FortiGate-6000 and FortiGate-7000 - Release Notes

Version 6.4.8 Build 1823

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

January 16, 2023
FortiGate-6000 and FortiGate-7000 6.4.8 Build 1823 Release Notes
01-648-773173-20230116

TABLE OF CONTENTS

Change log

Date	Change description
January 16, 2023	Corrected information about controlling SNAT port partitioning behavior, see Changing SNAT port partitioning behavior on page 9.
June 28, 2022	Known issue 792717 added to Known issues on page 62.
May 3, 2022	Corrections to Product integration and support on page 57.
April 29, 2022	Known issue 771680 added to Known issues on page 62.
April 19, 2022	Updated the following with information about the FIM-7941F: • Known issue 778239, see Known issues on page 62. • Improved the description of known issue 734898. • Maximum number of flow rules limited by hardware on page 11.
March 15, 2021	Known issue 786659 added to Known issues on page 62.
March 1, 2021	Known issue 778239 added to Known issues on page 62. New section: Maximum number of flow rules limited by hardware on page 11.
February 18, 2022	Known issue 783689 added to Known issues on page 62.
February 17, 2022	Initial version.

FortiGate-6000 and FortiGate-7000 6.4.8 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 6.4.8 Build 1823.

In addition, special notices, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 6.4.8 Release Notes also apply to FortiGate-6000 and 7000 for 6.4.8 Build 1823.

For FortiGate-6000 documentation for this release, see the FortiGate-6000 Handbook.

For FortiGate-7000E documentation for this release, see the FortiGate-7000E Handbook.

For FortiGate-7000F documentation for this release, see the FortiGate-7000F Handbook.

You can find the FortiGate-6000 and 7000 for FortiOS 6.4.8 firmware images on the Fortinet Support Download Firmware Images page by selecting the **FortiGate-6K7K** product.

Supported FortiGate-6000 and 7000 models

FortiGate-6000 and 7000 for FortiOS 6.4.8 Build 1823 supports the following models:

- FortiGate-6300F
- FortiGate-6301F
- FortiGate-6500F
- FortiGate-6501F
- FortiGate-7030E
- FortiGate-7040E
- FortiGate-7060E
- FortiGate-7121F

What’s new

The following new features have been added to FortiGate-6000 and 7000 for FortiOS 6.4.8 Build 1823.

SSL VPN tunnel mode load balancing

FortiGate-6000 and 7000 for FortiOS 6.4.8 supports load balancing SSL VPN tunnel mode sessions terminated by the FortiGate-6000 or 7000.

By default SSL VPN load balancing is disabled and a flow rule is required to send all SSL VPN sessions to one FPC or FPM. For example, the following flow rule sends all SSL VPN sessions to the primary FPC or FPM:

```
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"
   end
```

To support SSL VPN tunnel load balancing, you must disable all flow rules that match the SSL VPN traffic to be load balanced.

Then you can use the following new command to enable SSL VPN load balancing:

```
config load-balance setting
   set sslvpn-load-balance enable
end
```

When you enable SSL VPN load balancing, the FortiGate-6000 or 7000 restarts SSL VPN processes on the management board and the FPCs and on all FIMs and FPMs, resetting all current SSL VPN sessions.

SSL VPN load balancing statically allocates the IP addresses in SSL VPN IP pools to the FPCs or FPMs. Each FPC or FPM acquires a subset of the IP addresses in the IP pool. You may need to expand the number of IP addresses in your SSL VPN IP pools to make sure enough IP addresses are available for each FPC or FPM.

SSL VPN IP pool IP addresses are not re-allocated if an FPC or FPM goes down, is disabled, or is taken offline. The IP pool IP addresses assigned to the missing FPC or FPM are not available.

For SSL VPN load balancing to work properly, the DP processor load distribution method must be changed to a setting that does not include `src-port`. The following DP load distribution methods are supported for SSL VPN load balancing:

```
config load balance setting
   set dp-load-distribution-method {to-master | src-ip | dist-ip | src-
         dst-ip | dis-ip-dport}
end
```

FortiGate-7000F HA group ID range increased to 0 to 255

The range of the FortiGate-7000F HA group ID has been increased to 0 to 255:

```
config system ha
   set group-id 0-255
end
```

The HA group ID is used to calculate the MAC addresses assigned by the FGCP to the FortiGates in an FGCP cluster. Because of this change to the group ID range, after upgrading a FortiGate-7000F FGCP cluster to FortiOS 6.4.8, the MAC addresses assigned to the cluster interfaces by the FGCP will not be the same as the MAC addresses that were assigned before the firmware upgrade.

⚠ If you have upstream devices that perform MAC address checking and enforcement, traffic may be interrupted after the firmware upgrade because of the new MAC addresses.

Direct FortiGate-7000F to FortiAnalyzer logging

You can use the following option to support FortiGate-7000F direct logging for FortiAnalyzer log messages.

```
config log slbc global-setting
   set direct-log-mode faz-udp
end
```

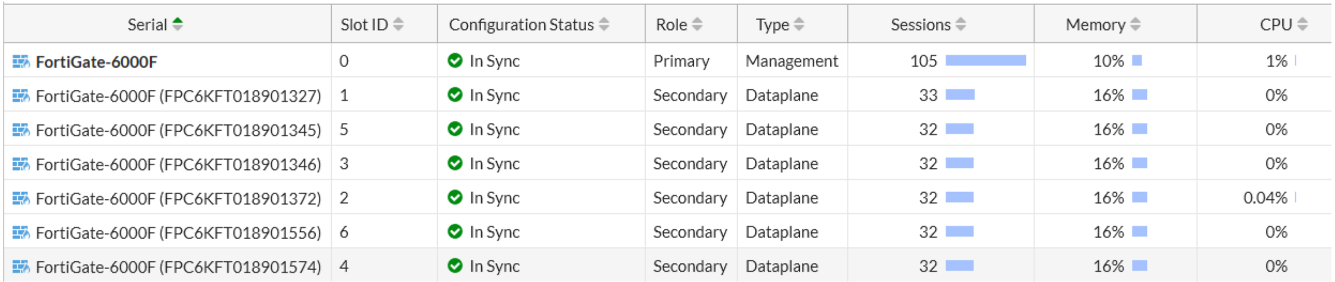
The `disabled` option has been removed from this command. Instead, you can use the following command to disable direct logging:

```
config log slbc global-setting
   unset direct-log-mode
end
```

Config sync monitor displays management and data plane resource usage

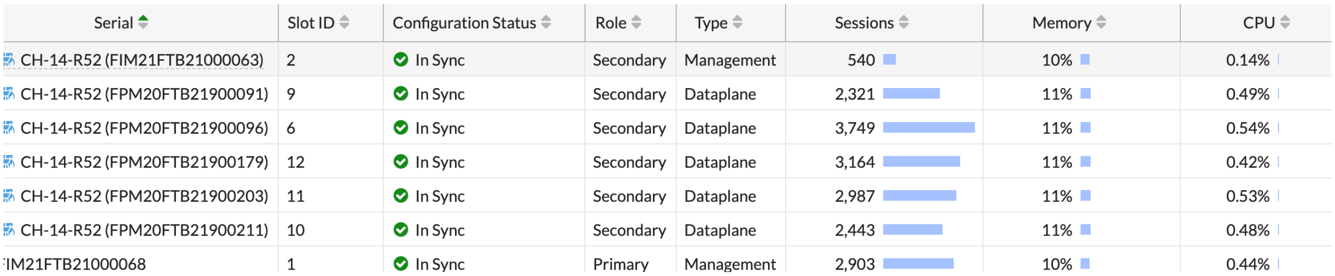
For FortiOS 6.4.8, the Configuration Sync Monitor now displays the current number of sessions, memory usage, and CPU usage for each component in a FortiGate-6000 or 7000. This display allows you to separate management plane resource usage (FortiGate-6000 management board or FortiGate-7000 FIMs) from data plane resource usage (FortiGate-6000 FPCs or FortiGate-7000 FIMs).

Example FortiGate-6310F Configuration Sync Monitor



Serial	Slot ID	Configuration Status	Role	Type	Sessions	Memory	CPU
FortiGate-6000F	0	✓ In Sync	Primary	Management	105	10%	1%
FortiGate-6000F (FPC6KFT018901327)	1	✓ In Sync	Secondary	Dataplane	33	16%	0%
FortiGate-6000F (FPC6KFT018901345)	5	✓ In Sync	Secondary	Dataplane	32	16%	0%
FortiGate-6000F (FPC6KFT018901346)	3	✓ In Sync	Secondary	Dataplane	32	16%	0%
FortiGate-6000F (FPC6KFT018901372)	2	✓ In Sync	Secondary	Dataplane	32	16%	0.04%
FortiGate-6000F (FPC6KFT018901556)	6	✓ In Sync	Secondary	Dataplane	32	16%	0%
FortiGate-6000F (FPC6KFT018901574)	4	✓ In Sync	Secondary	Dataplane	32	16%	0%

Example FortiGate-7121F Configuration Sync Monitor



Serial	Slot ID	Configuration Status	Role	Type	Sessions	Memory	CPU
CH-14-R52 (FIM21FTB21000063)	2	✓ In Sync	Secondary	Management	540	10%	0.14%
CH-14-R52 (FPM20FTB21900091)	9	✓ In Sync	Secondary	Dataplane	2,321	11%	0.49%
CH-14-R52 (FPM20FTB21900096)	6	✓ In Sync	Secondary	Dataplane	3,749	11%	0.54%
CH-14-R52 (FPM20FTB21900179)	12	✓ In Sync	Secondary	Dataplane	3,164	11%	0.42%
CH-14-R52 (FPM20FTB21900203)	11	✓ In Sync	Secondary	Dataplane	2,987	11%	0.53%
CH-14-R52 (FPM20FTB21900211)	10	✓ In Sync	Secondary	Dataplane	2,443	11%	0.48%
IM21FTB21000068	1	✓ In Sync	Primary	Management	2,903	10%	0.44%

Changing SNAT port partitioning behavior

You can use the following command to control how the FortiGate-6000 or 7000 partitions source NAT (SNAT) source ports among FPCs or FPMs:

```
config load-balance setting
   set nat-source-port {chassis-slots | enabled-slots}
end
```

`chassis-slots` this option statically allocates SNAT source ports to all FPCs or FPMs that are enabled when you enter the command. If you disable an FPC or FPM from the CLI or remove an FPM from its slot, the SNAT source ports assigned to that FPC or FPM will not be re-allocated to the remaining FPCs or FPMs. All FPCs or FPMs that are still operating will maintain the same SNAT source port allocation and active sessions being processed by the still operating FPCs or FPMs will not be affected.

