



# Release Notes

FortiManager Cloud 7.6.3



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<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>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



June 12, 2025

FortiManager Cloud 7.6.3 Release Notes

02-763-1148495-20250612

# TABLE OF CONTENTS

<b>Change log</b> .....	<b>4</b>
<b>FortiManager Cloud 7.6.3 release</b> .....	<b>5</b>
<b>Special Notices</b> .....	<b>6</b>
<b>Upgrade information</b> .....	<b>7</b>
Mandatory upgrades .....	8
Downgrading to previous firmware versions .....	9
<b>Product integration and support</b> .....	<b>10</b>
Web browser support .....	10
FortiOS support .....	10
FortiGate model support .....	11
Language support .....	11
<b>Resolved issues</b> .....	<b>12</b>
Device Manager .....	12
FortiSwitch Manager .....	12
Global ADOM .....	13
Others .....	13
Policy and Objects .....	14
Script .....	14
System Settings .....	14
VPN Manager .....	15
<b>Known issues</b> .....	<b>16</b>
New known issues .....	16
Existing known issues .....	16
AP Manager .....	16
Device Manager .....	17
Others .....	17
Policy & Objects .....	17
System Settings .....	18
VPN Manager .....	18
<b>Limitations of FortiManager Cloud</b> .....	<b>19</b>

# Change log

Date	Change Description
2025-04-23	Initial release.

# FortiManager Cloud 7.6.3 release

This document provides information about FortiManager Cloud version 7.6.3 build 3492.

---



The recommended minimum screen resolution for the FortiManager Cloud GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

---

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.6.3.

There are no special notices for this release.

# Upgrade information

A notification is displayed in the FortiManager Cloud notification drawer when a new version of the firmware is available. You can choose to upgrade immediately or schedule the upgrade for a later date.



Administrators can perform firmware upgrades from within the FortiManager Cloud *Dashboard* or notification drawer.

An administrator with *Super\_User* permissions is required to perform the upgrade.



To keep FortiManager Cloud secure and up to date, it is recommended that you upgrade your 7.6 release to the latest release build.

An email will be sent to notify you when an upgrade is mandatory. After receiving the notification, you will have 14 days to complete the upgrade. See [Mandatory upgrades on page 8](#)



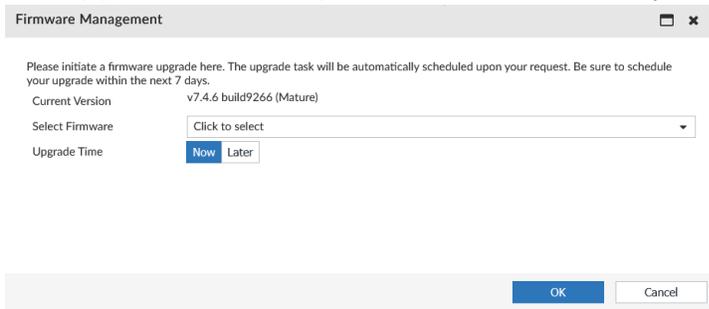
FortiManager Cloud supports FortiOS versions 7.6, 7.4, and 7.2. You must upgrade all managed FortiGates to FortiOS version 7.2 or later.

## To upgrade firmware from the notification drawer:

1. Go to FortiManager Cloud (<https://fortimanager.forticloud.com/>), and use your FortiCloud account credentials to log in. An administrator with *Super\_User* permissions is required to perform the upgrade.
2. Expand the notification drawer to view information about available firmware upgrades.

