



Release Notes

FortiManager Cloud 7.6.6



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



January 30, 2026

FortiManager Cloud 7.6.6 Release Notes

02-766-1249816-20260130

TABLE OF CONTENTS

Change log	4
FortiManager Cloud 7.6.6 release	5
Special Notices	6
FortiAI for FortiManager Cloud	6
Upgrade information	7
FortiManager Cloud upgrade path	8
Mandatory upgrades	8
Downgrading to previous firmware versions	9
Product integration and support	10
Web browser support	10
FortiOS support	10
FortiGate model support	11
Language support	11
Outbound connectivity from FortiManager Cloud	11
Resolved issues	12
Known issues	13
New known issues	13
Existing known issues	13
AP Manager	13
Device Manager	13
Others	14
Policy and Objects	15
System Settings	15
Limitations of FortiManager Cloud	16

Change log

Date	Change Description
2026-01-30	Initial release.

FortiManager Cloud 7.6.6 release

This document provides information about FortiManager Cloud version 7.6.6 build 3654.



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 7.6.6.

There are no special notices for this release.

FortiAI for FortiManager Cloud

FortiManager Cloud supports FortiAI with the following licenses:

- FC1-10-MVCLD-1118-01-DD: Support FortiAI for instances managing 10 devices/vdoms
- FC2-10-MVCLD-1118-01-DD: Support FortiAI for instances managing 100 devices/vdoms
- FC3-10-MVCLD-1118-01-DD: Support FortiAI for instances managing 1000 devices/vdoms

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.

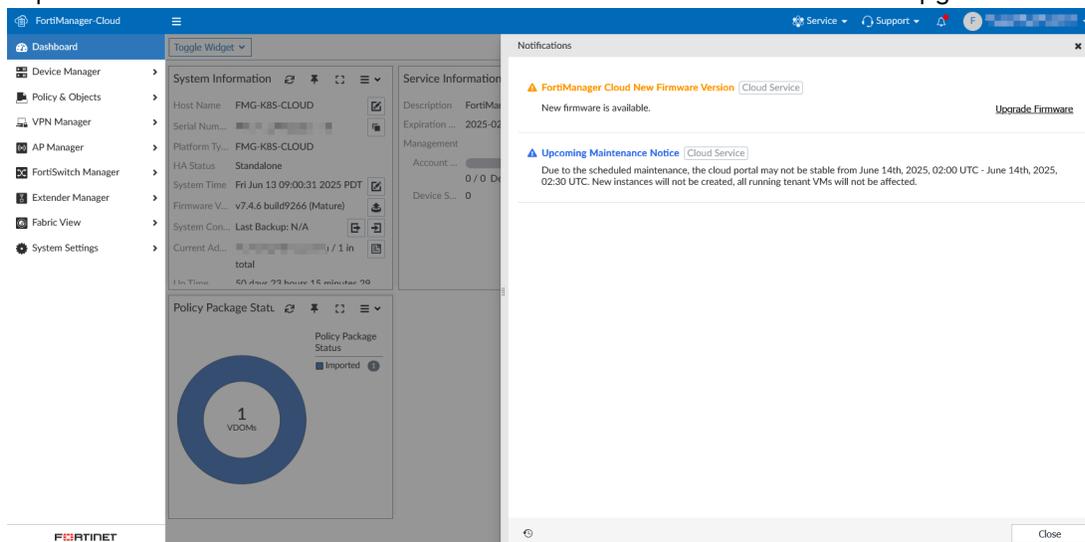
An email will be sent to notify you when an upgrade is mandatory. After receiving the notification, you will have 14 days to complete the upgrade. See [Mandatory upgrades on page 8](#)