You can use the following command to enable or disable an FPC or FPM from the CLI:

```
config workers
   edit <slot>
      set status {disable | enable}
   end
```

`enabled-slots` this option dynamically re-distributes SNAT source ports to enabled FPCs or enabled and installed FPMs. This is the default behavior and is recommended in most cases.

If an FPC or FPM is disabled or if an FPM is removed from its slot, SLBC dynamically re-allocates SNAT source ports among the remaining enabled FPCs or FPMs. This means that all configured SNAT source ports remain available. If

SNAT source ports are re-allocated when the FortiGate-7000 is actively processing traffic, some active sessions may be lost if their source ports are allocated to different FPCs or FPMs.

SNAT source ports are not dynamically reallocated if an FPC or FPM is powered off. To re-allocate SNAT source ports, the FPC or FPM must be disabled from the CLI or the FPM must be physically removed from its slot.

SD-WAN improvements

6.4.8 Build 1823 includes a number of improvements and bug fixes related to SD-WAN comparability with session-aware load balancing clustering (SLBC).

The primary FPC or FPM performs health checking and synchronizes SD-WAN routing decisions to the other FPCs or FPMs. In an FGCP HA cluster, the SD-WAN routing decisions are synchronized from the primary FPC or FPM of the primary FortiGate to the FPCs or FPMs in the secondary FortiGate.

The FortiGate-6000 and 7000 now support weight-based and volume-based SD-WAN load-balancing methods:

```
config system virtual-wan-link
   set load-balance-mode {weight-based | measured-volume-based}
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 6.4.8 Build 1823. The Special notices described in the FortiOS 6.4.8 release notes also apply to FortiGate-6000 and 7000 FortiOS 6.4.8 Build 1823.

Maximum number of flow rules limited by hardware

For all FortiGate-6000 and 7000 models, the CLI allows you to add up to 512 flow rules. However, the number of flow rules that you can add is actually limited by the FortiGate-6000 and 7000 internal switch hardware:

- All FortiGate-6000F models support up to 256 flow rules.
- All FortiGate-7000E models support up to 512 flow-rules.
- A FortiGate-7000F with FIM-7941Fs supports up to 492 flow rules.
- A FortiGate-7000F with FIM-7921Fs supports up to 52 flow rules.

VLAN ID 1 is reserved

When setting up VLANs, do not set the VLAN ID to 1. This VLAN ID is reserved by FortiOS. Any configurations that use a VLAN with VLAN ID = 1 will not work as expected.

Configuring the FortiGate-7000F SLBC management interface

To be able to use FortiGate-7000F special SLBC management interface features, such as being able to log into any FIM or FPM using the management interface IP address and a special port number, you need to use the following command to select a FortiGate-7000F management interface to be the SLBC management interface.

You can use any of the FIM or FPM management interfaces to be the SLBC management interface. The following example uses the MGMT 1 interface of the FIM in slot 1. In the GUI and CLI the name of this interface is 1-mgmt1.

Enter the following command to set the 1-mgmt1 interface to be the SLBC management interface:

```
config global
   config load-balance setting
      set slbc-mgmt-intf 1-mgmt1
   end
```

To manage individual FIMs or FPMs using special management ports, the SLBC interface must be connected to a network.

The `slbc-mgmt-intf` option is set to `1-mgmt1` by default (but this setting is not visible in the default configuration). If you decide to use a different management interface, you must also change the `slbc-mgmt-intf` to that interface.

FortiGate-6000F hardware generations

Two generations of FortiGate-6000F hardware are now available. Both generations support the same software features. Generation 2 has two hardware improvements:

- The FPCs include more memory.
- When connected to high-line AC power, generation 2 FortiGate-6000F models provide 1+1 PSU redundancy. When connected to high-line AC power, each PSU provides 2000W, which is enough power to run the entire system including all FPCs.

For more information on FortiGate-6000F generation 1 and generation 2, including supported firmware versions and how to determine the generation of your FortiGate-6000F hardware, see the Fortinet Knowledge base article: Technical Tip: Information on FortiGate-6000F series Gen1 and Gen2.

For more information on generation 1 and generation 2 AC PSUs, see FortiGate-6000F AC power supply units (PSUs).

Default FortiLink aggregate interface configuration may not work

The FortiGate-6000 and 7000 default configurations include an 802.3 aggregate interface named **fortilink**, intended to be used to connect to one or more managed FortiSwitches. To use this interface to connect to managed FortiSwitches you must add one or more interfaces to the aggregate interface and then connect your FortiSwitches to these interfaces.

Example fortilink interface configuration:

```
config system interface
   edit fortilink
      set vdom <vdom>
      set fortilink enable
      set ip <ip-address>
      set allowaccess ping fabric
      set type aggregate
      set member <interfaces>
      set lldp-reception enable
      set lldp-transmission enable
      set auto-auth-extension-device enable
      set lacp-mode static
   end
```

For this configuration to work `lacp-mode` must be set to `static`.

If you have problems with the fortilink interface, you should verify that `lacp-mode` is set to `static`. For example, if you have reset your FortiGate-6000 or 7000 to factory defaults, `lacp-mode` may get reset to `active`. If this happens, just change the setting back to `static`.

FPC failover in a standalone FortiGate-6000

A FortiGate-6000 will continue to operate even if one or more FPCs fail. If an FPC stops operating, sessions being processed by that FPC also fail. All new sessions are load balanced to the remaining FPCs. The FortiGate-6000 will continue to operate but with reduced performance because fewer FPCs are operating.

An FPC can fail because of a hardware malfunction, a software problem, or a power supply unit (PSU) failure. The FortiGate-6000 includes three hot-swappable PSUs in a 2+1 redundant configuration. At least two of the PSUs must be operating to provide power to the FortiGate-6000. If only one PSU is operating, only four of the FPCs will continue operating (usually the FPCs in slots 1 to 4). For more information about FPC failure with power loss, see AC power supply units (PSUs).

From the management board GUI dashboard, the Sensor Information dashboard widget displays information about the status of the power supplies. If all power supplies are operating, the widget displays their **Status** as **Normal**.

From the management board CLI, you can use the `execute sensor list` command to verify if the power supplies are operating. The command displays the current status of all FortiGate-6000 sensors including the power supply sensors. Power supply sensor entries should be similar to the following (shown for a FortiGate-6301E). The power supply sensor lines start with `PS{1|2|3}`:

```
65 PS1 VIN           alarm=0  value=122  threshold_status=0
66 PS1 VOUT_12V      alarm=0  value=12.032  threshold_status=0
67 PS1 Temp 1        alarm=0  value=24  threshold_status=0
68 PS1 Temp 2        alarm=0  value=36  threshold_status=0
69 PS1 Fan 1         alarm=0  value=8832  threshold_status=0
70 PS1 Status        alarm=0
71 PS2 VIN           alarm=0  value=122  threshold_status=0
72 PS2 VOUT_12V      alarm=0  value=12.032  threshold_status=0
73 PS2 Temp 1        alarm=0  value=24  threshold_status=0
74 PS2 Temp 2        alarm=0  value=37  threshold_status=0
75 PS2 Fan 1         alarm=0  value=9088  threshold_status=0
76 PS2 Status        alarm=0
77 PS3 VIN           alarm=0  value=122  threshold_status=0
78 PS3 VOUT_12V      alarm=0  value=12.032  threshold_status=0
79 PS3 Temp 1        alarm=0  value=23  threshold_status=0
80 PS3 Temp 2        alarm=0  value=37  threshold_status=0
81 PS3 Fan 1         alarm=0  value=9088  threshold_status=0
82 PS3 Status        alarm=0
```

Any non zero `alarm` or `threshold_status` values indicate a possible problem with that power supply.

If failed FPCs recover, the FortiGate-6000 will attempt to synchronize the configuration of the FPCs with the management board. If there have been few configuration changes, the failed FPCs may be able to become synchronized and operate normally. If there have been many configuration changes or a firmware upgrade, the FortiGate-6000 may not be able to re-synchronize the FPCs without administrator intervention. For example, see Synchronizing the FPCs with the management board on page 18.

You can't replace an FPC that fails because of a hardware failure. Instead, you should RMA the FortiGate-6000.

To show the status of the FPCs, use the `diagnose load-balance status` command. In the command output, if `Status Message` is `Running` the FPC is operating normally. The following example shows the status of FPCs, for a FortiGate-6301F:

```
diagnose load-balance status
===========================================================================
MBD SN: F6KF313E17900032
```