The screenshot shows the FortiManager Cloud web interface. On the left is a navigation menu with options like Dashboard, Device Manager, Policy & Objects, VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, Fabric View, and System Settings. The main content area is divided into several sections: System Information (Host Name: FMG-K8S-CLOUD, Serial Num..., Platform Ty..., HA Status: Standalone, System Time: Fri Jun 13 09:00:31 2025 PDT, Firmware V...: v7.4.6 build9266 (Mature), System Con...: Last Backup: N/A, Current Ad...: / 1 in total), Service Information (Description: FortiMa..., Expiration...: 2025-02, Management, Account..., Device S...: 0), and Policy Package Stat... (Policy Package Status: Imported, 1 VDOMs). On the right, a 'Notifications' drawer is open, displaying two notifications: 'FortiManager Cloud New Firmware Version' (with a yellow warning icon) and 'Upcoming Maintenance Notice' (with a blue information icon). The 'FortiManager Cloud New Firmware Version' notification includes the text 'New firmware is available.' and a button labeled 'Upgrade Firmware'. The 'Upcoming Maintenance Notice' includes the text 'Due to the scheduled maintenance, the cloud portal may not be stable from June 14th, 2025, 02:00 UTC - June 14th, 2025, 02:30 UTC. New instances will not be created, all running tenant VMs will not be affected.'

3. Click *Upgrade Firmware* to update the firmware immediately or to schedule upgrade of the firmware for a later date.



4. Click *OK* to perform or schedule the upgrade.

### To upgrade firmware from the Dashboard:

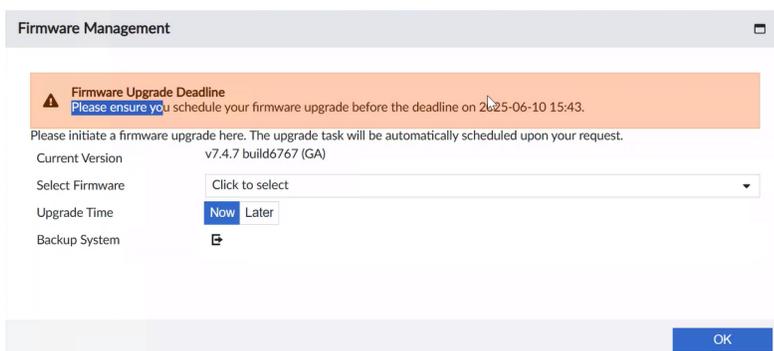
1. Log in to your FortiManager Cloud instance.
2. Go to *Dashboard* in the tree menu.
3. In the *System Information* widget, select the upgrade icon next to the firmware version.

The *Firmware Management* dialog appears. The current firmware version is displayed along with upgrade options.

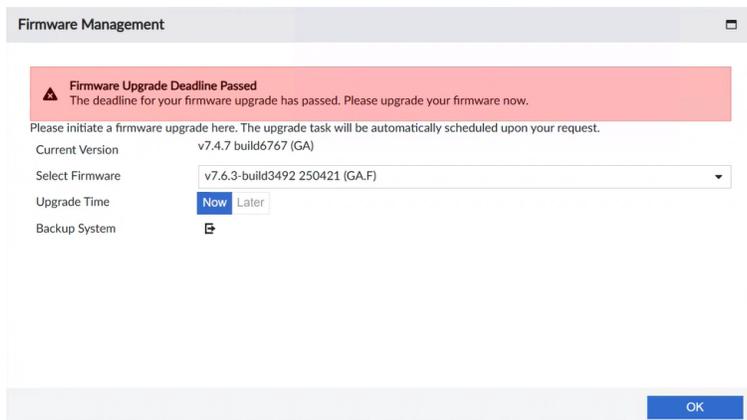
4. In the *Select Firmware* field, choose an available firmware version.
5. In the *Upgrade Time* choose *Now* or *Later*.
  - *Now*: Begin the upgrade immediately.
  - *Later*: Schedule the upgrade for a later time.
6. Click *OK*. The upgrade will be completed based on the selected options.

## Mandatory upgrades

When a firmware upgrade is mandatory, a *Firmware Management* dialog window will appear when you access your instance. This dialog provides details about the upgrade deadline and options for upgrading your firmware version. You can choose to upgrade immediately or schedule the upgrade for a later time. This dialog cannot be bypassed.



