FortiGate™ Multi-Threat Security System

Release Notes
FortiOS™ v3.00 MR6
Patch Release 3
Rev. 1.0

August 1, 2008

Table of Contents

Change Log

Revision	Change Description
1.0	• Added the following bugs to the Resolved Issues section for B0670 – Patch Release 3: 74002, 74066, 74065, 72918, 73837, 73882, 73416, 71105, 74899, 75047, 75342, 73412, 75210, 74554, 75443, 74654, 75148, 72410, 76307, 72275, 76485, 76601, 74053, 74891, 72122, 75405, 71707, 77676, 75113, 76724, 76575, 77467, 73415, 78514, 75336, 77702, 72601, 71946, 72032, 78853, 76950, 75809 and 78297.

© Copyright 2008 Fortinet Inc. All rights reserved.
Release Notes FortiOS™ v3.00 MR6 – Patch Release 3.

Trademarks
Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Registered customers with valid support contracts may enter their support tickets at the Fortinet Customer Support site:

https://support.fortinet.com

1 FortiOS v3.00 MR6 Release – Patch Release 3

This document outlines resolved issues of FortiOS v3.00 MR6 B0670 – Patch Release 3 firmware for the Fortinet FortiGate Multi-threat Security System. Please reference the full version of the FortiOS v3.00 MR6 release notes for new features and known issues. The following outlines the release status for each model.

Model	FortiOS v3.00 MR6 Patch Release 3 Status
FGT-30B	This model is released on a special branch based off of MR6 B0670 – fg300_mr6_30b/build_tag_5237. As such, the build number in the System > Status page and the output from the "`get system status`" CLI command displays 5237 as the build number. To confirm that you are running the proper build, the output from the "`get system status`" CLI command has a "Branch point:" field. This should read 670.
FGT-310B	This model is released on a special branch based off of MR6 B0670 – fg300_mr6_310B/build_tag_5232. As such, the build number in the System > Status page and the output from the "`get system status`" CLI command displays 5232 as the build number. To confirm that you are running the proper build, the output from the "`get system status`" CLI command has a "Branch point:" field. This should read 670.
FGT-5001A-DW	This model is released on a special branch based off of MR6 B0670 – fg300_mr6_5001a/build_tag_5238. As such, the build number in the System > Status page and the output from the "`get system status`" CLI command displays 5238 as the build number. To confirm that you are running the proper build, the output from the "`get system status`" CLI command has a "Branch point:" field. This should read 670.
All	All models are supported on the regular MR6 branch. This excludes FGT-224B.

1.1 General

The TFTP boot process erases all current firewall configuration and replaces it with the factory default settings.

IMPORTANT!

Monitor Settings for Web User Interface Access:

- Fortinet recommends setting your monitor to screen resolution of 1280x1024. This allows for all objects in the Web UI to be viewed properly.

BEFORE <u>any</u> upgrade,

- **[FortiGate Configuration]** Save a copy of your FortiGate unit configuration (including replacement messages) prior to upgrading.

- **[IPS Signature Settings]** Manual or automatic IPS signature updates from FortiGuard overwrites any changes to IPS signatures from their default values. Use the following command to prevent the changes.

```
config system autoupdate ips
      set accept-recommended-settings disable
```

AFTER <u>any</u> upgrade,

- **[WebUI display]** If you are using the Web UI, clear the browser cache prior to login on the FortiGate to ensure proper display of the Web UI screens.

- **[Update the AV/IPS definitions]** The AV/IPS signature included with an image upgrade may be older than ones currently available from the Fortinet's FortiGuard system. Fortinet recommends performing an "Update Now" as soon as possible after upgrading. Consult the FortiGate User Guide for detailed procedures.

2 Resolved Issues in FortiOS MR6 – Patch Release 3

The resolved issues listed below may not list every bug that has been corrected with this release. For inquires about a particular bug, contact Customer Support.

2.1 System

Description: Fix DNS cache poison vulnerability for the dns proxy.
Models Affected: All
Bug ID: 78514 **Status:** Fixed in MR6 – Patch Release 3.

Description: The FortiGate's kernel may crash in an event of IPSec tunnel failover.
Models Affected: All
Bug ID: 73882 **Status:** Fixed in MR6 – Patch Release 3.

Description: The CPU usage of the FortiGate's HTTP proxy (httpd) may go unexpectedly high after it handles more than 1024 requests to go to servers that are listening on port 8008 or 8010.
Models Affected: All
Bug ID: 73416 **Status:** Fixed in MR6 – Patch Release 3.

