FortiGate-6000 and FortiGate-7000 - Release Notes

Version 6.2.4 Build 1116

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

February 17, 2021
FortiGate-6000 and FortiGate-7000 6.2.4 Build 1116 Release Notes
01-624-634463-20210217

TABLE OF CONTENTS

Change log

Date	Change description
February 17, 2021	Added known issue 613617 to Known issues on page 65.
January 22, 2021	Added information about FortiGate-6000F hardware generation 1 and generation 2, see FortiGate-6000F hardware generations on page 22.
December 7, 2020	New section: More ARP queries than expected for one device - potential issue on large WiFi networks on page 28.
October 7, 2020	Updated HA graceful upgrade to FortiOS 6.2.4 on page 57 to add FortiOS 6.0.10 to the upgrade path.
September 21, 2020	Changes to Special configuration required for SSL VPN on page 38. Added known issue 664898.
August 24, 2020	Changes to the description of the recommended ICMP load balancing configuration for inter-cluster session synchronization as described in FortiGate-6000 inter-cluster session synchronization on page 8. VLAN IDs do not have to be same on peer clusters, as now correctly described in Example FortiGate-6000 inter-cluster session synchronization configuration on page 9. Fixed some broken links.
August 20, 2020	New section: Troubleshooting an FPC failure on page 25.
August 18, 2020	Added notes about finding the FortiGate-6000 and 7000 for FortiOS 6.2.4 firmware images on the Fortinet Support Download Firmware Images page by selecting the **FortiGate-6K7K** product.
August 17, 2020	Initial version.

FortiGate-6000 and FortiGate-7000 6.2.4 release notes

These platform specific release notes describe new features, special notices, upgrade information, product integration and support, resolved issues, and known issues for FortiGate-6000 and 7000 for 6.2.4 Build 1116.

In addition, special notices, new features and enhancements, changes in CLI defaults, changes in default values, changes in table size, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 6.2.4 Release Notes also apply to FortiGate-6000 and 7000 for 6.2.4 Build 1116.

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

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

You can find the FortiGate-6000 and 7000 for FortiOS 6.2.4 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 6.2.4 Build 1116 supports the following models:

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

What's new

The following new features have been added to FortiGate-6000 and 7000 for FortiOS 6.2.4 Build 1116. The new features and enhancements, changes in CLI defaults, changes in default behavior, changes in default values, and changes in table size described in the FortiOS 6.2.4 release notes also apply to FortiGate-6000 and 7000 FortiOS 6.2.4 Build 1116.

HA reserved management interface support

FortiOS 6.2.4 for FortiGate-6000 and 7000 supports HA reserved management interfaces.

- For the FortiGate-6000 you can configure mgmt1, mgmt2, and mgmt3 to be HA reserved management interfaces.
- For the FortiGate-7000 you can add one or more VLAN interfaces to the management LAG and configure these VLAN interfaces to be HA reserved management interfaces.

This feature allows you to select one or more interfaces in the `mgmt-vdom` VDOM to be HA reserved management interfaces. Once the interfaces are configured to be reserved management interfaces, you can log into each FortiGate-6000 or 7000 in the HA cluster and configure the reserved management interface with individual IP addresses and other settings as required. You can also configure routing for each reserved management interface. The result is that each FortiGate-6000 or 7000 in the cluster has its own management interface or interfaces and each of these interfaces has its own IP address that is not synchronized to the other FortiGate-6000 or 7000 in the cluster.

To configure an HA reserved management interface from the GUI go to **System > HA** and enable **Management Interface Reservation**. Select one or more interfaces to be HA reserved management interfaces. Optionally configure routing for each reserved management interface. This routing configuration is not synchronized and can be configured separately for each device in the cluster.

To configure an HA reserved management interface from the CLI:

```
config system ha
   set mode a-p
   set ha-mgmt-status enable
   set ha-direct enable
      config ha-mgmt-interfaces
         edit 0
            set interface <interface>
            set dst <destination-ip>
            set gateway <gateway-ip>
            set gateway6 <gateway-ipv6-ip>
         end
   end
```

Enabling `ha-direct` from the CLI is required if you plan to use the HA reserved management interface for SNMP, remote logging, or communicating with FortiSandbox. Enabling `ha-direct` is also required for some types of remote authentication, but is not required for RADIUS remote authentication.

For the FortiGate-6000, `<interface>` can be `mgmt1`, `mgmt2`, or `mgmt3`. You can only select an interface if it has not been used in another configuration.

For the FortiGate-7000, `<interface>` can be any VLAN interface that you have added to the FortiGate-7000 management interface (mgmt). Note that FortiGate-7000 management interface is a static lag and should not be changed.

For more information about this feature, see Out-of-band management.

FortiGate-6000 inter-cluster session synchronization

FortiOS 6.2.4 for FortiGate-6000 supports inter-cluster synchronization among up to four FortiGate-6000 FGCP clusters. Inter-cluster session synchronization uses FGSP to synchronize sessions between FGCP clusters. All of the FortiGate-6000s must be the same hardware model.

Enter the following command to enable inter-cluster session synchronization on each FortiGate-6000 FGCP cluster:

```
config system ha
   set inter-cluster-session-sync enable
end
```

Once you enable inter-cluster session synchronization, all FGSP configuration options are available on each FGCP cluster and you can set up session sync instances to synchronize sessions between the FGCP clusters in the same way as for standalone FortiGates.

FortiGate-6000 inter-cluster session synchronization uses the mgmt3 interface for session synchronization between FGCP clusters. When inter-cluster session synchronization is enabled, the mgmt3 interface cannot be used for any other purpose. The mgmt3 interfaces of all of the FGCP clusters must have IP addresses and must be able to communicate with each other. Since FortiGate-6000 currently supports only one interface for session synchronization, redundant session synchronization is not currently supported. You cannot use the ha1 and ha2 interfaces for inter-cluster session synchronization because they are being used for FGCP HA between the FortiGate-6000s in each FGCP cluster.

Inter-cluster session synchronization can use a lot of bandwidth if the clusters are busy. More bandwidth and lower latency for communication between the mgmt3 interfaces can improve session synchronization performance.

Inter-cluster session synchronization synchronizes sessions between the primary FortiGate-6000s in each cluster. FGCP HA then handles session synchronization between FortiGate-6000s in each FGCP cluster.

For more information about FortiOS inter-cluster session synchronization, see FGSP between FGCP clusters.

FortiGate-6000 Inter-cluster session synchronization has the following limitations:

- Inter-cluster session synchronization is available only for the FortiGate-6000 (and not the FortiGate-7000).
- The FGCP clusters cannot be configured for virtual clustering.
- NAT between mgmt3 interfaces is not supported.
- Standalone configuration synchronization between the FCGP clusters is not supported.
- Only the mgmt3 interface can be used to synchronize sessions between clusters.
- Inter-cluster session synchronization doesn't support setting up IPv6 session filters using the `config session-sync-filter` option.
- When ICMP load balancing is set to `to-master`, ICMP packets are not installed on the DP processor. In an inter-cluster session synchronization configuration with an asymmetry topology, synchronized ICMP packets will be dropped if the clusters have selected a different primary FPC. To avoid this possible traffic loss, set `dp-load-distribution-method` to `src-ip`, `dst-ip`, or `src-dst-ip`.
- Asymmetric IPv6 SCTP traffic sessions are not supported. These sessions are dropped.

- FGSP IPsec tunnel synchronization is not supported.
- Session synchronization packets cannot be fragmented. So the MTU for the mgmt3 interface should be supported by the network.
- Jumbo frames on the mgmt3 interface are not supported.
- To reduce the number of failovers and the amount of session synchronization traffic, configuring HA override on the FGCP clusters is not recommended.