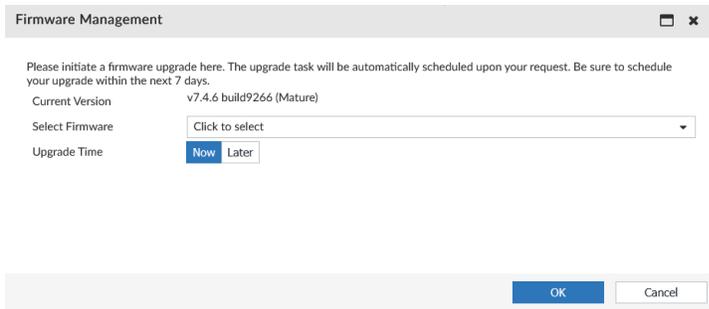
FortiManager Cloud supports FortiOS versions 7.6, 7.4, and 7.2. You must upgrade all managed FortiGates to FortiOS version 7.2 or later.

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.



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.

FortiManager Cloud upgrade path

When upgrading FortiManager Cloud between major/minor versions, you must first upgrade to the latest patch release for the current version and any intermediate versions.

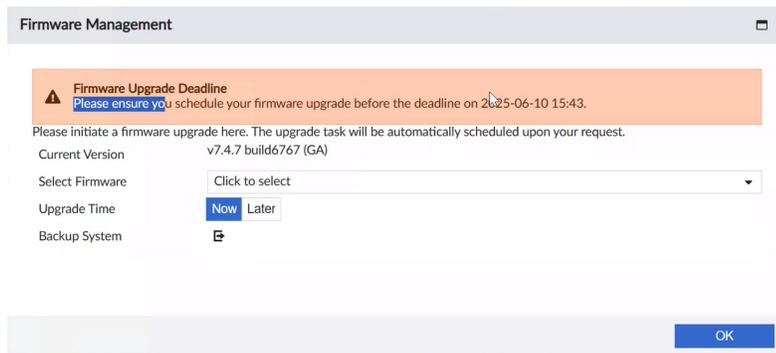
For example, in order to upgrade FortiManager Cloud from version 7.2.x to 7.6.x, you must first upgrade to the latest 7.2 patch version, followed by the latest 7.4 patch version, before finally upgrading to the target 7.6.x release.

The FortiManager Cloud firmware version selection menu only displays the next eligible version that your instance can be upgraded to in the path. In the example above, the 7.4 firmware would not be displayed as an option until you have updated to the latest available 7.2 patch version.

Mandatory upgrades

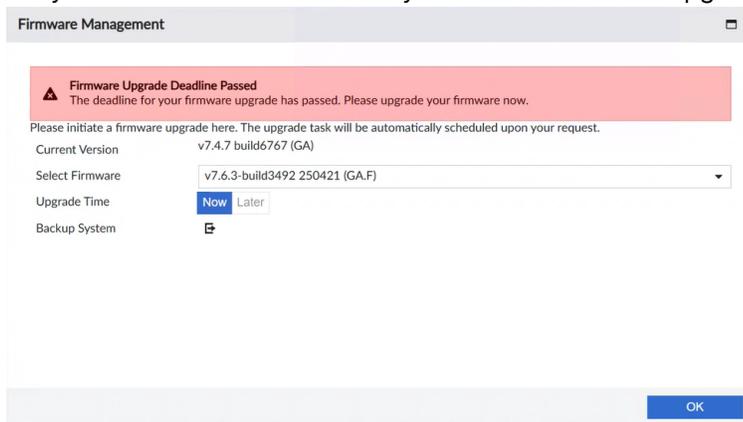
When a firmware upgrade is mandatory, a *Firmware Management* dialog window will appear when you access your instance. This dialog provides details about the upgrade deadline and options for upgrading your firmware

version. You can choose to upgrade immediately or schedule the upgrade for a later time. This dialog cannot be bypassed.