Description: If the wireless signal is dropped, the Sierra wireless card may not be able to re-establish the connection with FortiWifi-60B.
Models Affected: All
Bug ID: 73412 **Status:** Fixed in MR6 – Patch Release 2.

Description: User → Remote → TACACS+ server key is limited to 12 characters.
Models Affected: All
Bug ID: 75210 **Status:** Fixed in MR6 – Patch Release 3.

Description: Backplane interface status inadvertently changes to up after reboot.
Models Affected: All 5000 series blades.
Bug ID: 75443 **Status:** Fixed in MR6 – Patch Release 3.

Description: FSAE user entries may not get synced to slave if Active Directory server is in non-management VDOM in virtual cluster 2.
Models Affected: All
Bug ID: 76307 **Status:** Fixed in MR6 – Patch Release 3.

Description: FGT50B, FGT60B, FGT-100A and FGT-200A use incorrect MAC address.
Models Affected: FGT50B, FGT60B, FGT-100A and FGT-200A
Bug ID: 75113 **Status:** Fixed in MR6 – Patch Release 3.

Description: FSAE authenticated telnet session may get disconnected when corresponding firewall policy is modified.
Models Affected: All
Bug ID: 76575 **Status:** Fixed in MR6 – Patch Release 3.

Description: The FortiGate may assign same port number to multiple RTSP sessions, causing RTSP traffic problems.
Models Affected: All
Bug ID: 75336 **Status:** Fixed in MR6 – Patch Release 3.

Description: After successful NTLP authentication, the FortiGate shows a temporary “Authentication was successful” web page instead of directly proceeding to the actual website.
Models Affected: All
Bug ID: 72032 **Status:** Fixed in MR6 – Patch Release 3.

Description: Users may experience higher packet loss when traffic is traversing through aggregate interface with IPS enabled in protection profile.
Models Affected: All
Bug ID: 78853 **Status:** Fixed in MR6 – Patch Release 3.

Description: CPU usage by urlfilter daemon may unexpectedly rise to 100%, even when its not in use.
Models Affected: All
Bug ID: 76950 **Status:** Fixed in MR6 – Patch Release 3.

Description: The FortiGate may fail to update session timer when session state is changed, resulting in session table having sessions with invalid timers.
Models Affected: All
Bug ID: 75809 **Status:** Fixed in MR6 – Patch Release 3.

Description: The FortiGate sends different acct-session-id in access-request and accounting-request packets for the same session.
Models Affected: All
Bug ID: 72601 **Status:** Fixed in MR6 – Patch Release 3.

2.2 High Availability

Description: CPU usage for '`hasync`' daemon may spike to 99%, once every minute.
Models Affected: All
Bug ID: 73837 **Status:** Fixed in MR6 – Patch Release 3.

Description: Active-Passive HA cluster may cause packet duplication when used with Windows Network Load Balancing (NLB) service, if NAT is enabled in firewall policy.
Models Affected: All
Bug ID: 71105 **Status:** Fixed in MR6 – Patch Release 3.

Description: Uninterruptable upgrade feature does not work when upgrading from MR5 to MR6 Patch Release 2.
Models Affected: All
Bug ID: 74899 **Status:** Fixed in MR6 – Patch Release 3.

Description: SNMP response from slave FortiGate is not sent on port 161.
Models Affected: All
Bug ID: 75342 **Status:** Fixed in MR6 – Patch Release 3.

Description: `dhcpd` daemon may cause memory leaks on slave FortiGate.
Models Affected: All
Bug ID: 74554 **Status:** Fixed in MR6 – Patch Release 3.

Description: FortiGate cluster running in A-A mode may freeze when under heavy traffic.
Models Affected: All
Bug ID: 76485 **Status:** Fixed in MR6 – Patch Release 3.

2.3 Router

Description: Redistribute Static feature in OSPF does not work properly with point-to-point neighbors.
Models Affected: All
Bug ID: 75047 **Status:** Fixed in MR6 – Patch Release 3.

2.4 VPN

Description: SSLVPN daemon (`sslvpnd`) may crash if user tries to make any changes to SSLVPN web UI page after

session has expired.
Models Affected: All
Bug ID: 74002 **Status:** Fixed in MR6 – Patch Release 3.

Description: SSLVPN proxy may insert Javascript script outside HTML section of a web page when browsed using SSL VPN web mode.
Models Affected: All
Bug ID: 72410 **Status:** Fixed in MR6 – Patch Release 3.