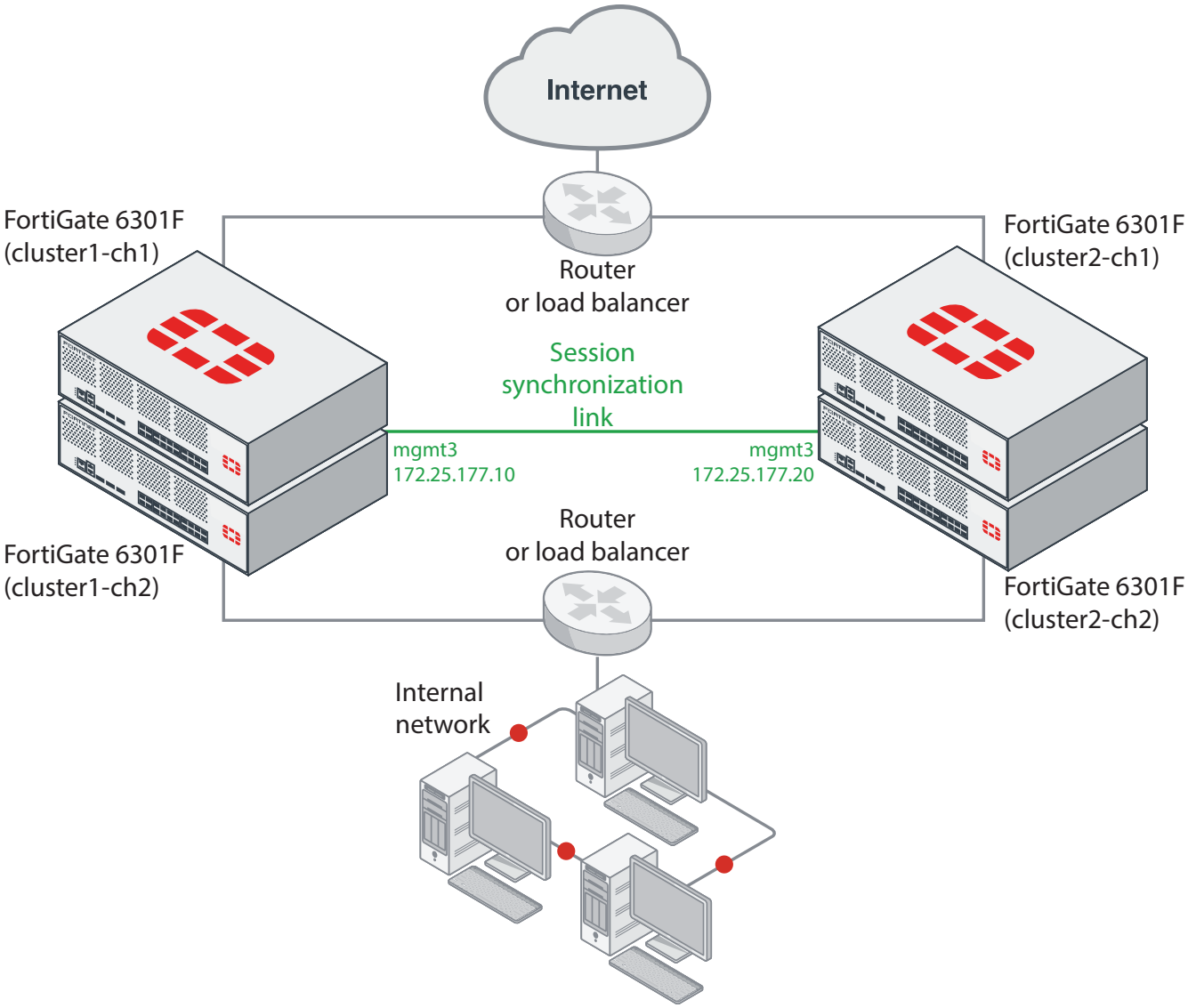
Example FortiGate-6000 inter-cluster session synchronization configuration

This example shows how to configure inter-cluster session synchronization between two FortiGate-6301F FGCP clusters. The configuration synchronizes sessions for the root VDOM and for a VDOM named vdom-1. The mgmt3 session synchronization interfaces of each FortiGate-6301F are connected to the 172.25.177.0/24 network.

The FortiGate-6301F clusters must have their own IP addresses and their own network configurations. The clusters in this example are named cluster1 and cluster2. The FortiGate-6301Fs in cluster1 have host names cluster1-ch1 and cluster1-ch2. The FortiGate-6301Fs in cluster2 have host names cluster2-ch1 and cluster2-ch2.

Configuring inter-cluster session synchronization consists of logging into each cluster, configuring mgmt3 to connect to the 172.25.177.0/24 network, adding a cluster sync instance, and enabling inter-cluster session synchronization. The FGCP synchronizes these settings to the secondary FortiGate-6301Fs in each cluster.

Example FortiGate-6000 inter-cluster session synchronization configuration



1. Configure the routers or load balancers to distribute sessions to the two FortiGate-6301F clusters.
2. Change the host names of the FortiGate-6301Fs in the two clusters to cluster1-ch1, cluster1-ch2, cluster2-ch1, and cluster2-ch2.
3. Configure VDOMs and network settings for each FortiGate-6301F to allow them to connect to their networks and route traffic.

   The names of the VDOMs and any VLANs and LAGs or other interfaces that you have added must be the same on both clusters, even though network addresses will be different. VLAN IDs can be different in each cluster as long as the names of the VLAN interfaces are the same.
4. On cluster1, configure the mgmt3 interface with an IP address on the 172.25.177.0/24 network:

   ```
   config system interface
      edit mgmt3
         set ip 172.25.177.10 255.255.255.0
      end
   ```
5. On cluster1, add a session synchronization instance for the root and vdom-1 VDOMs.

```
config system cluster-sync
   edit 1
      set peervd mgmt-vdom
      set peerip 172.25.177.20
      set syncvd root vdom-1
   end
```

Where, `peervd` will always be `mgmt-vdom` and `peerip` is the IP address of the mgmt3 interface of cluster2.

This configuration creates one `cluster-sync` instance that includes both VDOMs. You could have created a separate `cluster-sync` instance for each VDOM. If possible, however, avoid creating more than three `cluster-sync` instances. A fourth `cluster-sync` instance may experience reduced session synchronization performance.

6. On cluster1, enable inter-cluster session synchronization.

```
config system ha
   set session-pickup enable
   set inter-cluster-session-sync enable
end
```

Since FGCP HA is already configured on cluster1, all you have to do for inter-cluster session synchronization is to enable `session-pickup` and `inter-cluster-session-sync`. The complete HA FGCP and inter-cluster session synchronization configuration for cluster1-ch1 could look like the following:

```
config system ha
   set group-id 16
   set group-name "fgsp-fgcp-cluster1"
   set mode a-p
   set password <password>
   set hbdev "ha1" 50 "ha2" 100
   set chassis-id 1
   set session-pickup enable
   set inter-cluster-session-sync enable
end
```

7. On cluster 2, configure the mgmt3 interface with an IP address on the 172.25.177.0/24 network:

```
config system interface
   edit mgmt3
      set ip 172.25.177.20 255.255.255.0
   end
```

8. On cluster2, configure session synchronization for the root and vdom-1 VDOMs with the same configuration as cluster1.

```
config system cluster-sync
   edit 1
      set peervd mgmt-vdom
      set peerip 172.25.177.10
      set syncvd root vdom-1
   end
```

9. On cluster2, enable inter-cluster session synchronization.

```
config system ha
   set session-pickup enable
   set inter-cluster-session-sync enable
end
```

Since FGCP HA is already configured on cluster2, all you have to do for inter-cluster session synchronization is to enable `session-pickup` and `inter-cluster-session-sync`. The complete HA FGCP and inter-cluster session synchronization configuration for cluster2-ch1 could look like the following:

```
config system ha
   set group-id 20
   set group-name "fgsp-fgcp-cluster2"
```

```
    set mode a-p
    set password <password>
    set hbdev "ha1" 50 "ha2" 100
    set chassis-id 1
    set session-pickup enable
    set inter-cluster-session-sync enable
  end
```

Configure FortiGate-7000 FPMs to send logs to different syslog servers

Previous versions of FortiGate-7000 allowed you to use the VDOM exception configuration to:

- Set up each FPM in a FortiGate-7000 to send log messages to different FortiAnalyzers.
- Set up individual VDOMs on each FPM to send log messages to different FortiAnalyzers.

