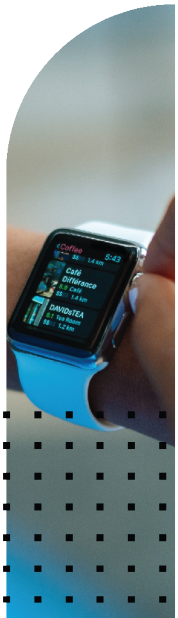
Release Notes

FortiGate-6000 and FortiGate-7000 7.0.10 Build 0117



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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 9, 2023
FortiGate-6000 and FortiGate-7000 7.0.10 Build 0117 Release Notes
01-7010-878858-20230309

TABLE OF CONTENTS

Change log

Date	Change description
March 9, 2023	The FortiGate 7081F is supported by FortiOS 7.0.10, see Supported FortiGate-6000 and 7000 models on page 5.
February 27, 2023	Initial version.

FortiGate-6000 and FortiGate-7000 7.0.10 release notes

These platform specific release notes describe new features, special notices, upgrade information, product integration and support, resolved issues, and known issues for FortiGate-6000 and 7000 for 7.0.10 Build 0117.

In addition, special notices, upgrade information, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 7.0.10 Release Notes also apply to FortiGate-6000 and 7000 for 7.0.10 Build 0117.

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

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

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

You can find the FortiGate-6000 and 7000 for FortiOS 7.0.10 firmware images on the Fortinet Support Download Firmware Images page by selecting the **FortiGate-6K7K** product.

Supported FortiGate-6000 and 7000 models

FortiGate-6000 and 7000 for FortiOS 7.0.10 Build 0117 supports the following models:

- FortiGate-6300F
- FortiGate-6301F
- FortiGate-6500F
- FortiGate-6501F
- FortiGate-7030E
- FortiGate-7040E
- FortiGate-7060E
- FortiGate-7081F
- FortiGate-7121F

What's new

The following new features have been added to FortiGate-6000 and 7000 for FortiOS 7.0.10 Build 0117.

Load balancing configuration to support multihop BFD (MBFD)

Support for multihop BFD (MBFD) was added to FortiOS 7.0.6 (see BFD for multihop path for BGP) and is supported by FortiGate-6000 and 7000 for FortiOS 7.0.10. Multihop BFD is supported for normal traffic and over IPsec VPN tunnels that are terminated by the FortiGate-6000 or 7000.

The multihop control protocol uses TCP and UDP traffic on port 4784. Multihop control traffic is not load balanced by DP or NP7 processors. Instead, a flow rule is used to send all multihop control traffic to a single FPC or FPM.

The following flow rule has been added to the FortiOS 7.0.10 default flow rules for traffic that cannot be load balanced to send all multihop control traffic to the primary FPC or FPM. This flow rule should be enabled if you configure multihop BFD support on your FortiGate-6000 or 7000.

```
config load-balance flow-rule
   edit 22
      set status disable
      set vlan 0
      set ether-type ip
      set protocol udp
      set src-l4port 0-0
      set dst-l4port 4784-4784
      set action forward
      set forward-slot master
      set priority 5
      set comment "Flow Rule for Multihop BFD"
   end
```

When upgrading to FortiOS 7.0.10, this flow rule will be added to the default flow rules configuration and will be disabled. You need to enable it if you want to use multihop BFD.

Resetting your FortiGate-6000 or 7000 running FortiOS 7.0.10 to factory defaults enables the multihop BFD flow rule.

ZTNA support

Zero Trust Network Access (ZTNA) features are now supported by FortiGate-6000 and 7000 for FortiOS 7.0.10. No special configuration is required to support ZTNA. For more information about ZTNA, see Zero Trust Network Access.

DLP fingerprinting support

DLP fingerprinting is now supported by FortiGate-6000 and 7000 for FortiOS 7.0.10. No special configuration is required to support DLP fingerprinting. For more information about DLP fingerprinting, see DLP fingerprinting.

DLP archiving is not supported by FortiGate-6000 and 7000 for FortiOS 7.0.10.

