FortiGate-6000 and FortiGate-7000 - Release Notes

Version 6.0.6 Build 6392

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

July 15, 2019
FortiGate-6000 and FortiGate-7000 6.0.6 Build 6392 Release Notes
01-606-557996-20200715

TABLE OF CONTENTS

Change log

Date	Change description
July 15, 2010	Minor updates to HA graceful upgrade to FortiOS 6.0.6 on page 38.
December 20, 2019	Initial version.

FortiGate-6000 and FortiGate-7000 6.0.6 release notes

This document provides release information for FortiGate-6000 and 7000 for FortiOS 6.0.6 build 6392.

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

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

Supported models

FortiGate-6000 and FortiGate-7000 for FortiOS 6.0.6 Build 6392 supports the following models:

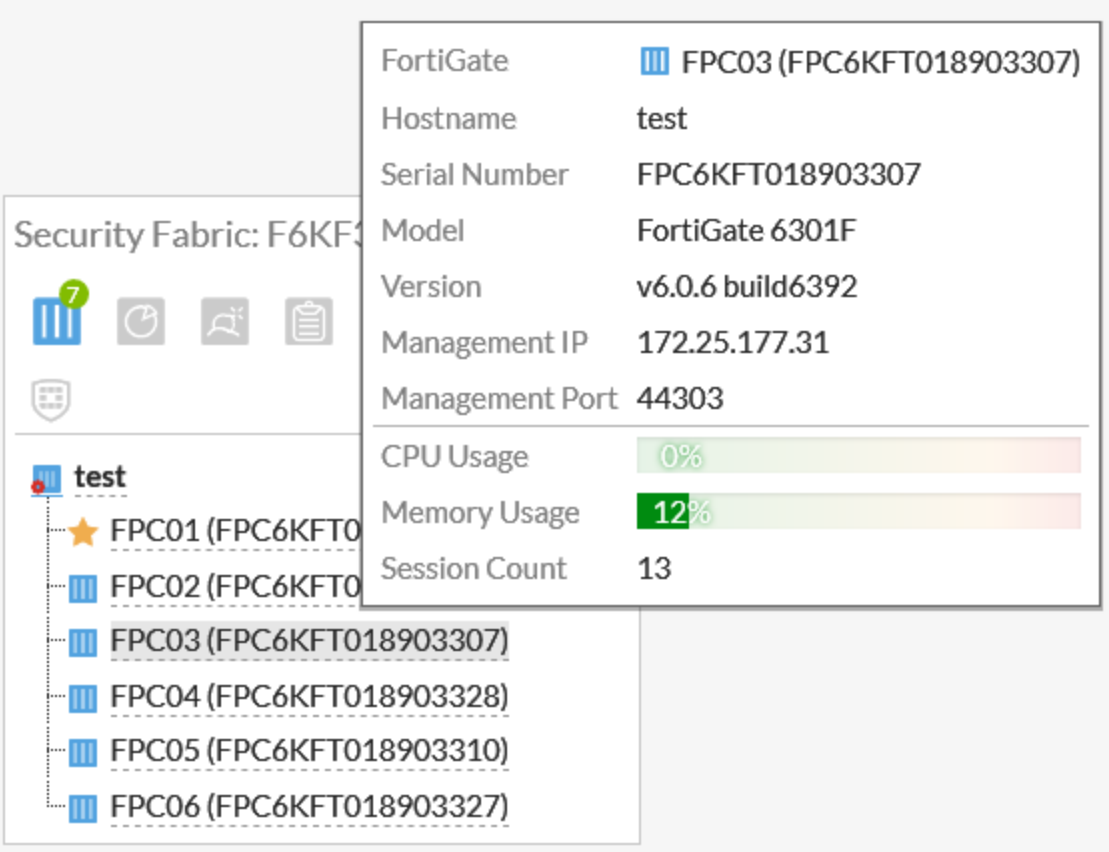
- FortiGate-6300F
- FortiGate-6301F
- FortiGate-6500F
- FortiGate-6501F
- FortiGate-7030E
- FortiGate-7040E
- FortiGate-7060E

What's new

The following new features have been added to FortiGate-6000 and 7000 for FortiOS 6.0.6 build 6392.

Security Fabric dashboard widget improvements

The Security Fabric dashboard widget uses a star icon to highlight the primary (master) FPC or FPM. You can also hover your mouse cursor over individual FPCs, FIMs, or FPMs on the Security Fabric dashboard widget to display information about the component. Information includes the management IP and special HTTPS management port number. You can also click on any component and select an option to view the component on a Security Fabric topology or log into it using the management IP address and special management port number.



Standalone configuration synchronization

FortiGate-6000 and 7000 for FortiOS 6.0.6 supports configuration synchronization (also called standalone configuration synchronization) for two FortiGate-6000s or two FortiGate-7000s. Configuration synchronization means that most configuration changes made to one of the FortiGate-6000s or 7000s are automatically synchronized to the other one.

Use the following command on both FortiGates to enable configuration synchronization:

```
config system ha
   set standalone-config-sync enable
end
```

In addition to enabling configuration synchronization, you must set up HA heartbeat connections between the FortiGate-6000s or 7000s. One HA heartbeat connection is required, two are recommended. Use the following command to enable heartbeat configuration for the FortiGate-6000 HA1 and HA2 interfaces. The FortiGate-7000 configuration would include the 1-M1, 1-M2, 2-M1, and 2-M2 interfaces.

```
config system ha
   set hbdev ha1 50 ha2 50
end
```

When you enable configuration synchronization and configure and connect the heartbeat devices, FGCP primary unit selection criteria selects a config sync primary (or master) FortiGate. Normally, the FortiGate with the highest serial number becomes the config sync primary and the other FortiGate becomes the config sync secondary.