```
Primary FPC Blade: slot-2

    Slot  1: FPC6KF3E17900200
     Status:Working   Function:Active
     Link:      Base: Up          Fabric: Up
     Heartbeat: Management: Good   Data: Good
     Status Message:"Running"
   Slot  2: FPC6KF3E17900201
     Status:Working   Function:Active
     Link:      Base: Up          Fabric: Up
     Heartbeat: Management: Good   Data: Good
     Status Message:"Running"
   Slot  3: FPC6KF3E17900207
     Status:Working   Function:Active
     Link:      Base: Up          Fabric: Up
     Heartbeat: Management: Good   Data: Good
     Status Message:"Running"
   Slot  4: FPC6KF3E17900219
     Status:Working   Function:Active
     Link:      Base: Up          Fabric: Up
     Heartbeat: Management: Good   Data: Good
     Status Message:"Running"
   Slot  5: FPC6KF3E17900235
     Status:Working   Function:Active
     Link:      Base: Up          Fabric: Up
     Heartbeat: Management: Good   Data: Good
     Status Message:"Running"
   Slot  6: FPC6KF3E17900169
     Status:Working   Function:Active
     Link:      Base: Up          Fabric: Up
     Heartbeat: Management: Good   Data: Good
     Status Message:"Running"
```

FortiGate-6000 HA, FPCs, and power failure

If one or more FPCs in the primary FortiGate-6000 fails, the cluster renegotiates and the FortiGate-6000 with the most operating FPCs becomes the primary FortiGate-6000. An FPC failure can occur if an FPC shuts down due to a software crash or hardware problem, or if the FPC is manually shut down.

FPCs also shut down if two of the three FortiGate-6000 power supply units (PSUs) become disconnected from their power source. The FortiGate-6000 includes three hot-swappable PSUs in a 2+1 redundant configuration. At least two of the PSUs must be operating to provide power to the FortiGate-6000. If only one PSU is operating, only four of the FPCs will continue running (usually the FPCs in slots 1 to 4). For more information about FPC failure with power loss, see AC power supply units (PSUs).

From the management board GUI dashboard, the Sensor Information dashboard widget displays information about the status of the power supplies. If all power supplies are operating, the widget displays their **Status** as **Normal**.

From the management board CLI, you can use the `execute sensor list` command to verify if the power supplies are operating. The command displays the current status of all FortiGate-6000 sensors including the power supply sensors. Power supply sensor entries should be similar to the following (shown for a FortiGate-6301E). The power supply sensor lines start with `PS{1|2|3}`:

```
65 PS1 VIN          alarm=0  value=122  threshold_status=0
66 PS1 VOUT_12V     alarm=0  value=12.032  threshold_status=0
67 PS1 Temp 1       alarm=0  value=24  threshold_status=0
68 PS1 Temp 2       alarm=0  value=36  threshold_status=0
69 PS1 Fan 1        alarm=0  value=8832  threshold_status=0
70 PS1 Status       alarm=0
71 PS2 VIN          alarm=0  value=122  threshold_status=0
72 PS2 VOUT_12V     alarm=0  value=12.032  threshold_status=0
73 PS2 Temp 1       alarm=0  value=24  threshold_status=0
74 PS2 Temp 2       alarm=0  value=37  threshold_status=0
75 PS2 Fan 1        alarm=0  value=9088  threshold_status=0
76 PS2 Status       alarm=0
77 PS3 VIN          alarm=0  value=122  threshold_status=0
78 PS3 VOUT_12V     alarm=0  value=12.032  threshold_status=0
79 PS3 Temp 1       alarm=0  value=23  threshold_status=0
80 PS3 Temp 2       alarm=0  value=37  threshold_status=0
81 PS3 Fan 1        alarm=0  value=9088  threshold_status=0
82 PS3 Status       alarm=0
```

Any non zero `alarm` or `threshold_status` values indicate a possible problem with that power supply.

After the primary FortiGate-6000 in an HA cluster experiences an FPC failure, the cluster negotiates and the FortiGate-6000 with the most operating FPCs becomes the new primary FortiGate-6000. The new primary FortiGate-6000 sends gratuitous arp packets out all of its connected interfaces to inform attached switches to send traffic to it. Sessions then resume with the new primary FortiGate-6000.

If the secondary FortiGate-6000 experiences an FPC failure, its status in the cluster does not change. In future cluster negotiations the FortiGate-6000 with an FPC failure is less likely to become the primary FortiGate-6000.

To prevent multiple failovers, if an FPC failure occurs in an HA cluster with override enabled, you should disable override until you can fix the problems and get all the FPCs up and running and synchronized.

After an FPC failure, sessions and configuration changes are not synchronized to the failed FPCs.

If failed FPCs recover in the secondary FortiGate-6000, it will continue to operate as the secondary FortiGate-6000 and will attempt to re-synchronize the FPCs with the management board. This process may take a few minutes, but if it is successful, the secondary FortiGate-6000 can return to fully participate in the cluster.

If there have been many configuration changes, the FPCs need to be manually synchronized with the management board. Log into the CLI of each out of synch FPC and enter the `execute factoryreset` command to reset the configuration. After the FPC restarts, the management board will attempt to synchronize its configuration. If the configuration synchronization is successful, the FPC can start processing traffic again.

If there has been a firmware upgrade, and the firmware running on the failed FPC is out of date, you can upgrade the firmware of the FPC as described in the section: Installing firmware on an individual FPC on page 27.

You can optionally use the following command to make sure the sessions on the FPCs in the secondary FortiGate-6000 are synchronized with the sessions on the FPCs in the primary FortiGate-6000.

```
diagnose test application chlbd 10
```

Once all of the FPCs are operating and synchronized, the secondary FortiGate-6000 can fully participate with the cluster.

For more information about troubleshooting FPC failures, see Troubleshooting an FPC failure on page 16.

Troubleshooting an FPC failure

This section describes some steps you can use to troubleshoot an FPC failure or to help provide information about the failure to Fortinet Support.

Displaying FPC link and heartbeat status

Start by running the `diagnose load-balance status` command from the management board CLI to check the status of the FPCs. The following output shows the FPC in slot 1 operating normally and a problem with the FPC in slot 2:

```
diagnose load-balance status
==========================================================================
MBD SN: F6KF31T018900143
  Primary FPC Blade: slot-1

     Slot  1: FPC6KFT018901327
       Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
     Slot  2:
       Status:Dead      Function:Active
       Link:      Base: Up          Fabric: Down
       Heartbeat: Management: Failed Data: Failed
       Status Message:"Waiting for management heartbeat."
       ...
```

If both the base and fabric links are down

If the `diagnose load-balance status` command shows that both the base and fabric links are down, the FPC may be powered off or shut down.

1. From the management board CLI, run the `execute sensor list` command to check the status of the power supplies. Look for the `PS1`, `PS2`, and `PS3` output lines.

   For example, for PS1:

   ```
   ...
   65 PS1 VIN           alarm=0  value=122  threshold_status=0
   66 PS1 VOUT_12V      alarm=0  value=12.032  threshold_status=0
   67 PS1 Temp 1        alarm=0  value=26  threshold_status=0
   68 PS1 Temp 2        alarm=0  value=38  threshold_status=0
   69 PS1 Fan 1         alarm=0  value=8832  threshold_status=0
   70 PS1 Status        alarm=0
   ...
   ```

   If the power supplies are all OK, the output for all of the PS lines should include `Alarm=0` and `Status=0`.
2. If the command output indicates problems with the power supplies, make sure they are all connected to power.

   If they are connected, there may be a hardware problem. Contact Fortinet Support for assistance.
3. If the power supplies are connected and operating normally, set up two SSH sessions to the management board.
4. From SSH session 1, enter the following command to connect to the FPC console:

   ```
   execute system console-server connect <slot_id>
   ```

5. Press Enter to see if there is any response.
6. From SSH session 2, use the following commands to power the FPC off and back on:
   ```
   execute load-balance slot power-off <slot_id>
   execute load-balance slot power-on <slot_id>
   ```
7. From SSH session1, check to see if the FPC starts up normally after running the `power-on` command.
8. If SSH session 1 shows the FPC starting up, when it has fully started, use the `get system status` command to compare the FPC and management board FortiOS versions.

   If the versions don't match, see Updating FPC firmware to match the management board on page 18
9. If the FPC doesn't start up there may be a hardware problem, contact Fortinet Support for assistance.

If only one link is down

If the base or fabric link is up, then check the Heartbeat line of the `diagnose load-balance status` output. The following conditions on the FPC can cause the management heartbeat to fail:

- The FPC did not start up correctly.
- The FPC software may have stopped operating because a process has stopped.
- The FPC may have experienced a kernel panic.
- The FPC may have experienced a daemon or processes panic.

To get more information about the cause:

1. Set up two SSH sessions to the management board.
2. From SSH session 1, enter the following command to connect to the FPC console:
   ```
   execute system console-server connect <slot_id>
   ```
3. Press Enter to see if there is any response.
4. If there is a response to SSH session 1 and if you can log into the FPC from SSH session 1:
   a. Dump the crash log by entering:
      ```
      diagnose debug crashlog read
      ```
   b. Use the `get system status` command to compare the FPC and management board FortiOS versions.

      If the versions don't match, see Updating FPC firmware to match the management board on page 18.
5. If there is no response to SSH session1, or if you cannot log into the FPC from SSH session 1, switch to SSH session 2.
   a. From SSH session 2, run the NMI reset command:
      ```
      execute load-balance slot nmi-reset <slot_id>
      ```
   b. From SSH session 1, check to see if any messages appear.
   c. If a kernel panic stack trace is displayed, save it.

      The FPC should automatically reboot after displaying the stack trace.
   d. If nothing happens on SSH session 1, go back to SSH session 2, and run the following commands to power off and power on the FPC:
      ```
      execute load-balance slot power-off <slot_id>
      execute load-balance slot power-on <slot_id>
      ```
   e. If SSH session 1 shows the FPC starting up, when it has fully started, use the `get system status` command to compare the FPC and management board FortiOS versions.

      If the versions don't match, see Updating FPC firmware to match the management board on page 18.
   f. If the versions match, start an SSH session to log into the FPC, and dump the comlog by entering:
      ```
      diagnose debug comlog read
      ```

If the comlog was not enabled, it will be empty.

g. Also dump the crash log if you haven't been able to do so by entering:

```
diagnose debug crashlog read
```

h. Contact Fortinet Support for assistance.

If requested you can provide the comlog and crashlog to help determine the cause of the problem.

Updating FPC firmware to match the management board

Use the following steps to update the firmware running on the FPC to match the firmware running on the management board.

1. Obtain a FortiGate-6000 firmware image file that matches the version running on the management board and add it to an FTP or TFTP server or a to USB key.
2. Use the following command to upload the firmware image file to the internal FortiGate-6000 TFTP server:
   ```
   execute upload image {ftp | tftp | usb}
   ```
3. Then from management board CLI, use the following command to upgrade the firmware running on the FPC:
   ```
   execute load-balance update image <slot_id>
   ```
4. After the firmware has upgraded, use `get system status` on the FPC to confirm it is running the same firmware version as the management board.

Troubleshooting configuration synchronization issues

After confirming that the management board and the FPC are running the same firmware build, use the following command to determine if configuration synchronization errors remain:

```
diagnose sys confsync status
```

In the command output, `in_sync=1` means the FPC is synchronized and can operate normally, `in_sync=0` means the FPC is not synchronized. If the FPC is up but not synchronized, see Troubleshooting Tip: FortiGate 7000 Series blade config synchronization issues (confsync) for help troubleshooting configuration synchronization issues.

Synchronizing the FPCs with the management board

After you install firmware on the management board from the BIOS after a reboot, the firmware version and configuration of the management board will most likely not be synchronized with the FPCs. You can verify this from the management board CLI using the `diagnose sys confsync status | grep in_sy` command. The `in_sync=0` entries in the following example output for a FortiGate-6301F show that the management board (serial number ending in 143) is not synchronized with the FPCs.

```
diagnose sys confsync status | grep in_sy
FPC6KFT018901327, Secondary, uptime=59.44, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901372, Secondary, uptime=58.48, priority=20, slot_id=1:2, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901346, Secondary, uptime=58.44, priority=21, slot_id=1:3, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901574, Secondary, uptime=58.43, priority=22, slot_id=1:4, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901345, Secondary, uptime=57.40, priority=23, slot_id=1:5, idx=1, flag=0x4, in_sync=0
```

```
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901556, Secondary, uptime=58.43, priority=24, slot_id=1:6, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901327, Secondary, uptime=59.44, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=0
FPC6KFT018901345, Secondary, uptime=57.40, priority=23, slot_id=1:5, idx=2, flag=0x4, in_sync=0
FPC6KFT018901346, Secondary, uptime=58.44, priority=21, slot_id=1:3, idx=3, flag=0x4, in_sync=0
FPC6KFT018901372, Secondary, uptime=58.48, priority=20, slot_id=1:2, idx=4, flag=0x4, in_sync=0
FPC6KFT018901556, Secondary, uptime=58.43, priority=24, slot_id=1:6, idx=5, flag=0x4, in_sync=0
FPC6KFT018901574, Secondary, uptime=58.43, priority=22, slot_id=1:4, idx=6, flag=0x4, in_sync=0
```

You can also verify the synchronization status from the management board Configuration Sync Monitor.

To re-synchronize the FortiGate-6000, which has the effect of resetting all of the FPCs, re-install firmware on the management board.

You can also manually install firmware on each FPC from the BIOS after a reboot. This multi-step manual process is just as effective as installing the firmware for a second time on the management board to trigger synchronization to the FPCs, but takes much longer.

1. Log in to the management board GUI.
2. Install a firmware build on the management board from the GUI or CLI. The firmware build you install on the management board can either be the same firmware build or a different one.

   Installing firmware synchronizes the firmware build and configuration from the management board to the FPCs.
3. Check the synchronization status from the Configuration Sync Monitor or using the `diagnose sys confsync status | grep in_sy` command. The following example FortiGate-6301F output shows that the management board is synchronized with all of the FPCs because each line includes `in_sync=1`.

```
diagnose sys confsync status | grep in_sy
FPC6KFT018901327, Secondary, uptime=3773.96, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=1
F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901372, Secondary, uptime=3774.26, priority=20, slot_id=1:2, idx=1, flag=0x4, in_sync=1
F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901346, Secondary, uptime=3774.68, priority=21, slot_id=1:3, idx=1, flag=0x4, in_sync=1
F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901574, Secondary, uptime=3774.19, priority=22, slot_id=1:4, idx=1, flag=0x4, in_sync=1
F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901345, Secondary, uptime=3773.59, priority=23, slot_id=1:5, idx=1, flag=0x4, in_sync=1
F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901556, Secondary, uptime=3774.82, priority=24, slot_id=1:6, idx=1, flag=0x4, in_sync=1
F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901327, Secondary, uptime=3773.96, priority=19, slot_id=1:1, idx=1, flag=0x24, in_sync=1
FPC6KFT018901345, Secondary, uptime=3773.59, priority=23, slot_id=1:5, idx=2, flag=0x24, in_sync=1
FPC6KFT018901346, Secondary, uptime=3774.68, priority=21, slot_id=1:3, idx=3, flag=0x24, in_sync=1
FPC6KFT018901372, Secondary, uptime=3774.26, priority=20, slot_id=1:2, idx=4, flag=0x24, in_sync=1
FPC6KFT018901556, Secondary, uptime=3774.82, priority=24, slot_id=1:6, idx=5, flag=0x24, in_sync=1
FPC6KFT018901574, Secondary, uptime=3774.19, priority=22, slot_id=1:4, idx=6, flag=0x24, in_sync=1
```

More management connections than expected for one device

The FortiGate-6000 and 7000 may show more management-related network activity than most FortiGate devices. This occurs because many management functions are handled independently by each FortiGate-6000 management board and individual FPCs and by each FortiGate-7000 FIM and FPM.

For example, when a FortiGate-6000 first starts up, the management board and all of the FPCs perform their DNS lookups. Resulting in more DNS-related traffic during startup than expected for a single device. Once the system is processing data traffic, the amount of management traffic would be proportional to the amount of traffic the system is processing.

More ARP queries than expected for one device - potential issue on large WiFi networks

The FortiGate-6000 and 7000 sends more ARP queries than expected because each FPC and FPM builds its own ARP table to be able to communicate with devices in the same broadcast domain or layer 2 network. This behavior does not cause a problem with most layer 2 networks. However, because the ARP traffic for all of the FPCs or FPMs comes from the same mac and IP address, on networks with broadcast filtering or ARP suppression, some of the FortiGate-6000 or 7000 ARP queries and replies may be suppressed. If this happens, FPCs or FPMs may not be able to build complete ARP tables. An FPC or FPM with an incomplete ARP table will not be able to forward sessions to some destinations that it should be able to reach, resulting in dropped sessions.

Broadcast filtering or ARP suppression is commonly used on large WiFi networks to control the amount of ARP traffic on the WiFi network. Dropped FortiGate-6000 or 7000 sessions have been seen when a FortiGate-6000 or 7000 is connected to the same broadcast domain as a large WiFi network with ARP suppression.

To resolve this dropped session issue, you can remove broadcast filtering or ARP suppression from the network. If this is not an option, Fortinet recommends that you install a layer 3 device to separate the FortiGate-6000 or 7000 from the WiFi network broadcast domain. ARP traffic is reduced because the FPCs or FPMs no longer need to add the addresses of all of the WiFi devices to their ARP tables since they are on a different broadcast domain. The FPCs or FPMs just need to add the address of the layer 3 device.

FGCP HA and VDOM mode

To successfully form an FGCP HA cluster, both FortiGate-6000s or 7000s must be operating in the same VDOM mode (Multi or Split-Task). You can change the VDOM mode after the cluster has formed.

Resolving FIM or FPM boot device I/O errors

If an FIM or FPM has boot device I/O errors, messages similar to the following appear during console sessions with the module:

```
EXT2-fs (sda1): previous I/O error to superblock detected
```

```
EXT2-fs (sda3): previous I/O error to superblock detected
```

If you see boot device I/O errors similar to these, you should contact Fortinet Support (https://support.fortinet.com) for assistance with finding the underlying cause of these errors.

Once the underlying cause is determined and resolved, you use BIOS commands to reformat and restore the affected boot device as described in the following sections.

Formatting an FIM boot device and installing new firmware

You can use the following steps to format an FIM boot device and install new firmware from a TFTP server.

1. Set up a TFTP server and copy the firmware file to the TFTP server default folder.
2. Set up your network to allow traffic between the TFTP server and one of the FIM MGMT interfaces.
3. Using the console cable supplied with your FortiGate-7000, connect the SMM Console 1 port on the FortiGate-7000 to the USB port on your management computer.
4. Start a terminal emulation program on the management computer. Use these settings:

   Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.
5. Press Ctrl-T to enter console switch mode.
6. Repeat pressing Ctrl-T until you have connected to the FIM to be updated. Example prompt for the FIM in slot 2:
   `<Switching to Console: FIM02 (9600)>`
7. Optionally log in to the FIM's CLI.
8. Reboot the FIM.

   You can do this using the `execute reboot` command from the CLI or by pressing the power switch on the FIM front panel.
9. When the FIM starts up, follow the boot process in the terminal session, and press any key when prompted to interrupt the boot process.
10. To format the FIM boot disk, press F.
11. Press Y to confirm that you want to erase all data on the boot disk and format it.

    When the formatting is complete the FIM restarts.
12. Follow the boot process in the terminal session, and press any key when prompted to interrupt the boot process.
13. To set up the TFTP configuration, press C.
14. Use the BIOS menu to set the following. Change settings only if required.

    `[P]: Set image download port`: MGMT1 (the connected MGMT interface.)

    `[D]: Set DHCP mode`: Disabled

    `[I]: Set local IP address`: The IP address of the MGMT interface that you want to use to connect to the TFTP server. This address must not be the same as the FortiGate-7000 management IP address and cannot conflict with other addresses on your network.

    `[S]: Set local Subnet Mask`: Set as required for your network.

    `[G]: Set local gateway`: Set as required for your network.

    `[V]: Local VLAN ID`: Should be set to `<none>`. (use -1 to set the Local VLAN ID to `<none>`.)

    `[T]: Set remote TFTP server IP address`: The IP address of the TFTP server.

    `[F]: Set firmware image file name`: The name of the firmware image file that you want to install.
15. To quit this menu, press Q.
16. To review the configuration, press R.
    To make corrections, press C and make the changes as required. When the configuration is correct, proceed to the

next step.

17. To start the TFTP transfer, press T.

    The firmware image is uploaded from the TFTP server and installed on the FIM. The FIM then restarts with its configuration reset to factory defaults. After restarting, the FIM configuration is synchronized to match the configuration of the primary FIM. The FIM restarts again and can start processing traffic.

18. Once the FIM restarts, verify that the correct firmware is installed.

    You can do this from the FIM GUI dashboard or from the FPM CLI using the `get system status` command.

19. Enter the `diagnose sys confsync status | grep in_sy` command to verify that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

    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.

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

Formatting an FPM boot device and installing new firmware

You can use the following steps to format an FPM boot device and install new firmware from a TFTP server.

1. Set up a TFTP server and copy the firmware file into the TFTP server default folder.
2. Log into to the primary FIM CLI and enter the following command:

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

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

3. Set up your network to allow traffic between the TFTP server and a MGMT interface of one of the FIMs.

   You can use any MGMT interface of either of the FIMs. When you set up the FPM TFTP settings below, you select the FIM that can connect to the TFTP server. If the MGMT interface you are using is one of the MGMT interfaces connected as a LAG to a switch, you must shutdown or disconnect all of the other interfaces that are part of the LAG from the switch. This includes MGMT interfaces from both FIMs

4. Using the console cable supplied with your FortiGate-7000, connect the SMM Console 1 port on the FortiGate-7000 to the USB port on your management computer.
5. Start a terminal emulation program on the management computer. Use these settings:

   Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.

6. Press Ctrl-T to enter console switch mode.
7. Repeat pressing Ctrl-T until you have connected to the module to be updated. Example prompt:

```
<Switching to Console: FPM03 (9600)>
```

8. Optionally log into the FPM's CLI.
9. Reboot the FPM.

   You can do this using the `execute reboot` command from the FPM's CLI or by pressing the power switch on the FPM front panel.

10. When the FPM starts up, follow the boot process in the terminal session and press any key when prompted to interrupt the boot process.
11. To format the FPM boot disk, press F.
12. Press Y to confirm that you want to erase all data on the boot disk and format it.

    When the formatting is complete the FPM restarts.

13. Follow the boot process in the terminal session, and press any key when prompted to interrupt the boot process.
14. To set up the TFTP configuration, press C.
15. Use the BIOS menu to set the following. Change settings only if required.

    `[P]: Set image download port`: FIM01 (the FIM that can communicate with the TFTP server).

    `[D]: Set DHCP mode`: Disabled.

    `[I]: Set local IP address`: The IP address of the MGMT interface of the selected FIM that you want to use to connect to the TFTP server. This address must not be the same as the FortiGate-7000 management IP address and cannot conflict with other addresses on your network.

    `[S]: Set local Subnet Mask`: Set as required for your network.

    `[G]: Set local gateway`: Set as required for your network.

    `[V]: Local VLAN ID`: Should be set to `<none>`. (use -1 to set the Local VLAN ID to `<none>`.)

    `[T]: Set remote TFTP server IP address`: The IP address of the TFTP server.

    `[F]: Set firmware image file name`: The name of the firmware image file that you want to install.
16. To quit this menu, press Q.
17. To review the configuration, press R.

    To make corrections, press C and make the changes as required. When the configuration is correct proceed to the next step.
18. To start the TFTP transfer, press T.

    The firmware image is uploaded from the TFTP server and installed on the FPM. The FPM then restarts with its configuration reset to factory defaults. After restarting, the FPM configuration is synchronized to match the configuration of the primary FPM. The FPM restarts again and can start processing traffic.
19. Once the FPM restarts, verify that the correct firmware is installed.

    You can do this from the FPM GUI dashboard or from the FPM CLI using the `get system status` command.
20. Enter the `diagnose sys confsync status | grep in_sy` command to verify that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

    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.

    If you enter the `diagnose sys confsync status | grep in_sy` command before the FPM has restarted, it will not appear in the command output. As well, the Configuration Sync Monitor will temporarily show that it is not synchronized.
21. 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.

Before downgrading from FortiOS 6.4.8 remove virtual clustering

If you are operating a FortiGate-6000 or 7000 system running FortiOS 6.4.8 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
```

Adding flow rules 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 (the following example uses `edit 0` to add the DHCP relay flow using the next available flow rule index number):

```
config load-balance flow-rule
  edit 0
    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
```

The default configuration also includes the following flow rules for IPv6 DHCP traffic:

```
   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
```

These flow rules handle traffic when the IPv6 DHCP client sends requests to a DHCP server using port 547 and the DHCP server responds using port 546. 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 547. If this DHCP relay traffic passes through the FortiGate-7000 you must add a flow rule similar to the following to support port 547 DHCP traffic in both directions (the following example uses `edit 0` to add the DHCP relay flow using the next available flow rule index number):

```
config load-balance flow-rule
  edit 0
    set status enable
    set vlan 0
    set ether-type ipv6
    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 547-547
    set dst-l4port 547-547
    set action forward
    set forward-slot master
    set priority 5
    set comment "dhcpv6 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 rebootor detailed procedures for upgrading FortiGate-6000 firmware from the BIOS.

Installing firmware on an individual 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, Secondary, uptime=615368.33, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=1
   F6KF31T018900143, Primary, uptime=615425.84, priority=1, slot_id=1:0, idx=0, flag=0x10, in_sync=1
   FPC6KFT018901372, Secondary, uptime=615319.63, priority=20, slot_id=1:2, idx=1, flag=0x4, in_sync=1
   F6KF31T018900143, Primary, uptime=615425.84, priority=1, slot_id=1:0, idx=0, flag=0x10, in_sync=1
   FPC6KFT018901346, Secondary, 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 individual FIMs or FPMs

You can install firmware on individual FIMs or FPMs by logging into the FIM or FPM GUI or CLI. You can also setup a console connection to the FortiGate-7000 front panel SMM and install firmware on individual FIMs or FPMs from a TFTP server after interrupting the FIM or FPM boot up sequence from the BIOS.

Normally you wouldn't need to upgrade the firmware on individual FIMs or FPMs because the FortiGate-7000 keeps the firmware on all of the FIMs and FPMs synchronized. However, FIM or FPM firmware may go out of sync in the following situations:

- Communication issues during a normal FortiGate-7000 firmware upgrade.
- Installing a replacement FIM or FPM that is running a different firmware version.
- Installing firmware on or formatting an FIM or FPM from the BIOS.

To verify the firmware versions on each FIM or FPM you can check individual FIM and FPM GUIs or enter the `get system status` command from each FIM or FPM CLI. You can also use the `diagnose sys confsync status | grep in_sy` command to see if the FIMs and FPMs are all synchronized. In the command output, `in_sync=1` means the FIM or FPM is synchronized. `In_sync=0` means the FIM or FPM is not synchronized, which could indicated the FIM or FPM is running a different firmware build than the primary FIM.

The procedures in this section work for FIMs or FPMs in a standalone FortiGate-7000. These procedures also work for FIMs or FPMs in the primary FortiGate-7000 in an HA configuration. To upgrade firmware on an FIM or FPM in the secondary FortiGate-7000 in an HA configuration, you should either remove the secondary FortiGate-7000 from the HA configuration or cause a failover so that the secondary FortiGate-7000 becomes the primary FortiGate-7000.

In general, if you need to update both FIMs and FPMs in the same FortiGate-7000, you should update the FIMs first as the FPMs can only communicate through FIM interfaces.

Upgrading the firmware on an individual FIM

During the upgrade, the FIM will not be able to process traffic. However, the other FIM and the FPMs should continue to operate normally.

To upgrade the firmware on a individual FIM from the GUI

1. Connect to the FIM GUI using the SLBC management IP address and the special management port number for that FIM. For example, for the FIM in slot 2, browse to https://<SLBC-management-ip>:44302.
2. Start a normal firmware upgrade. For example,
   a. Go to **System > Firmware** and select **Browse** to select the firmware file to install.
   b. Follow the prompts to select the firmware file, save the configuration, and upload the firmware file to the FPM.
3. After the FIM restarts, verify that the new firmware has been installed.

   You can do this from the FIM GUI dashboard or from the FIM CLI using the `get system status` command.
4. Use the `diagnose sys confsync status | grep in_sy` command to verify that the configuration of the FIM has been synchronized. The field `in_sync=1` indicates that the configurations of that FIM or FPM is synchronized.

   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.

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.

To upgrade the firmware on a individual FIM from the CLI using TFTP

1. Put a copy of the firmware file on a TFTP server that is accessible from the SLBC management interface.
2. Connect to the FIM CLI by using an SSH client. For example, to connect to the CLI of the FIM in slot 2, connect to <SLBC-management-ip>:2201.
3. Enter the following command to upload the firmware file to the FIM:

   ```
   execute upload image tftp <firmware-filename> comment <tftp-server-ip-address>
   ```
4. After the FIM restarts, verify that the new firmware has been installed.

   You can do this from the FIM GUI dashboard or from the FIM CLI using the `get system status` command.
5. Use the `diagnose sys confsync status | grep in_sy` command to verify that the configuration of the FIM has been synchronized. The field `in_sync=1` indicates that the configurations of that FIM or FPM is synchronized.

   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.

   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.

Upgrading the firmware on an individual 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 slot containing the FPM to be upgraded.
2. Log in to the FPM GUI or CLI using its special port number.

   To upgrade the firmware on the FPM in slot 3 from the GUI:

   a. Connect to the FPM GUI by browsing to https://<SLBC-management-ip>:44303.

   b. Go to **System > Firmware** and select **Browse** to select the firmware file to install.

   c. Follow the prompts to select the firmware file, save the configuration, and upload the firmware file to the FPM.

   To upgrade the firmware on an FPM from the CLI using TFTP see Installing FPM firmware from the BIOS after a reboot.
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. Use the diagnose sys confsync status | grep in_sy to verify that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of that FIM or FPM is synchronized.

   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.

   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.

IPsec VPN notes and limitations

FortiGate-6000 and 7000 for FortiOS 6.4.8 FortiOS 6.2.7 supports the following features for IPsec VPN tunnels terminated by the FortiGate:

- Interface-based IPsec VPN (also called route-based IPsec VPN) is supported. Policy-based IPsec VPN is not supported.
- Static and dynamic routing (BGP, OSPF, and RIP) over IPsec VPN tunnels is supported.
- The FortiGate-6000 and 7000 use load balancing to select an FPC or FPM to terminate traffic for a new tunnel instance and all traffic for that tunnel instance is terminated on the same FPC or FPM. You can optionally use the IPsec tunnel phase 1 configuration to select a specific FPC or FPM to terminate all tunnel instances started by that phase 1.
- When an IPsec VPN tunnel is initialized, the SA is synchronized to all FPCs or FPMs in the FortiGate-6000 or 7000, or in both FortiGate-6000s and 7000s in an HA configuration.
- Site-to-Site IPsec VPN is supported.
- Dialup IPsec VPN is supported. The FortiGate-6000 or 7000 can be the dialup server or client.
- Policy routes cannot be used for communication over IPsec VPN tunnels.
- VRF routes cannot be used for communication over IPsec VPN tunnels.
- IPv6 clear-text traffic (IPv6 over IPv4 or IPv6 over IPv6) is not supported.
- IPsec SA synchronization between HA peers is supported.
- 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.

SSL VPN configuration with SSL VPN load balancing disabled

If you are not using SSL VPN load balancing (see SSL VPN tunnel mode load balancing on page 7), using a FortiGate-6000 or 7000 as an SSL VPN server requires you to manually add an SSL VPN load balancing flow rule to configure the FortiGate-6000 or 7000 to send all SSL VPN sessions to the primary FPC (FortiGate-6000) or the primary FPM (FortiGate-7000). To match SSL VPN server traffic, the flow 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"
   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 or FPM. 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 or FPM.

As a best practice, if you add a flow rule for SSL VPN, Fortinet recommends using a custom SSL VPN port (for example, 10443 instead of 443). This can improve performance by allowing SSL traffic on port 443 that is not part of your SSL VPN to be load balanced to FPCs or FPMs instead of being sent to the primary FPC or FPM by the SSL VPN flow rule.

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:

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

You can also make the SSL VPN flow rule more specific by including the SSL VPN server interface in the flow rule. For example, if your FortiGate-6000 or 7000 listens for SSL VPN sessions on the port12 interface:

```
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 also 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:

```
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 6.4.8 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-7000E HA heartbeat switch configuration

FortiGate-7000E for FortiOS 6.4.8 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-7000E 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-7000Es 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-6000F, 7000E, and 7000F for FortiOS 6.4.8 have the same default flow rules with one exception.

The FortiGate-6000F and 7000E include the following flow rule:

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

For the FortiGate-7000F, the corresponding flow rule is:

```
config load-balance flow-rule
    edit 20
        set status enable
        set vlan 0
        set ether-type ip
        set protocol vrrp
        set action forward
        set forward-slot master
        set priority 6
        set comment "vrrp to primary blade"
    next
end
```

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 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 primary 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 primary 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 primary 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 System Information dashboard widget also shows the host name and serial number. 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 | set-primary-worker}
     <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 SLBC management interface IP address with a special port number.

You use the following command to configure the SLBC management interface:

```
config global
   config load-balance setting
      set slbc-mgmt-intf <interface>
   end
```

Where <interface> becomes the SLBC management interface.

To enable using the special management port numbers to connect to individual FIMs and FPMs, the SLBC management 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 SLBC management interface with an invalid IP address, or disable management or administrative access for the SLBC management interface.

You can connect to the GUI of CLI of individual FIMs or FPMs using the SLBC management interface IP address followed by a special port number. For example, if the SLBC management interface IP address is 192.168.1.99, to connect to the GUI of the FPM in slot 3, browse to:

```
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.

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 FIM or FPM you have logged into, the GUI header banner and the CLI prompt shows its hostname. The System Information dashboard widget also shows the host name and serial number. The CLI prompt also shows the slot address in the format `<hostname> [<slot address>] #`.

Logging in to different FIMs or FPMs allows you to use dashboard widgets, FortiView, or Monitor GUI pages to view the activity of that FIM or FPM. 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.

FortiGate-7000 special management port numbers (slot numbers in order as installed in the chassis)

Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
11	FPM11	8011	44311	2311	2211	16111
9	FPM09	8009	44309	2309	2209	16109
7	FPM07	8007	44307	2307	2207	16107
5	FPM05	8005	44305	2305	2205	16105
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
8	FPM08	8008	44308	2308	2208	16108
10	FPM10	8010	44310	2310	2210	16110
12	FPM12	8012	44312	2312	2212	16112

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 11	FPM11	8011	44311	2311	2211	16111
Ch1 slot 9	FPM09	8009	44309	2309	2209	16109
Ch1 slot 7	FPM07	8007	44307	2307	2207	16107
Ch1 slot 5	FPM05	8005	44305	2305	2205	16105

Chassis and Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Ch1 slot 3	FPM03	8003	44303	2303	2203	16103
Ch1 slot 1	FIM01	8001	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
Ch1 slot 8	FPM08	8008	44308	2308	2208	16108
Ch1 slot 10	FPM10	8010	44310	2310	2210	16110
Ch1 slot 12	FPM12	8012	44312	2312	2212	16112
Ch2 slot 11	FPM11	8031	44331	2331	2231	16131
Ch2 slot 9	FPM09	8029	44329	2329	2229	16129
Ch2 slot 7	FPM07	8027	44327	2327	2227	16127
Ch2 slot 5	FPM05	8025	44325	2325	2225	16125
Ch2 slot 3	FPM03	8023	44323	2323	2223	16123
Ch2 slot 1	FIM01	8021	44321	2321	2221	16121
Ch2 slot 2	FIM02	8022	44322	2322	2222	16122
Ch2 slot 4	FPM04	8024	44324	2324	2224	16124
Ch2 slot 6	FPM06	8026	44326	2326	2226	16126
Ch2 slot 8	FPM08	8028	44328	2328	2228	16128
Ch2 slot 10	FPM10	8030	44330	2330	2230	16130
Ch2 slot 12	FPM12	8032	44332	2332	2232	16132

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 6.4.8 release notes.

You can find the FortiGate-6000 and 7000 for FortiOS 6.4.8 firmware images on the Fortinet Support Download Firmware Images page by selecting the **FortiGate-6K7K** product.

HA graceful upgrade to FortiOS 6.4.8

Use the following steps to upgrade a FortiGate-6000 or 7000 HA cluster with `uninterruptible-upgrade` enabled from FortiOS 6.2.9 build 1206 or 6.4.6 build 1783 to FortiOS 6.4.8 Build 1823.

You cannot use the information in this section to upgrade a FortiGate-7121F from FortiOS 6.4.6 build 1783 to FortiOS 6.4.8 Build 1823. Instead, see the section, Upgrading a FortiGate-7121F from FortiOS 6.4.6 to 6.4.8 on page 53.

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 6.2.9 or 6.4.6 to FortiOS 6.4.8:

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 6.4.8 firmware for FortiGate-6000 or 7000 from the https://support.fortinet.com FortiGate-6K7K 6.4.8 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 a FortiGate-6301F:

```
get system status
Version: FortiGate-6301F v6.4.8,build1823,220216(GA)
...
```

Upgrading a FortiGate-7121F from FortiOS 6.4.6 to 6.4.8

Use the following information to upgrade a standalone FortiGate-7121F or a FortiGate-7121F FGCP HA cluster from 6.4.6 build 1783 to FortiOS 6.4.8 Build 1823.

FortiOS 6.4.8 increases the FortiGate-7121F boot partition size. This change allows the FortiGate-7121F to support larger more complex configurations that include more VDOMs and firewall policies. Because of the boot partition size increase, the process of upgrading from a FortiGate-7121F from 6.4.6 build 1783 to 6.4.8 Build 1823 is a manual process that will take longer than normal and during this time the FortiGate-7121F will not be able to process traffic.

As well, graceful upgrade from 6.4.6 build 1783 to FortiOS 6.4.8 is not supported for a FortiGate-7121F FGCP cluster. Instead you must change the FortiGate-7121Fs to operate as standalone FortiGates and upgrade each one separately before reforming the cluster.

You can use a normal firmware upgrade procedure to upgrade a FortiGate-7121F from FortiOS 6.2.9 build 1206 to FortiOS 6.4.8 Build 1823 because the partition size was increased for FortiOS 6.2.9.

The following procedure describes how to power down the FIMs and FPMs, install a special firmware image on each FIM, upload the special firmware image file to the TFTP server of the FIM in slot 1, and then install this firmware image on each FPM. Once both FIMs and all FPMs are running the special firmware image, you can use a normal firmware upgrade procedure to upgrade the FortiGate-7121F firmware to FortiOS 6.4.8 Build 1823

Contact Fortinet Technical Support by logging to https://support.fortinet.com for assistance with upgrading your FortiGate-7121F to FortiOS 6.4.8 . The support team can supply you with the special firmware image file and assist with the following procedures.

The following procedures use the FortiGate-7121F system management module (SMM) console ports. For information about how to connect to and use these console ports, see Using the FortiGate-7121F SMM console ports.