Changes in CLI

The following CLI changes are included with FortiGate-6000 and FortiGate-7000 FortiOS 7.0.10 Build 0117. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
858651	The `config vpn ssl settings` option `tunnel-addr-assigned-method` has been removed from the CLI because this option is not compatible with FortiGate-6000 and 7000 load balancing.
781179	The `config system central-management` option `fmg-source-ip` has been removed from the CLI because this option is not compatible with FortiGate-6000 and 7000 load balancing.
820988	The `config system snmp community` option `source-ip` has been removed from the CLI because this option is not compatible with FortiGate-6000 and 7000 load balancing.

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 7.0.10 Build 0117. The Special notices described in the FortiOS 7.0.10 release notes also apply to FortiGate-6000 and 7000 FortiOS 7.0.10 Build 0117.

FortiGate 7000E and 7000F GTP load balancing and fabric channel usage

On a FortiGate 7000E or 7000F, when GTP load balancing is enabled, GTP tunnels are synchronized over the fabric channel backplane (also called the data channel). The fabric channel is also used for SLBC session synchronization. On a busy FortiGate 7000E or 7000F that is also load balancing GTP tunnels, the system may experience more lost SLBC heartbeats than normal.

To avoid missed heartbeats, you should increase the `max-miss-heartbeats` load balancing setting.

For example, when GTP load balancing is enabled, on a FortiGate 7000E Fortinet recommends setting the `max-miss-heartbeats` to 40.

```
config load-balance setting
   set max-miss-heartbeats 40
   set gtp-load-balance enable
end
```

For more information about GTP load balancing, see FortiGate-7000E FortiOS Carrier GTP load balancing or FortiGate-7000F FortiOS Carrier GTP load balancing.

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

The default `configure load-balance flow-rule` command contains the recommended default flow rules that control how the FortiGate-6000 or 7000 handles traffic types that cannot be load balanced. Most of the flow rules in the default configuration are enabled and are intended to send common traffic types that cannot be load balanced to the primary FPC or FPM. FortiGate-6000F, 7000E, and 7000F for FortiOS 7.0.10 have the same default flow rules with one exception.

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

```
config load-balance flow-rule
    edit 20
        set status enable
        set vlan 0
        set ether-type ip
        set protocol vrrp
        set action forward
```

```
        set forward-slot all
        set priority 6
        set comment "vrrp to all blades"
    next
end
```

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

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

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

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

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

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

```
        set ether-type ip
        set protocol tcp
        set src-l4port 179-179
        set dst-l4port 0-0
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp src"
    next
    edit 4
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 179-179
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp dst"
    next
    edit 5
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 520-520
        set dst-l4port 520-520
        set action forward
        set forward-slot master
        set priority 5
        set comment "rip"
    next
    edit 6
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 521-521
        set dst-l4port 521-521
        set action forward
        set forward-slot master
        set priority 5
        set comment "ripng"
    next
    edit 7
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
```

```
        set src-l4port 67-67
        set dst-l4port 68-68
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 server to client"
    next
    edit 8
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 68-68
        set dst-l4port 67-67
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 client to server"
    next
    edit 9
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 1723-1723
        set dst-l4port 0-0
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp src"
    next
    edit 10
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1723-1723
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp dst"
    next
    edit 11
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 3784-3784
        set action forward
        set forward-slot master
```

```
        set priority 5
        set comment "bfd control"
    next
    edit 12
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 3785-3785
        set action forward
        set forward-slot master
        set priority 5
        set comment "bfd echo"
    next
    edit 13
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 547-547
        set dst-l4port 546-546
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv6 server to client"
    next
    edit 14
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 546-546
        set dst-l4port 547-547
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv6 client to server"
    next
    edit 15
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 224.0.0.0 240.0.0.0
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 multicast"
    next
    edit 16
```

```
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ff00::/8
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 multicast"
    next
    edit 17
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 2123-2123
        set action forward
        set forward-slot master
        set priority 5
        set comment "gtp-c to primary blade"
    next
    edit 18
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1000-1000
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "authd http to primary blade"
    next
    edit 19
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1003-1003
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "authd https to primary blade"
    next
    edit 20
        set status enable
        set vlan 0
        set ether-type ip
        set protocol vrrp
```

```
        set action forward
        set forward-slot all
        set priority 6
        set comment "vrrp to all blades"
    next
end
```

Upgrade information

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

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

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

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

See also, Upgrade information in the FortiOS 7.0.10 release notes.

You can find the FortiGate-6000 and 7000 for FortiOS 7.0.10 firmware images on the Fortinet Support Download Firmware Images page by selecting the **FortiGate-6K7K** product.