All configuration changes that you make to the primary are synchronized to the secondary. To avoid synchronization problems, Fortinet recommends making all configuration changes to the primary.

Selecting the config sync primary

You can use device priority to select one of the FortiGates to become the config sync primary. For example, the following command enables configuration synchronization and sets a higher device priority than the default of 128 to make sure that this FortiGate becomes the primary.

```
config system ha
   set standalone-config-sync enable
   set priority 250
end
```

Settings that are not synchronized

Configuration synchronization does not synchronize settings that identify the FortiGate to the network. The following settings are not synchronized:

- Transparent mode management IPv4 and IPv6 IP addresses and default gateways.
- All `config system cluster-sync` settings.
- All `config system interface` settings except `vdom`, `vlanid`, `type` and `interface`.
- All `config firewall sniffer` settings.
- All router BFD and BFD6 settings.
- The following BGP settings: `as`, `router-id`, `aggregate-address`, `aggregate-address6`, `neighbor-group`, `neighbor`, `network`, and `network6`.

- The following OSPF settings: `router-id`, `area`, `ospf-interface`, `network`, `neighbor`, and `summary-address`.
- The following OSPF6 settings: `router-id`, `area`, and `ospf6-interface`.
- All RIP settings.
- All policy routing settings.
- All static routing settings.

Limitations

When configuration synchronization is enabled, there are some limitations, including but not limited to the following:

- Configuration synchronization does not support graceful HA firmware upgrades. If you upgrade the firmware of the config sync primary, the secondary also upgrades at the same time, disrupting network traffic. You can avoid traffic interruptions by disabling configuration synchronization and upgrading the firmware of each FortiGate separately.
- The configuration settings that are synchronized might not match your requirements. The current design and implementation of configuration synchronization is based on requirements from specific customers and might not work for your implementation.
- It can be difficult to control which FortiGate-6000 becomes the config sync primary and the config sync primary can dynamically change without notice. This could result in accidentally changing the configuration of the secondary or overwriting the configuration of the intended primary.

FortiLink support

FortiGate-6000 and 7000 for FortiOS 6.0.6 supports managing FortiSwitch devices over FortiLink. You can manage up to 300 FortiSwitch devices from one FortiGate-6000 or 7000.

FortiGate-6000 and 7000 for FortiOS 6.0.6 does not support upgrading managed FortiSwitch firmware from the **FortiOS Managed FortiSwitch GUI** page. Instead you must use the FortiGate-6000 or 7000 CLI or log into the managed FortiSwitch to upgrade managed FortiSwitch firmware.

Use the following command to enable Fortilink support:

```
config system global
   set switch-controller enable
end
```

The Managed FortiSwitch GUI pages appear under the **WiFi & Switch Controller** GUI menu.

A FortiGate-6000 or 7000 manages one or more FortiSwitches through one active FortiLink. The FortiLink can consist of one physical interface or multiple physical interfaces in a LAG. To set up a FortiGate interface as a FortiLink, from the GUI go to **Network > Interface**, select an interface, and set the **Addressing mode** to **Dedicated to FortiSwitch**.

You can also use the following CLI command to set the port7 interface of a FortiGate-6000 device to be the FortiLink:

```
config system interface
   edit port7
      set auto-auth-extension-device enable
      set fortilink enable
   end
```

```
end
```

You can use any traffic interface as the FortiLink. Using the HA and management interfaces is not supported.

For more information about FortiLink support and managing FortiSwitches, see FortiSwitch devices managed by FortiOS.

FortiGate-7000 FortiLink limitations

The FortiGate-7000 has the following FortiLink limitations:

- The FIM in slot 1 (FIM-01) must be the primary FIM. FortiLink will not work if FIM-02 is the primary FIM.

In an HA configuration, if the FIM in slot 1 of the primary FortiGate-7000 fails, the secondary FortiGate-7000 becomes the new primary FortiGate-7000 with a functioning FIM in slot 1 and FortiLink support continues after the failover.

- FortiGate-7000 for FortiOS 6.0.6 does not support upgrading managed FortiSwitch firmware from the **FortiOS Managed FortiSwitch GUI** page. Instead you must use the FortiGate-7000 CLI or log into the managed FortiSwitch to upgrade managed FortiSwitch firmware.

In-band management support

FortiOS 6.0.6 for FortiOS-6000 and FortiGate-7000 supports in-band management connections to all data interfaces. You can connect to physical interface IP addresses as well as in-band VLAN interfaces and LAGs.

No configuration changes are required to support in-band management, other than setting administrative access settings for the data interface that you want to use to manage the FortiGate-6000 or 7000. 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 FortiGate-7000 primary FIM. Administrators with VDOM-level access can log into to their VDOM if they connect to a data interface that is in their VDOM.

Previous versions of FortiOS for FortiGate-6000 and 7000 included the `config system set motherboard-traffic-forwarding` command to allow limited in-band management. This command has been removed from FortiOS 6.0.6.

In-band management limitations

In-band management has the following limitations:

- In-band management does not support using special port numbers to connect to individual FPCs, FIMs, or FPMs. If you have logged in using an in-band management connection, the special management HTTPS port numbers appear on the Security Fabric dashboard widget when you hover over individual FPCs, FIMs, or FPMs. You can click on an FPC, FIM, or FPM in the Security Fabric dashboard widget and select **Login to...** to log into the GUI of that FPC, FIM, or FPM. This action creates an out-of-band management connection by crafting a URL that includes the IP address of the FortiGate-6000 mgmt1 interface or the FortiGate-7000 mgmt interface, plus the special HTTPS port number required to connect to that FPC, FIM, or FPM.
- The data interfaces must have IPv4 IP addresses, IPv6 in-band management is not supported.
- In-band management connections to the IP address of a VDOM link interface is not supported.

