tool>) in the Fortinet documentation library to find supported upgrade paths for all FortiGate models and firmware versions.

A similar upgrade path tool is also available from Fortinet Support: <https://support.fortinet.com>.

In some cases, these upgrade path tools may recommend slightly different upgrade paths. If that occurs, the paths provided by both tools are supported and you can use either one.

See also, [Upgrade information](#) in the [FortiOS 6.2.3 release notes](#).

HA graceful upgrade to FortiOS 6.2.3

Use the following steps to upgrade a FortiGate-6000 or 7000 HA cluster with `uninterruptible-upgrade` enabled from FortiOS 6.0.8, 6.0.9, or 6.0.10 to FortiOS 6.2.3.

Enabling `uninterruptible-upgrade` allows you to upgrade the firmware of an operating FortiGate-6000 or 7000 HA configuration with only minimal traffic interruption. During the upgrade, the secondary FortiGate upgrades first. Then a failover occurs and the newly upgraded FortiGate becomes the primary FortiGate and the firmware of the new secondary FortiGate upgrades.

To perform a graceful upgrade of your FortiGate-6000 or 7000 from FortiOS 6.0.8, 6.0.9, or 6.0.10 to FortiOS 6.2.3:

1. Use the following command to enable `uninterruptible-upgrade` to support HA graceful upgrade:

```
config system ha
    set uninterruptible-upgrade enable
end
```
2. Download FortiOS 6.2.3 firmware for FortiGate-6000 or 7000 from the <https://support.fortinet.com> FortiOS 6.2.3 firmware image folder.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. Verify that you have installed the correct firmware version. For example, for the FortiGate-7040E:

```
get system status
Version: FortiGate-7040E v6.2.3,build6252,200221 (GA)
...
```

About FortiGate-6000 firmware upgrades

The management board and the FPCs in your FortiGate-6000 system run the same firmware image. You upgrade the firmware from the management board GUI or CLI just as you would any FortiGate product.

You can perform a graceful firmware upgrade of a FortiGate-6000 FGCP HA cluster by enabling `uninterruptible-upgrade` and `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption. For more information about graceful HA upgrades, see [HA cluster firmware upgrades](#).

Upgrading the firmware of a standalone FortiGate-6000, or FortiGate-6000 HA cluster with `uninterruptable-upgrade` disabled interrupts traffic because the firmware running on the management board and all of the FPCs upgrades in one step. These firmware upgrades should be done during a quiet time because traffic will be interrupted during the upgrade process.

A firmware upgrade takes a few minutes, depending on the number of FPCs in your FortiGate-6000 system. Some firmware upgrades may take longer depending on factors such as the size of the configuration and whether an upgrade of the DP3 processor is included.

Before beginning a firmware upgrade, Fortinet recommends that you perform the following tasks:

- Review the latest release notes for the firmware version that you are upgrading to.
- Verify the recommended upgrade path, as documented in the release notes.
- Back up your FortiGate-6000 configuration.



Fortinet recommends that you review the services provided by your FortiGate-6000 before a firmware upgrade and then again after the upgrade to make sure that these services continue to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

About FortiGate-7000 firmware upgrades

All of the FIMs and FPMs in your FortiGate-7000 system run the same firmware image. You upgrade the firmware from the primary FIM GUI or CLI just as you would any FortiGate product.

You can perform a graceful firmware upgrade of a FortiGate-7000 FGCP HA cluster by enabling `uninterruptible-upgrade` and `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption. For more information about graceful HA upgrades, see [HA cluster firmware upgrades](#).

Upgrading the firmware of a standalone FortiGate-7000, or FortiGate-7000 HA cluster with `uninterruptable-upgrade` disabled interrupts traffic because the firmware running on the FIMs and FPMs upgrades in one step. These firmware upgrades should be done during a quiet time because traffic will be interrupted during the upgrade process.

A firmware upgrade takes a few minutes, depending on the number of FIMs and FPMs in your FortiGate-7000 system. Some firmware upgrades may take longer depending on factors such as the size of the configuration and whether an upgrade of the DP2 processor is included.

