Release Notes

FortiManager Cloud 7.4.10

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

September 19, 2022
FortiManager Cloud 7.4.10 Release Notes
02-721-843127-20220919

TABLE OF CONTENTS

Change log

Date	Change Description
2026-02-02	Initial release of FortiManager Cloud 7.4.10.

FortiManager Cloud 7.4.10 release

This document provides information about FortiManager Cloud version 7.4.10 build 6146.

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 7.4.10.

Device database enters an incorrect state

The device database in FortiManager Cloud 7.4.8 may enter into an incorrect state. When this occurs, the following symptoms may be observed:

- Copy errors for valid objects during the install process, such as "datasrc invalid. detail: copy datasrc failed, attr [attribute_name] value[object_name]".
- Integrity check failures when running "`diagnose pm2 check-integrity device`".
- Unexpected configuration loss during the *Install Device Settings* operation. Some configuration elements may be deleted, such as firewall policies.

The following workaround is available. If you continue to experience issues, please contact Fortinet Support.

Workaround:

- Run integrity check "diagnose pm2 check-integrity device" and identify device with error.
- Retrieve config from device to fix the error.

Upgrade information

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

In FortiManager Cloud 7.4.3 and later, administrators must perform firmware upgrades from within the FortiManager Cloud Dashboard or firmware upgrade notification drawer.

An administrator with Super_User permissions is required to perform the upgrade.

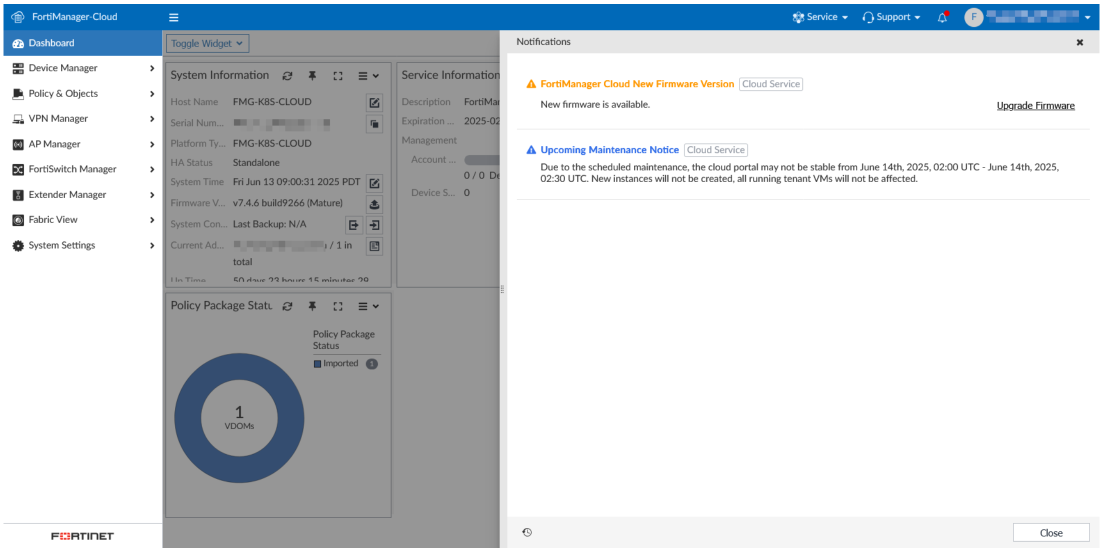
To keep FortiManager Cloud secure and up to date, it is recommended that you upgrade your 7.4 release to the latest release build.

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 7.4, 7.2, and 7.0. You must upgrade all managed FortiGates to FortiOS version 7.0 or later.

To upgrade firmware from the instance:

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.



