



# FortiGate-6000 and FortiGate-7000 - Release Notes

Version 6.0.9 Build 6783

**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](mailto:techdoc@fortinet.com)



July 15, 2020

FortiGate-6000 and FortiGate-7000 6.0.9 Build 6783 Release Notes

01-609-621068-2020715

# TABLE OF CONTENTS

<b>Change log</b>	<b>5</b>
<b>FortiGate-6000 and FortiGate-7000 6.0.9 release notes</b>	<b>6</b>
Supported FortiGate-6000 and 7000 models	6
<b>What's new</b>	<b>7</b>
HA heartbeat VLAN double-tagging	7
New protocol for handling HA chassis ID conflicts	7
<b>Special notices</b>	<b>9</b>
Default Security Fabric configuration	9
Adding a flow rule to support DHCP relay	9
Limitations of installing FortiGate-6000 firmware from the BIOS after a reboot	10
Limitations of installing FortiGate-7000 firmware from the BIOS after a reboot	11
Installing firmware on an individual FortiGate-6000 FPC	11
Installing firmware on an individual FortiGate-7000 FPM	12
SD-WAN is not supported	13
IPsec VPN feature notes	13
FortiGate-6000 and FortiGate-7000 IPsec VPN	13
FortiGate-6000 IPsec VPN	13
FortiGate-7000 IPsec VPN	13
Quarantine to disk not supported	14
Local out traffic is not sent to IPsec VPN interfaces	14
Special configuration required for SSL VPN	14
If you change the SSL VPN server listening port	14
Adding the SSL VPN server IP address	15
Example FortiGate-6000 HA heartbeat switch configurations	15
Example triple-tagging compatible switch configuration	15
Example double-tagging compatible switch configuration	16
Example FortiGate-7000 HA heartbeat switch configuration	17
Example triple-tagging compatible switch configuration	17
Example double-tagging compatible switch configuration	19
Default FortiGate-6000 and 7000 configuration for traffic that cannot be load balanced	20
<b>Managing individual FortiGate-6000 management boards and FPCs</b>	<b>26</b>
Special management port numbers	26
HA mode special management port numbers	27
Connecting to individual FPC consoles	28
Connecting to individual FPC CLIs	29
Performing other operations on individual FPCs	29
<b>Managing individual FortiGate-7000 FIMs and FPMs</b>	<b>30</b>
Special management port numbers	30
HA mode special management port numbers	31
Managing individual FIMs and FPMs from the CLI	32
Connecting to individual FIM and FPM CLIs of the secondary FortiGate-7000 in an HA configuration	32

<b>Upgrade information</b>	<b>33</b>
HA graceful upgrade to FortiOS 6.0.9	33
HA graceful upgrade from FortiOS 5.6.7, 5.6.11, or 6.0.4 to FortiOS 6.0.9	34
About FortiGate-6000 firmware upgrades	35
About FortiGate-7000 firmware upgrades	35
<b>Product integration and support</b>	<b>37</b>
FortiManager and FortiAnalyzer support	37
FortiGate-6000 6.0.9 special features and limitations	37
FortiGate-7000 6.0.9 special features and limitations	37
Maximum values	37
<b>Resolved issues</b>	<b>38</b>
<b>Known issues</b>	<b>39</b>

# Change log

Date	Change description
July 15, 2020	Updates to <a href="#">HA graceful upgrade to FortiOS 6.0.9 on page 33</a> . New section: <a href="#">HA graceful upgrade from FortiOS 5.6.7, 5.6.11, or 6.0.4 to FortiOS 6.0.9 on page 34</a> .
June 9, 2020	Corrected the FortiManager and FortiAnalyzer versions listed in <a href="#">FortiManager and FortiAnalyzer support on page 37</a> .
April 21, 2020	Added resolved issue 599999 to the <a href="#">Resolved issues</a> list.
April 9, 2020	Added a resolved issue from 508610 to the <a href="#">Resolved issues</a> list and added an unresolved issue from 508610 to the <a href="#">Known issues</a> list.
April 6, 2020	Initial version.

# FortiGate-6000 and FortiGate-7000 6.0.9 release notes

These platform specific release notes describe new features, special notices, upgrade information, product integration and support, and resolved issues for FortiGate-6000 and 7000 for FortiOS 6.0.9 Build 6783. FortiGate-6000 and 7000 for FortiOS 6.0.9 Build 6783 also includes the special notices, product integration and support, resolved issues, and known issues described in the [FortiOS 6.0.9 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 FortiGate-7000 for FortiOS 6.0.9 Build 6783 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 6.0.9 Build 6783. This release also includes the bug fixes described in [Resolved issues on page 38](#).