- Large (or jumbo) packets from in-band management sessions are fragmented by the FPCs or FPMs before they are forwarded to the management board or primary (master) FIM.
- SNMP in-band management is not supported.
- VRF routes are not applied to outgoing in-band management traffic.
- Changes made on the fly to administrative access settings are not enforced for in-progress in-band management sessions. The changes apply to new in-band sessions only. For example, if an administrator is using SSH for an in-band management connection and you change the SSH administrative port, that in-band management session can continue. Any out-of-band management sessions would need to be restarted with the new port number. New in-band SSH management sessions need to use the new port number. HTTPS access works the same way; however, HTTPS starts new sessions every time you navigate to a new GUI page. So an on the fly change would affect an HTTPS in-band management session whenever the administrator navigates to a new GUI page.
- In-band management is not supported for connections to data interfaces that are in a transparent mode VDOM.

HA route-ttl option available

You can now use the HA route time to live (`route-ttl`) option to control how long routes remain active in the new primary (master) FortiGate-6000 or 7000 after an FGCP HA failover. The default `route-ttl` is 600 seconds. The range is 5 to 3600 seconds (one hour). You can use the following command to change the `route-ttl` time.

```
config system ha
   set route-ttl <time>
end
```

FortiOS 6.0.6 for FortiGate-6000 and 7000 does not support the `route-wait` and `route-hold` options.

To maintain communication sessions through a new primary FortiGate, routes remain active in the routing table for the `route-ttl` time while the new primary FortiGate acquires new routes. Normally keeping `route-ttl` to the default value of 600 seconds (10 minutes) is acceptable because acquiring new routes and populating the routing tables of multiple FPCs or FIMs and FPMs can take a few minutes.

If the primary FortiGate needs to acquire a very large number of routes, or if for other reasons there is a delay in acquiring all routes, the primary FortiGate may not be able to maintain all communication sessions after a failover.

You can increase the `route-ttl` time if you find that communication sessions are lost after a failover. Increasing the `route-ttl` time allows the primary unit to use synchronized routes that are already in the routing table for a longer period of time while waiting to acquire new routes.

Enhanced MAC (EMAC) VLAN support

The media access control (MAC) virtual local area network (VLAN) feature allows you to configure multiple virtual interfaces with different MAC addresses (and therefore different IP addresses) on a physical interface.

For more information about EMAC VLAN support, see Enhanced MAC VLANs.

Use the following command to configure an EMAC VLAN:

```
config system interface
   edit <interface-name>
      set type emac-vlan
      set vlan-id <VLAN-ID>
      set interface <physical-interface>
   end
```

New command to temporarily select the primary (master) FPC or FPM

You can log into the FortiGate-6000 management board CLI or the FortiGate-7000 primary FIM CLI and use the following command to force one of the FPCs or FPMs to always be the primary or master FPC or FPM:

```
execute load-balance slot set-master-worker <slot>
```

Where `<slot>` is the FPC or FPM slot number.

The change takes place right away and all new primary FPC or FPM sessions are sent to the new primary FPC or FPM. Sessions that had been processed by the former primary FPC or FPM do not switch over, but continue to be processed by the former primary FPC or FPM.

This command is most often used for troubleshooting or testing. Since it is not a configuration change, if the FortiGate-6000 or 7000 reboots, the usual primary FPC or FPM selection process occurs.

Changes to FortiGate-7000 license handling

You can use the FortiGate-7000 `execute load-balance license-mgmt {list | reset}` command to list or reset the licenses that you have added for strong crypto, additional FortiClient licenses, or more VDOMs. The FortiGate-7000 platform uses the System Management Module (SMM) (or shelf manager) to manage these licenses for all of the FIMs or FPMs in your FortiGate-7000.

The `execute load-balance license-mgmt list` command lists all of the licenses currently managed by the SMM.

You can use the following command to reset all or one of the licenses that are currently managed by the SMM.

```
execute load-balance reset {all | crypto-key | forticlient | vdom}
```

When you reset one or more licenses, the SMM removes the licenses from all of the FIMs and FPMs in the FortiGate-7000. The FortiGate-7000 doesn't need to restart to reset these licenses.

FortiGate-6000 FN-TRAN-SFP+GC transceiver support

FortiOS 6.0.6 adds support to the FortiGate-6000 for FN-TRAN-SFP+GC transceivers. These 10GigE SFP+ transceivers can be connected to any FortiGate-6000 management, HA, or data interface. To use these transceivers with an interface, the interface speed must be set to `10000full`.

FortiGate-6000 IPsec VPN load balancing support

FortiGate-6000 for FortiOS 6.0.6 supports IPsec VPN load balancing for IPsec VPN sessions terminated by the FortiGate-6000 when static routes are used for communication over the VPN tunnel. If dynamic routing is required, then IPsec VPN load balancing must be disabled.

As well, because of static routing support, FortiGate-6000 for FortiOS 6.0.6 no longer requires you to add source and destination subnets to phase 2 configurations.

You can enable or disable IPsec VPN load balancing using the following command:

```
config load-balance settings
   set ipsec-load-balance {enable | disable}
end
```

For the FortiGate-6000, IPsec load balancing is enabled by default. For the FortiGate-7000, IPsec load balancing is not supported and is disabled by default

If IPsec load balancing is enabled, the DP3 processor load balances IPsec VPN traffic to the FPCs according to the `dp-load-distribution-method` configuration. If you disable IPsec load balancing, all IPsec sessions are sent to the primary FPC.

Previous versions of FortiOS for FortiGate-6000 used load balancing flow rules. These rules are no longer required and Fortinet recommends that you manually remove them. See Manually deleting IPsec VPN load balancing flow rules on page 39.