Description: The FortiGate may not be able to connect to HTTPS sites through SSL-VPN Web mode if the server is using cipher
suite with Diffie-Hallman method.
Models Affected: All
Bug ID: 74891 **Status:** Fixed in MR7.

Description: The FortiGate's event log shows INVALID-SPI messages every time IPSec SA is re-negotiated.
Models Affected: All
Bug ID: 71707 **Status:** Fixed in MR6 – Patch Release 3.

Description: IKE daemon `(iked)` may cause memory leak when using aggressive-mode IPSec connection.
Models Affected: All
Bug ID: 77676 **Status:** Fixed in MR6 – Patch Release 3.

Description: SSLVPN tunnel connection to the FortiGate may change physical interface's TCP MSS value to 964.
Models Affected: All
Bug ID: 76724 **Status:** Fixed in MR6 – Patch Release 3.

Description: Users using IPSecuritas VPN client software may not be able to establish an IPSec tunnel with FortiGate if Xauth is enabled.
Models Affected: All
Bug ID: 77467 **Status:** Fixed in MR6 – Patch Release 3.

Description: CPU usage of SSLVPN daemon may get stuck at high 90ies, even if no sslvpn user is connected.
Models Affected: All
Bug ID: 77702 **Status:** Fixed in MR6 – Patch Release 3.

2.5 Antivirus

Description: The HTTP proxy may incorrectly terminate a session when a TCP reset is received and there is still data to be read from the kernel.
Models Affected: All
Bug ID: 74654 **Status:** Fixed in MR6 – Patch Release 3.

Description: The HTTP proxy may not close client connection when a RESET packet is received, resulting in high cpu usage by HTTP daemon (`thttp`).
Models Affected: All
Bug ID: 76601 **Status:** Fixed in MR6 – Patch Release 3.

2.6 Web Filter

Description: FortiGuard web filtering feature incorrectly rates URL's with port numbers as invalid URL.
Models Affected: All
Bug ID: 72122 **Status:** Fixed in MR6 – Patch Release 3.

Description: Web filter does not handle CGI parameters in URL's properly.

Models Affected: All
Bug ID: 73415 **Status:** Fixed in MR6 – Patch Release 3.

2.7 Instant Message

The following IMs and their versions were tested in FortiOS v3.00 MR6 Patch Release 3.

IM Client	Versions	Comment
AIM	6.5.5.2	none
AIM Classic	5.9.6089	none
ICQ	6.0 Build 6059	none
Yahoo! Messenger	8.3.0.2	none
MSN Messenger	7.0 (7.0.0820)	none
MSN Live Messenger	8.5 (8.5.1302.1018)	none

Description: The following table describes the resolved issues for each of the IMs supported by FortiOS v3.00 MR6 Patch Release 3.
Models Affected: All
Bug ID: See table

Clients Affected	Versions	Description/Models Affected/Status/BugID
AIM Classic	5.9.6089	**Description:** IM daemon (`imd`) may randomly crash when instant messaging options are enabled in protection profile. **Models Affected:** All **Status**: Fixed in MR6 – Patch Release 3. **Bug ID:** 74053
Yahoo Messenger MSN Live Messenger	8.1.0421 8.5	**Description:** Yahoo and MSN messenger file transfers may cause IM daemon (`imd`) to crash, if AV scanning is enabled in protection profile. **Models Affected:** All **Status**: Fixed in MR6 – Patch Release 3. **Bug ID:** 75405

2.8 Voice Over IP (VoIP)

Description: Phone may fail to register when registration request needs to pass through two VDOM's with the SCCP enabled in the protection profile.
Models Affected: All
Bug ID: 78297 **Status:** Fixed in MR6 – Patch Release 3.

2.9 Log & Report

Description: The connection between the FortiAnalyzer and the slave FortiGate keeps disconnecting every 10 seconds.
Models Affected: All
Bug ID: 74066 **Status:** Fixed in MR6 – Patch Release 3.

Description: When the local disk log space reaches 95%, a purge and roll of logs can be configured. When this threshold is reached, the FortiGate may not delete the oldest log files on the disk.
Models Affected: All
Bug ID: 74065 **Status:** Fixed in MR6 – Patch Release 3.

Description: FortiGate log message may show an empty value for source and/or destination interface fields.
Models Affected: All
Bug ID: 72918 **Status:** Fixed in MR6 – Patch Release 3.