After the deadline has passed, you can still connect to your instance's GUI to see the *Firmware Management* dialog window, however, you will only have the option to upgrade immediately. This dialog cannot be bypassed and you will not be able to access your instance until the upgrade is completed.



## Downgrading to previous firmware versions

Downgrade to previous versions of FortiManager Cloud firmware is not supported.

# Product integration and support

FortiManager Cloud version 7.6.3 supports the following items:

- [Web browser support on page 10](#)
- [FortiOS support on page 10](#)
- [FortiGate model support on page 11](#)
- [Language support on page 11](#)

## Web browser support

FortiManager Cloud version 7.6.3 supports the following web browsers:

- Microsoft Edge 114
- Mozilla Firefox version 96
- Google Chrome version 114

Other web browsers may function correctly, but are not supported by Fortinet.

## FortiOS support

FortiManager Cloud version 7.6.3 supports the following FortiOS versions:

- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later



For the complete list of supported FortiOS versions including versions with compatibility issues, see the [FortiManager Release Notes](#).

---

## FortiGate model support

FortiManager Cloud version 7.6.3 supports the same FortiGate models as FortiManager 7.6.3.

For a list of supported FortiGate models, see the [FortiManager 7.6.3 Release Notes](#) on the [Document Library](#).

## Language support

The following table lists FortiManager Cloud language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French	✓	✓
Japanese	✓	✓
Korean	✓	✓
Spanish	✓	✓
Portuguese		✓

To change the FortiManager Cloud language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

# Resolved issues

The following issues have been fixed in 7.6.3. To inquire about a particular bug, please contact [Customer Service & Support](#).

## Device Manager

Bug ID	Description
995919	Cannot config system password-policy expire-day for FortiGates.
1004220	The SD-WAN Overlay template creates route-map names that exceed the 35-character limit.
1079654	Firewall address entries are incorrectly generated when creating a bridge/mesh-type SSID.
1080940	In an IPSEC tunnel template, deleting an IPSEC tunnel that is not the last one in the template causes the configuration of the last remaining tunnel to disappear when you revisit the template.
1086303	An installation error may occur when binding and installing the created VLAN interface to the software switch due to ip-managed-by-fortiipam. No issues have been observed with the installation of VLAN interfaces or physical interfaces.
1099270	Unable to upgrade of FortiGate HA devices via Firmware Templates.
1110780	FortiManager Cloud does not allow creating the local-in policy with SD-WAN zone.
1124171	FortiManager Cloud retrieves the device configuration from the ZTP FortiGate after the image upgrade is performed, due to the 'Enforce Firmware' feature. This action erases all settings in the device database on the FortiManager Cloud side, and as a result, AutoLink installation will not be completed successfully.
1128094	After upgrading to v7.2.10, the entries under <i>Network Monitor &gt; Routing (Static &amp; Dynamic)</i> no longer appear.

## FortiSwitch Manager

Bug ID	Description
1026433	When navigating to <i>FortiSwitch Manager &gt; FortiSwitch VLAN &gt; "BUILD-VLAN"</i> and enabling the DHCP Server, the Advanced options are missing the "filename" field.

Bug ID	Description
1089719	FortiSwitch 110G is not supported.
1097467	There is a mismatch in the per-VDOM limit between the Managed FortiSwitch on the FortiManager Cloud and the actual FortiGate, causing a copy failure error when installing the configuration. So far, this issue has been observed on the FGT-90G.

## Global ADOM

Bug ID	Description
1111249	Unable to assign Global Policy to any ADOM, when firewall address with metadata variables has been used.

## Others

Bug ID	Description
1052341	Not able to select Address type MAC in SD-WAN rule source address.
1106312	The Table View and Device History sections under the <i>SD-WAN Manager's</i> Network tab do not properly display all detailed information, such as Interfaces, Link Mode, and other relevant data. (This issue was initially reported in relation to FortiGate 7.6.1).
1114809	After upgrading the FortiManager Cloud using the "Upgrade Image via FortiGuard" feature, the FortiManager Cloud JSON API login may fail, leading to service disruptions. This issue is important for FortiPortal and other FortiManager Cloud API clients.
1117603	Some compatibility issues have been encountered with FortiOS 7.4.7, please review the Release Notes.