Before beginning a firmware upgrade, Fortinet recommends that you perform the following tasks:

- Review the latest release notes for the firmware version that you are upgrading to.
- Verify the recommended upgrade path as documented in the release notes.
- Back up your FortiGate-7000 configuration.



Fortinet recommends that you review the services provided by your FortiGate-7000 before a firmware upgrade and then again after the upgrade to make sure the services continues to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade, and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

Product integration and support

This section describes FortiGate-6000 and 7000 for FortiOS 6.2.3 Build 6252 product integration and support information. The [Product integration and support](#) information described in the [FortiOS 6.2.3 release notes](#) also applies to FortiGate-6000 and 7000 FortiOS 6.2.3 Build 6252.

FortiGate-6000 and 7000 require the following or newer versions of FortiManager and FortiAnalyzer:

- FortiGate-6000: FortiManager or FortiAnalyzer 6.2.4 or 6.4.0.
- FortiGate-7000: FortiManager or FortiAnalyzer 6.2.4 or 6.4.0.

FortiGate-6000 6.2.3 special features and limitations

FortiGate-6000 for FortiOS 6.2.3 has specific behaviors that may differ from FortiOS features. For more information, see the [Special features and limitations for FortiGate-6000 v6.2.3](#) section of the FortiGate-6000 handbook.

FortiGate-7000 6.2.3 special features and limitations

FortiGate-7000 for FortiOS 6.2.3 has specific behaviors that may differ from FortiOS features. For more information, see the [Special features and limitations for FortiGate-7000 v6.2.3](#) section of the FortiGate-7000 handbook.

Maximum values

Maximum values for FortiGate-6000 and FortiGate-7000 for FortiOS 6.2.3 are available from the FortiOS Maximum Values Table (<https://docs.fortinet.com/max-value-table>).

Resolved issues

The following issues have been fixed in FortiGate-6000 and FortiGate-7000 FortiOS 6.2.3 Build 6252. For inquiries about a particular bug, please contact [Customer Service & Support](#). The [Resolved issues](#) described in the [FortiOS 6.2.3 release notes](#) also applies to FortiGate-6000 and 7000 FortiOS 6.2.3 Build 6252.

Bug ID	Description
459424	Accurate resource usage information now appears on the Edit Virtual Domain Settings GUI page.
496437 562712	Resolved multiple issues with management traffic and VDOM link interfaces.
522667 596641	Resolved an issue that prevented MAC addresses from being synchronized to all components in a FortiGate-6000 or 7000 operating in transparent mode.
554882	Resolved a synchronization issue that prevented a FortiManager from recognizing when a new FortiGate-6000 or 7000 joined an HA cluster.
564049	When an FPC or FPM fails, management sessions from the FPC to the management board or from the FPM to the primary FIM are now removed from the management board or primary FPC session table.
567546	Resolved an error with how the DP processor handles fragmented packets.
571328	Dates and times shown in the firewall policy list Last Used column are now accurate.
571808	The SSL VPN web portal history section now shows the history messages.
572012	Resolved an issue that could prevent firmware images installed on the FortiGate-6000 management board from the BIOS after a reboot from being synchronized to the FPCs.
572022	The <code>diagnose rsso query ip</code> command now displays the correct information when the command is run from the FortiGate-6000 management board CLI.
572838	In an HA configuration, backup routes (proto=20) are now successfully installed on the management boards of both FortiGate-6000s, when the primary FPC fails over to another slot.
573191	The FortiGate-7000 <code>get system ha status</code> command output now includes serial numbers of the FIMs in both chassis.
574190	Changing the global IPS configuration using the <code>config ips global</code> command no longer requires restarting the system for the change to take effect.
574357	Resolved an issue that sometimes prevented two factor authentication from working.
577563	To speed up synchronization when a FortiGate-6000 starts, the management board uploads a copy of its configuration file to the internal TFTP server and as each FPC starts up it downloads that configuration file. This can improve startup times, especially if the configuration is very large. When the system is operating, normal configuration synchronization keeps the FPCs synchronized with the management board.
578555	RADIUS authentication is now applied to administrator sessions by master FPC instead of the management board.