HA graceful upgrade to FortiOS 7.0.10

Use the following steps to upgrade a FortiGate-6000 or 7000 HA cluster with `uninterruptible-upgrade` enabled from FortiOS 6.4.10 build 1875 or FortiOS 7.0.5 build 0057 to FortiOS 7.0.10 Build 0117.

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

Upgrading to FortiOS 7.0.10 Build 0117 may include updating the FortiGate-6000 or 7000E DP processor firmware. The DP processor firmware upgrade occurs during the normal firmware upgrade process and no extra steps are required. It just may take longer to run the upgrade than normal.

Upgrading to FortiOS 7.0.10 Build 0117 will not update the FortiGate-7000F NP7 processor firmware.

To perform a graceful upgrade of your FortiGate-6000 or 7000 from FortiOS 6.4.10 or 7.0.5 to FortiOS 7.0.10:

1. Use the following command to enable `uninterruptible-upgrade` to support HA graceful upgrade:
   ```
   config system ha
      set uninterruptible-upgrade enable
   end
   ```
2. Download FortiOS 7.0.10 firmware for FortiGate-6000 or 7000 from the https://support.fortinet.com FortiGate-6K7K 7.0.10 firmware image folder.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.

4. Verify that you have installed the correct firmware version. For example, for a FortiGate-6301F:

```
get system status
Version: FortiGate-6301F v7.0.10,build0117,230224 (GA.M)
...
```

About FortiGate-6000 firmware upgrades

The management board and the FPCs in your FortiGate 6000F 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 an FGCP cluster by setting `upgrade-mode` to `uninterruptible` and enabling `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.

Upgrading the firmware of a standalone FortiGate 6000F, or FortiGate 6000F HA cluster with `upgrade-mode` set to `simultaneous` 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 6000F 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 6000F configuration.

To make sure a FortiGate-7000 firmware upgrade is successful, before starting the upgrade Fortinet recommends you use health checking to make sure the management board and the FPCs are all synchronized and operating as expected.

If you are following a multi-step upgrade path, you should re-do health checking after each upgrade step to make sure all components are synchronized before the next step.

You should also perform a final round of health checking after the firmware upgrade process is complete.

For recommended health checking commands, see the following Fortinet community article:

Technical Tip: FortiGate-6000/7000 Chassis health check commands.

Fortinet recommends that you review the services provided by your FortiGate 6000F 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 setting `upgrade-mode` to `uninterruptible` and enabling `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.

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

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

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

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

To make sure a FortiGate-7000 firmware upgrade is successful, before starting the upgrade Fortinet recommends you use health checking to make sure the FIMs and FPMs are all synchronized and operating as expected.

If you are following a multi-step upgrade path, you should re-do health checking after each upgrade step to make sure all components are synchronized before the next step.

You should also perform a final round of health checking after the firmware upgrade process is complete.

For recommended health checking commands, see the following Fortinet community article:

Technical Tip: FortiGate-6000/7000 Chassis health check commands.

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

Product integration and support

This section describes FortiGate-6000, 7000E, and 7000F for FortiOS 7.0.10 Build 0117 product integration and support information. The Product integration and support information described in the FortiOS 7.0.10 release notes also applies to FortiGate-6000, 7000E, and 7000F for FortiOS 7.0.10 Build 0117.

FortiGate-6000, 7000E, and 7000F for FortiOS 7.0.10 Build 0117 require the following or newer versions of FortiManager and FortiAnalyzer:

- FortiGate-6000: FortiManager or FortiAnalyzer 7.0.6, and 7.2.3.
- FortiGate-7000E and 7000F: FortiManager or FortiAnalyzer 7.0.6, and 7.2.3.

FortiGate-6000 7.0.10 special features and limitations

FortiGate-6000 for FortiOS 7.0.10 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-6000 v7.0.10 section of the FortiGate-6000 handbook.

FortiGate-7000E 7.0.10 special features and limitations

FortiGate-7000E for FortiOS 7.0.10 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000E v7.0.10 section of the FortiGate-7000E handbook.

FortiGate-7000F 7.0.10 special features and limitations

FortiGate-7000F for FortiOS 7.0.10 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000F v7.0.10 section of the FortiGate-7000F handbook.