FortiGate-7000 IPsec VPN load balancing changes

FortiGate-7000 for FortiOS 6.0.6 does not support IPsec VPN load balancing and `ipsec-vpn-load-balance` must be disabled (and is disabled by default). Just like the FortiGate-6000, when `ipsec-vpn-load-balance` is disabled, all IPsec VPN traffic is sent to the primary FPM and no load balancing flow rules are required.

Previous versions of FortiOS for FortiGate-7000 used load balancing flow rules. These rules are no longer required and Fortinet recommends that you manually remove them. See Manually deleting IPsec VPN load balancing flow rules on page 39.

As well, FortiGate-7000 for FortiOS 6.0.6 no longer requires you to add source and destination subnets to phase 2 configurations.

New execute factoryreset3 command

You can log into a FortiGate-6000 FPC or FortiGate-7000 FPM or FIM and use the following command to reset the configuration of the component to the factory default configuration and shut the component down. This command is normally used in preparation for resetting and shutting down a FortGate-6000 or 7000.

```
execute factoryreset3
```

New FortiGate-6000 data interface maximum MTU

You can now set the FortiGate-6000 data interface MTU value to a maximum of 9216. Due to hardware limitations, the FortiGate-7000 MTU maximum value remains as 9198.

FortiGate-6000 real servers maximum value increase

The FortiGate-6000 maximum value for the number of real servers per virtual server has been increased to 1024. The FortiGate-7000 value remains at 32. You can review these and other maximum values in the FortiOS Maximum Values Table (https://docs.fortinet.com/max-value-table).

Fragmented ICMP packet handling improvements

Previous versions of FortiOS would handle fragmented ICMP packets in the following way:

1. The FortiGate-6000 DP3 processor and the FortiGate-7000 DP2 processor would broadcast all non-header fragmented ICMP packets to all FPCs or FPMs.
2. FPCs or FPMs that also received the header fragments of these packets would re-assemble the packets correctly.
3. FPCs or FPMs that did not receive the header fragments would discard the non-header fragments.

FortiOS 6.0.6 supports the following more efficient load balancing of fragmented ICMP packets:

1. When the DPx processor receives a header fragment packet, if a matching session is found, the DPx processor creates an additional fragment session matching the source-ip, destination-ip, and IP identifier (IPID) of the header fragment packet.
2. Subsequent non-header fragments will match this fragment session and be forwarded to the same FPC or FPM as the header fragment.

You can use the following command to enable or disable this method of handling fragmented ICMP packets. The option is enabled by default.

```
config load-balance setting
   set dp-fragment-session {disable | enable}
end
```

The age of the fragment session can be controlled using the following command:

```
config system global
   set dp-fragment-timer <timer>
end
```

The default `<timer>` value is 120 seconds.

New command to rollback firmware

From the FortiGate-6000 management board or the FortiGate-7000 primary FIM, you can use the following command to change the firmware image that the management board and all of the FPCs or all of the FIMs and FPMs load the

next time the FortiGate-6000 or 7000 starts up.

```
execute set-next-reboot rollback
```

This command causes each component to select the firmware image stored on its non-active partition the next time the system starts up. This new command replaces the need to log into each component CLI and running the `execute set-next-reboot {primary | secondary}` command.

New command to display the process name associated with a process ID

You can use the following command to display the process name associated with a process ID (PID):

```
diagnose sys process nameof <pid>
```

Where `<pid>` is the process ID.

Changes in how to manage individual components in HA mode

FortiOS 6.0.6 no longer supports using the `execute load-balance slot manage` command to access the CLI of the other chassis in a FortiGate-6000 or 7000 HA configuration.

Instead, from the primary or master FortiGate-6000 or 7000 CLI you must use the `execute ha manage` command to log into the secondary FortiGate-6000 or 7000. This command logs you into the secondary FortiGate-6000 management board or FortiGate-7000 primary FIM. From here you can use the `execute load-balance slot manage` command to access the CLIs of different FPCs or FIMs and FPMs in the secondary FortiGate-6000 or 7000.

Changes to checking configuration synchronization

FortiOS 6.0.6 for FortiGate-6000 and 7000 changes the information provided by the following commands:

- `diagnose sys confsync status`
- `diagnose sys confsync showcsum`
- `diagnose sys ha checksum cluster`

For details about the new functionality:

- For the FortiGate-6000, see Confirming that FortiGate-6000 components are synchronized and Confirming that the FortiGate-6000 HA cluster is synchronized.
- For the FortiGate-7000, see Confirming that the FortiGate-7000 is synchronized and Confirming that the FortiGate-7000 HA cluster is synchronized.

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 6.0.6 build 6392.

Resolving HA cluster chassis ID conflicts

In a FortiGate-6000 or 7000 FGCP HA configuration, if both FortiGates in the cluster are incorrectly configured with the same chassis ID, the FortiGate with the lowest serial number will be shut down. The other FortiGate will continue to operate as a standalone FortiGate in HA mode.

You can resolve the chassis ID conflict by restarting the shut down FortiGate-6000 or 7000 and configuring the FortiGate-6000s or 7000s with different chassis IDs. You should prevent the devices from forming a cluster before you change the chassis IDs. For example, you could change the chassis ID of the operating device or revert it to standalone mode before re-starting the shut down FortiGate.

Once both FortiGates are operating in HA mode with different chassis IDs, they will negotiate to form a cluster, and if their chassis IDs are different the cluster will begin to operate normally.

Also, if you are setting up a cluster of FortiGate-6301Fs or 6501Fs, before you configure HA, consider using the `execute disk list` command on each FortiGate to verify that they both have the same disk and RAID configuration. If the disk or RAID configurations are different, when the cluster forms the FortiGate that would become the secondary will be shut down. You can use the `execute disk format` command to format the disks and the `execute disk raid` command to set both FortiGates to the same RAID mode.