Description: The quarantine daemon (`quard`) may crash when freeing an unattached buffer, causing full content archiving to cease.
Models Affected: All
Bug ID: 71946 **Status:** Fixed in MR6 – Patch Release 3.

2.10 Wi-Fi

Description: FortiGate has lower throughput when wireless client is connected using EVDO card.
Models Affected: All
Bug ID: 72275 **Status:** Fixed in MR6 – Patch Release 3.

3 Upgrade Information

3.1 Upgrading from FortiOS v2.50

Upgrades from FortiOS v2.50 to FortiOS v3.00 directly is NOT supported. Upgrade to at least FortiOS v2.80 MR11 prior to upgrading to FortiOS v3.00 MR6 Patch Release 3. Refer to the FortiOS v2.80 MR11 release notes for upgrade procedures.

3.2 Upgrading from FortiOS v2.80

Upgrade to FortiOS v2.80 MR11 prior to upgrading to FortiOS v3.00 MR6 Patch Release 3. Refer to the FortiOS v2.80 MR11 release notes for upgrade procedures.

The following are caveats when upgrading from FortiOS v2.80 MR11 to FortiOS v3.00 MR6 Patch Release 3.

[Deprecated IPS Groups]
Certain IPS groups found in FortiOS v2.80 have been removed and their corresponding signatures merged into other IPS groups. As such, those IPS groups are lost when upgrading to FortiOS v3.00 MR6 Patch Release 3. To restore the lost group signature settings, perform the following steps:

- Identify which "lost" IPS group you currently have configured in FortiOS v2.80 from the list found in Appendix A.
- Note the signatures settings that are contained in the FortiOS v2.80 group, and identify in the table the equivalent FortiOS v3.00 group(s) that contains the signature.
- Repeat step 1-2 for each "lost" group.
- After upgrading to FortiOS v3.00 MR6 Patch Release 3, for each group lost, manually configure the equivalent signature settings under the FortiOS v3.00 group(s).

[IPSec VIP]
FortiOS v2.80 supports VIPs configured on a `config vpn ipsec vip`, which essentially is a proxy ARP. There is no such command in FortiOS v3.00, but rather is replaced by the `config system proxy-arp` command. The upgrade scripts do not support this in FortiOS v3.00 MR4. You will need to reconfigure any FortiOS v2.80 IPSec VIPs to use the `system proxy-arp` command in FortiOS v3.00. The command is valid on a per VDom basis in NAT mode. The following is an example CLI configuration.

```
config system proxy-arp
      edit 1
            set ip 192.168.5.111
            set interface "port1"
            next
      edit 2
            set ip 192.168.5.110
            set interface "port3"
            next
      end
```

[FortiOS v2.80 PING Generators]
PING generators in FortiOS v2.80 are able to bring up two tunnels automatically, but FortiOS v3.00 `auto-negotiate` command, which is disabled by default, replaces this functionality. The feature is available in the IPSec phase 2 configurations for both IPSec tunnels and IPSec interfaces.

[Web Filter and Spam Filter Lists]
In FortiOS v2.80, the following lists can be backuped and restored, but in FortiOS v3.00, the lists are stored in the system configuration file and therefore, can not be restored.

1. Web Filtering

2. Web Content Block
3. Web URL Block List
4. Web URL Exempt List

5. Spam Filtering
6. IP Address
7. RBL & ORDBL
8. Email Address
9. MIME Headers
10. Banned Word

FortiOS v3.00 has a feature whereby CLI commands can be imported from a file - see Section 3.2.11: Bulk CLI Configuration Importing. If the FortiOS v2.80 lists are converted to FortiOS v3.00 CLI commands and saved in a text file, the file can be imported using the Bulk CLI Import. Refer to Appendix B: Mapping FortiOS v2.80 Web Filtering and Spam Filtering Lists to FortiOS v3.00 CLI Commands for help on creating a text to import these lists.

[ActiveX, Cookie, and Java Applet Filter]
In FortiOS v2.80, ActiveX, Cookie, and Java Applet filtering must be enabled in the Web Filter > Script Filter page and then in the protection profile under Web Filtering. FortiOS v3.00 has removed the necessity to enable this filtering under the Web Filter > Script Filter page. It now is accomplished only through the protection profile. On upgrading from FortiOS v2.80 to FortiOS v3.00, if any of ActiveX, Cookie, and Java Applet filtering are enabled under the Web Filter > Script Filter page, that setting will be reflected in every protection profile.