The screenshot shows a 'Firmware Management' dialog window. At the top, there is a warning banner with a triangle icon and the text 'Firmware Upgrade Deadline'. Below the banner, it says 'Please ensure you schedule your firmware upgrade before the deadline on 2025-06-10 15:43.' Below this, there is a message: 'Please initiate a firmware upgrade here. The upgrade task will be automatically scheduled upon your request.' The dialog contains several fields: 'Current Version' is 'v7.4.7 build6767 (GA)'; 'Select Firmware' is a dropdown menu with 'Click to select' displayed; 'Upgrade Time' has two buttons, 'Now' (highlighted in blue) and 'Later'; and 'Backup System' has a checkbox icon. At the bottom right, there is an 'OK' button.

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.



The screenshot shows the same 'Firmware Management' dialog window, but the warning banner is now red and says 'Firmware Upgrade Deadline Passed'. Below the banner, it says 'The deadline for your firmware upgrade has passed. Please upgrade your firmware now.' The message below remains the same: 'Please initiate a firmware upgrade here. The upgrade task will be automatically scheduled upon your request.' The fields are: 'Current Version' is 'v7.4.7 build6767 (GA)'; 'Select Firmware' is a dropdown menu with 'v7.6.3-build3492 250421 (GA,F)' displayed; 'Upgrade Time' has two buttons, 'Now' (highlighted in blue) and 'Later'; and 'Backup System' has a checkbox icon. At the bottom right, there is an 'OK' button.

Downgrading to previous firmware versions

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

Product integration and support

FortiManager Cloud version 7.6.6 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](#)
- [Outbound connectivity from FortiManager Cloud on page 11](#)

Web browser support

FortiManager Cloud version 7.6.6 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 7.6.6 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 7.6.6 supports the same FortiGate models as FortiManager 7.6.6.

For a list of supported FortiGate models, see the [FortiManager 7.6.6 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*.

Outbound connectivity from FortiManager Cloud

FortiManager Cloud supports initiating outbound traffic to supported external services such as public cloud connectors (for example, AWS, Azure) and on-premises systems (for example, Cisco ISE) when these endpoints are reachable over the public Internet.

For more information, see [External Connectors in the FortiManager Administration Guide](#).

Resolved issues

There are no resolved issues identified for the release of FortiManager Cloud 7.6.6.

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 7.6.6.

Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.6.6.

AP Manager

Bug ID	Description
1086946	The FortiAP upgrade via FortiManager 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.

Device Manager

Bug ID	Description
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.
1028515	The Greenwich time zone on FortiGate does not supported on the FortiManager.
1112389	<i>FortiView</i> and <i>Log View</i> fail to display logs when FortiAnalyzer is configured as a managed device in FortiManager.

Bug ID	Description
1136080	Starting from version 7.2.11, FortiGate devices use a different password type for the administrator's password field. FortiManager versions released before this change cannot verify the administrator password when installing to an FortiGate, which may result in an installation failure.
1136726	Enabling the Power Supply Failure option in an SNMP v2 configuration applied via a System Template results in the following installation error: multi-option(power-blade-down) not exist".

Others

Bug ID	Description
1081121	The syslog server is unable to receive FortiManager event logs when the reliable option is enabled.
1105387	The upgrade task failed when the FortiManager attempted to send the image to the FortiGates. The image file transfer between FortiManager and FortiGate appeared to fail over the FGFM tunnel. FortiManager timed out and was unable to retrieve the FortiGate version (first observed in FortiGate version 7.6.1) Workaround: Enable option "Let Device Download Firmware From FortiGuard" in FortiManager side.
1143100	Unable to add physical FortiProxy to FortiManager.
1149980	FortiManager attempts to install a config to FortiProxy may result in the removal of physical ports. This can occur randomly and originates from the FortiProxy side, due to syntax support compatibility issues. A fix is planned for the next FortiProxy release.
1185269	The local log syslog feature set <code>facility</code> is not functioning properly.
1196043	Failed to create <i>Event Handlers</i> or <i>Reports</i> on FortiManager when a Fortinet Fabric Connection is established on FortiAnalyzer to connect to the FortiManager device. Workaround: Go back to the specific ADOM on FortiAnalyzer and create the <i>Event Handlers</i> or <i>Reports</i> there. After synchronization, the new entries should become available on FortiManager.
1203535	FortiManager does not support the <code>diagnose fsm fap-fsw-contract-download</code> request, so the <code>fgdhttpd</code> daemon rejects FortiGate attempts to retrieve FortiAP/FortiSwitch registration status.
1217534	During an upgrade of an FortiGate-HA cluster via FortiManager Cloud, if the <code>disk-check</code> feature is enabled, it may cause all cluster members to reboot simultaneously. This can result in an unexpected traffic interruption. Workaround: To prevent this issue, disable the disk check before performing the upgrade: <code>config fmupdate fwm-setting</code>

