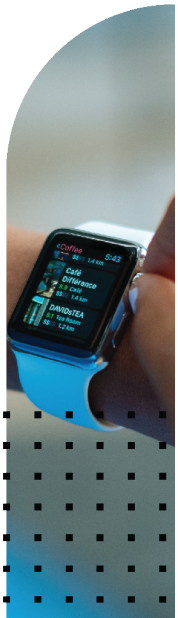
Release Notes

FortiGate-6000 and FortiGate-7000 7.0.5 Build 0057



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

February 23, 2023
FortiGate-6000 and FortiGate-7000 7.0.5 Build 0057 Release Notes
01-705-805444-20230223

TABLE OF CONTENTS

Change log

Date	Change description
February 23, 2023	Corrections to FPM-7620F 1 and 2 (P1 and P2) interface changes on page 9.
February 3, 2023	Added 878934 to Known issues on page 28.
December 12, 2022	New section: FPM-7620F 1 and 2 (P1 and P2) interface changes on page 9.
October 20, 2022	Updated Product integration and support on page 23 with the versions of FortiManager and FortiAnalyzer that are compatible with FortiGate-6000 and 7000 for FortiOS 7.0.5.
October 18, 2022	New information and corrections added to Using data interfaces for FGSP session synchronization on page 6. Corrections to Synchronizing sessions between FortiGate-7000E FGCP clusters on page 6.
September 26, 2022	Initial version.

FortiGate-6000 and FortiGate-7000 7.0.5 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 7.0.5 Build 0057.

In addition, special notices, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 7.0.5 Release Notes also apply to FortiGate-6000 and 7000 for 7.0.5 Build 0057.

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 7.0.5 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 7.0.5 Build 0057 supports the following models:

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

What's new

The following new features have been added to FortiGate-6000 and 7000 for FortiOS 7.0.5 Build 0057.

Using data interfaces for FGSP session synchronization

FortiGate-6000 and 7000 FGSP supports using up to eight physical data interfaces for FGSP session synchronization.

Use the following command to select up to eight physical data interfaces to use for FGSP session synchronization:

```
config system standalone-cluster
   set data-intf-session-sync-dev <interface-name> [<interface-name> ...]
end
```

You can use these individual interfaces or VLANs added to these interfaces for FGSP session synchronization. You can also create LAGs of two or more of these physical interfaces and use the LAGs for FGSP session synchronization. You can also add a VLAN to a LAG and use this VLAN for FGSP session synchronization.

Fortinet recommends:

- Use a data interface LAG for FGSP session synchronization. A LAG supports higher throughput than a single interface and also provides redundancy.
- Do not use FGSP session synchronization data interfaces for other traffic.
- Enable jumbo frames on the data interfaces, LAGs, and VLANs that you use for FGSP session synchronization.
- Keep the FGSP session synchronization data interfaces in a separate dedicated VDOM. Any VLANs you add to these interfaces or LAGs that you create for FGSP session synchronization should also be in the same dedicated VDOM. You must then specify this VDOM as the `peervd` in the `config system cluster-sync` configuration.

  For example, you could create a VDOM called `fgsp-sync` and add the data interfaces, VLANs and LAGs that you are using for FGSP session synchronization to that VDOM. Then you can create the following `config system cluster-sync` instance to synchronize sessions from the root VDOM:

  ```
  config system cluster-sync
     edit 1
        set peervd fgsp-sync
        set peerip <ip-address>
        set syncvd root
     end
  ```

Synchronizing sessions between FortiGate-7000E FGCP clusters

FortiGate-7000E for FortiOS 7.0.5 supports using FGSP to synchronize sessions among up to four FortiGate-7000E FGCP clusters. All of the FortiGate-7000Es must be the same hardware model.

FGSP between FGCP clusters synchronizes sessions between the primary FortiGate-7000Es in each cluster. FGCP HA then handles session synchronization between FortiGate-7000Es in each FGCP cluster.