FortiGate-7000 for FortiOS 6.2.4 now supports the same functionality for syslog servers.

This configuration is only supported for `fortianalyzer` and `syslogd` and not for `fortianalyzer2`, `fortianalyzer3`, `fortianalyzer-cloud`, `syslogd2`, `syslogd3`, and `syslogd4`.

When you have completed the VDOM exception configurations described in this section, the FIMs and FPMs will have different logging configurations. In addition, some configurations that are affected by the logging configuration (for example, DLP content archiving) will be different on some modules. Because of this, using the various methods available to check for synchronization between modules will show that the configurations of the modules are not synchronized. The FortiGate-7000 will continue to operate normally even with these configuration synchronization issues.

Some VDOM exception options not supported in HA mode

When a FortiGate-7000 is operating in FGCP HA mode, only the following `vdom-exception` options can be configured:

```
log.fortianalyzer.setting
log.fortianalzer.override-setting
log.syslogd.setting
log.syslogd.override-setting
```

The CLI returns an error message if you attempt to configure a `vdom-exception` that is not configurable in HA mode.

Also in HA mode, only the primary FortiGate-7000 can send log messages from individual VDOMs because only the data interfaces on the primary FortiGate-7000 are active.

Configuring individual FPMs to send logs to different FortiAnalyzers

The following steps show how to configure the two FPMs in a FortiGate-7040E to send log messages to different FortiAnalyzers. The FPMs connect to their FortiAnalyzers through the FortiGate-7000 management interface. This procedure assumes you have the following three FortiAnalyzers:

FortiAnalyzer IP address	Intended use
172.25.176.10	The FIMs send log messages to this FortiAnalyzer.
172.25.176.100	The FPM in slot 3 sends log messages to this FortiAnalyzer.
172.25.176.110	The FPM in slot 4 sends log messages to this FortiAnalyzer.

This procedure involves creating a FortiAnalyzer configuration template on the primary FIM that is synchronized to the FPMs. You then log into each FPM and change the FortiAnalyzer server IP address to the address of the FortiAnalyzer that the FPM should send log messages to.

This configuration is only supported for `fortianalyzer` and not for `fortianalyzer2`, `fortianalyzer3`, and `fortianalyzer-cloud`.

1. Log into the primary FIM CLI using the FortiGate-7040E management IP address.
2. Create a FortiAnalyzer configuration template on the primary FIM.

```
config global
   config log fortianalyzer setting
      set status enable
      set server 172.25.176.10
      set upload-option realtime
   end
```

This configuration will be synchronized to all of the FIMs and FPMs.

The FortiAnalyzer VDOM exception configuration requires `upload-option` to be set to `realtime`.

3. Enter the following command to prevent the FortiGate-7040E from synchronizing FortiAnalyzer settings between FIMs and FPMs:

```
config system vdom-exception
   edit 1
      set object log.fortianalyzer.setting
   end
```

4. Log into the CLI of the FPM in slot 3:

   For example, you can start a new SSH connection using the special management port for slot 3:

```
ssh <management-ip>:2203
```

   Or you can use the following command from the global primary FIM CLI:

```
execute load-balance slot manage 3
```

FortiOS will log you out of the CLI of the FPM in slot 3 in less than 60 seconds. You should have enough time to change the FortiAnalyzer server IP address as described in the next step, but not much else. If you run out of time on your first attempt, you can keep trying until you succeed.

5. Change the FortiAnalyzer server IP address:

```
config global
   config log fortianalyzer setting
      set server 172.25.176.100
   end
```

You should see messages similar to the following on the CLI:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync out
     of sync for a while.
The Serial Number for FortiAnalyzer is not entered.
In order to verify identity of FortiAnalyzer serial number is needed.
If serial number is not set, connection will be set as unverified and
access to local config and files will be accessible only with user name/password.
FortiGate can establish a connection to obtain the serial number now.Do you want to try to
     connect now? (y/n)y
```

If `upload-option` is not set to `realtime`, messages similar to the following appear and your configuration change will not be saved:

```
Please change configuration on FIMs. Changing configuration on FPMs may
     cause confsync out of sync for a while.
Can only set upload option to real-time mode when Security Fabric is
     enabled.
object set operator error, -39 discard the setting
Command fail. Return code -39
```

6. Enter Y to confirm the serial number. Messages similar to the following should appear:

```
Obtained serial number from X509 certificate of Fortianalyzer is: <serial>
Serial number from certificate MUST be the same as serial number observed in Fortianalyzer.
If these two serial numbers don't match, connection will be dropped.
Please make sure the serial numbers are matching.
In case that Fortianalyzer is using a third-party certificate, certificate verification
     must be disabled.
Do you confirm that this is the correct serial number? (y/n)y
```

7. Enter Y to confirm the serial number.
8. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.
9. Log into the CLI of the FPM in slot 4.
10. Change the FortiAnalyzer server IP address:

```
config global
   config log fortianalyzer setting
      set server 172.25.176.110
   end
```

When you change the FortiAnalyzer server IP address, messages appear like they did when you were logged into the FPM in slot 3 and you can confirm the FortiAnalyzer serial number.

11. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

Configuring VDOMs on individual FPMs to send logs to different FortiAnalyzers

The following steps describe how to override the global FortiAnalyzer configuration for individual VDOMs on individual FPMs. The example shows how to configure the root VDOMs on the each of the FPMs in a FortiGate-7040E to send log messages to different FortiAnalyzers. Each root VDOM connects to FortiAnalyzer through a root VDOM data interface. This procedure assumes you have the following two FortiAnalyzers:

FortiAnalyzer IP address	Intended use
172.25.176.120	The root VDOM on the FPM in slot 3 sends log messages to this FortiAnalyzer.
172.25.176.130	The root VDOM on the FPM in slot 4 sends log messages to this FortiAnalyzer.

This configuration is only supported for `fortianalyzer` and not for `fortianalyzer2`, `fortianalyzer3`, and `fortianalyzer-cloud`.

1. Log into the primary FIM CLI using the FortiGate-7040E management IP address.
2. Use the following command to prevent the FortiGate-7040E from synchronizing FortiAnalyzer override settings between FPMs:

```
config global
   config system vdom-exception
      edit 1
         set object log.fortianalyzer.override-setting
      end
   end
```

3. Log into the CLI of the FPM in slot 3:

   For example you can start a new SSH connection using the special management port for slot 3:

```
ssh <management-ip>:2203
```

   Or you can use the following command from the global primary FIM CLI:

```
execute load-balance slot manage 3
```

The system will log you out of the CLI of the FPM in slot 3 in less than 60 seconds. You should have enough time to complete the following steps. If you run out of time on your first attempt, you can keep trying until you succeed.

4. Access the root VDOM of the FPM in slot 3 and enable overriding the FortiAnalyzer configuration for the root VDOM.