Maximum values

Maximum values for FortiGate-6000 and FortiGate-7000 for FortiOS 7.0.10 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 7.0.10 Build 0117. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 7.0.10 release notes also apply to FortiGate-6000 and 7000 FortiOS 7.0.10 Build 0117.

Bug ID	Description
664063	The `diagnose sys ha dump_by device` command now displays device information for the secondary FortiGate-6000 or 7000 in an FGCP HA cluster.
674979	The GUI now shows the correct amount of traffic on FortiGate-6000 HA interfaces.
714476	Resolved an issue that prevented console baud rate changes from being synchronized to all FPCs or FPMs if the baud rate change was made from a console session.
735464	The `diagnose ips filter` command is now successfully broadcast from the management board or the primary FIM to all FPCs or FPMs.
763820	Resolved an issue that prevented configuring the FortiGate-7000F to use some management interfaces as HA management interfaces even though the interface was available.
768931	The FortiGate-7000F GUI now correctly shows FPM-7620F P1 and P2 split interfaces.
781387	Resolved an issue that could cause the `httpsd` process to crash when working with a large complex configuration.
787646 878934	Resolved an issue related to how FortiOS updates large routing configurations that could cause the `fctrlproxyd` process to periodically use excessive amounts of CPU time (up to 99%), usually as a result of routing configuration changes. Restarting the `fctrlproxyd` process no longer causes interface flapping.
803536	Resolved an issue that could cause a FortiGate-6000 or 7000 to incorrectly synchronize routes after various failover scenarios.
814343	Resolved an issue that could cause the FortiGate-6000 management board freeze while starting up and display a message similar to `[cmf_get_entry_size:83] table=0x7f54b8ab8054, node_id=0`.
814434	Resolved an issue that caused a kernel crash when changing the `max-miss-heartbeat` option of the `config load-balance setting` command.
814698 852406	Multiple improvements to FGSP session synchronization.
815874 822410	Resolved an issue with retrieving dynamic addresses and resolved a GUI issue that prevented the FortiGate-6000 and 7000 from supporting ZTNA.
819329	Resolved an issue that prevented administrators from pinging the remote interface of a GRE tunnel from the FortiGate-6000 or 7000 CLI.
823129	The FortiGate-7121F now correctly forwards all ICMPv6 non-0x80/81 traffic to the primary FPM.

Bug ID	Description
824205	If an FPM completes starting up when no FIMs are running the FPM can't download the current miglogdisk_info file from the primary FIM. If this happens, the FPM will restart by which time an FIM should be running.
828623	The `diagnose sys sdn status` command now shows the correct information for a Cisco ACI connector.
830454	Changing the FPC or FPM that an IPsec tunnel is using no longer causes traffic in the tunnel to be blocked.
833488	Resolved a CMDB issue that can cause the `fcnacd` process to add a VDOM during stress testing.
835277 860240	Resolved an issue that resulted in the FortiGate-7000 session counter reporting incorrect session counts.
835847	Resolved an issue that prevented automation stitches from updating the password policy.
839887	Resolved an issue that prevented the `miglogdisk_info` file from being updated correctly when a FortiGate-7121F starts up or restarts.The `miglogdisk_info` file that is present on all FIMs and FPMs should be updated by reading current log disk information every time a FortiGate-7121F chassis restarts. This problem also caused FPMs to be out of synchronization.
839987	Resolved an issue with FGCP HA status synchronization between the management board and FPCs or between FIMs and FPMs that could cause traffic to be blocked. The problem would usually occur after the FortiGate-6000s or 7000s in the cluster restarted (for example, after a firmware upgrade).
840459	The information displayed by the `diagnose load-balance switch stats egress` command is now correct.
844424	A Transceiver is not detected message is no longer displayed for FIM-7921F interfaces for some supported transceivers.
845278	Resolved an issue that prevented ICMP error messages from being broadcast to all FortiGate-7000 FPMs when asymmetric routing is enabled.
847503	Resolved an issue with how SDN connector dynamic addresses are handled that prevented dynamic SDN connector addresses from being synchronized to all FPCs or FPMs in the secondary FortiGate-6000 or 7000.
848609	Resolved an issue that blocked IPv6 VIP traffic.
849022	IPv6 router advertisement (RA) packets received by the management board or primary FIM are now broadcast to all FPCs or FPMs.
850284	Active FTP data sessions are no longer handled by different FPCs or FPMs in the FortiGate-6000s or 7000s in an FGSP cluster.
851129	Log messages now correcty include the correct slot number of the reporting device in the slot= field.
852236	Resolved an issue that caused interface bandwidth dashboard widgets to show incorrect bandwidth usage spikes on interfaces used for FGCP HA heartbeat traffic when the HA cluster is processing high amounts of traffic.