Bug ID	Description
579400	Resolved an issue that caused the authd process to use excessive amounts of CPU time.
580690	Resolved an issue that caused port address translation (PAT) to occur when a one-to-one IP pool is added to a firewall policy.
581627	You can no longer configure management interfaces to be FortiLink interfaces.
583124	Resolved an issue that caused the FortiGate-6000 or 7000 to send incorrect data usage information to RADIUS to Accounting Servers and to only send it from the management board or primary FIM. The FPC or FPM that originally authenticated the RADIUS session now periodically collects accounting data from all FPCs or FPMs and sends the aggregated data to the RADIUS server.
583190	The crashlog will now include system reboot messages.
587041	Active RSO sessions are now synchronized to an FPC after it restarts.
587124	The diagnose firewall auth command now provides more accurate and readable results when run from the management board or primary FIM.
587218	RADIUS accounting STOP message now successfully removes users from the RADIUS user lists on all FPCs or FPMs.
587432	The malicious certificate DB version is now synchronized to all FPCs or FIMs and FPMs.
587987	Resolved a high memory usage problem.
588655	TACACS+ logins are correctly logged out when the idle period is reached.
588925	The FortiGuard GUI page no longer repeats license information multiple times.
588963	The Security Rating feature now correctly appears on the GUI.
588980	The DP processor now handles UDP sessions with destination port 4500 correctly.
589515	Incorrect bandwidth statistics in VLAN interfaces.
589590	Authenticated users can now be de-authenticated if the FPC or FPM that originally authenticated the user has shut down.
590020	Resolved an issue that caused the hasync process to use excessive amounts of memory on the primary FPC or FPM.
590047	Resolved an issue that caused the FortiGate-6000 management board GUI to incorrectly show the status of a PPPoE interface as failed.
590237	The hataik process no longer incorrectly reports a role change before a cluster has formed.
590588	The <code>get system session6 list</code> command, run for a VDOM from the management board CLI, now displays information from all FPCs or FPMs.
591241	Traffic shaping can now be configured from the GUI.
593255	The FortiGate-6000 and 7000 now notifies FortiManager of a static routing change.
593360	The <code>config system ips global set engine-count</code> command now knows the correct number of available CPU cores depending on the FortiGate-7000 FIM or FPM.

Bug ID	Description
593509	Resolved an issue that caused the <code>confsyncd</code> process to use excessive amounts of memory.
593765	Resolved an issue that caused Security Fabric automation to send extra emails.
593989	Resolved an issue that could prevent upgrading the firmware of a single FortiGate-6000 or 7000 operating in HA mode with uninterruptible upgrade enabled.
594442	Resolved an issue that prevented IPv6 ping from working between two VDOMs when they are connected over a npu vdom link.
595193	Health checking of IPv6 real servers now works as expected.
596013	Resolved an issue that caused FortiGate-7000 management traffic to fail when the FIM in slot 1 is shut down and the FIM in slot 2 becomes the primary FIM.
597216	Resolved an issue that prevented the FortiGate-6000 or 7000 from downloading firmware upgrades from a TFTP server.
599999	The trusted host feature now works as expected when connecting to the GUI using special management port numbers.
600727	Resolved an IPsec VPN phase 2 route synchronization issue.
601650	The <code>execute clear system arp table</code> command, run from the management board or primary FIM, now successfully clears arp entries on FPCs or FPMs.
602038	Standalone configuration synchronization no longer incorrectly synchronizes the FortiGate-6000 or 7000 global management IP address.
602699	Corrected an error with how SNMP reports CPU information for the FortiGate-7030E
604212	Corrected errors with the options available for configuring FortiGate-6000 interface speeds.
604984	Resolved an issue that prevented SDN connector dynamic firewall addresses from being synchronized to all FPCs or FPMs.
605609	On the FortiGate-6000 and 7000, the default value of the <code>config system csf configuration-sync</code> option has been changed to <code>local</code> .
605904	Resolved an issue that caused SDN connectors to fail after multiple HA failovers.
607624	The <code>diagnose test application radiusd 2</code> command now shows results from all FPCs or FPMs.