```
config vdom
   edit root
      config log setting
         set faz-override enable
      end
```

   A message similar to the following appears; which you can ignore:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync out
     of sync for a while.
```

5. Configure FortiAnalyzer override to send log messages to a FortiAnalyzer with IP address 172.25.176.120:

```
config log fortianalyzer override-setting
   set status enable
   set server 172.25.176.120
```

```
end
```

You should see messages similar to the following on the CLI:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync out
     of sync for a while.
The Serial Number for FortiAnalyzer is not entered.
In order to verify identity of FortiAnalyzer serial number is needed.
If serial number is not set, connection will be set as unverified and
access to local config and files will be accessible only with user name/password.
FortiGate can establish a connection to obtain the serial number now.Do you want to try to
     connect now? (y/n)y
```

6. Enter Y to confirm the serial number. Messages similar to the following should appear:

```
Obtained serial number from X509 certificate of Fortianalyzer is: <serial>
Serial number from certificate MUST be the same as serial number observed in Fortianalyzer.
If these two serial numbers don't match, connection will be dropped.
Please make sure the serial numbers are matching.
In case that Fortianalyzer is using a third-party certificate, certificate verification
     must be disabled.
Do you confirm that this is the correct serial number? (y/n)y
```

7. Enter Y to confirm the serial number.
8. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute
9. Log into the CLI of the FPM in slot 4.
10. Access the root VDOM of the FPM in slot 4 and enable overriding the FortiAnalyzer configuration for the root VDOM.

```
config vdom
   edit root
      config log setting
         set faz-override enable
      end
```

A message similar to the following appears; which you can ignore:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync out
     of sync for a while.
```

11. Configure FortiAnalyzer override to send log messages to a FortiAnalyzer with IP address 172.25.176.130:

```
config log fortianalyzer override-setting
   set status enable
   set server 172.25.176.130
end
```

Messages appear like they did when you were logged into the FPM in slot 3 and you can confirm the FortiAnalyzer serial number.

12. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

Configuring individual FPMs to send logs to different syslog servers

The following steps show how to configure the two FPMs in a FortiGate-7040E to send log messages to different syslog servers. The FPMs connect to the syslog servers through the FortiGate-7000 management interface. This procedure assumes you have the following three syslog servers:

syslog server IP address	Intended use
172.25.176.20	The FIMs send log messages to this syslog server.
172.25.176.200	The FPM in slot 3 sends log messages to this syslog server.
172.25.176.210	The FPM in slot 4 sends log messages to this syslog server.

This procedure involves creating a syslog configuration template on the primary FIM that is synchronized to the FPMs. You then log into each FPM and change the syslog server IP address to the address of the syslog server that the FPM should send log messages to.

This configuration is only supported for `syslogd` and not for `syslogd2`, `syslogd3`, and `syslogd4`.

1. Log into the primary FIM CLI using the FortiGate-7040E management IP address.
2. Create a syslog configuration template on the primary FIM.

```
config global
   config log syslogd setting
      set status enable
      set server 172.25.176.20
   end
```

   This configuration will be synchronized to all of the FIMs and FPMs.
3. Enter the following command to prevent the FortiGate-7040E from synchronizing syslog settings between FIMs and FPMs:

```
config system vdom-exception
   edit 1
      set object log.syslogd.setting
   end
```

4. Log into the CLI of the FPM in slot 3:

   For example, you can start a new SSH connection using the special management port for slot 3:

```
ssh <management-ip>:2203
```

   Or you can use the following command from the global primary FIM CLI:

```
execute load-balance slot manage 3
```

FortiOS will log you out of the CLI of the FPM in slot 3 in less than 60 seconds. You should have enough time to change the syslog server IP address as described in the next step, but not much else. If you run out of time on your first attempt, you can keep trying until you succeed.

5. Change the syslog server IP address:

```
config global
   config log syslogd setting
      set server 172.25.176.200
   end
```

   A message similar to the following appears; which you can ignore:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync out
      of sync for a while.
```

6. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

7. Log into the CLI of the FPM in slot 4.
8. Change the syslog server IP address:

```
config global
   config log syslogd setting
      set server 172.25.176.210
   end
```

   A message similar to the following appears; which you can ignore:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync out
     of sync for a while.
```

9. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

Configuring VDOMs on individual FPMs to send logs to different syslog servers

The following steps describe how to override the global syslog configuration for individual VDOMs on individual FPMs. The example shows how to configure the root VDOMs on the each of the FPMs in a FortiGate-7040E to send log messages to different sylog servers. Each root VDOM connects to a syslog server through a root VDOM data interface. This procedure assumes you have the following two syslog servers:

syslog server IP address	Intended use
172.25.176.220	The root VDOM on the FPM in slot 3 sends log messages to this syslog server.
172.25.176.230	The root VDOM on the FPM in slot 4 sends log messages to this syslog server.

This configuration is only supported for `syslogd` and not for `syslogd2`, `syslogd3`, and `syslogd4`.

1. Log into the primary FIM CLI using the FortiGate-7040E management IP address.
2. Use the following command to prevent the FortiGate-7040E from synchronizing syslog override settings between FPMs:

```
config global
   config system vdom-exception
      edit 1
         set object log.syslogd.override-setting
      end
   end
```

3. Log into the CLI of the FPM in slot 3:

   For example you can start a new SSH connection using the special management port for slot 3:

```
ssh <management-ip>:2203
```

   Or you can use the following command from the global primary FIM CLI:

```
execute load-balance slot manage 3
```

The system will log you out of the CLI of the FPM in slot 3 in less than 60 seconds. You should have enough time to complete the following steps. If you run out of time on your first attempt, you can keep trying until you succeed.

4. Access the root VDOM of the FPM in slot 3 and enable overriding the syslog configuration for the root VDOM.

```
config vdom
   edit root
      config log setting
         set syslog-override enable
      end
```

A message similar to the following appears; which you can ignore:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync out
     of sync for a while.
```

5. Configure syslog override to send log messages to a syslog server with IP address 172.25.176.220:

```
config log syslogd override-setting
   set status enable
   set server 172.25.176.220
end
```

A message similar to the following appears; which you can ignore:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync out
     of sync for a while.
```

6. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.
7. Access the root VDOM of the FPM in slot 4 and enable overriding the syslog configuration for the root VDOM.

```
config vdom
   edit root
      config log setting
         set syslog-override enable
      end
```

A message similar to the following appears; which you can ignore:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync out
     of sync for a while.
```

8. Configure FortiAnalyzer override to send log messages to a FortiAnalyzer with IP address 172.25.176.130:

```
config log syslogd override-setting
   set status enable
   set server 172.25.176.230
end
```

A message similar to the following appears; which you can ignore:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync out
     of sync for a while.
```

9. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

IPv6 ECMP support

FortiOS 6.2.4 for FortiGate-6000 and 7000 now includes support for most FortiOS IPv6 ECMP functionality.

Before setting up IPv4 or IPv6 ECMP you need to use the following command to configure the DP processor to operate with VDOM-based session tables:

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

Once you have enabled VDOM-based session tables, you can enable and configure IPv4 and IPv6 ECMP as you would for any FortiGate.