### 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 6.0.9 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 16](#).

For a FortiGate-7000 double-tagging example, see [Example double-tagging compatible switch configuration on page 19](#).

### 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-  
d="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.



# Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for FortiGate-6000 and 7000 6.0.9 Build 6783. The [Special Notices](#) described in the [FortiOS 6.0.9 release notes](#) also apply to FortiGate-6000 and 7000 FortiOS 6.0.9 Build 6783.

## Default Security Fabric configuration

The FortiGate-6000 uses the Security Fabric for communication and synchronization between the management board and FPCs. The FortiGate-7000 uses the Security Fabric for communication and synchronization among FIMs and FPMs. Changing the default Security Fabric configuration could disrupt this communication and affect system performance.

Default Security Fabric configuration:

```
config system csf
    set status enable
    set configuration-sync local
    set management-ip 0.0.0.0
    set management-port 0
end
```

As of version 6.0.6 you can no longer change the `status` to `disable`.

For the FortiGate-6000 and 7000 to operate normally, you must not change the Security Fabric configuration.

## Adding a flow rule to support DHCP relay

The FortiGate-6000 and 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 firmware on individual FIMs and FPMs](#) 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 7000 for FortiOS 6.0.9 does not support SD-WAN.

## IPsec VPN feature notes

This section contains notes and limitations for FortiGate-6000 and 7000 IPsec VPNs for FortiOS 6.0.9.

### FortiGate-6000 and FortiGate-7000 IPsec VPN

The following notes and limitations apply to both FortiGate-6000 and 7000 IPsec VPNs for FortiOS 6.0.9:

- Site-to-Site IPsec VPN is supported.
- Dialup IPsec VPN is supported. The FortiGate-6000 or 7000 can be the dialup server or client.
- Interface-based IPsec VPN (also called route-based IPsec VPN) is supported. Policy-based IPsec VPN is not supported.
- Static routes can point at IPsec VPN interfaces and can be used for routing the traffic inside IPsec VPN tunnels.
- 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.
- IPsec SA synchronization between HA peers is not supported. After an HA failover, IPsec VPN tunnels have to be re-initialized.

### FortiGate-6000 IPsec VPN

The following notes and limitations apply to FortiGate-6000 IPsec VPNs for FortiOS 6.0.9:

- The FortiGate-6000 supports load balancing IPsec VPN tunnels to multiple FPCs as long as only static routes are used over the IPsec VPN tunnels.
- If FortiGate-6000 IPsec VPN load balancing is not enabled, you can use static or dynamic routing (RIP, OSPF, BGP) over IPsec VPN tunnels.
- With FortiGate-6000 IPsec VPN load balancing enabled, the FortiGate-6000 DP3 processor terminates individual IPsec VPN tunnels on different FPCs. All traffic to and from a specific tunnel is processed by the same FPC. Individual tunnel SAs are not synchronized to other FPCs. One result of this setup is that traffic cannot travel between two tunnels since the two tunnels could be terminated on different FPCs. With IPsec load balancing enabled, traffic cannot travel between two IPsec VPN tunnels.
- Traffic between two IPsec VPN tunnels is supported if load balancing is disabled. In this case, all IPsec VPN tunnels are terminated on the primary FPC and traffic between IPsec VPN tunnels is supported.

### FortiGate-7000 IPsec VPN

The following notes and limitations apply to FortiGate-7000 IPsec VPNs for FortiOS 6.0.9:

- Dynamic routing (RIP, OSPF, BGP) over IPsec VPN tunnels is supported.
- The FortiGate-7000 does not support load-balancing IPsec VPN tunnels to multiple FPMs. All IPsec VPN tunnels are terminated on the primary FPM and traffic between IPsec VPN tunnels is supported.

## 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 6.0.9 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 6.0.9 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 6.0.9 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`). Each default flow rule also includes 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 FortGate 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 6.0.9 Release Notes](#).

## HA graceful upgrade to FortiOS 6.0.9

Use the following steps to upgrade a FortiGate-6000 or 7000 HA cluster with `uninterruptible-upgrade` enabled from FortiOS 6.0.6 build 6392 or from FortiOS 6.0.8 build 6599 to 6.0.9 Build 6783.



To perform a graceful upgrade from FortiOS 5.6.7, 5.6.11, or 6.0.4 to FortiOS 6.0.9 Build 6783 you must use an upgrade support image. See [HA graceful upgrade from FortiOS 5.6.7, 5.6.11, or 6.0.4 to FortiOS 6.0.9 on page 34](#).