Bug ID	Description
852500	The FortiGate-6000F management board and FPCs now have the same default IPS socket size. FortiGate-7000 FIMs and FPMs now also all have the same default IPS socket size.
852500	The FortiGate-6000F management board and FPCs now have the same default IPS socket size. FortiGate-7000 FIMs and FPMs now also all have the same default IPS socket size.
852770	Resolved an issue that could prevent the GUI or CLI from displaying correct information about the transceivers installed in management interfaces.
853079 849650 848879	Resolved multiple issues related to support for EMAC VLAN interfaces.
855340	Resolved an issue that prevented LDAP user authentication from timing out when LDAP users were configured with `auth-timeout-type` set to `hard-timeout`.
859366	Resolved an issue that prevented IPv6 static routes added to a transparent mode VDOM from being synchronized to all FPCs or FPMs.
860197	Resolved an issue that could cause users to see an incomplete web filter override page.
861137	DLP fingerprinting now correctly downloads a DLP fingerprint data base when the FortiGate-6000 or 70000 first starts up and the `period` option of a DLP fingerprint configuration is set to `none`.
861381	Resolved an issue that prevented FPCs or FPMs from downloading DLP fingerprint files from an SMB server through the mgmt-vdom VDOM.
861449	DLP fingerprint files are now downloaded from an SMB server by the management board or primary FIM and then synchronized to the FPCs or FPMs. In previous releases, individual FPCs or FPMs would independently download DLP fingerprint files from the SMB server.
863640	FortiGate-7000 FIM and FPMs no longer have different default values for proxy-worker-count, scanunit-count, sslvpn-max-worker-count, and wad-worker-count.
863756	The `diagnose debug flow filter <vdom-name>` command now correctly synchronizes the `<vdom-name>` to all FPCs or FPMs.
864629	Resolved an issue that caused excessive CPU usage when entering a command similar to `dnsproxy-worker-count 48`.
867044 837304	Restoring a VDOM configuration no longer changes the IPv6 interface `ra-send-mtu` setting.
867093	Resolved an issue that could sometime cause IPsec VPN NAT traversal UDP sessions to be installed on the wrong FPC or FPM.
868372	Resolved an issue that caused FGSP to stop working if the FGSP configuration includes cluster synch entries that use different peer VDOMs.
871289	Firmware image protection has been added to the FortiGate-6000 and 7000 platforms.
871978	Resolved a FortiGate-6000 issue that could cause some interfaces to flap after manually disabling and re-enabling an interface.
872852	Improved SLBC and HA configuration synchronization because of the extra data overhead involved in

Bug ID	Description
	synchronizing the configuration to the secondary FortiGate 7121F in an HA cluster when each FortiGate 7121F has up to 440 interfaces.
874339	Resolved an configuration system looping issue that could cause excessive CPU usage.
874355	Resolved an issue that under some network conditions, could result in lost HA heartbeats , causing an HA failover for an FortiGate-6000 or 7000 FGCP HA cluster.
874491	Resolved an issue that prevented the `execute load-balance slot` command from allowing access to some of the FPMs in a FortiGate-7060E.
879293	Administrators with read only access can now use the `diagnose sniffer packet` command.

882040
725821
	Support for multihop BFD (MBFD) was added to FortiOS 7.0.6 (see BFD for multihop path for BGP) and is supported by FortiGate-6000 and 7000 for FortiOS 7.0.10.
	The following flow rule has been added to the FortiOS 7.0.10 default flow rules for traffic that cannot be load balanced to send all multihop control traffic to the primary FPC or FPM. This flow rule should be enabled if you configure multihop BFD support on your FortiGate-6000 or 7000.
	`config load-balance flow-rule`
	`edit 22`
	`set status disable`
	`set vlan 0`
	`set ether-type ip`
	`set protocol udp`
	`set src-l4port 0-0`
	`set dst-l4port 4784-4784`
	`set action forward`
	`set forward-slot master`
	`set priority 5`
	`set comment "Flow Rule for Multihop BFD"`
	`end`

Known issues

The following issues have been identified in FortiGate-6000 and FortiGate-7000 FortiOS 7.0.10 Build 0117. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 7.0.10 release notes also apply to FortiGate-6000 and 7000 FortiOS 7.0.10 Build 0117.