VDOM-based session tables

In an ECMP configuration, because of load balancing, return traffic could enter through a different interface than the one it exited from. If this happens, the DP processor operating with default interface-based session tables may not be able to send the return traffic to the FPC or FPM that processed the incoming session, causing the return traffic to be dropped. Operating with VDOM-based session tables solves this problem, allowing traffic received on a different interface to be properly identified and sent to the correct FPC or FPM.

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

IPv4 and IPv6 ECMP load balancing

You can use the following command to configure the IPv4 ECMP load balancing method for a VDOM:

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

With VDOM-based session tables enabled, the FortiGate-6000 and 7000 support all ECMP load balancing methods except `usage-based`. If you select `usage-based`, all IP v4 traffic uses the first IPv4 ECMP route instead of being load balanced among all IPv4 ECMP routes. All other IPv4 ECMP load balancing methods are supported.

See this link for information about how to support IPv6 ECMP load balancing: Technical Tip: ECMP – Load balancing algorithms for IPv4 and IPv6.

Enabling auxiliary session support

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

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

By default, for FortiOS 6.2.4 the `auxiliary-session` option is disabled. This can block some TCP traffic when ECMP is enabled. If this occurs, enabling `auxiliary-session` may solve the problem. For more information, see Technical Tip: Enabling auxiliary session with ECMP or SD-WAN.

Configuration sync monitor improvements

The FortiGate-6000 and 7000 configuration sync monitor (available on the global GUI from **Monitor > Configuration Sync Monitor**) includes a new **Total Heartbeat Packets** column that lists the number of heartbeat packets received from each FPC, FIM or FPM. In addition you can also now select the columns that appear on the Configuration Sync Monitor.

Transparent mode VDOMs support data interfaces for management traffic

You can set up IPv4 and IPv6 in-band management connections to all FortiGate-6000 and 7000 data interfaces by setting up administrative access for the data interface that you want to use to manage the FortiGate-6000. For in-band management of a transparent mode VDOM, you must also set up the transparent mode management IP address.

Connecting to a data interface for management is the same as connecting to one of the management interfaces. For example, you can log in to the GUI or CLI of the FortiGate-6000 management board or the primary FortiGate-7000 FIM.

Administrators with VDOM-level access can log into to their VDOM if they connect to a data interface that is in their VDOM.

Web filtering override user list synchronized

The web filter override user list is now synchronized to all FPCs or FPMs. Web Filter override users no longer have to re-authenticate if the DP processor forwards their session to a different FPC or FPM before the override times out.

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for FortiGate-6000 and FortiGate-7000 6.2.4 Build 1116. The Special notices described in the FortiOS 6.2.4 release notes also apply to FortiGate-6000 and 7000 FortiOS 6.2.4 Build 1116.

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).

SDN connector support

FortiGate-6000 and 7000 for FortiOS 6.2.4 supports the following SDN connectors:

- Cisco Application Centric Infrastructure (ACI)
- Amazon Web Services (AWS)
- Microsoft Azure
- VMware NSX
- VMware ESXi
- Kubernetes
- Oracle Cloud Infrastructure (OCI)
- OpenStack (Horizon)

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

FortiGate-6000 FPCs and power failure

The FortiGate-6000 includes three hot-swappable power supplies in a 2+1 redundant configuration. At least two of the power supplies must be operating to provide power to the FortiGate-6000. If only one power supply is operating, only four of the FPCs will continue operating (usually the FPCs in slots 1 to 4).

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.

A FortiGate-6000 will continue to operate even if multiple FPCs stop operating. 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.

If power is reconnected and the 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 to Synchronize the FPCs with the management board.

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
  Master 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"
```

For more information about troubleshooting FPC failures, see Troubleshooting an FPC failure on page 25.

FortiGate-6000 HA, FPCs, and power failure

In a FortiGate-6000 HA cluster, if the FPCs in the primary FortiGate-6000 shut down because two of the power supplies fail or become disconnected from power, the cluster renegotiates and the FortiGate-6000 with the most operating FPCs becomes the primary FortiGate-6000.

If the FPCs in the secondary FortiGate-6000 shut down because two power supplies have failed or disconnected, its status in the cluster does not change. In future cluster negotiations the FortiGate-6000 with shut down FPCs 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-synchronze 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 the configuration of the FPC. 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 a 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 1.

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.

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
  Master 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 27
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 27.

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 27.
   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.

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. This procedure is based on the procedure Installing FIM firmware from the BIOS after a reboot on page 1.

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.

   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.
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. Verify that the configuration has been synchronized.
    The following command output shows the sync status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=1
```

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

    The command output also shows that the uptime of the FIM in slot 2 is lower than the uptime of the other modules, indicating that the FIM in slot 2 has recently restarted.

    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. This procedure is based on the procedure Installing FIM firmware from the BIOS after a reboot on page 1.

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 FIM 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. Verify that the configuration has been synchronized.

    The following command output shows the sync status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

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

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

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

    If you enter the `diagnose sys confsync status | grep in_sy` command before the 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 6.2.4 remove virtual clustering

If you are operating a FortiGate-6000 or 7000 system running FortiOS 6.2.4 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 a flow rule to support DHCP relay

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

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

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

```
      set vlan 0
      set ether-type ipv4
      set src-addr-ipv4 0.0.0.0 0.0.0.0
      set dst-addr-ipv4 0.0.0.0 0.0.0.0
      set protocol udp
      set src-l4port 68-68
      set dst-l4port 67-67
      set action forward
      set forward-slot master
      set priority 5
      set comment "dhcpv4 client to server"
   end
```

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

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

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

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

See Installing FortiGate-6000 firmware from the BIOS after a reboot for detailed procedures for upgrading FortiGate-6000 firmware from the BIOS.

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

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

See Installing FIM firmware from the BIOS after a reboot and Installing FPM firmware from the BIOS after a rebootor detailed procedures for upgrading FortiGate-6000 firmware from the BIOS.

Installing firmware on an individual FortiGate-6000 FPC

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

1. Copy the firmware image file to a TFTP server, FTP server, or USB key.
2. To upload the firmware image file onto the FortiGate-6000 internal TFTP server, from the management board CLI, enter one of the following commands.
   - To upload the firmware image file from an FTP server:
     ```
     execute upload image ftp <image-file-and-path> <comment> <ftp-server-address>
          <username> <password>
     ```
   - To upload the firmware image file from a TFTP server:
     ```
     execute upload image tftp <image-file> <comment> <tftp-server-address>
     ```
   - To upload the firmware image file from a USB key:
     ```
     execute upload image usb <image-file-and-path> <comment>
     ```
3. Enter the following command to install the firmware image file on to an FPC:
   ```
   execute load-balance update image <slot-number>
   ```
   where `<slot-number>` is the FPC slot number.

   This command uploads the firmware image to the FPC and the FPC restarts. When the FPC starts up, the configuration is reset to factory default settings and then synchronized by the management board. The FPC restarts again, rejoins the cluster, and is ready to process traffic.
4. To verify that the configuration of the FPC has been synchronized, enter the `diagnose sys confsync status | grep in_sy` command. The command output below shows an example of the synchronization status of some of the FPCs in an HA cluster of two FortiGate-6301F devices. The field `in_sync=1` indicates that the configuration of the FPC is synchronized.