For details about FGSP between FGCP clusters, see: Synchronizing sessions between FGCP clusters.

You can use data interfaces or data interface LAGs as FGSP session synchronization interfaces. The M1 and M2 interfaces are used for FGCP HA heartbeat between the FortiGate-7000Es in each FGCP cluster.

FortiGate-7000E synchronizing sessions between FGCP clusters has the following limitations:

- The FGCP clusters cannot be configured for virtual clustering.
- NAT between the session synchronization interfaces is not supported.
- Standalone configuration synchronization between the FCGP clusters is not supported.
- Inter-cluster session synchronization doesn't support setting up IPv6 session filters using the `config session-sync-filter` option.
- When ICMP load balancing is set to `to-master`, ICMP packets are not installed on the DP processor. In an FGSP between FGCP session synchronization configuration with an asymmetry topology, synchronized ICMP packets will be dropped if the clusters have selected a different primary FPC. To avoid this possible traffic loss, set `dp-icmp-distribution-method` to `src-ip`, `dst-ip`, or `src-dst-ip`.
- Asymmetric IPv6 SCTP traffic sessions are not supported. These sessions are dropped.
- FGSP IPsec tunnel synchronization is not supported.
- Session synchronization packets cannot be fragmented. So the MTU for the session synchronization interface should be supported by the network.
- To reduce the number of failovers and the amount of session synchronization traffic, configuring HA override on the FGCP clusters is not recommended.

FGCP HA in-band management for management interfaces

The FortiGate-6000 and 7000 now support FGCP HA in-band management for FortiGate-6000 and 7000 management interfaces (mgmt, mgmt1, mgmt2, and mgmt3).

HA in-band management allows you to add a second management IP address to one or more FortiGate-6000 or 7000 management interfaces. The management IP address is accessible from the network that the interface is connected to. This setting is not synchronized, so each FortiGate-6000 or 7000 in the cluster can have their own in-band management IP addresses; providing management access to the secondary FortiGate-6000 or 7000.

FortiGate-6000 and 7000 does not support HA in-band management for data interfaces.

FortiGate-6000 HA in-band management configuration:

```
config vdom
   edit mgmt-vdom
      config system interface
         edit {1-mgmt1 | 1-mgmt2 | 1-mgmt3 | 2-mgmt1 | 2-mgmt2 | 2-mgmt3}
            set management-ip <ip address>
         end
```

FortiGate-7000E HA in-band management configuration:

```
config vdom
   edit mgmt-vdom
      config system interface
         edit mgmt
            set management-ip <ip address>
```

```
        end
```

You can also remove individual mgmt interfaces from the FortiGate-7000E LAG and add an in-band management address to these interfaces.

FortiGate-7000F HA in-band management configuration.

```
config vdom
   edit mgmt-vdom
      config system interface
         edit {1-mgmt1 | 1-mgmt2 | 2-mgmt1 | 2-mgmt2}
            set management-ip <ip address>
         end
```

The `management-ip` option is available only when HA is enabled.

To support HA in-band management, the FortiGate-6000 and 7000 now handle HA virtual MAC addresses in the same way as other FortiGates.

FortiGate-7000E and 7000F PFCP support

FortiOS Carrier 7.0.5 for FortiGate-7000E and 7000F includes support for load balancing the Packet Forwarding Control Protocol (PFCP). PFCP is a new addition to 3GPP that provides 4G Control plane and User Plane Separation (CUPS) and 5G signaling evolution. When PFCP is used as the control plane, the user plane is GTPv1-U. PFCP takes many of the roles that are provided by GTP-C in 3G/4G networks today and provides session awareness and tracking of GTPv1-U user plane traffic while also providing control plane initiation.

PFCP support includes supporting PFCP session synchronization for FGCP HA.