---

Enabling `uninterruptible-upgrade` allows you to upgrade the firmware of an operating FortiGate-6000 or 7000 HA cluster 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 to FortiOS 6.0.9:

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

```
config system ha
    set session-pickup enable
    set uninterruptible-upgrade enable
end
```

2. Download the FortiGate-6000 or 7000 FortiOS 6.0.9 Build 6783 image file from the <https://support.fortinet.com> FortiOS 6.0.9 firmware image folder.
3. Perform a normal upgrade of your HA cluster.
4. Wait a few minutes, and when the upgrade is complete, verify that you have installed the correct interim firmware version. For example, for the FortiGate-6301F:

```
get system status
Version: FortiGate-6301F v6.0.9,build6783,200331 (GA)
...
```

## HA graceful upgrade from FortiOS 5.6.7, 5.6.11, or 6.0.4 to FortiOS 6.0.9

Use the following steps to upgrade a FortiGate-6000 or 7000 HA cluster with `uninterruptible-upgrade` enabled from FortiOS 5.6.7, 5.6.11, or 6.0.4 to 6.0.9 Build 6783.

Enabling `uninterruptible-upgrade` allows you to upgrade the firmware of an operating FortiGate-6000 or 7000 HA cluster 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.

This procedure supports upgrading from the following firmware versions:

- FortiOS 5.6.7 build 4214 or 4261.
- FortiOS 5.6.11 build 4279.
- FortiOS 6.0.4 build 6145 or 8405.

Performing this upgrade requires installing an interim upgrade support image before installing the final FortiOS 6.0.9 firmware image.

Starting image	Upgrade support image	Final image
5.6.7 build 4214 or 4261	6.0.4 build 8428	6.0.9 Build 6783
5.6.11 build 4279	6.0.4 build 8428	6.0.9 Build 6783
6.0.4 build 6145 or 8405	6.0.4 build 8428	6.0.9 Build 6783

You can download the upgrade support image from the <https://support.fortinet.com> FortiOS 6.0.6 firmware image download folder. The upgrade support images have the following file names:

- FortiGate 6000F: **FGT\_6000F-v6-build8428-Upgrade-Support-FORTINET.out**
- FortiGate 7000E: **FGT\_7000E-v6-build8428-Upgrade-Support-FORTINET.out**

To verify that you have installed the correct upgrade support image, after installing it you can use the `get system status` command or the **System Information** dashboard widget to verify that the firmware version is FortiOS 6.0.4 B8428.

To perform a graceful upgrade of your FortiGate-6000 or 7000 from FortiOS 5.6.7, 5.6.11, or 6.0.4 to 6.0.9 Build 6783:

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

```
config system ha
    set session-pickup enable
    set uninterruptible-upgrade enable
end
```

2. Download the FortiGate-6000 or 7000 upgrade support image file from the <https://support.fortinet.com> FortiOS 6.0.6 firmware image folder.
3. Perform a normal upgrade of your HA cluster using the upgrade support image.
4. Verify that you have installed the correct interim firmware version. For example, for the FortiGate-7040E:

```
get system status
Version: FortiGate-7040E v6.0.4,build8428,190813 (GA)
...
```

5. Download the FortiGate-6000 or 7000 FortiOS 6.0.9 Build 6783 image file from the <https://support.fortinet.com>

FortiOS 6.0.9 firmware image folder.