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

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

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

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

Installing firmware on an individual FortiGate-7000 FPM

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

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

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

1. Log in to the primary FIM CLI and enter the following command:
   `diagnose load-balance switch set-compatible <slot> enable elbc`
   Where `<slot>` is the number of the FortiGate-7000 slot containing the FPM to be upgraded.
2. Log in to the FPM GUI or CLI using its special port number (for example, for the FPM in slot 3, browse to https://192.168.1.99:44303 to connect to the GUI) and perform a normal firmware upgrade of the FPM.
3. After the FPM restarts, verify that the new firmware has been installed.
   You can do this from the FPM GUI dashboard or from the FPM CLI using the `get system status` command.
4. Verify that the configuration has been synchronized. The following command output shows the sync status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

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

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

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

   If you enter the `diagnose sys confsync status | grep in_sy` command before the FIM has completely restarted, it will not appear in the command output. As well, the Configuration Sync Monitor will temporarily show that it is not synchronized.
5. Once the FPM is operating normally, log back in to the primary FIM CLI and enter the following command to reset the FPM to normal operation:
   `diagnose load-balance switch set-compatible <slot> disable`
   Configuration synchronization errors will occur if you do not reset the FPM to normal operation.

SD-WAN is not supported

FortiGate-6000 and FortiGate-7000 Version 6.2.4 does not support SD-WAN because of the following known issues:

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

IPsec VPN features that are not supported

FortiOS 6.2.4 for FortiGate-6000 and FortiGate-7000 does not support the following IPsec VPN features:

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

Quarantine to disk not supported

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

Local out traffic is not sent to IPsec VPN interfaces

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

Special configuration required for SSL VPN

Using a FortiGate-6000 or 7000 as an SSL VPN server requires you to manually add an SSL VPN load 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 6.2.4 allows you use proprietary triple-tagging or double-tagging for HA heartbeat packets.

Example triple-tagging compatible switch configuration

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

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

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

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

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

```
config system ha
   set ha-port-dtag-mode proprietary
   set hbdev ha1 50 ha2 100
```

```
    set hbdev-vlan-id 4091
    set hbdev-second-vlan-id 4092
end
```

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

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

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

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

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

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

Example double-tagging compatible switch configuration

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

The FortiGate-6000 HA heartbeat configuration is.

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

Example third-party switch configuration:

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

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

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

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

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

Example FortiGate-7000 HA heartbeat switch configuration

FortiGate-7000 for FortiOS 6.2.4 allows you use proprietary triple-tagging or double-tagging for HA heartbeat packets.

Example triple-tagging compatible switch configuration

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

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

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

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

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

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

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

```
get system ha status
...
HBDEV stats:
 FG74E83E16000015(updated 1 seconds ago):
   1-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=579602089/2290683/0/0,
tx=215982465/761929/0/0, vlan-id=4086
   2-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=577890866/2285570/0/0,
tx=215966839/761871/0/0, vlan-id=4086
   1-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=579601846/2290682/0/0,
tx=215982465/761929/0/0, vlan-id=4087
   2-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=577890651/2285569/0/0,
tx=215966811/761871/0/0, vlan-id=4087
 FG74E83E16000016(updated 1 seconds ago):
   1-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=598602425/2290687/0/0,
tx=196974887/761899/0/0, vlan-id=4086
   2-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=596895956/2285588/0/0,
tx=196965052/761864/0/0, vlan-id=4086
   1-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=598602154/2290686/0/0,
tx=196974915/761899/0/0, vlan-id=4087
   2-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=596895685/2285587/0/0,
tx=196965080/761864/0/0, vlan-id=4087
...
```

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

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

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

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

Example double-tagging compatible switch configuration

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

The FortiGate-7040E HA heartbeat configuration is.

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

```
   set hbdev-second-vlan-id 4087
end
```

Example third-party switch configuration:

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

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

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

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

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

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

The default `configure load-balance flow-rule` command contains the recommended default flow rules that control how the FortiGate-6000 or 7000 handles traffic types that cannot be load balanced. Most of the flow rules in the default configuration are enabled and are intended to send common traffic types that cannot be load balanced to the primary FPC or FPM. FortiGate-6000 and 7000 for FortiOS 6.2.4 have the same default flow rules.

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

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

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

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

```
        set dst-l4port 88-88
        set action forward
        set forward-slot master
        set priority 5
        set comment "kerberos dst"
    next
    edit 3
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 179-179
        set dst-l4port 0-0
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp src"
    next
    edit 4
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 179-179
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp dst"
    next
    edit 5
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 520-520
        set dst-l4port 520-520
        set action forward
        set forward-slot master
        set priority 5
        set comment "rip"
    next
    edit 6
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 521-521
        set dst-l4port 521-521
        set action forward
        set forward-slot master
        set priority 5
```

```
        set comment "ripng"
    next
    edit 7
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 67-67
        set dst-l4port 68-68
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 server to client"
    next
    edit 8
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 68-68
        set dst-l4port 67-67
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 client to server"
    next
    edit 9
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 1723-1723
        set dst-l4port 0-0
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp src"
    next
    edit 10
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1723-1723
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp dst"
    next
```

```
edit 11
    set status enable
    set vlan 0
    set ether-type ip
    set protocol udp
    set src-l4port 0-0
    set dst-l4port 3784-3784
    set action forward
    set forward-slot master
    set priority 5
    set comment "bfd control"
next
edit 12
    set status enable
    set vlan 0
    set ether-type ip
    set protocol udp
    set src-l4port 0-0
    set dst-l4port 3785-3785
    set action forward
    set forward-slot master
    set priority 5
    set comment "bfd echo"
next
edit 13
    set status enable
    set vlan 0
    set ether-type ipv6
    set src-addr-ipv6 ::/0
    set dst-addr-ipv6 ::/0
    set protocol udp
    set src-l4port 547-547
    set dst-l4port 546-546
    set action forward
    set forward-slot master
    set priority 5
    set comment "dhcpv6 server to client"
next
edit 14
    set status enable
    set vlan 0
    set ether-type ipv6
    set src-addr-ipv6 ::/0
    set dst-addr-ipv6 ::/0
    set protocol udp
    set src-l4port 546-546
    set dst-l4port 547-547
    set action forward
    set forward-slot master
    set priority 5
    set comment "dhcpv6 client to server"
next
edit 15
    set status enable
    set vlan 0
    set ether-type ipv4
```

```
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 224.0.0.0 240.0.0.0
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 multicast"
    next
    edit 16
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ff00::/8
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 multicast"
    next
    edit 17
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 2123-2123
        set action forward
        set forward-slot master
        set priority 5
        set comment "gtp-c to master blade"
    next
    edit 18
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1000-1000
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "authd http to master blade"
    next
    edit 19
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1003-1003
        set tcp-flag any
        set action forward
```

```
        set forward-slot master
        set priority 5
        set comment "authd https to master blade"
    next
    edit 20
        set status enable
        set vlan 0
        set ether-type ip
        set protocol vrrp
        set action forward
        set forward-slot all
        set priority 6
        set comment "vrrp to all blades"
    next
end
```

Managing individual FortiGate-6000 management boards and FPCs

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

Special management port numbers

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

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

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

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

`https://192.168.1.99:44301`

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

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

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

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

FortiGate-6000 special management port numbers

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

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

To verify which slot you have logged into, the GUI header banner and the CLI prompt shows the current hostname. The 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 Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 1 (FPC01)	8021	44321	2321	2221	16121
Slot 2 (FPC02)	8022	44322	2322	2222	16122
Slot 3 (FPC03)	8023	44323	2323	2223	16123
Slot 4 (FPC04)	8024	44324	2324	2224	16124
Slot 5 (FPC05)	8025	44325	2325	2225	16125
Slot 6 (FPC06)	8026	44326	2326	2226	16126
Slot 7 (FPC07)	8027	44327	2327	2227	16127
Slot 8 (FPC08)	8028	44328	2328	2228	16128
Slot 9 (FPC09)	8029	44329	2329	2229	16129
Slot 10 (FPC10)	8030	44330	2330	2230	16130

Connecting to individual FPC consoles

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

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

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

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

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

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

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

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

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

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

Connecting to individual FPC CLIs

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

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

Where:

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

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

Performing other operations on individual FPCs

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

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

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

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

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

Managing individual FortiGate-7000 FIMs and FPMs

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

Special management port numbers

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

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

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

`https://192.168.1.99:44303`

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

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

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

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

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

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

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

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

To verify which module you have logged into, the GUI header banner and the CLI prompt shows its hostname. The 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 modules allows you to use FortiView or Monitor GUI pages to view the activity of that module. Even though you can log in to different modules, you can only make configuration changes from the primary FIM; which is usually the FIM in slot 1.