PFCP support also includes a new default flow rule. This flow rule is disabled by default. When enabled, this flow rule sends all PFCP traffic to the primary FPM.

```
edit 21
        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 8805-8805
        set action forward
        set forward-slot master
        set priority 5
        set comment "pfcp to primary blade"
end
```

For more information about PFCP and FortiOS Carrier, see FortiOS Carrier PFCP protection.

FortiGate-7000F NP7 processors support offloading DoS policies

The FortiGate-7000F supports using the NP7 processors in the FPMs to offload DoS firewall policy sessions. DoS policies are offloaded when the `policy-offload-level` option of the `cofig system npu` command is set to `dos-ofload`:

```
config system npu
   set policy-offload-level {dos-offload | full-offload}
      config dos-options
         set npu-dos-meter-mode {global | local}
         set npu-dos-tpe-mode {disable | enable}
      end
```

These commands are only available for the FortiGate-7000F. The FortiGate-7000F does not support hyperscale firewall features (you cannot set `policy-offload-level` to `full-offload`).

`disable` is the default setting. Offloading DoS policy sessions to NP7 processors is disabled. All sessions are initiated by the CPU. Sessions that can be offloaded are sent to the NP7 processors in the FPMs.

`dos-offload` offload DoS policy sessions to the NP7 processors in the FPMs. All other sessions are initiated by the CPU. Sessions that can be offloaded are sent to NP7 processors in the FPMs.

`npu-dos-meter-mode` select `global` (the default) to configure DoS metering across all NP7 processors. Select `local` to configure metering per NP7 processor.

DoS metering controls how the threshold for each configured anomaly is distributed among NP7 processors. For example, for an FPM with two NP7 processors and the `tcp_syn_flood` anomaly threshold set to 400. If `npu-dos-meter-mode` is set to `global`, the threshold of 400 is divided between the NP7 processors and the `tcp_syn_flood` threshold would be set to 200 for each NP7 (for a total threshold of 400 for the FPM). If `npu-dos-meter-mode` is set to `local`, then each NP7 would have a threshold of 400 (for a total threshold of 800 for a the FPM).

`npu-dos-tpe-mode` select `enable` (the default) to insert the dos meter ID into the session table. Select `disable` if you don't want to insert the DoS meter into the session table. If set to enable, `UDP_FLOOD` and `ICMP_FLOOD` DoS protection applies to offloaded sessions. If set to disable, `UDP_FLOOD` and `ICMP_FLOOD` DoS protection will not apply to offloaded sessions.

FPM-7620F 1 and 2 (P1 and P2) interface changes

The default speed of the FPM-7620F 1 and 2 (P1 and P2) interfaces has been changed from 100Gbps to 400Gbps. These interfaces can operate at 400Gbps, 100Gbps, and 40Gbps. Even though the default speed has changed, after a firmware upgrade to FortiOS 7.0.5 the configured speed of the P1 and P2 interfaces will not change as part of the upgrade process. You can; however, change the interface speed manually from the CLI.

If the FPM-7620F is installed in a FortiGate-7000F with two FIM-7941Fs, you can also make the following changes:

- Split each of the 1 and 2 (P1 and P2) interfaces into four 100GigE CR2 interfaces.
- Split each of the 1 and 2 (P1 and P2) interfaces into four 25GigE CR or 10GigE SR interfaces.

Changing the FPM-7620F 1 and 2 (P1 and P2) interfaces

You can change the speed of the 1 and 2 (P1 and P2) interfaces to 400G, 100G, or 40G using the `config system interface` command.

When the FPM-7620F is installed in a FortiGate-7000F with two FIM-7941Fs, you can also make the following changes:

- Split the interface into four 100GigE CR2 interfaces.
- Split the interface into four 25GigE CR or 10GigE SR interfaces.

All of these operations, except changing the interface speed using the `config system interface` command, require a system restart. Fortinet recommends that you perform these operations during a maintenance window and plan the changes to avoid traffic disruption.