Known issues

The following issues have been identified in FortiGate-6000 and FortiGate-7000 FortiOS 6.2.3 Build 6252. For inquiries about a particular bug, please contact [Customer Service & Support](#). The [Known issues](#) described in the [FortiOS 6.2.3 release notes](#) also applies to FortiGate-6000 and 7000 FortiOS 6.2.3 Build 6252.

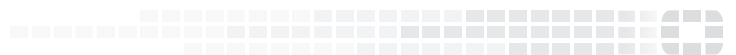
Bug ID	Description
515590	The Session Rate: Management dashboard widget shows incorrect information when viewed on VDOM dashboards.
561722	<p>Policies that block or allow devices based on device detection and identification using FortiClient may not work as expected because the MAC addresses used to identify the devices are not synchronized to all FPCs or FPMs. You can work around this issue using a flow rule similar to the following:</p> <pre>config load-balance flow-rule edit 28 set status enable set ether-type ip set protocol tcp set dst-l4port 8013-8013 set forward-slot load-balance set comment "FCT Telemetry" end</pre> <p>It may also work to change the load distribution method:</p> <pre>config load-balance setting set dp-load-distribution-method src-ip config workers edit 1 end end</pre>
581243	Under some conditions (for example, high CPU usage) the <code>get system status</code> command on some FPCs or FPMs may show an incorrect primary (master) FPC or FPM.
581990	Running the <code>diagnose sys logdisk status</code> command on a FortiGate-6301F or 6501F may show the status of the log disk as <code>unknown</code> even if the disk is available and in a known good state.
584078	When logged into an individual FPC or FPM, the Load Balance Monitor GUI page incorrectly shows all real servers as being down.
589613	Local-in deny policies may not successfully block the specified local-in traffic.
590136	In a virtual clustering configuration, under some conditions some FortiGate-6000 or 7000 components may not be able to reach DNS servers and will generate DNS error log messages.
591251	Enabling disk logging on a FortiGate-6501F or 6301F or enabling sending logs to a syslog server on a FortiGate-6000 or 7000 from the GUI does not work unless FortiAnalyzer logging is enabled.
601677	Under some conditions caused by communication problems, the <code>get system status</code> command run on a FortiGate-7000 primary FPM may incorrectly show that another FPM is the primary FPM or the <code>FPM Master</code> field show N/A.

Bug ID	Description
600504	IPv6 ECMP is not supported.
603601 604304 606091	This release supports many, but not all, SDN connectors. Some workarounds may be required to support some features. For more information, see SDN connector support on page 24 .
605065	You cannot set a management interface LAG to be the SLBC management interface by adding it to the <code>config load-balance setting slbc-mgmt-intf</code> option. For more information, see Management interface LAG limitations on page 1 .
605069	FortiGate-6000 FPCs and the management board assign different MAC addresses to a management interface LAG. The management board uses the MAC address of the second interface in the member list while the FPCs use the MAC address of the first interface in the member list.
605073	The GUI or CLI doesn't prevent you from adding mgmt3 to a management lag.
605371	By default, for FortiOS 6.2.3 the <code>auxiliary-sessions</code> option of the <code>config system settings</code> command is disabled and with ECMP enabled, some TCP sessions may unexpectedly be blocked. For more information, see Enabling auxiliary session support on page 21 .
605411	Management traffic (local in and local out) is not accepted by inter-VDOM link interfaces if the inter-VDOM link type is set to <code>ppp</code> (point to point). The type is set to <code>ppp</code> by default when you add an inter-VDOM link from the GUI or CLI. To support management connections to the inter-VDOM link interfaces, you must manually change the type to <code>ethernet</code> from the CLI using the following command: <pre>config system vdom-link edit link-name set type ethernet end</pre>
606120	Usage-based ECMP load balancing is not supported. If the <code>config system settings v4-ecmp-mode</code> option is set to <code>usage-based</code> , all traffic uses the first ECMP route instead of being load balanced among all ECMP routes. All other ECMP load balancing options are supported, including <code>source-ip-based</code> , <code>weight-based</code> , and <code>source-dest-ip-based</code> .
606785	If you manually disable an interface that has been added to a LAG group, the interface disappears from the GUI interface list. To get the interface to appear on the list, you must enable it from the CLI.
607139	In a virtual clustering configuration, if virtual cluster 1 and virtual cluster 2 are on different FortiGates then dial up VPN servers in VDOMs in virtual cluster 2 will not work correctly because of missing IPsec routes. The workaround until this issue is resolved is to keep VDOMs with VPN servers in virtual cluster 1.
607536	An "image upgrade failed" message may appear on the GUI after a successful graceful upgrade of an HA cluster.
607649	If the FortiGate-6000 mgmt1, mgmt2, or mgmt3 interfaces are HA monitored interfaces they cannot be added to a management interface LAG.
607921	The Configuration Sync Monitor may show incorrect status information for the secondary FortiGate-6000 management board or FortiGate-7000 primary FIM.