Default Security Fabric configuration

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

Default Security Fabric configuration:

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

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

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

Adding a flow rule to support DHCP relay

The FortiGate-6000 and 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 firmware on individual FIMs and FPMs for detailed procedures for upgrading FortiGate-6000 firmware from the BIOS.

Installing firmware on an individual FortiGate-6000 FPC

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

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

   This command uploads the firmware image to the FPC and the FPC restarts. When the FPC starts up, the configuration is reset to factory default settings and then synchronized by the management board. The FPC restarts again, rejoins the cluster, and is ready to process traffic.
4. To verify that the configuration of the FPC has been synchronized, enter the `diagnose sys confsync`

`status | grep in_sy` command. The command output below shows an example of the synchronization status of some of the FPCs in an HA cluster of two FortiGate-6301F devices. The field `in_sync=1` indicates that the configuration of the FPC is synchronized.

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

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

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

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

Installing firmware on an individual FortiGate-7000 FPM

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

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

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

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

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

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

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

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

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

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

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

SD-WAN is not supported

FortiGate-6000 and FortiGate-7000 Version 6.0.6 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 6.0.6 for FortiGate-6000 and FortiGate-7000 does not support the following IPsec VPN features:

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

Quarantine to disk not supported

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

Local out traffic is not sent to IPsec VPN interfaces

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

Special configuration required for SSL VPN

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

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

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

If you change the SSL VPN server listening port

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

```
config load-balance flow-rule
   edit 26
      set status enable
      set ether-type ipv4
      set protocol tcp
      set src-interface port12
```

```
    set dst-l4port 10443-10443
    set forward-slot master
    set comment "ssl vpn server to primary worker"
  end
```

Adding the SSL VPN server IP address

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

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

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

Example FortiGate-6000 HA heartbeat switch 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-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 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-6000s in the HA configuration, 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 hbdev "ha1" 50 "ha2" 100
  set hbdev-vlan-id 4091
  set hbdev-second-vlan-id 4092
```

```
end
```

2. Use the `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 port 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 FortiGate-7000 HA heartbeat 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 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 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
```

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

The default `configure load-balance flow-rule` command contains the recommended default flow rules that control how the FortiGate-6000 or 7000 handles traffic types that cannot be load balanced. Most of the flow rules in the default configuration are enabled and are intended to send common traffic types that cannot be load balanced to the primary FPC or FPM. FortiGate-6000 and 7000 for FortiOS 6.0.6 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 CLI prompt also shows slot address in the format `<hostname> [<slot address>] #`.

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

HA mode special management port numbers

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

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

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

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

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

Connecting to individual FPC consoles

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

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

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

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

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

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

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

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

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

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

Connecting to individual FPC CLIs

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

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

Where:

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

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

Performing other operations on individual FPCs

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

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

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

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

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

Managing individual FortiGate-7000 FIMs and FPMs

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

Special management port numbers

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

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

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

`https://192.168.1.99:44303`

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

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

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

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

FortiGate-7000 special management port numbers

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

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

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

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

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

HA mode special management port numbers

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

FortiGate-7000 HA special management port numbers

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

Managing individual FIMs and FPMs from the CLI

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

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

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

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

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

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

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

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

Upgrade information

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

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

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

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

HA graceful upgrade to FortiOS 6.0.6

Use the following steps to upgrade a FortiGate-6000 or 7000 HA cluster with `uninterruptible-upgrade` enabled from FortiOS 5.6.7, 5.6.11, or 6.0.4 to FortiOS 6.0.6 Build 6392.

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

This procedure supports upgrading from the following firmware versions:

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

Performing this upgrade requires installing an interim upgrade support image before installing the final FortiOS 6.0.6 firmware image.

Starting image	Upgrade support image	Final image
5.6.7 build 4214 or 4261	6.0.4 build 8428	6.0.6 Build 6392
5.6.11 build 4279	6.0.4 build 8428	6.0.6 Build 6392
6.0.4 build 6145 or 8405	6.0.4 build 8428	6.0.6 Build 6392

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

- FortiGate 6000F: **FGT_6000F-v6-build8428-Upgrade-Support-FORTINET.out**
- FortiGate 7000E: **FGT_7000E-v6-build8428-Upgrade-Support-FORTINET.out**

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

To perform a graceful upgrade of your FortiGate-6000 or 7000 to FortiOS 6.0.6 Build 6392:

1. Use the following command to enable `uninterruptible-upgrade` to support HA graceful upgrade:
   ```
   config system ha
      set session-pickup enable
      set uninterruptible-upgrade enable
   end
   ```
2. Download the FortiGate-6000 or 7000 upgrade support image file from the https://support.fortinet.com FortiOS 6.0.6 firmware image folder.
3. Perform a normal upgrade of your HA cluster using the upgrade support image.
4. Verify that you have installed the correct interim firmware version. For example, for the FortiGate-7040E:
   ```
   get system status
   Version: FortiGate-7040E v6.0.4,build8428,190813 (GA)
   ...
   ```
5. Download the FortiGate-6000 or 7000 FortiOS 6.0.6 build 6392 firmware image file from the https://support.fortinet.com FortiOS 6.0.6 firmware image folder.
6. Perform a normal upgrade of your HA cluster to FortiOS 6.0.6 Build 6392.
7. Wait a few minutes, and when the upgrade is complete, verify that you have installed the correct firmware version. For example, for the FortiGate-7040E:
   ```
   get system status
   Version: FortiGate-7040E v6.0.6,build6392,190822 (GA)
   ...
   ```
8. After the firmware upgrade, you should manually delete IPsec VPN load balancing flow rules, see Manually deleting IPsec VPN load balancing flow rules on page 39.