You should change interface types or split interfaces on both FortiGate-7000Fs before forming an FGCP HA cluster. If you decide to change interface type or split interfaces after forming a cluster, you need to remove the backup FortiGate-7000F from the cluster and change interfaces as required on both FortiGate-7000Fs separately. After the FortiGate-7000Fs restart, you can re-form the cluster. This process will cause traffic interruptions.

Splitting the P1 or P2 interfaces into four 100GigE CR2 interfaces

When the FPM-7620F is installed in a FortiGate-7000F with two FIM-7941Fs, you can use the following command to split the P1 or P2 interfaces into four 100GigE CR2 interfaces. To split P1 of the FPM-7620F in slot 6 (6-P1) and P2 of the FPM-7620F in slot 7 (7-P2) enter the following command:

```
config system global
   set split-port 6-P1 7-P2
end
```

The FortiGate-7000F reboots and when it starts up:

- Interface 6-P1 has been replaced by four 100GigE CR2 interfaces named 6-P1/1 to 6-P1/4.
- Interface 7-P2 has been replaced by four 100GigE CR2 interfaces named 7-P2/1 to 7-P2/4.

Splitting the P1 or P2 interfaces into four 25GigE CR or 10GigE SR interfaces

When the FPM-7620F is installed in a FortiGate-7000F with two FIM-7941Fs, you can use the following command to split the P1 or P2 interfaces into four 25GigE CR interfaces. The following command converts the interface into a 100GigE QSFP28 interface then splits this interface into four 25 GigE CR interfaces. To split P1 of the FPM-7620F in slot 8 (8-P1) and P2 of the FPM-7620F in slot 9 (9-P2) enter the following command:

```
config system global
   set qsfpdd-100g-port 8-P1 9-P2
   set split-port 8-P1 9-P2
end
```

The FortiGate-7000F reboots and when it starts up:

- Interface 8-P1 has been replaced by four 25GigE CR interfaces named 8-P1/1 to 8-P1/4.
- Interface 9-P2 has been replaced by four 25GigE CR interfaces named 9-P2/1 to 9-P2/4.

If you want some or all of these interfaces to operate as 10GigE SR interfaces you can use the `config system interface` command to change the interface speed. You can change the speed of some or all of the individual split interfaces depending on whether the transceiver installed in the interface slot supports different speeds for the split interfaces.

Changes in CLI

The following CLI changes are included with FortiGate-6000 and FortiGate-7000 FortiOS 7.0.5 Build 0057. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
810837	When creating a new interface on the FortiGate-6000 or 7000, by default the `device-identification` option is now set to `disable`.

802420	When setting up FortiGate-6000 and 7000 FGSP cluster sync instances, the default value of the `peervd` option is now `mgmt-vdom`. This change has been made because FortiGate-6000 and 7000 FGSP only supports using interfaces in the mgmt-vdom as cluster sync interfaces unless you are using data interfaces for FGSP session synchronization.
	`config system cluster-sync`
	`edit 1`
	`set peervd <vdom-name>`
	`set peerip <ip-address>`
	`set syncvd <vdom-name>`
	`end`

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for FortiGate-6000 and FortiGate-7000 7.0.5 Build 0057. The Special notices described in the FortiOS 7.0.5 release notes also apply to FortiGate-6000 and 7000 FortiOS 7.0.5 Build 0057.

ZTNA not supported by this release

Zero Trust Network Access (ZTNA) features are not supported by FortiOS 7.0.5 Build 0057 for FortiGate-6000 and 7000. For a list of ZTNA-related issues, see Known issues on page 28.

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 7.0.5 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
    edit 21
        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 8805-8805
        set action forward
```

```
        set forward-slot master
        set priority 5
        set comment "pfcp to primary blade"
    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 7.0.5 release notes.

You can find the FortiGate-6000 and 7000 for FortiOS 7.0.5 firmware images on the Fortinet Support Download Firmware Images page by selecting the **FortiGate-6K7K** product.