Bug ID	Description
	<pre> set check-fgt-disk disable end </pre>
1230277	If the ADOM in an earlier FortiManager version contains DLP dictionary entries named fg-* which are reserved in FortiManager 7.6 the upgrade from ADOM 7.4 to 7.6 will fail. The upgrade process attempts to copy these reserved-name objects, but ADOM 7.6 does not allow them to be created or modified.

Policy and Objects

Bug ID	Description
1101351	Unable to create ZTNA Server with SAML SSO Server
1160047	Application control category "GenAI" is missing in FortiManager, but present in FortiGate. Workaround: Copy a FortiGate application list (Applist) from the CLI that includes Category 36, and insert it into a CLI template in FortiManager. Assign CLI template to FortiGate.
1171027	NAT64 policy and CNAT cannot be created or modified in FortiManager.
1189177	The FortiManager configuration attempted to change the order of custom service objects, but this returned an "Unknown action 0" error.
1200063	Failed to update EMS tags from EMS cloud server on FortiManager v7.6.x.
1202792	The installation may fail with a Current passphrase is invalid error. This can occur when installing an SSID with an MPSK profile, where the MPSK passphrase is not inherited during copy operations or after a FortiManager upgrade.
1209756	Policy package installation fails for FGT-30G due to SSL VPN settings not supported by this FortiGate model.
1224582	FortiManager tries to delete access-proxy and all ZTNA-related configuration from the firewall.
1224598	The Policy Package Diff does not display any differences and throws an error.

System Settings

Bug ID	Description
1158131	The GUI permits configuring the management port to a port number already in use, resulting in loss of access to the GUI.

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"> • <i>System Resources, Unit Operation, Alert Message Console, and FortiGuard License Status</i> widgets are unavailable. • The <i>Service Information</i> widget replaces the <i>License Information</i> widget.
Device Manager	Yes	<ul style="list-style-type: none"> • Add Device: <ul style="list-style-type: none"> • Cannot discover a new device, but can add a model device. • Add FortiAnalyzer: Cannot add a managed FortiAnalyzer device. • Devices & 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. • Remote access to managed FortiGate: Remote FortiGate GUI access is not supported by FortiManager Cloud. Remote access to FortiGate using SSH is supported.
Policy & Objects	Yes	<ul style="list-style-type: none"> • 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.
AP Manager	Yes	
VPN Manager	Yes	
Fabric View	Yes	
FortiGuard	Not applicable	<ul style="list-style-type: none"> • FortiManager Cloud does not provide the FortiGuard update service because managed devices can update directly from FortiGuard Cloud.
FortiSwitch Manager	Yes	
System Settings	Yes	<ul style="list-style-type: none"> • License Information: Available with FortiManager Cloud entitlement information only. • Administrator: The FortiCloud user ID is the administrator's user name. Additional administrators cannot be added directly from FortiManager Cloud. • Trusted Hosts: Not supported. • Create Clone: Create Clone option is unavailable. • Profile: Available for configuring profiles for Cloud IAM users with custom permissions to FortiManager Cloud. • ADOM:

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



The FortiManager Cloud portal does not support IAM user groups.



www.fortinet.com

Copyright © 2026 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.