Bug ID	Description
700630	Some GUI pages may randomly take longer to load than expected or not load at all.
724543	Interface bandwidth dashboard widgets show incorrect outbound bandwidth usage.
782978	When setting up a FortiGate-6000 or 7000 FGCP HA cluster, one of the FortiGates in the cluster may be running an older firmware version. During cluster formation, the newer firmware version is installed on FortiGate running the older firmware version. After the firmware is downloaded and before the FortiGate restarts, the console may display incorrect error messages. Even when these error messages appear the FortiGate should start up normally, running the newer firmware version, and should be able to join the cluster.
785815	An FPM may display an incorrect checksum message on the console while restarting. The FPM will continue to operate normally after fully starting.
803082	Policy statistics data that appear on the GUI firewall policy pages and in FortiView may be incorrect.
807425	After successfully resetting a managed FortiSwitch from the FortiGate-6000 or 7000 GUI, a Failed to factory reset FortiSwitch message may appear.
813569	Operating a FortiGate-6000 or 7000 as an SSL VPN client is not supported.
830454	Changing the FPC or FPM that an IPsec tunnel is using can cause traffic in the tunnel to be blocked. The problem is a timing issue, so sometimes traffic will be unaffected when making this configuration change and other times it may be blocked.
832353	After factory resetting an FPM, if the configuration synchronized to it contains EMAC VLAN interfaces, the MAC addresses of the EMAC VLAN interfaces on the FPM may be different from the MAC addresses of the same EMAC VLAN interfaces on the primary FIM. The configuration synchronization checksum for the FPM is the same as for the other FPMs and FIMs, even though the EMAC VLAN interfaces have different MAC addresses.

840762	In some cases, the GUI will not display the Configuration Sync Monitor GUI page. You can work around this issue by stopping the `node.js` process. Once the `node.js` process is stopped, you will loose access to the GUI for a few seconds. Once `node.js` restarts you can access the GUI and the Configuration Sync Monitor GUI page should be available.
	You can use the following command to find the `node.js` process number:
	`diagnose sys process pidof node`
	The output of this command will be the `node.js` process number. Enter the following command to stop the `node.js` process.
	`diagnose sys kill 9 <node.js-process-number>`

Bug ID	Description
843473	The checksum of the root VDOM is missing from some parts of the output of the `diagnose sys confsync showcsum` command.
846164	In some cases IPv6 traffic fails because the DP processor sends IPv6 traffic to the wrong FPC.
856706	After an IPsec tunnel is started on a primary FortiGate-6000 or 7000 in an FGCP HA configuration, the IPsec SA is synchronized on the secondary FortiGate-6000 or 7000 in the cluster. However, after a short while, the IPsec SA can be deleted from the secondary FortiGate. If this causes IPsec tunnels to go down after a failover, you can enter the command `diagnose vpn ike gateway flush` on the new primary FortiGate-6000 or 7000 to flush and then restore all IPsec VPN tunnels.
871968	Fragmented packets are blocked by EMAC VLAN interfaces.
879106	FortiGate-6000 and 7000 do not support adding an EMAC VLAN interface to a VLAN interface. You can add an EMAC VLAN interface to a VLAN interface, but this could result in duplicate MAC addresses and duplicate HA virtual MAC addresses.
881414	In some rare cases, an FPC or FPM may assign one or more FortiGate-6000 or FortiGate-7000 FIM network interfaces the HA virtual mac address 00:00:00:00:00:00. You can use the `diagnose hardware deviceinfo nic` command to find the `Current_HWaddr` address assigned to each interface by each FPC or FPM. You can work around this issue by running the `diagnose sys ha mac` command from the FortiGate-6000 management board CLI or FortiGate-7000 primary FIM CLI to recalculate HA virtual MAC addresses for all interfaces for all FPCs or FPMs. This command has been temporarily added for this release to help with this issue. If the FortiGate-6000 or 70000 restarts or if you change the interface configuration (for example by changing the split interface configuration), the problematic HA virtual MAC address may revert to 00:00:00:00:00:00 and you will have to run the `diagnose sys ha mac` command again.

www.fortinet.com