HA graceful upgrade to FortiOS 7.0.5

Use the following steps to upgrade a FortiGate-6000 or 7000 HA cluster with `uninterruptible-upgrade` enabled from FortiOS 6.4.8 build 1823 to FortiOS 7.0.5 Build 0057. You can also use these steps to upgrade a FortiGate-7121F-2 running FortiOS 6.4.8 NPI build 4175. The FortiGate-7121F -2 contains FIM-7941Fs.

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

To perform a graceful upgrade of your FortiGate-6000 or 7000 from FortiOS 6.2.9 or 6.4.6 to FortiOS 7.0.5:

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 7.0.5 firmware for FortiGate-6000 or 7000 from the https://support.fortinet.com FortiGate-6K7K 7.0.5 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 v7.0.5,build0057,220922 (GA)
   ...
   ```

About FortiGate-6000 firmware upgrades

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

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

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

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

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

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

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

About FortiGate-7000 firmware upgrades

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

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

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

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

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

- Review the latest release notes for the firmware version that you are upgrading to.
- Verify the recommended upgrade path as documented in the release notes.

- Back up your FortiGate-7000 configuration.

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

Product integration and support

This section describes FortiGate-6000, 7000E, and 7000F for FortiOS 7.0.5 Build 0057 product integration and support information. The Product integration and support information described in the FortiOS 7.0.5 release notes also applies to FortiGate-6000, 7000E, and 7000F for FortiOS 7.0.5 Build 0057.

FortiGate-6000, 7000E, and 7000F for FortiOS 7.0.5 Build 0057 require the following or newer versions of FortiManager and FortiAnalyzer:

- FortiGate-6000: FortiManager or FortiAnalyzer 7.0.6, and 7.2.2.
- FortiGate-7000E and 7000F: FortiManager or FortiAnalyzer 7.0.6, and 7.2.2.

FortiGate-6000 7.0.5 special features and limitations

FortiGate-6000 for FortiOS 7.0.5 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-6000 v7.0.5 section of the FortiGate-6000 handbook.

FortiGate-7000E 7.0.5 special features and limitations

FortiGate-7000E for FortiOS 7.0.5 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000E v7.0.5 section of the FortiGate-7000E handbook.

FortiGate-7000F 7.0.5 special features and limitations

FortiGate-7000F for FortiOS 7.0.5 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000F v7.0.5 section of the FortiGate-7000F handbook.

Maximum values

Maximum values for FortiGate-6000 and FortiGate-7000 for FortiOS 7.0.5 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 7.0.5 Build 0057. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 7.0.5 release notes also apply to FortiGate-6000 and 7000 FortiOS 7.0.5 Build 0057.

Bug ID	Description
575103	When setting up FGSP cluster sync instances, you can now only use the `down-intfs-before-sess-sync` option to shut down data interfaces. The `down-intfs-before-sess-sync` option allows you to shut down some interfaces on a failed FortiGate when it is starting up so that it will not accept packets until session synchronization is complete.
647254 802105	Duplicate IPv4 ECMP routes no longer appear on FPCs or FPMs on the secondary FortiGate-6000 or 7000 in an FGCP cluster.
652140	Resolved an issue with CLI error checking when adding source and destination interfaces to an FGSP session sync filter.
654054	Resolved an issue that could sometimes block incoming SSL VPN traffic terminated by the FortiGate-6000 or 7000.
682426 776795	The `ha-direct` FGCP HA option now works as expected on the FortiGate-6000 and 7000 to allow local out traffic (such as sending log messages out an HA dedicated management interface).
719609	Resolved an issue that blocked fragmented ICMP traffic from passing through EMAC VLAN interfaces.
731710	Resolved an issue with how console baud rate changes are synchronized to FPCs or FIMs and FPMs that caused the console to display unsupported characters after changing the console baud rate.