If you are operating a FortiGate-7121F FGCP HA cluster where the boot partition size of one of the FortiGate-7121Fs has been increased but one hasn't, you can use the following steps to increase the boot partition of just one of the FortiGate-7121Fs. The remaining FortiGate-7121F can continue to process traffic:

1. Back up the configuration of the FortiGate-7121F that does not have the increased boot partition.
2. Run the `execute factoryreset` command from the CLI of the primary FIM to reset all of the FIMs and FPMs to factory defaults.
3. Configure the mgmt interface of the FortiGate-7121F to be able to connect to the TFTP server and use the procedures below to increase the boot partition size and upgrade to 6.4.8.
4. Then, when you restore the configuration of the FortiGate-7121F it will re-join the cluster.

Installing the special firmware image on the FIMs

1. Set up a TFTP server that can communicate with the 1-mgmt1 interface and upload the special FortiGate-7000F firmware build **(file name: FGT_7000F-v6-build8176-FORTINET.out**) to the TFTP server.
2. Connect to one of the FortiGate-7121F system management module (SMM) console ports.

   You can also use SSH to connect to the SMM MGMT interface.
3. From the SMM console or SSH connection, connect to the FortiOS CLI of the FIM in slot 1.

   Press Ctrl-T to enter console mode. Repeat pressing Ctrl-T until you connect to slot 1. Example prompt:
   ```
   <Switching to Console: FIM01 (9600)>
   ```
4. Enter the command `execute shutdown` to power off all of the FIMs and FPMs in the chassis.

   The FIMs and FPMs take a few minutes to shut down.
5. Power off all FIMs and FPMs using the `fru deactivate <slot>` command, for example:

   From the SMC SDI CLI you can use the following command to power off the FIM in slot 1:
   ```
   fru deactivate 1
   ```
   From the SMC SDI CLI you can use the following command to power off the FPM in slot 3:
   ```
   fru deactivate 3
   ```
6. Use the following command to power on the FIM in slot 1
   ```
   fru activate 1
   ```
7. While the FIM is starting, interrupt the start process by pressing any key.

   If the FIM has already started, you can run the `execute reboot` command to restart it.
8. From the BIOS, press `F` to format the flash.
9. From the BIOS, upload the special firmware image from the TFTP server.

   See Installing FIM firmware from the BIOS after a reboot for more information.
10. Press Ctrl-T to enter console mode.
11. Repeat pressing Ctrl-T to connect to the FortiOS CLI of the FIM in slot 2.
12. Use the following command to power on the FIM in slot 2:
    ```
    fru activate 2
    ```
13. Starting from step 7, repeat the previous steps to interrupt the start process by pressing any key and install the special firmware build on the FIM in slot 2.

Installing the special firmware image on the FPMs

1. Make sure the 1-mgmt1 interface of the FIM in slot 1 can connect to the TFTP server.

   To do this you may need to add an IP address for the 1-mgmt-1 interface and a default route for the mgmt-vdom VDOM.
2. Upload the special firmware image file to the TFTP server running on the FIM in slot 1.

   To do this, from the FortiOS CLI of the FIM in slot 1, enter:
   ```
   execute upload image tftp <image-file> comment <tftp-server-ip-address>
   ```
3. For the CLI of the FIM in slot 1, use the following command to verify that the firmware image has been uploaded to the TFTP server of the FIM in slot 1:
   ```
   fnsysctl ls -l /data2/tftproot
      -rw-r--r-- 1 0 0 Mon Nov 22 15:40:38 2021 79259649 image.out
      -rw-r--r-- 1 0 0 Mon Nov 22 15:35:57 2021 1 miglogdisk_info
   ```
   In the above example output, `image.out` is the firmware image to be installed on each FPM.
4. From the SMM console connection, press Ctrl-T until you can connect to the FPM in slot 3.

5. From the SMC SDI CLI, use the following command to power on the FPM in slot 3:

   ```
   fru activate 3
   ```

6. While the FPM is starting, interrupt the start process by pressing any key.

   If the FPM has already started, you can run the `execute reboot` command to restart it.

7. From the BIOS, press `F` to format the flash.
8. From the BIOS, press `C` to configure TFTP parameters, and use the following settings to upload the firmware image from the TFTP server of the FIM in slot 1:

   ```
   Image download port:    FIM01 TFTP Server
   DHCP status:            disabled
   Local VLAN ID:          none
   Local IP address:       169.254.254.3
   Local subnet mask:      255.255.255.0
   Local gateway:          10.160.62.1
   TFTP server IP address: 169.254.254.1
   Firmware file name:     image.out
   ```

   The `Local IP address` is `169.254.254.<slot>`, where `<slot>` is the slot number.

   `Firmware file name` the file name is `image.out`.

9. From the BIOS, press `T` to start the TFTP transfer.

   The firmware image file is uploaded to the FPM.

10. From the BIOS, press `D` to install the image as the default firmware image.

    The FPM installs the firmware image and restarts.

11. Repeat these steps for each FPM.

Installing FortiOS 6.4.8 Build 1823 firmware

Once all of the FIMs and FPMs are running the special firmware build, use a normal firmware upgrade procedure to upgrade the FortiGate-7121F firmware to FortiOS 6.4.8 Build 1823.

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.

Upgrading the firmware of a standalone FortiGate-6000, or FortiGate-6000 HA cluster with `uninterruptible-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.

Upgrading the firmware of a standalone FortiGate-7000, or FortiGate-7000 HA cluster with `uninterruptible-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.

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, 7000E, and 7000F for FortiOS 6.4.8 Build 1823 product integration and support information. The Product integration and support information described in the FortiOS 6.4.8 release notes also applies to FortiGate-6000, 7000E, and 7000F for FortiOS 6.4.8 Build 1823.

FortiGate-6000, 7000E, and 7000F for FortiOS 6.4.8 Build 1823 require the following or newer versions of FortiManager and FortiAnalyzer:

- FortiGate-6000: FortiManager or FortiAnalyzer 6.4.8, 7.0.4, and 7.2.1.
- FortiGate-7000E and 7000F: FortiManager or FortiAnalyzer 6.4.8, 7.0.4, and 7.2.1.

FortiGate-6000 6.4.8 special features and limitations

FortiGate-6000 for FortiOS 6.4.8 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-6000 v6.4.8 section of the FortiGate-6000 handbook.

FortiGate-7000E 6.4.8 special features and limitations

FortiGate-7000E for FortiOS 6.4.8 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000E v6.4.8 section of the FortiGate-7000E handbook.

FortiGate-7000F 6.4.8 special features and limitations

FortiGate-7000F for FortiOS 6.4.8 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000F v6.4.6 section of the FortiGate-7000F handbook.

Maximum values

Maximum values for FortiGate-6000 and FortiGate-7000 for FortiOS 6.4.8 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 6.4.8 Build 1823. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 6.4.8 release notes also apply to FortiGate-6000 and 7000 FortiOS 6.4.8 Build 1823.

Bug ID	Description
511091 593747 615509 697873 751856 765696 765704 766337 767074 768357 768402 770588 768585 768027 766285 769377 771802 762281 593781 735634	Improvements to SD-WAN compatibility with SLBC.
544748	Setting the `source-ip` option when using the `config system ntp` command no set up NTP time services no longer prevents the FortiGate-6000 or 7000 from accessing the configured NTP server.
585437	Resolved some issues with link monitoring that could sometimes lead to incorrect link monitoring information appearing on some FPCs or FPMs.
594258	FortiSwitch management over FortiLink now works as expected on a FortiGate-7000 system when FIM2 is the primary FIM.
612483	Management connections to FortiManager, FortiAnalyzer, and FortiGuard from a FortiGate-6000 or 7000 traffic interface now works as expected.
674435	Web filtering quotas now work as expected.
677002	Resolved an issue that prevented FGSP configuration changes from being synchronized to all FPCs or FPMs.
693325	The `slbc-mgmt-intf` option is set to `1-mgmt1` by default and this setting is now visible from the default configuration.
695060	Changing FGSP settings using the `config system standalone-cluster` command no longer

Bug ID	Description
	requires restarting the FortiGate-6000 or 7000 for the configuration changes to be synchronized to all FPCs or FPMs.
695189	Resolved an issue that caused the output of the `diagnose test application fctrlproxyd 1` to contain MAC addresses that incorrectly appear as `00:00:00:00:00:00`.
696715	Resolved an issue that caused the `diagnose sys link-monitor stat` command to displ;ay error messages.
697423	FortiGate-7121F cross-FIM LAGs now work as expected.
700337	Design changes implemented for FGSP to improve performance if the configuration includes more than three cluster sync entries.
704635	All supported transceiver types are now displayed correctly on the FortiGate-7000F GUI.
705958	Dialup server IPsec VPN tunnels are now successfully synchronized to all FPCs or FPMs when `mode-cfg` is enabled.
714538	The `telnetd` process now runs on FortiGate-7000F FIMs and the `execute load-balance slot manage` command works as expected when run from a FortiGate-7000F FIM CLI.
737087	Resolved an issue that could sometimes cause FortiGate-7000F NP7 load balancers to drop IPv6 FTP packets passing through a VLAN interface.
738266	The status of IPv6 links is now correctly synchronized to all FPCs and FPMs.
739043	Added the slot ID field to SSL log messages sent to FortiAnalyzer.
739627	Resolved an issue that prevented traffic log messages from being recorded for proxy sessions. Because of this the output of the `diagnose wad stats policy list` command is incorrect. As well, the wrong session count information was displayed on the firewall policy GUI.
740196	The get system {session | session6} status command now displays information for the FortiGate-6000 management board and all FPCs or for the FortiGate-7000 FIMs and FPMs.
744344	FortiGate-6000 and 7000 mirroring SSL inspected traffic (also called SSL port mirroring) now works as expected.
744596	Resolved an issue that could prevent RADIUS users from having to re-authenticate after the RADIUS server session timeout.
744636	Resolved an issue that could prevent FortiGate-6000 or 7000 FGCP clusters from synchronizing files received from FortiGuard after the cluster has been operating for 497 days.
746201	Resolved an issue that prevented dial-up IPsec VPN routes from being synchronized after a primary FPC or FPM failover.
747177	Resolved an FortiGate-7121F-related issue that caused latency with IPv6 active or passive FTP sessions.