HA mode special management port numbers

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

FortiGate-7000 HA special management port numbers

Chassis and Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Ch1 slot 5	FPM05	8005	44305	2305	2205	16105
Ch1 slot 3	FPM03	8005	44303	2303	2203	16103
Ch1 slot 1	FIM01	8003	44301	2301	2201	16101
Ch1 slot 2	FIM02	8002	44302	2302	2202	16102
Ch1 slot 4	FPM04	8004	44304	2304	2204	16104
Ch1 slot 6	FPM06	8006	44306	2306	2206	16106
Ch2 slot 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	8025	44323	2323	2223	16123

Chassis and Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Ch2 slot 1	FIM01	8023	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

Managing individual FIMs and FPMs from the CLI

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

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

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

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

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

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

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

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

Upgrade information

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

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

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

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

See also, Upgrade information in the FortiOS 6.2.4 release notes.

You can find the FortiGate-6000 and 7000 for FortiOS 6.2.4 firmware images on the Fortinet Support Download Firmware Images page by selecting the **FortiGate-6K7K** product.

HA graceful upgrade to FortiOS 6.2.4

Use the following steps to upgrade a FortiGate-6000 or 7000 HA cluster with `uninterruptible-upgrade` enabled from FortiOS 6.0.8, 6.0.9, 6.0.10, or 6.2.3 to FortiOS 6.2.4.

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

To perform a graceful upgrade of your FortiGate-6000 or 7000 from FortiOS 6.0.8, 6.0.9, 6.0.10, or 6.2.3 to FortiOS 6.2.4:

1. Use the following command to enable uninterruptible-upgrade to support HA graceful upgrade:
   ```
   config system ha
      set uninterruptible-upgrade enable
   end
   ```
2. Download FortiOS 6.2.4 firmware for FortiGate-6000 or 7000 from the https://support.fortinet.com FortiGate-6K7K 6.2.4 firmware image folder.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. Verify that you have installed the correct firmware version. For example, for the FortiGate-7040E:

   ```
   get system status
   Version: FortiGate-7040E v6.2.4,build1116,200813 (GA)
   ...
   ```

About FortiGate-6000 firmware upgrades

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

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

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

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

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

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

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

About FortiGate-7000 firmware upgrades

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

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

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

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

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

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

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

Product integration and support

This section describes FortiGate-6000 and 7000 for FortiOS 6.2.4 Build 1116 product integration and support information. The Product integration and support information described in the FortiOS 6.2.4 release notes also applies to FortiGate-6000 and 7000 FortiOS 6.2.4 Build 1116.

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

- FortiGate-6000: FortiManager or FortiAnalyzer 6.2.6 or 6.4.2.
- FortiGate-7000: FortiManager or FortiAnalyzer 6.2.6 or 6.4.2.

FortiGate-6000 6.2.4 special features and limitations

FortiGate-6000 for FortiOS 6.2.4 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-6000 v6.2.4 section of the FortiGate-6000 handbook.

FortiGate-7000 6.2.4 special features and limitations

FortiGate-7000 for FortiOS 6.2.4 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000 v6.2.4 section of the FortiGate-7000 handbook.

Maximum values

Maximum values for FortiGate-6000 and FortiGate-7000 for FortiOS 6.2.4 are available from the FortiOS Maximum Values Table (https://docs.fortinet.com/max-value-table).

Resolved issues

The following issues have been fixed in FortiGate-6000 and FortiGate-7000 FortiOS 6.2.4 Build 1116. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 6.2.4 release notes also apply to FortiGate-6000 and 7000 FortiOS 6.2.4 Build 1116.

Bug ID	Description
508610	Resolved an issue that could light the LEDs of interfaces that are not connected.
513339	Finisar FCLF8521p2BTL (FG-TRAN-GC) and (FS-TRAN-GC) FCLF8522P2BTL transceivers are now supported.
516970	The `Telnet-to-console line connected` message has been corrected to read `Network-to-console line connected`.
570475	Selecting **Clear Counters** on the firewall policy list GUI page now successfully clears the counters for the selected policy.
594750	Resolved an issue that prevented FSSO users from being removed when de-authenticated on Firewall User Monitor page.
601849	The FortiView quarantine monitor GUI page now works as expected when you select **All-FortiGate**.
602530	Resolved an issue that caused `httpsd` process crashes.
604304	More SDN connectors supported. For more information, see SDN connector support on page 22.
605411	Management traffic (local in and local out) is now accepted by inter-VDOM link interfaces if the inter-VDOM link type is set to ppp (point to point).
606543	The correct list of interfaces appears on the **Allow other FortiGates to join** list on the Security Fabric GUI page.
607418	Resolved an issue that prevented the Firewall User Monitor from displaying if FortiOS is managing a large number of users.
607521	Resolved an issue that removed logged in LDAP users after a secondary FortiGate joined the primary FortiGate in an HA configuration.
607772	Resolved an issue that caused the system to enter conserve mode and not be able to recover after logging in thousands of LDAP users.
607921	The Configuration Sync Monitor now shows correct status information for the secondary FortiGate-6000 management board or FortiGate-7000 primary FIM.
610828	Resolved an issue that delayed synchronizing RSSO users to all FPCs or FPMs.
611558	Resolved an issue that could sometimes cause synchronization delays after making configuration changes on a system managing many logged in users.

Bug ID	Description
612357	The `execute factoryreset-shutdown` command now successfully resets the configuration to factory defaults when run on a secondary FortiGate-6000F in an HA cluster with `uninterruptible-upgrade` enabled.
612444	When a FortiGate-6000 or 7000 forms a cluster with another FortiGate-6000 or 7000 already operating in HA mode, the active RSSO user list is now successfully synchronized to the FPCs or FPMs in the newly joined FortiGate-6000 or 7000.
613295	Resolved an issue that caused a FortiGate-6000 or 7000 to be out of sync after disabling the FortiOS Carrier license.
614858	Web filter override policies no longer time out early.
620231	Resolved some GUI performance issues.
620233	Resolved an issue that could cause the Configuration Sync Monitor to display incorrect synchronization status information.
620338	Users can now ping the FortiGate-6000 or 7000 internal network LAN interface from a remote host through an IPsec tunnel.
621375	Resolved an issue that could cause an HA graceful firmware upgrade to time out if the configuration has a large number of VDOMs.
622081	Resolved an issue that caused FPC or FPM synchronization issues after upgrading an HA cluster with `uninterruptable-upgrade` disabled.
623123	Resolved a performance issue that caused unexpected HA failovers for an HA cluster with a large number of VLANs.
623471	Resolved an issue with automatically changing the time after daylight saving time started.
624655	Performing an SNMP walk no longer times out on `bgp4PathAttrIpAddrPrefix` when the system has a large BGP configuration.
624927	The `fgHaStatsGlobalChecksum` SNMP query now receives the correct information from a FortiGate-6000 or 7000 HA cluster.
626073	The FortiGate-6000 management board now correctly aggregates SNMP logs for an `fgFwPolStatsEntry` query.
626086	Performing an SNMP walk no longer fails on a FortiGate-7000 when the primary FPM has different VDOM IDs than the primary FIM.
627404	Resolved an issue that caused the GUI to incorrectly show Cisco ACI connector status as down.
632416	Log messages stating that the backplane channel is unstable are no longer generating when making configuration changes.
633182	The ESXi SDN connector now stays up on the FortiGate-6000 management board and on all FPCs.
633224	Resolved an issue that caused FPMs to crash with NP6 LACP errors after rebooting when the FortiGate-6000 has multiple LACP LAG interfaces.
633561	Resolved an issue that prevented pinging VLAN interfaces in a transparent mode VDOM.