734898	Resolved an issue that could cause the `cmdbsvr` application to crash with a signal 11 segmentation fault when a FortiGate-6000 or 7000 is very busy while making configuration changes.
752402	Resolved an issue that sometimes blocked traffic from passing through a FortiGate-7000F because FortiOS assigned an incorrect MAC address to a VLAN interface.
762210	Resolved an issue that would result in fragmented and non-fragmented ICMP packets from the same session being sent to different FPCs or FPMs.
765407	Resolved an issue that prevented using management interfaces on the secondary FIM in a FortiGate-7000F for FGSP heartbeat traffic.
771680	Configuring SSL VPN Web portals from the GUI now works correctly.
771802	Improvements to SD-WAN compatibility with SLBC.
776828 778392 689047 801738 814002 813223	Multiple FortiOS 7.0.5 kernel fixes.

Bug ID	Description
777336	Resolved a FortiGate-7000 issue that could cause local out traffic from FIMs and FPMs to have overlapping SNAT port ranges.
777415 780296 813096 814330 821710 823335	Resolved a number of issues with synchronizing SDN connector information among components within a FortiGate-6000 or 7000 or between FortiGate-6000s or 7000s in an FGCP HA configuration.
778260	DP session monitoring no longer incorrectly refreshes DP IPSec sessions.
779078	Resolved an issue that caused some synchronized sessions to stay in the CLOSE_WAIT state on the secondary FortiGate-6000 or 7000 in an FGCP cluster.
783689	Resolved an issue that caused FortiGate-6000F DC models with only one DC PSU connected to power to become unstable, causing some FPCs to restart.
784653 827567	Resolved an issue with FortiGate-7000F signature handling that resulted in Fail to append signature error messages and causes the GUI and CLI to indicate that the firmware is not certified.
786659	Resolved an issue that caused the `confsyncd` process running on the primary FIM of the primary FortiGate-7121F to crash, preventing configuration changes from synchronizing to the FPMs in the primary FortiGate-7121F.
787419	Resolved an issue that prevented some user generated certificates from being deleted during a factory reset.
789847	The CLI no longer allows you to split the FIM-7921F P1 and P2 interfaces. Splitting these interfaces is not supported by the FIM-7921F hardware.
792617 786529	Resolved multiple issues that could cause the `confsyncd` process to crash.
792717	Resolved an issue that caused large numbers of IPsec VPN clients with dead peer detection (DPD) enabled to temporarily block dialup IPsec VPN tunnel traffic.
795166 796821 795103	Resolved multiple TPM issues.
796260 822433	Resolved an issue that could cause the link monitor status to appear incorrectly down for FPCs in the secondary FortiGate-6000 in an FGCP HA cluster after performing a non-graceful firmware upgrade.
803585	Resolved memory leak issues that could cause a FortiGate-6000 or 7000 to enter conserve mode and become unresponsive because of high memory utilization.
805704	Resolved an issue with the stability of L2TP sessions.
805808 820426	Resolved an issue on the FortiGate-7121F that could cause TCP packets to be dropped because of how NP7 processors handle packet fragmenting for sessions with proxy inspection and antivirus.
805972	Resolved an issue that could cause an FIM in slot 2 to appear on the FortiGate-7000 GUI when the system only includes one FIM in slot 1.

Bug ID	Description
808859	The Security Fabric no longer sends CSF discovery packets when the `log-unification` Security Fabric option is disabled.
809019	Resolved an issue that prevented the secondary FortiGate-6000 or 7000 in an FGCP HA cluster from replying to SNMP queries sent to one of the secondary FortiGate's in-band management IP addresses.
811615	Resolved an issue that prevented GTP tunnels from being synchronized to the secondary FortiGate-7000 in an FGCP HA cluster running FortiOS Carrier after the secondary FortiGate-7000 restarts.
813646	Time zone changes are now successfully synchronized to all FPCs or all FIMs and FPMs.
816012	The FortiGate-6000 no longer indicates that interfaces configured for 1G speed are always up when the interface socket contains a CR transceiver.
817282	Fixed some `cmdb` and configuration synchronization memory leaks that could cause the FortiGate-6000 management board to experience high memory usage.