Other supported upgrade paths

FortiGate-6000 and 7000 for FortiOS 6.0.6 also supports the following upgrade paths for a standalone FortiGate-6000 or a FortiGate-6000 HA cluster with `uninterruptible-upgrade` disabled:

- 5.6.7 build 4214 or 4261 -> 6.0.4 build 8405 -> 6.0.6 build 6392
- 5.6.11 build 4279 -> 6.0.6 build 6392
- 6.0.4 build 6145 or 8405 -> 6.0.6 build 6392

Perform the upgrade during a maintenance window, because traffic will be interrupted during the upgrade.

After the firmware upgrade, you should manually delete IPsec VPN load balancing flow rules, see Manually deleting IPsec VPN load balancing flow rules on page 39.

Manually deleting IPsec VPN load balancing flow rules

Previous versions of FortiOS for FortiGate-6000 and 7000 used load balancing flow rules to handle IPsec VPN traffic. The default versions of these flow rules sent all IPv4 and IPv6 IPsec VPN traffic to the primary (master) FPC or FPM. Enabling IPsec VPN load balancing by enabling the `ipsec-load-balance` option of the `config load-balance settings` command enabled these flow rules. Disabling IPsec VPN load balancing disabled them.

For FortiOS 6.0.6, you no longer need these flow rules and they should be manually removed after upgrading to FortiOS 6.0.6. Upgrading to FortiOS 6.0.6 does not automatically remove them. For more information, see FortiGate-6000 IPsec VPN load balancing support on page 13 and FortiGate-7000 IPsec VPN load balancing changes on page 13.

Example IPv4 and IPv6 IPsec VPN flow rules that can be removed after upgrading to FortiOS 6.0.6:

```
edit 18
        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 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 ike"
    next
    edit 19
        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 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 ike-natt dst"
    next
    edit 20
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol esp
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 esp"
    next
    edit 21
        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 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
```

```
        set priority 5
        set comment "ipv4 ike"
    next
    edit 22
        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 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 ike-natt dst"
    next
    edit 23
        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 esp
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 esp"
    next
```

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

See the Product integration and support section of the FortiOS 6.0.6 release notes for product integration and support information for FortiGate-6000 and 7000 for FortiOS 6.0.6.

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

- FortiGate-6000: FortiManager or FortiAnalyzer 6.0.7 or 6.2.2.
- FortiGate-7000: FortiManager or FortiAnalyzer 6.0.7 or 6.2.1.

FortiGate-6000 6.0.6 special features and limitations

FortiGate-6000 for FortiOS 6.0.6 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-6000 v6.0.6 section of the FortiGate-6000 handbook.

FortiGate-7000 6.0.6 special features and limitations

FortiGate-7000 for FortiOS 6.0.6 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000 v6.0.6 section of the FortiGate-7000 handbook.

Maximum values

Maximum values for FortiGate-6000 and FortiGate-7000 for FortiOS 6.0.6 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 6.0.6 build 6392. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
579859	The `diagnose sys ha checksum cluster` command now displays the correct checksums and can be used to confirm that an HA cluster is synchronized.
403070	The forticldd process no longer sends update requests to FortiCloud every few seconds.
478397 551411	You can now enter single-character BIOS commands when connecting to an FPC over telnet using the management IP address and special telnet management port number.
491756	The `least-rtt` firewall server load balancing method now works as expected.
502507	Improved the information displayed by the `diagnose load-balance dp show lpm bucket-table` command.
502923 541322	When administrators de-authenticate an FSSO user from the Firewall Users Monitor GUI, the user is now successfully de-authenticated from all FPCs/FPMs in both chassis in an HA configuration.
503453 550940	The auto install feature now works as expected for the FortiGate-6000 and 7000 platforms. This feature configures the FortiGate to automatically install firmware from a connected USB drive when the system starts. You can use the `config system auto-install` command to enable the auto install feature.
565704	Routing tables no longer show routes from other VDOMs.
514361	Outgoing clear-text traffic from IPsec VPN sessions is now load balanced correctly.
518276	Using the `get system interface transceiver` command to display information for one transceiver now works as expected.
522617	The `diagnose sys session6 list` command output now includes slot numbers, similar to the output of the `diagnose sys session list` command.
524863	The SD-WAN `measured-volume-based` load balancing option has been removed because it is not supported by FortiGate-6000 and 7000 Session-Aware Load Balancing Clustering (SLBC).
526387	The `source-ip` option is now available for per-VDOM FortiAnalyzer logging configurations.
528496	Information displayed by the `diagnose debug authd fsso list` command is now consistent across all FPCs, FIMs, and FPMs.
534912	VRF routing is now fully supported. VRF routes are now successfully synchronized across all FPCs, FIMs, and FPMs.
540170	Information about data heartbeat status is now more reliable.
542085	Output from more diagnose commands added to the output created by the `execute tac report` command.