[Static Routes without Device Setting Configured]
In FortiOS v2.80, the device setting for a static route is optional. FortiOS v3.00 MR6 Patch Release 3 has made this setting mandatory. If the device setting is not configured, the static route is dropped upon upgrade to FortiOS v3.00 MR6 Patch Release 3.

[Log Filtering Changes]
In FortiOS v2.80, log filtering to a device, such as FortiAnalyzer, hard disk, or memory, is controlled on a global basis meaning, once log filtering is enabled for an event, any firewall policy that produces such an event results in a log message sent to that device. In FortiOS v3.00, log filtering is controlled in two ways:

- On a per-device basis
  `config log <device> filter`

- On a per-protection profile basis
  ```
  config firewall profile
      edit <profile name>
  ```

The per-device filters control whether or not log messages are sent to the device. The per-protection profile filters control whether or not matching traffic through a protection profile results in a log message sent to the device. Upon upgrade from FortiOS v2.80 to FortiOS v3.00, only the per-device log filters are retained - protection profile is altered to accommodate logging, except for `log-web-ftgd-err`, which is enabled by default. After upgrading, review the firewall policies that require logging to be enabled.

[VDom Licensing]
FortiOS v2.80 supports additional virtual domains by way a FortiOS image that contains a hardcoded number of VDoms in it. FortiOS v3.00 uses a VDom license key to upgrade the number of VDoms on high-end models FGT-3000 and up. Upon upgrading from FortiOS v2.80, the VDoms and all of their entries associated configuration are retained, but in the event of a factory reset and a configuration restore, the FortiGate will fail to add all of the VDoms. If you are running FortiOS v2.80 with more than the default number of VDoms, follow these steps when upgrading to FortiOS v3.00:

- Backup configuration for FortiOS v2.80.
- Upgrade to FortiOS v3.00 MR6 Patch Release 3.
- Backup configuration for FortiOS v3.00 MR6 Patch Release 3.

- Contact Customer Support to obtain a FortiOS v3.00 VDom license key. If you are running an HA cluster, you need a license key for each unit in the cluster.
- In the event the configuration needs to be reloaded, the VDom license key needs to be configured first.

Another scenario occurs with FortiOS v2.80 and upgrading with an image that contains additional VDoms. Below are the necessities for this scenario to occur:

- FortiGate is running FortiOS v2.80 with additional VDoms, such 25 VDoms
- Not all VDoms are configured, for example only 15

After upgrading to FortiOS v3.00 MR6 Patch Release 3, if the FortiGate does not let you add 16th VDom. You must contact Customer Support to obtain a FortiOS v3.00 VDom license key, install it, and then add additional VDoms.

Alert E-mail Replacement Messages]
Alert E-mail was modified in FortiOS v3.00 MR6 Patch Release 3. The FortiGate generates and formats its own message for the alert e-mail. Thus any modified alert e-mail replacement messages are not retained upon upgrade to FortiOS v3.00 MR6 Patch Release 3.

[Alert E-mail Filter]
The Alert E-mail filter feature has been changed in FortiOS v3.00 MR6 Patch Release 3. Now, alert e-mails are sent based on category or thresholds. See Section 4.14.4 Alert E-mail Enhancement.

[Administrative Users]
In FortiOS v2.80, an admin user is a global setting, not a per-VDom and thus does not belong to a management VDom. After upgrading to FortiOS v3.00 MR6 Patch Release 3, all v2.80 administrative users are assigned to the root VDom by default. If the management VDom is not assigned to the root VDom, then administrative users, except for the default "admin" user, will fail to login to the management VDom after upgrading.

[Policy Routing]
Both "input-device" and "output-device" are mandatory attributes from FortiOS v3.00 MR2. However, "output-device" is not a mandatory attribute in FortiOS v2.80, therefore, policy routes without "output-device" configured are lost after upgrading to FortiOS v3.00 MR6 Patch Release 3.

[VLANs under WLAN Interfaces]
FortiOS v3.00 MR6 Patch Release 3 does not support VLANs under the WLAN interface and thus any configuration settings referring to the VLANs, as well as the VLANs themselves, are lost upon upgrade to FortiOS v3.00 MR6 Patch Release 3.