## Policy and Objects

Bug ID	Description
986256	When creating the application list on the FortiManager Cloud, if the Category ID is set to 33 or 34, the installation does not display any errors. However, these invalid categories cannot be set on the FortiGate. Consequently, the assigned application list entry will be created without a specific category and will default to the "block" action. This behavior may cause network interruptions.
1030914	Copy and paste function in GUI removes name of the policy rule and adds unwanted default security profiles (SSL-SSH no-inspection and default PROTOCOL OPTIONS).
1077964	After ZTNA server real server address type changes from FQDN to IP, the policy installation may fail; FortiManager Cloud pushes ZTNA server config with wrong order.
1101436	The "sni-server-cert-check" cannot be disabled on SSL-SSH inspection profile for "ftps" "pop3s" and "smtps".
1109061	FortiManager Cloud tries to set the inspection mode for the deny policies.
1112011	When a policy package contains a globally assigned policy, installing a local ADOM policy package (with the "Install On" feature enabled for a specific device) may not function properly. The policy could be installed on all devices instead of the intended one.

## Script

Bug ID	Description
1085374	FortiManager Cloud does not support exporting the TCL scripts via CLI.

## System Settings

Bug ID	Description
1108205	ADOM lock override does not work even though lock-preempt has been enabled.
1115464	When any interfaces have the serviceaccess feature enabled (fgtupdates, fclupdates, and webfilter-antispam), changing the IP address on the desired interfaces may not immediately affect the listening port for that IP. As a result, the user might not be able to access the GUI using the newly configured IP address (assuming default port 443 is being used).

## VPN Manager

Bug ID	Description
1084434	Unable to rename the address objects (either source and/or destination) used in Phase2 quick selectors in IPSec VPN without an installation error.

# Known issues

Known issues are organized into the following categories:

- [New known issues](#)
- [Existing known issues](#)

To inquire about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

## New known issues

No new issues have been identified in version 7.6.3.

## Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.6.3.

### AP Manager

Bug ID	Description
1086946	The FortiAP upgrade via FortiManager Cloud may fail (on FortiGate 7.6.1). The process could stop at the controller_download_image step or experience a prolonged stall, eventually resulting in a timeout.
1131117	Not able to activate Factory Default profiles, GUI returns error "The selected platform is no longer supported."
1150508	Unable to set the Override Radio feature for managed APs under the AP Manager. Workarounds: <ul style="list-style-type: none"><li>• Run a script on device database or on remote FortiGate Directly (via CLI);</li><li>• Or set the configuration directly on the remote FortiGate and wait for the changes to be reflected on the FortiManager Cloud.</li></ul>

## Device Manager

Bug ID	Description
974925	The NTP Server setting may not display the correct configuration. This issue might occur on managed devices running FortiOS version 7.4.2 or higher. <b>Workaround:</b> Edit NTP server setting under CLI configuration.
980362	The Firmware Version column in <i>Device Manager</i> incorrectly shows 'Upgrading FortiGate from V1 to V2' even after a successful upgrade has been completed.
1136080	Starting from version 7.2.11, FGT devices use a different password type for the administrator's password field. FortiManager Cloud versions released before this change cannot verify the administrator password when installing to an FGT, which may result in an installation failure.

## Others

Bug ID	Description
1065593	Not able to upgrade ADOM.
1105387	The upgrade task failed when the FortiManager Cloud attempted to send the image to the FortiGates. The image file transfer between FortiManager Cloud and FortiGate appeared to fail over the FGFM tunnel. FortiManager Cloud timed out and was unable to retrieve the FortiGate version (first observed in FortiGate version 7.6.1) <b>Workaround:</b> Enable option "Let Device Download Firmware From FortiGuard" in FortiManager Cloud side.
1126662	In a FortiGate HA setup running on the public cloud platform, the FortiManager Cloud attempts to install changes on static routes, which may cause routes to be deleted after an HA failover.