Bug ID	Description
608940	Management traffic can't be sent over an inter-VDOM link. For example, you can't connect from the mgmt-vdom to FortiGuard by creating an inter-VDOM link between mgmt-vdom and a VDOM connected to the internet. You also can't use inter-VDOM links to connect from mgmt-vdom to a FortiManager. To communicate with FortiGuard, mgmt-vdom must be able to connect to the internet or to a FortiManager without going through an inter-VDOM link.
608632	FortiGate-6000 dataplane sessions and session rate dashboard widgets show incorrect information when viewed from a traffic VDOM dashboard.
609131	When DHCP leases are cleared from the primary FortiGate in an HA cluster, they are not cleared from the secondary FortiGate.
610494	Virtual clustering is not supported when operating in Split-Task VDOM mode. Virtual clustering GUI and CLI options to configure virtual clustering when operating in Split-Task VDOM mode will be removed in a future release.
610779	In some FortiGate-6000 and 7000 configurations, the forwarding information base (FIB) routing database may not be synchronized to all FPCs or FPMs. You can resolve this issue by forcing the FPCs or FPMs to re-synchronize the FIB by logging into the FPC or FPM CLI and entering <code>diagnose test application chlbd 3</code> . This problem can be difficult to detect because there can be a very large number of routes to compare. You can use the command <code>diagnose ip route list grep -c "proto=1[1,8]"</code> from each FPC or from each FPM to display the number of routes. If one component has a different (usually lower) number, you can use the <code>diagnose</code> command to re-synchronize it.
611830	Error checking does not prevent you from moving a VDOM between virtual clusters that causes a VLAN to be in a different virtual cluster than the physical interface or LAG that the VLAN has been added to. FortiGate-6000 and 7000 virtual clustering requires that a VLAN must be in the same virtual cluster as the physical or LAG interface that the VLAN has been added to. See Virtual clustering VLAN/VDOM limitation on page 13 .
611834	In a virtual clustering configuration, if a VLAN interface is in a different virtual cluster than the physical interface that it was added to, traffic to and from that interface can pass through the virtual cluster that contains the physical interface.
612357	The <code>execute factoryreset-shutdown</code> command will not completely reset the configuration to factory defaults when run on a secondary FortiGate-6000F in an HA cluster with <code>uninterruptible-upgrade</code> enabled.
612444	When a FortiGate-6000 or 7000 forms a cluster with another FortiGate-6000 or 7000 already operating in HA mode, the active RSSO user list is not synchronized to the FPCs or FPMs in the newly joined FortiGate-6000 or 7000. This can happen, for example, in an operating cluster if one of the FortiGate-6000s or 7000s in the cluster restarts.
613295	When converting a FortiGate-6000 or 7000 system from FortiOS Carrier to normal FortiOS, after the system restarts it may be out of sync. You can resolve this problem by logging into the management board or primary FIM CLI and entering the following command to reset the <code>darrp-optimize-schedules wireless controller</code> setting. <pre>config wireless-controller setting unset darrp-optimize-schedules end</pre>



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.