747523
747335
	The FortiGate-7121F can now successfully reassemble fragmented packets if `ip-ressembly` is enabled using the following command:
	`config system npu`
	`   config ip-reassembly`
	`      set status enable`

Bug ID	Description
	`end`
747814	Removing an FPM from a FortiGate-7121F no longer causes synchronization issues.
748021	Resolved an issue that prevented FortiGate-7121F NP7 ESP sessions from expiring on time.
748258	The output of the `get transceiver info` command no longer includes error messages.
749074	Firewall sessions for firewall uses that authenticate using RADIUS are deleted when the firewall authentication idle time is reached and the FortiGate is configured to ignore RADIUS session timeouts set by the RADIUS server. Before this bug was fixed, RADIUS user sessions would never time out if the FortiGate was configured to ignore RADIUS session timeouts.
749357	Resolved a memory leak that caused high memory usage on the primary FPC or FPM.
753586	Management traffic can now be sent over an inter-VDOM link. For example, you can connect from the mgmt-vdom to FortiGuard by creating an inter-VDOM link between mgmt-vdom and a VDOM connected to the internet. You can also use inter-VDOM links to connect from mgmt-vdom to a FortiManager.
755579	You can now successfully use the FortiManager Connect to CLI via SSH device manager option to connect to the FortiGate-6000 or 7000 CLI.
755833	Resolved a timing issue that could cause an FPM to stop starting up and display a waiting for data heartbeat message after using the system management module to cycle the power of both FIMs.
757521	Resolved an issue that could result in the output of the `get sys interface transceiver` command missing the serial numbers of some supported transceivers.
757780 768778	The primary FPC or FPM GUI firewall policy GUI pages now display the correct firewall policy usage data (for example, active sessions, hit counts, and so on).
758217	The global command `get ipsec tunnel list` now lists status information for IPsec tunnels from all VDOMs.
758445	Increase the FortiGate-7000F boot partition size. This change allows the FortiGate-7000F to support larger more complex configurations that include more VDOMs and firewall policies. Because of this change, the process of upgrading a FortiGate-7000F system to 6.4.8 Build 1823 will take longer than normal and during this time the FortiGate-7000F will not be able to process traffic.
758714	Resolved an issue that would sometimes cause the FortiGate-7121F to unexpectedly select a new primary FPM.

758785	The following commands now work as expected when input from the management board or the primary FIM:
	`get vpn ssl monitor`
	`diagnose vpn ssl list`
	`diagnose vpn ssl mux`
	`diagnose vpn ssl statistics`

760263	When an FPC or FPM is disabled, its entry is now removed from the Security Fabric tree.

Bug ID	Description
760778 746476	All CLI command output, GUI pages, log messages, and SNMP queries and traps use the terminology "primary" and "secondary" in place of "master" and "slave". This change does not currently apply to config CLI options. The command `execute load-balance slot set-master-worker` has been changed to `execute load-balance slot set-primary-worker`.
761052	Resolved an issue that prevented management traffic from being sent from an IPsec VPN interface.
763074	Resolved an issue that could cause two interfaces to be incorrectly assigned the same SNMP index.
767175	Resolved an issue that prevented switching a VDOM between transparent and NAT mode if all licensed VDOMs have been created.
767666	Resolved an issue that caused traffic to be dropped after adding an EMAC-VLAN interface
769865	Information formerly displayed by Management plane and data plane dashboard widgets is not displayed by the Configuration Sync Monitor.
770280 753798 746008	FortiGate-6000s or 7000s in a virtual clustering configuration can now correctly resolve domain names.
771677	Resolved an issue with displaying firewall policy statistics on the FortiGate-6000 management board GUI.
772287	Local-in and local-out traffic now works as expected for FPCs or FPMs on a FortiGate 6000 or 7000 that is operating as the primary FortiGate for virtual cluster 2.
772294	Resolved an issue with IPv4 BFD packet handling that blocked finding OSPF and BGP neighbors.
772414	Resolved an issue that sometimes prevented sending log messages from FPCs or FPMs.
778296	Resolved an issue that could block passthrough or local-in traffic for a newly-created VDOM. The issue did not affect local-out traffic.

Common vulnerabilities and exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
752134	FortiOS 6.4.8 for FortiGate-6000 and 7000 series is no longer vulnerable to the following PSIRT incident number: • CVE-2021-42757

Known issues

The following issues have been identified in FortiGate-6000 and FortiGate-7000 FortiOS 6.4.8 Build 1823. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 6.4.8 release notes also apply to FortiGate-6000 and 7000 FortiOS 6.4.8 Build 1823.

Bug ID	Description
653092	You cannot use the SLBC management interface IP address to manage a FortiGate-6000 or 7000 by connecting to a data interface.
674979	The GUI incorrectly shows more traffic on FortiGate-6000 HA interfaces than what is actually occurring.
682426	Traffic log messages are only transmitted through a dedicated HA management interface when `ha-direct` is enabled.
715541	FortiGate-7000E platforms do not support using a LAG for FGSP session synchronization.
724543	Outbound bandwidth traffic statistics are showing incorrectly on individual FIM and FPM GUI pages.
734898	Under some conditions when a FortiGate-6000 or 7000 is very busy, when making configuration changes either manually or using a script, the `cmdbsvr` application may crash with a signal 11 segmentation fault. This problem can occur on a standalone FortiGate-6000 or 7000 or on FortiGate-6000s or 7000s in an FGCP HA cluster.
752402	In some cases traffic may be blocked from passing through a FortiGate-7000F because FortiOS assigned an incorrect MAC address to a VLAN interface. This problem may resolve itself after the system has been operating for a few minutes. Restarting the FortiGate-7000F will also resolve the problem.
767742	Because of a limitation of the FIM-7921F switch hardware, the FortiGate-7121F with FIM-7921Fs does not support adding VLANs to flow rules. The `vlan` setting of the `config load-balance flow-rule` command is ignored.
771680	Configuring SSL VPN Web portals from the GUI does not work correctly. Configuring SSL VPN Web portals from the CLI does work as expected.
773766	The `fnbamd` and `radiusd` processes may crash when the FortiGate-6000 or 7000 is managing large numbers of single sign on users.
777415	In a FortiGate-6000 or 7000 FGCP HA configuration, dynamic addresses received by an SDN connector may not be synchronized to the secondary FortiGte-6000 or 7000 in the cluster.
778239	For all FortiGate-6000 and 7000 models, the CLI allows you to add up to 512 flow rules. However, the number of flow rules that you can add is actually limited by the FortiGate-6000 and 7000 internal switch hardware: • All FortiGate-6000F models support up to 256 flow rules. • All FortiGate-7000E models support up to 512 flow-rules. • A FortiGate-7000F with FIM-7941Fs supports up to 492 flow rules. • A FortiGate-7000F with FIM-7921Fs supports up to 52 flow rules.

Bug ID	Description
780296	IP addresses received by an ACI SCN connector are not always synchronized to all FPCs or FPMs, especially if a relatively large number of address are to be synchronized, for example 2000 addresses.
782095	FortiGate-6000 FGCP cluster interfaces may be assigned virtual MAC addresses that overlap with the virtual MAC addresses assigned to the interfaces of other FortiGates in FGCP clusters, even if they have different group IDs. If you have a FortiGate-6000 FGCP cluster on the same network as FGCP clusters with other FortiGates, you can work around this issue by setting the group IDs of other FortiGate clusters on the same network to a value of 81 or higher.

782338	A single SSL VPN user session can tie up multiple IP addresses, resulting in no more IP addresses being available for new SSL VPN sessions. You may be able to help reduce the impact of this issue by disabling limiting user logins, by entering the following command:
	`config vpn ssl web portal`
	`   edit "name"`
	`   set limit-user-logins disable`
	`end`
	You can also use the following command to list all active SSL VPN tunnels:
	`execute vpn sslvpn list`
	The command output lists all active SSL VPN tunnels in order by index number. If there are missing index numbers, you can use the following command to delete tunnels with those missing index numbers, freeing up the IP addresses that were tied up by those tunnels:
	`execute vpn sslvpn del-tunnel <missing index>`

782640	When viewing FortiView pages from a VDOM the FortiGate-6000 or 7000 may not be able to retrieve data from FortiAnalyzer. The FortiView pages will display the error message "Failed to retrieve FortiView data".
782978	If you attempt to create an FGCP HA cluster and the FortiGate-6000s or 7000s making up the cluster have difference firmware versions, the CLI of one of the FortiGate-6000s or 7000s may display incorrect error messages after restarting.
783689	Because of a software issue, FortiGate-6000F DC models with only one DC PSU connected to power may become unstable, causing some FPCs to restart. A single DC PSU should be able to supply sufficient power to operate the management board and all of the FPCs in every FortiGate-6000F DC model.
786659	If you are managing a FortiGate-7121F FGCP HA cluster using FortiManger, in some cases the `confsyncd` process running on the primary FIM of the primary FortiGate-7121F can crash and after the crash, configuration changes are no longer synchronized to the FPMs in the primary FortiGate-7121F. This problem does not to affect the secondary FortiGate-7121F in the cluster, so to resume normal operation you can cause an HA failover, causing the secondary FortiGate-7121F to become the primary FortiGate-7121F. Check with Fortinet Support for assistance with restoring operation of the primary FortiGate-7121F.
792717	A dialup IPSec VPN tunnel can take a couple of minutes before allowing traffic through it, even though the tunnel appears to be up when viewed from the FortiGate GUI or CLI. This can happen if dead peer detection (DPD) is enabled on a large number of VPN clients accessing the tunnel. Receiving the DPD messages from many clients at the same time can trigger this issue. To work around the problem, you can disable dead peer detection on all FortiClients that access the tunnel.