Bug ID	Description
543532	FPCs, FIMs, and FPMs now appear in slot number order on the Security Fabric dashboard widget.
547149	DPx sessions for long-lived IPv4 ICMP and UDP sessions are no longer prematurely removed from FGSP peers.
548254	Error messages no longer appear when enabling or disabling FortiAnalyzer logging from the Security Fabric Settings GUI page.
548305	Resolved an issue that prevented recording log messages for dropped packets during some testing scenarios.
548530	Resolved an issue that prevented changing logging options while configuring a firewall policy from the GUI.
549110	On a FortiGate-7000 HA configuration, disconnecting the secondary FortiGate-7000 using the **Remove device from HA cluster** button on the **System > HA** GUI page now successfully removes both FIMs from the cluster.
549167	The **Monitor > Load Balance Monitor** GUI page now shows server load balancing data aggregated for all FPCs or FPMs as well as for individual FPCs or FPMs.
550313	Resolved an issue with virtual server SSL offloading that caused the wad process to crash.
550378 553133	Using the `diagnose load-balance dp find` command is now more intuitive.
550426	IPv6 router advertisements are now only sent by the FortiGate-6000 management board or the FortiGate-7000 primary FIM and not also by all FPCs or FPMs.
550455	IPsec VPN NAT-T tunnels no longer fail with clear text traffic.
550701	Resolved an issue that caused the wad process to generate signal 6 (aborted) messages.
550846	Resolved an issue that caused cross-FIM LAGs to be deleted from a FortiGate-7000 FGSP configuration.
551087	FortiGate-6501s or 6301s with different RAID configurations cannot be added to the same HA cluster. Both FortiGate-6501Fs or FortiGate-6301Fs in a cluster must now have the same RAID configuration.
551239 553416	Resolved issues that caused dropped sessions after an HA failover.
551548 554779 537631	FortiGate-7000 font panel graphics now appear correctly on the **Network > Interfaces** GUI page when logged into a backup FIM or FPM.
551924	The `get system performance stats` command output now includes IPv6 data.
552388	FortiGate-6000 and 7000 devices now just set up one SSL tunnel when connecting to FortiGuard. Individual tunnels are no longer set up by each FPC, FIM, or FPM.
552523	Resolved an issue that sometimes displayed a `Waiting for data heartbeat message` when switching between standalone and active-passive HA.
552859	Only the FortiGate-6000 management board or the primary FortiGate-7000 FIM connect to the configured NTP server. Individual FPCs, FIMs, or FPMs no longer connect to the NTP server.

Bug ID	Description
552903	Resolved an issue that caused advanced configuration script uploads to fail for FGSP.
553301	Resolved an issue that caused FIMs to record high numbers of link change and link initialize events.
553375	If both systems in an HA configuration have the same chassis ID, the system with the lowest serial number will now be shut down.
554009	Resolved an issue that could cause applying a FortiOS Carrier license to fail.
554980	Improved the help and syntax checking of the `execute load-balance slot manage` command.
555097	FTP throughput improvements.
555283	The FortiGate-7000 setting of the `config load-balance slbc-mgmt-intf` option can no longer be changed.
555410	Resolved a synchronization issue for IPS and application control signatures.
555598	The AWS Connector feature now works as expected.
555827	Resolved an issue that prevented the FortiGate-6000 management board GUI from displaying all IPsec tunnels.
556005	Many routing-related commands are now usable from the management board CLI instead of requiring connecting to individual FPCs.
556096	Resolved an issue with synchronizing routes to all FPCs in an FGSP cluster.
556842	SSL VPN can now listen on LACP LAG interfaces.
557053	Resolved an FGSP synchronization issue that would show that some devices in the cluster were "unreachable" or "connecting" instead of showing them as connected.
557132	The `10000auto` option is no longer available when configuring the speed of FortiGate-6000 SFP28 data interfaces (ports 1 to 24).
557140	Resolved an issue that caused high CPU use after loading a saved configuration file.
557162	Debug messages triggered by the `diagnose ip router bgp xxx` command now appear on the management board CLI.
558170	Resolved an issue that blocked SNMP access to FIM1 when using the UDP special management port of 16101.
558263	Corrected an issue with the `config load-balance setting config workers` command that allowed adding workers that did not exist.
558478	Resolved an HA synchronization error caused by the `config system central-management` configuration.
559214	Resolved an issue that caused ICMP traffic to be distributed to more than one FPC or FPM.
559650	Resolved an issue that caused inconsistent MAC addresses to be assigned to EMAC VLAN interfaces.
562440	Corrected the management data displayed on the **Resource Usage** dashboard widgets.
563415	The `config system settings set motherboard-traffic-forwarding` command has been removed as it is no longer required to allow management access from data interfaces.

Bug ID	Description
563821	Resolved a data plane heartbeat issue found after rebooting both FortiGate-6000s or 7000s in an FGCP HA configuration.
563832	Resolved a local certificate synchronization issue.
563912	Resolved an issue that caused trunk IDs to not be synchronized after a graceful upgrade of an HA cluster.
564173	Resolved an issue that caused communication errors between FIMs after a factory reset.
564289	Resolved an issue that caused synchronization delays after disconnecting a FortiGate-6000 or 7000 from an HA cluster.
564618	Improvements to NTP time syncing between FortiGate-6000 and 7000 components in standalone and HA configurations.
564708	Improvements to how firewall policy stats are updated on the management board GUI.
566022	Security Fabric status can no longer be manually disabled from the CLI.
566108	Resolved issues with handling long VDOM names.
566458	Removed the `remote-console-access` option from the `config system console-server` command.
567083	Corrected the firewall policy bytes count displayed on firewall policy list GUI pages.
567200	Corrected the help displayed on the CLI for FortiGate-6000 `execute load-balance slot set-master-worker` command.
567434	Resolved an issue that caused DNS lookups to fail after a reboot or factory reset.
567558	Resolved an issue that prevented FPCs from sending management heartbeats after entering conserve mode.
567719	Resetting the primary FIM on a FortiGate-7000 in HA mode no longer removes the FortiGate-7000 from the HA cluster.
568646	The `get system arp` command now displays data for all FPCs, FIMs, and FPMs.
569047	Corrected the help for the `config load-balance settings set weight` CLI command.
569961	Resolved an issue with adding and configuring custom devices.
571122	Corrected the list of options that appears on the CLI for the `diagnose hardware` command.
571156	Resolved a redundant interface synchronization issue.
571468	Resolved an issue involving the hasync and authd processes that could cause an HA cluster to crash after a failover.
572067	Resolved issues with assigning MAC addresses to cross-FIM LAGs.
572076	Remote access now works correctly after changing the HA mode and chassis ID at the same time.
572147	Resolved a MAC address error that appeared after a LAG was deleted and a new LAG added that included interfaces from the original LAG.
572190	Resolved an issue with displaying routes and status for IPsec interfaces on the management board or