[IPSec Related Setting]
Following parameters in a phase1 policy based IPSec tunnel were LOST upon upgrade from FortiOS v2.80 to FortiOS v3.00 MR6 Patch Release 3.:

```
config vpn ipsec phase1
      set dpd [enable|disable]
      set dpd-idleworry <integer>
      set dpd-idlecleanup <integer>
```

Following parameters in a phase2 policy based IPSec tunnel were LOST upon upgrade from FortiOS v2.80 to FortiOS v3.00 MR6 Patch Release 3.:

```
config vpn ipsec phase2
      set bindtoif <interface name>
      set internetbrowsing <interface name>
```

[IPS Predefined Signatures]
The severities of the predefined IPS signatures have been set to recommended levels and can not be altered. Upon upgrading from FortiOS v3.00 MR3 or earlier to FortiOS v3.00 MR6 Patch Release 3, the severities are reset to the recommended values.

[IPSec Manual Keys in a VDom Configuration]

IPSec tunnels configured in a non-root VDom that use manual keys are not retained upon upgrade if the tunnel was not referenced by a firewall policy.

[Static Routes without Device Setting Configured]
In FortiOS v2.80, the device setting for a static route is optional. FortiOS v3.00 MR6 Patch Release 3 has made this setting mandatory. If the device setting is not configured, the static route is dropped upon upgrade.

[HA Monitor Interfaces WLAN]
The WLAN interface can not be used as a monitored interface as of FortiOS v3.00 MR6 Patch Release 3, therefore, upgrading from FortiOS v2.80 to FortiOS v3.00 MR6 Patch Release 3 results in this configuration being lost.

[SSL-VPN Firewall Policies Without Groups]
An SSL-VPN firewall policy is configured without a group is lost upon upgrading to FortiOS v3.00 MR6 Patch Release 3.

[VPN IPSec Phase1 with Type DDNS]
Prior to FortiOS v3.00 MR4, the following IPSec Phase 1 configuration was accepted by the FortiGate even though the configuration was invalid:

```
config vpn ipsec phase1
      set type ddns
      set peertype one
      set peerid aaa
```

From FortiOS v3.00 MR4, this no longer is accepted and therefore, the upgrade from FortiOS v2.80 to FortiOS v3.00 MR6 Patch Release 3 results in loss of configuration.

[VPN PPTP Non-Firewall User Group]
Choosing a user group whose type is NOT equal to firewall when configuring PPTP, results in loss of configuration when upgrading from FortiOS v2.80 to FortiOS v3.00 MR6 Patch Release 3.

[DDNS Server – vavic.com]
The DDNS service for "vavic.com" changed for FortiOS v3.00 MR6 Patch Release 3. The domain is retrieved automatically based on the user's account. Thus, upgrading from FortiOS v2.80 to FortiOS v3.00 MR6 Patch Release 3 will cause loss of configuration for this setting.

[System DHCP Exclude Range]
In FortiOS v280,MR11&MR12, “system dhcp exclude_range” is a standalone section to indicate the IP address that should be exempted from DHCP address pool, in FortiOS v300 MR6 Patch Release 3 , this feature is implement by setting a “config exclude-range” section under “config system dhcp server”. Upgrade from FortiOS v280 to FortiOS v300 MR6 Patch Release 3 will copy these settings to every DHCP server settings:

```
config system dhcp server
      config exclude-range
            edit 1
                  set start-ip 192.168.1.100
                  set end-ip 192.168.1.200
            next
```

[Firewall IP Pools with Class D IP Addresses]
Firewall IP pools using a Class D IP address are lost upon upgrading to FortiOS v3.00 MR6 Patch Release 3, since the configuration is now verified to be below 224.0.0.0.

[Firewall Profiles/Schedule]
In v280, firewall profile and firewall schedule onetime/recurring is a global settings , start from FortiOS v300 MR5, these settings were moved to per-VDom, the upgrade from v280 to FortiOS v300 MR6 Patch Release 3 will copy these three section to every VDom.

[Firewall Service Custom]
In v280, firewall service custom is a global settings , start from FortiOS v300 MR5, these settings were moved to per-VDom, the upgrade from v280 to FortiOS v300 MR6 Patch Release 3 will copy this section to every VDom.

[Firewall VPN Policies Sharing the Same Manual Key]
In FortiOS v2.80, VPN tunnels can be shared across firewall policies, but in FortiOS v3.00 VPN tunnels are assigned to an interface and because the upgrade script assigns the VPN tunnel to one interface, subsequent policies using the VPN tunnel are lost.

3.3 Upgrading from FortiOS v3.00 MR4 and MR5

Upgrading from FortiOS v3.00 MR4 and MR5 to FortiOS v3.00 MR6 Patch Release 3 is supported. MR6 officially supports upgrade from the most recent Patch Release in MR4 and MR5. Customers upgrading from MR3 should upgrade to the latest patch build in MR5 prior to upgrading to MR6.