Bug ID	Description
633597	Resolved an issue that could prevent the FortiGate-7000 primary FIM from connecting to an FSSO server.
633925	Resolved an issue that displayed error messages on some FPC consoles in an HA configuration after a firmware upgrade.
634049	Resolved an issue that prevented synchronizing GTP-C tunnels to a restarted FPM.
634949	Resolved a VRRP issue that prevented transparent mode VDOMs from processing management traffic correctly whenVRRP is enabled.
635122	Resolved an issue that caused traffic to be blocked for 2-3 seconds during an FGCP HA failover.
635163	The `diagnose sys sdn status` command when run from the management board no longer shows that all are SND connectors are down while no ACI connectors are configured.
635189	The ACI SDN command to clear all dynamic addresses now also clears addresses on the FPMs and FPCs.
637640 641678	Resolved an issue with the IPS that could cause CA certificates to be removed from the IPS configuration when deleting a VDOM.
638568	Resolved an issue with the information displayed on the Firewall User Monitor when displaying information about LDAP and FSSO users.
638601	Resolved an issue that prevented FSSO users from being removed from FPCs in an HA configuration when de-authenticated from the Firewall User Monitor.
638988	Resolved an issue that could prevent the `src-dst-ip` load balancing distribution method from being implemented correctly on some hardware components after a reboot.
639064	Resolved an issue that prevented displaying information on FPCs about traffic matching a firewall policy with the `negate` option enabled.
639210	FSSO sessions re now successfully removed after FSSO users log off.
640028	Resolved an issue that caused the `sessionsync` process to use excessive amounts of CPU resources.
640388	The IPsec VPN monitor on the primary FIM GUI now displays correct status information for DDNS tunnels.
640687	Resolved an issue that could change the `chassis-id` after restoring the configuration of a FortiGate-6000 or 7000 in an HA cluster.
640698	Resolved an issue that could result in an FPM or FPC having an incorrect special management port number after changing the HA chassis ID.
641455	Resolved an issue that prevented logged off FSSO users from being removed from the secondary FortiGate-6000 or 7000 in an HA configuration.
642400	Resolved an issue with virtual clustering that prevented log messages from being recorded by FortiAnalyzer for a VDOM when the primary virtual cluster for that VDOM was switch from the primary to the secondary FortiGate.
642524	Synchronizing IPv6 static routes when they are added to a transparent mode VDOM to FPC or FPM FIBs no longer requires a reboot.

Bug ID	Description
643811	Resetting the uptime of a FortiGate-6000 or 7000 HA cluster no longer causes a split brain scenario.
645802	FSSO logins from a PC with multiple network interfaces are now shown correctly on the Firewall Users Monitor.
648298	Resolved an issue that displayed error messages during system startup after installing a new firmware build from the BIOS after a reboot.
651033	Adding multiple resource usage widgets to the same dashboard no longer slows down GUI performance.
653000	Resolved an issue that caused the FortiGate-6000 `csfd` process to crash.

Known issues

The following issues have been identified in FortiGate-6000 and FortiGate-7000 FortiOS 6.2.4 Build 1116. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 6.2.4 release notes also apply to FortiGate-6000 and 7000 FortiOS 6.2.4 Build 1116.

Bug ID	Description
479303	VLAN interface status monitoring using the `config system ha-monitor` command does not work.
600879	Firewall policy packet capturing, turned on by enabling `capture` in a firewall policy, does not work.
603601	Cisco ACI SDN connector traffic uses a data interface instead of a management interface.
606529	The FortiGate-6000 and 7000 are not compatible with FortiNAC.
608729	IPsec phase 2 auto-negotiation does not work with VPN load-balancing.
612622	SSL sessions to FortiSandbox are not initiated when `set source-ip` is enabled.
613139	DNS requests logs may contain incorrect source IP addresses.

613617	The `source-ip` setting when configuring FortiGuard and FortiSandbox and other services may not work as expected. As a result of configuring a `source-ip`, only the FortiGate-6000 management board or the FortiGate-7000 primary FIM can connect to the service. Services that only require management board or primary FIM connections will operate as expected. However, many services require FPCs or FPMs to be able to connect to the service. In these cases, setting a `source-ip` prevents FPCs and FPMs from connecting to the service.
	For example, when you set a `source-ip` using the following command, only the management board or primary FIM can contact FortiGuard for updates.
	`config system fortiguard`
	`  set source-ip <ip-address>`
	`end`

624678	SSLVPN web mode RDP traffic is not load balanced to FPCs or FPMs.
627903 605065	You cannot set a management interface LAG to be the SLBC management interface by adding it to the `config load-balance setting slbc-mgmt-intf` option.
632954	In a FortiGate-6000 or 7000 HA configuration, if you configure a VLAN interface to be the system management interface, you cannot connect to individual FPMs or FPCs on the secondary FortiGate-6000 or 7000 using special management port numbers.
632961	In a FortiGate-7000 HA configuration, the secondary FortiGate-7000 cannot synchronize with the primary FortiGate-7000 after loading a configuration file with an external security fabric configuration.
635442	SDN connector dynamic addresses are not synchronized between the FortiGate-6000s or 7000s in an FGCP HA cluster.
635310	VLAN interfaces added to accelerated npu_vdom link interfaces cannot pass traffic.
635591	The `reportd` process may consume excessive amounts of CPU time.
640520	The `diagnose wad session` command is not available.

Bug ID	Description
643032	In an HA configuration, the secondary FortiGate-6000 or 7000 may incorrectly generate event log messages similar to: `Files were dropped by quard to FortiSandbox: 0 reached max retries.`
649682	In some cases of FortiGate-6000 HA clusters with large configurations, the secondary FortiGate-6000 may not be able to synchronize with the primary FortiGate-6000. To workaround this issue, remove the secondary FortiGate-6000 from the cluster, reset it to factory defaults, and then restore its configuration using a backed up configuration file from the primary FortiGate-6000.
650894	The FortiManager IPsec Tunnel monitor may incorrectly show that FortiGate-6000 IPsec tunnels are down.
651743	IPsec SAs are not synchronized between cluster units in FCGP HA clusters.
652777	Because of an issue with how IPsec sessions are handled, the same session may incorrectly contain the `synced` and `nosyn_ses` flags.
653636	Some of the interfaces in a FortiGate-7000 cross-FIM LAG remain in the negotiating state instead of switching to the established state. You can workaround this problem by using the `fnsysctl ifconfig <interface> {down | up}` command to bring the problematic LAG members down and then back up.
654420	In an HA configuration, the secondary FortiGate-6000 or 7000 may record the following critical event log: `Scanunit initiated a virus engine/definitions update.`
664898	When a DoS attack is successfully detected and blocked, because the threshold is determined per-FPC or per-FPM, the FortiGate-6000 or 7000 does not create an anomaly log message or quarantine the source of the attack.