Bug ID	Description
	primary FIM GUI Route Monitor.
572527	Resolved an issue with the confsynchbd process that caused HA failovers.
572594	Resolved a timing issue that resulted in traffic being temporarily blocked after a graceful firmware upgrade of a FortiGate-6000 or 7000 HA configuration.
573155	Resolved an issue that caused incorrect virtual MAC addresses to be created after turning on HA active-passive mode.
573377	The IPsec VPN Monitor GUI page no longer shows host names of FPCs or FPMs that dot not have active IPsec VPN tunnels.
573907	When logged into an FPC or FPM, the `diagnose debug authd fsso list` command now shows the logged in FSSO users for that FPC or FPM.
574249	FIM interfaces no longer appear to incorrectly have virtual MAC addresses.
574495	Interfaces removed from a LAG no longer have incorrect VLAN IDs.
574869	Fragmented and pinhole sessions are now correctly shown when you view the session list (for example with the `diagnose sys session list` command).
575044	Resolved an error with synchronizing link monitor states to FPCs or FPMs.
575578	Redundant interface MAC addresses are now successfully synchronized after a graceful upgrade of an HA cluster.
575907	Resolved an issue with synchronizing MAC addresses after moving an interface from one LAG to another.
576360	Resolved an issue that caused the link local addresses of LAGs or redundant interfaces to be incorrect on the secondary FortiGate-6000 or 7000 in an HA configuration.
576642	Resolved an issue that prevented the IPsec VPN tunnels page from appearing for administrators who logged in using an administrator account with the prof_admin administrator profile.
577715	Resolved an issue that could cause the fctrlproxyd process to use 99% of CPU resources.

Known issues

The following issues have been identified in FortiGate-6000 and FortiGate-7000 FortiOS 6.0.6 build 6392. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
579729	The `execute dhcp lease-list` command does not display any results.
578158	In some cases the IPv4 Policy and IPv6 Policy GUI pages do not display any firewall polices.
578839	FSSO users are not always synchronized among all FPCs or FPMs.
567546	Some fragmented packets in UDP sessions are broadcast to all FPCs or FPMs by the DP processor instead of being sent to a specific FPC or FPM as a fragment session.
578361	Authenticated firewall users may have to log in again after upgrading an HA cluster to FortiOS 6.0.6.
565115	After backing up and restoring the configuration of the secondary FortiGate-6000 or 7000 in an HA cluster, the DLP sensor configuration will have changed, causing the primary and secondary devices to be out of sync.
574657	FortiGate-7000 and FortiGate-6000 for FortiOS 6.0.6 does not support upgrading managed FortiSwitch firmware from the **FortiOS Managed FortiSwitch GUI** page. Instead you must use the FortiGate-6000 or 7000 CLI or log into the managed FortiSwitch to upgrade managed FortiSwitch firmware.
573088	TCP or UDP sessions with SNAT enabled and with fragmented packets fail because the DP processor sends fragmented packets to the incorrect FPC or FIM.
552604	Offloading multicast traffic to NP6 processors is not supported in this release. Even if you have enabled `auto-assic-offload` in a multicast firewall policy, multicast traffic is not offloaded.
574190	Changing the global IPS configuration using the `config ips global` command can reduce overall system performance until the system restarts. To avoid this performance reduction, only make changes to the IPS global configuration during maintenance windows and restart the system after the configuration change is made. You can also use the `diagnose test application ipsmonitor 99` command to restart the IPS engine.
568375	When managing a FortiGate-6000 or 7000 from in-band (traffic) interfaces, jumbo frames are not supported and will be fragmented upon egressing the device.
554882	If you replace a failed FortiGate-6000 or 7000 in an HA configuration with a replacement device, FortiManager may not automatically recognize that the new device as part of the HA configuration. If a failover occurs and the new device becomes the primary or master, FortiManager may not recognize the cluster.
562712	In-band management connections to the IP address of a VDOM link interface is not supported.
564049	Management traffic received from a data interface is interrupted and sessions can't resume if the FPC or FPM that was processing the traffic fails. The sessions don't fail over to another FPC or FPM.
564357	When the telnet port used for administration is changed on the fly, administrative telnet sessions received by a data interface that are active at the time of the configuration change are not interrupted.

Bug ID	Description
572340	Outgoing management traffic does not follow VRF static routes. Instead, this traffic uses the first listed matching static route in the routing table.
570580	Changes made to local-in firewall policies don't affect local-in management traffic received by data interfaces.
577266	After deleting a FortiGate-7000 HA configuration from FortiManager, the secondary FortiGate-7000 in the cluster will have synchronization errors because the central management configuration is successfully removed from the primary FIM but not from the other FIM and FPMs.
574566	The managed FortiSwitch topology is incorrect when the managed FortiSwitch is connected to a FortiGate-7000 LAG.
571398	After upgrading to FortiOS 6.0.6, to configure your system for IPsec VPN load balancing you must manually enable IPsec VPN load balancing and manually delete IPsec VPN load balancing rules. See Upgrade information on page 38.
459424	Statistics on the **System > VDOM** GUI page may be incorrect.
565082	CPU information on the primary FIM CPU Usage dashboard widget should show CPU usage for all FPCs, or FIMs and FPMs.
561722	Firewall policies designed to identify traffic from known devices may not be able to detect traffic from the known devices.
549983	FortiManager in-band management connections to the IP address of a VDOM link interface are not supported.
578625	In some cases, some routes may not be correctly synchronized to all FPCs or FPMs.
577214	The miglogd process sometimes crashes for unknown reasons.