[FGT-50B Upgrade]
This model uses a different flash technology from other FortiGate models and the partition layout from MR4 to MR5 changed, which causes a loss of the entire configuration. The upgrade is supported from FortiOS v3.00 MR4 B0483 Patch Release 5. See the upgrade path below. The arrows indicate "upgrade to".

MR4 B0480 Patch Release 4
↓
MR4 B0483 Patch Release 5
↓
MR5 B0574 Patch Release 5
↓
MR6 B0670 Patch Release 3

After every upgrade, ensure that the build number and branch point match the image that was loaded.

[FWF-50B Upgrade]
This model uses a different flash technology from other FortiGate models and the partition layout from MR4 to MR6 changed, which causes a loss of the entire configuration. The upgrade is supported from FortiOS v3.00 MR4 B0483 Patch Release 5. See the upgrade path below. The arrows indicate "upgrade to".

MR4 B0477 (br300_mr4_fwf50b/build_tag_5011)
↓
MR4 B0483 Patch Release 5 (br300_mr4_fwf50b/build_tag_6281)
↓
MR5 B0574 Patch Release 5
↓
MR6 B0670 Patch Release 3

After every upgrade, ensure that the build number and branch point match the image that was loaded.

[FGT-60B/FWF-60B Upgrade]
These models use a different flash technology from other FortiGate models and the partition layout from MR4 to MR6 changed, which causes a loss of the entire configuration. The introduction of these models was based on an MR4 special branch and their MR5 release also is based on a special branch. See the upgrade path below. The arrows indicate "upgrade to".

MR4 B0479 (br300_fgt60b/build_tag_5040)
↓
MR4 B0479 (br300_fgt60b/build_tag_5060)

↓
MR5 B0574 Patch Release 5 (br300_mr5_60b/build_tag_5158)
↓
MR6 B0670 Patch Release 3

After every upgrade, ensure that the build number and branch point match the image that was loaded.

[VPN PPTP Non-Firewall User Group]
Choosing a user group which type is NOT equal to firewall when configuring PPTP, results in loss of configuration when upgrading from FortiOS v300 MR4/MR5 to FortiOS v3.00 MR6 Patch Release 3.

[DDNS Server – vavic.com]
The DDNS service for "vavic.com" changed for FortiOS v3.00 MR5. The domain is retrieved automatically based on the user's account. Thus, upgrading from FortiOS v3.00 MR4 to FortiOS v3.00 MR6 Patch Release 3 will cause loss of configuration for this setting.

[Firewall IP Pools with Class D IP Addresses]
Firewall IP pools using a Class D IP address are lost upon upgrading to FortiOS v3.00 MR6 Patch Release 3, since the configuration is now verified to be below 224.0.0.0.

[Web Activity Report Configuration]
Some of the web activity report configuration under "`config log report`" may be lost upon upgrading to FortiOS v3.00 MR6 Patch Release 3.

1. `wf-block-user`
2. `wf-tu-hit`
3. `wf-cat-url`
4. `wf-pa-date`
5. `wf-pa-month`
6. `wf-pa-hour`
7. `wf-pa-date`
8. `wf-pa-month`

[User Peers]
User peers that are configured without a certificate authority (ca) or a subject are not retained upon upgrading to FortiOS v3.00 MR6 Patch Release 3. In MR6 Patch Release 3, at least one of these fields may be a mandatory setting.

3.4 Downgrading to FortiOS v3.00

Downgrading to FortiOS v3.00 results in configuration loss on ALL models. Only the following settings are retained:

- operation modes
- interface IP/management IP
- route static table
- DNS settings
- VDom parameters/settings
- admin user account
- session helpers
- system access profiles

3.5 Downgrading to FortiOS v2.80

Downgrading to FortiOS v2.80 results in configuration loss on ALL models. Only the following settings are retained:

- operation modes
- interface IP/management IP

- route static table
- DNS settings
- VDom parameters/settings
- admin user account
- session helpers
- system access profiles

The FGT1000A-FA2 does not support downgrade to FortiOS v2.80. With the introduction of the FortiClient Check feature, the flash card has a different partition layout than that in FortiOS v2.80.

3.6 Downgrading to FortiOS v2.50

Downgrading to FortiOS v2.50 results in loss of configuration on ALL models.