## Policy & Objects

Bug ID	Description
971065	When the number of Custom Internet Services exceeds 256, installation fails due to this limitation.

## System Settings

Bug ID	Description
1063040	<p>Unable to import a local certificate into FortiManager Cloud. This issue may occur if the certificate is encrypted with a newer OpenSSL version that FortiManager Cloud does not yet support.</p> <p><b>Workaround:</b> Convert the latest certificate to the legacy format before uploading it to FortiManager Cloud.</p>

## VPN Manager

Bug ID	Description
1115582	<p>If users reopen the IPsec Tunnel template and close it without making any changes, FortiManager Cloud might still display the following error message in the install log: "Error: VPN IPsec phase1-interface psksecret...Minimum psksecret length is 6..."</p>

# Limitations of FortiManager Cloud

This section lists the features currently unavailable in FortiManager Cloud.

Feature	Feature available?	Details of limitations and unsupported features
Dashboard	Yes	<ul style="list-style-type: none"> <li>• <i>System Resources, Unit Operation, Alert Message Console, and FortiGuard License Status</i> widgets are unavailable.</li> <li>• The <i>Service Information</i> widget replaces the <i>License Information</i> widget.</li> </ul>
Device Manager	Yes	<ul style="list-style-type: none"> <li>• Add Device: <ul style="list-style-type: none"> <li>• Cannot discover a new device, but can add a model device.</li> </ul> </li> <li>• Add FortiAnalyzer: Cannot add a managed FortiAnalyzer device.</li> <li>• Devices &amp; Groups: The <i>IP Address</i> of managed devices displayed in the Device Manager is the NATed IP address from the cloud infrastructure, not the real connecting IP address.</li> <li>• Remote access to managed FortiGate: Remote FortiGate GUI access is not supported by FortiManager Cloud. Remote access to FortiGate using SSH is supported.</li> </ul>
Policy & Objects	Yes	<ul style="list-style-type: none"> <li>• Because Fortinet cannot host LDAP servers for customers, FortiManager Cloud can only connect to a remote LDAP server on the Internet. You can use NAT with a VIP.</li> </ul>
AP Manager	Yes	
VPN Manager	Yes	
Fabric View	Yes	
FortiGuard	Not applicable	<ul style="list-style-type: none"> <li>• FortiManager Cloud does not provide the FortiGuard update service because managed devices can update directly from FortiGuard Cloud.</li> </ul>
FortiSwitch Manager	Yes	
System Settings	Yes	<ul style="list-style-type: none"> <li>• License Information: Available with FortiManager Cloud entitlement information only.</li> <li>• Administrator: The FortiCloud user ID is the administrator's user name. Additional administrators cannot be added directly from FortiManager Cloud.</li> <li>• Trusted Hosts: Not supported.</li> <li>• Create Clone: Create Clone option is unavailable.</li> <li>• Profile: Available for configuring profiles for Cloud IAM users with custom permissions to FortiManager Cloud.</li> <li>• ADOM: <ul style="list-style-type: none"> <li>• ADOMs cannot be created.</li> </ul> </li> </ul>

Feature	Feature available?	Details of limitations and unsupported features
		<ul style="list-style-type: none"><li>• Advanced ADOM mode is not supported.</li><li>• Enabling FortiAnalyzer: FortiAnalyzer Features cannot be enabled from FortiManager Cloud.</li><li>• Remote Authentication Server: Remote Authentication Server is unavailable.</li><li>• SAML SSO: SAML SSO unavailable.</li><li>• HA: HA unavailable.</li><li>• SNMP monitoring tool is not supported.</li><li>• Fabric Management: Fabric Management is not supported on FortiManager Cloud.</li></ul>



The FortiManager Cloud portal does not support IAM user groups.

---



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.