6. Perform a normal upgrade of your HA cluster to FortiOS 6.0.9 Build 6783.
7. Wait a few minutes, and when the upgrade is complete, verify that you have installed the correct firmware version. For example, for the FortiGate-6301F:

```
get system status
Version: FortiGate-6301F v6.0.9,build6783,200331 (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 6.0.9 Build 6783 product integration and support information. The [Product Integration and Support](#) information described in the [FortiOS 6.0.9 release notes](#) also applies to FortiGate-6000 and 7000 FortiOS 6.0.9 Build 6783.

## FortiManager and FortiAnalyzer support

FortiGate-6000 and 7000 for 6.0.9 Build 6783 require the following or newer versions of FortiManager and FortiAnalyzer:

- FortiGate-6000: FortiManager or FortiAnalyzer 6.2.5 and 6.4.1.
- FortiGate-7000: FortiManager or FortiAnalyzer 6.2.5 and 6.4.1.

## FortiGate-6000 6.0.9 special features and limitations

FortiGate-6000 for FortiOS 6.0.9 has specific behaviors that may differ from FortiOS features. For more information, see the [Special features and limitations for FortiGate-6000 v6.0.9](#) section of the FortiGate-6000 handbook.

## FortiGate-7000 6.0.9 special features and limitations

FortiGate-7000 for FortiOS 6.0.9 has specific behaviors that may differ from FortiOS features. For more information, see the [Special features and limitations for FortiGate-7000 v6.0.9](#) section of the FortiGate-7000 handbook.

## Maximum values

Maximum values for FortiGate-6000 and FortiGate-7000 for FortiOS 6.0.9 are available from the FortiOS Maximum Values Table (<https://docs.fortinet.com/max-value-table>).

For changes in maximum values in this release, see [Changes in Table Size](#) in the [FortiOS 6.0.9 Release Notes](#).

# Resolved issues

The following issues have been fixed in FortiGate-6000 and 7000 FortiOS 6.0.9 Build 6783. For inquiries about a particular bug, please contact [Customer Service & Support](#). The [Resolved Issues](#) described in the [FortiOS 6.0.9 release notes](#) also apply to FortiGate-6000 and 7000 FortiOS 6.0.9 Build 6783.

Bug ID	Description
508610	Resolved an issue that prevented the FortiGate-6000 and 7000 from recognizing some Finisar transceivers. For example, the FCLF8521p2BTL (FG-TRAN-GC) and (FS-TRAN-GC) FCLF8522P2BTL are now recognized.
513339	Resolved issues that prevented FortiOS from recognizing some supported FS-TRAN-GC transceivers.
599999	The trusted host feature now works as expected when connecting to the GUI using special management port numbers.
603564	Resolved a synchronization issue that prevented a new FortiGate-7000 from joining an HA cluster if the primary FortiGate-7000 is configured with split ports.
612450	Improved how the FortiGate-6000 or 7000 reacts to disabling FPCs or FPMs. With this improvement, when disabled FPCs or FPMs are re-enabled, they are now more likely to successfully re-join the SLBC cluster.
614444	Resolved an issue that caused the primary FPC or FPM to experience unexpectedly high CPU usage. Resolving the bug involved a code change that improves the efficiency of some VDOM-related processes.
618777	Resolved an issue that prevented certificates created as part of the global configuration from being available for individual VDOMs.

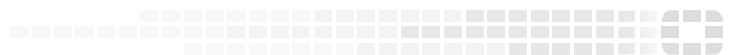
# Known issues

The following issues have been identified in FortiGate-6000 and FortiGate-7000 FortiOS 6.0.9 Build 6783. For inquiries about a particular bug, please contact [Customer Service & Support](#). The [Known Issues](#) described in the [FortiOS 6.0.9 release notes](#) also apply to FortiGate-6000 and 7000 FortiOS 6.0.9 Build 6783.

Bug ID	Description
508610	FortiGate-6000 and 7000 interface status LEDs do not accurately show link status for copper SPF transceivers that use the RX_LOS pin to indicate link status.
600879	The feature to enable packet capturing from a firewall policy is not available.
611558	In some cases on a FortiGate-7000, configuration changes may not successfully be synchronized to all of the FPMs. If this occurs you can run the command <code>killall confsyncd</code> on the FPM that is out of sync to stop the <code>confsyncd</code> process. The process should restart and re-synchronize the configuration; which can take about 30 seconds.
612622	Quarantined files are not sent to FortiSandbox when the <code>config system fortisandbox</code> configuration includes a setting for the <code>source-ip</code> option.
616110	After an FGCP HA failover, its possible that traffic may not be able to pass through a transparent mode VDOM until the FDB MAC table expires in approximately 6 minutes.
616728	If you factory reset the backup FortiGate-6000 or 7000 in an FGCP cluster and then re-configure the backup FortiGate to join with the correct HA settings, the backup FortiGate will not be able to join the cluster again until it is manually restarted.
619094	In an FGSP configuration with asymmetric routing and four FortiGate-6000s or 7000s, the first reply packet of all new sessions is dropped.
619237	When a FortiGate-6000 or 7000 is idle, the <code>src-vis</code> process can use excessive amounts of CPU resources and cause 100% <code>softirq</code> usage on each CPU on the primary FPC or FPM.
621375	A graceful upgrade of an FGCP HA cluster may fail if the configuration includes a large number of VDOMs. The upgrade process times out waiting for the backup FortiGate-6000 or 7000 to upgrade and start up.
621978	VRRP packets that should be blocked are incorrectly sent to the secondary FPCs or FPMs.



**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.