819521 818058	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.
819962	FortiGate-6000 and 7000 SDN connector dynamic object resolution should now work as expected.
821125	Resolved an issue with IPsec tunnel synchronization that caused IPsec tunnels to block traffic if the firewall policy included one or more user groups. Traffic would be blocked because the user group id was not being synchronized correctly.
822791 807725 653092 811240 811279	When a FortiGate-6000 and 7000 management interface is configured to be an HA reserved management interface (using the `ha-mgmt-interface` HA option), the interface now correctly reverts to using its own permanent MAC address, instead of using the virtual MAC address assigned to the interface by the FGCP.
822976	Resolved an issue that caused some routes used by IPsec VPNs to be unexpectedly missing from the kernel routing table.
823970	Enabling or disabling an inactive SDN connector no longer affects dynamic addresses received from active SDN connectors.
824789	IPsec tunnels now support authenticating users added to the FortiGate configuration as local users.
825031	Fixed an SDN connector memory leak.
825086	Resolved an issue with how virtual MAC address were calculated that caused local in and local out traffic to be blocked after configuring virtual clustering and enabling virtual cluster 2.
826344	Resolved an issue that created duplicate IPsec VPN event log messages.
828072	Resolved an issue that would sometimes mean that UTM security events are not linked to forward traffic logs.
830531	The SNMP sysName field no longer includes a serial number. The sysName field now just returns the host name.

Bug ID	Description
832121	Resolved an issue that caused IPv6 link-local addresses to not be updated to use HA virtual MAC addresses after enabling FGCP HA.
835699	Resolved an issue that caused configuration synchronization looping because incorrect checksums were generated for certificates. As a result, the system would incorrectly determine that certificates were not synchronized and attempt to re-synchronize them.

Known issues

The following issues have been identified in FortiGate-6000 and FortiGate-7000 FortiOS 7.0.5 Build 0057. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 7.0.5 release notes also apply to FortiGate-6000 and 7000 FortiOS 7.0.5 Build 0057.

Bug ID	Description
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.
803536	A FortiGate-6000 or 7000 may not correctly synchronize routes after various failover scenarios. For example, after a FortiGate-6000 selects a new primary FPC, the routes on the FPC that was the primary FPC should have their protocol changed, but this change may not always occur.
811782	UDP-encapsulated ESP (UESP) sessions that use the normal IKE port (port 4500) are load balanced by the DP or NP7 processor in the same way as normal IPSec traffic. You can use the `ipsec-tunnel-slot` option when creating a phase 1 configuration to control how UESP tunnels are load balanced. However, if UESP sessions use a custom IKE port, the DP or NP7 processor does not handle them as IPsec packets. Instead , they are load balanced by the DP or NP7 processor in the same way as any other traffic. If required, you can adjust load balance settings or add a flow rule for UESP sessions using a custom IKE port.
813569	Operating a FortiGate-6000 or 7000 as an SSL VPN client is not supported.
820988	When configuring an SNMP community, the `source-ip` option is not supported for the FortiGate-6000 and 7000. When the `source-ip` option is configured, SNMP can't send traps for this community.
827937 815874 822410	Multiple issues with Zero Trust Network Access (ZTNA) features. FortiOS 7.0.5 for FortiGate-6000 and 7000 does not support ZTNA.
824205	If an FPM completes starting up when no FIMs are running or all FIMs are in the process of starting up, there is a chance that the FPM will not be synchronized once the primary FIM has restarted.
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.

Bug ID	Description
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.
833488	A CMDB issue can result in the `fcnacd` process adding a VDOM during stress testing.
878934	Some relatively large routing configurations may 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 is not recommended because this will not resolve the high CPU usage problem and can cause interface flapping.

www.fortinet.com