4 Image Checksums

```
17f5c38b314fe4a24886a41fd49c2326 *FGT_1000AFA2-v300-build0670-FORTINET.out
26eaa4204635fb972fba4d3092e763eb *FGT_1000A_LENC-v300-build0670-FORTINET.out
878a5d50e8862be7c5fa88a2c521dc95 *FGT_1000A-v300-build0670-FORTINET.out
76ac9c483b0565b3d9fc024637ae792e *FGT_100A-v300-build0670-FORTINET.out
8045d595d83c21946a2cb33db5a0a6ba *FGT_100-v300-build0670-FORTINET.out
12e7d411a2122f4ac0269f0098969e96 *FGT_1K-v300-build0670-FORTINET.out
c0bddaf1450fd3a5da631658c2bd136a *FGT_200A-v300-build0670-FORTINET.out
8c2200a9f885023d624ab9d9dbfd69e5 *FGT_200-v300-build0670-FORTINET.out
7d8e11a488d3fe05362aefc0d5617bfa *FGT_3000-v300-build0670-FORTINET.out
2a50509dd3aaa5edeee274a3548feae3 *FGT_300A-v300-build0670-FORTINET.out
a2df3486d0a4224cf26eedb520a7d2a8 *FGT_300-v300-build0670-FORTINET.out
89bc95879b64e95476881086c33dbd09 *FGT_3016B-v300-build0670-FORTINET.out
bb58223c8c4f1fc381e3f5103e2d1afc *FGT_3600A-v300-build0670-FORTINET.out
91159a71def43378a94abdcdded8eefe *FGT_3600-v300-build0670-FORTINET.out
4ba8d7c38cfec0a3ede2e6553f65d784 *FGT_3810A-v300-build0670-FORTINET.out
cf762adf119b47b1768a40f4b69ddae4 *FGT_400A-v300-build0670-FORTINET.out
9231ba51e03257c3934f4ec7bfc2225f *FGT_400-v300-build0670-FORTINET.out
4f02f2057f7601462e2e6d3b6759b9fc *FGT_5001FA2-v300-build0670-FORTINET.out
d723d34996d162677bc415f3d166a041 *FGT_5001-v300-build0670-FORTINET.out
0f571fc7d900ce5762bbab5f7dbdfd6c *FGT_5002FB2-v300-build0670-FORTINET.out
af94b96ced99f99ff4d0c2f2937bb89d *FGT_5005FA2-v300-build0670-FORTINET.out
44d7c91ee38f66ce9e8b7fbaf94c6dec *FGT_500A-v300-build0670-FORTINET.out
109c80d6926f9853eb12ee74f372df30 *FGT_500-v300-build0670-FORTINET.out
61acdc0c6013219d92a4594503bec950 *FGT_50A-v300-build0670-FORTINET.out
3cd88d6f1a1d74667923322aa24ff813 *FGT_50B-v300-build0670-FORTINET.out
ef3269f5267c3a4865b1bbbceb794013 *FGT_60ADSL-v300-build0670-FORTINET.out
a7a74840da6c0c66eaab447a419579d8 *FGT_60B-v300-build0670-FORTINET.out
c59d1896890e3e92432f10cba3bdaabd *FGT_60M-v300-build0670-FORTINET.out
2717388b5438be91b2cc16a7974f06bb *FGT_60-v300-build0670-FORTINET.out
54fe0493930cf47638b7d5ced6c2a06a *FGT_800F-v300-build0670-FORTINET.out
83707fc9bdc2665596aba293e8d2bd8f *FGT_800-v300-build0670-FORTINET.out
2deb69d5fe261907d757778b60aca1f0 *FWF_50B-v300-build0670-FORTINET.out
546c402f0adce1341ca77454edf9a52a *FWF_60AM-v300-build0670-FORTINET.out
0030a3f01af20d4f58780bd88082a658 *FWF_60A-v300-build0670-FORTINET.out
f0c15a4f30780b817abe751a8b0782c7 *FWF_60B-v300-build0670-FORTINET.out
009a8fc55f7c947634bc1999df016d3f *FWF_60-v300-build0670-FORTINET.out
0f791b584d3aeb5b088c31c080a0bd91 *FGT_30B-v300-build0670-FORTINET.out
2e7be812b8dcbb5fe1f25d30bfd91b7f *FGT_310B-v300-build0670-FORTINET.out
40df6952935050ba6b56643b916bf2bb *FGT_5001A-v300-build0670-FORTINET.out
```

(End of Release Notes.)