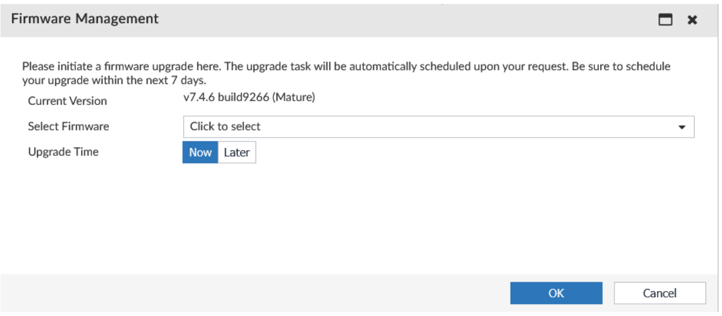
Host Name FMG-K8S-CLOUD
Serial Num... [redacted]
Platform Ty... FMG-K8S-CLOUD
HA Status Standalone
System Time Fri Jun 13 09:00:31 2025 PDT
Firmware V... v7.4.6 build9266 (Mature)
System Con... Last Backup: N/A
Current Ad... [redacted] / 1 in total
Up Time 50 days 23 hours 15 minutes 29

Description FortiMan
Expiration ... 2025-02
Management
Account ...
0 / 0 De
Device S... 0

FortiManager Cloud New Firmware Version Cloud Service
New firmware is available. Upgrade Firmware

Upcoming Maintenance Notice Cloud Service
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.



Firmware Management

Please initiate a firmware upgrade here. The upgrade task will be automatically scheduled upon your request. Be sure to schedule your upgrade within the next 7 days.

Current Version: v7.4.6 build9266 (Mature)

Select Firmware: Click to select

Upgrade Time: Now | Later

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

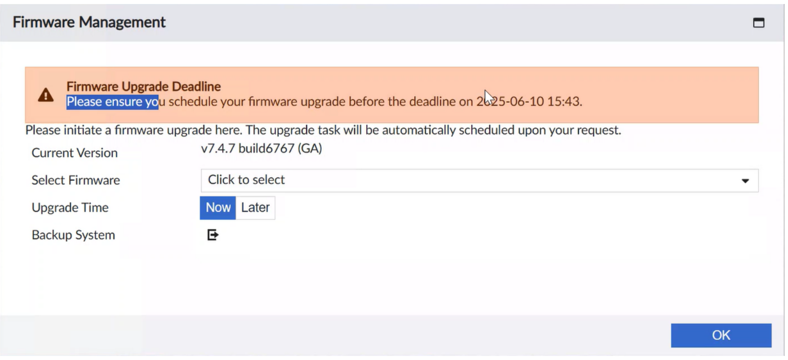
When upgrading FortiManager Cloud between major/minor versions, you must first upgrade to the latest patch release for the current version and any intermediate versions.

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 by bypassed.

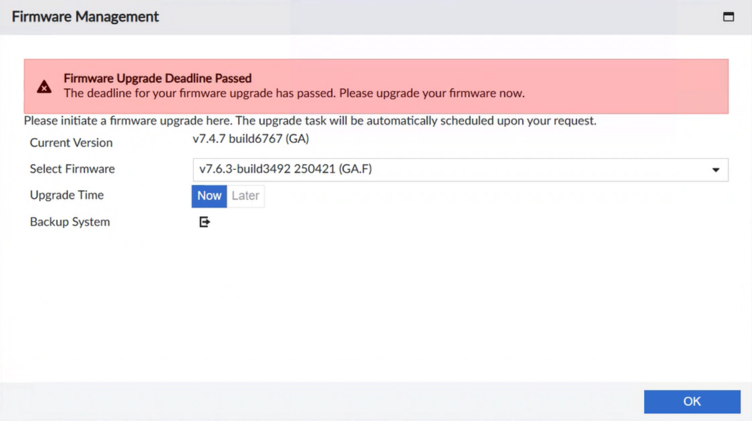


Firmware Upgrade Deadline
Please ensure you schedule your firmware upgrade before the deadline on 2025-06-10 15:43.

Please initiate a firmware upgrade here. The upgrade task will be automatically scheduled upon your request.

Current Version v7.4.7 build6767 (GA)
Select Firmware Click to select
Upgrade Time Now Later
Backup System

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 by bypassed and you will not be able to access your instance until the upgrade is completed.



Firmware Upgrade Deadline Passed
The deadline for your firmware upgrade has passed. Please upgrade your firmware now.

Please initiate a firmware upgrade here. The upgrade task will be automatically scheduled upon your request.

Current Version v7.4.7 build6767 (GA)
Select Firmware v7.6.3-build3492 250421 (GA.F)
Upgrade Time Now Later
Backup System

Downgrading to previous firmware versions

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

Product integration and support

FortiManager Cloud version 7.4.10 supports the following items:

- Web browser support on page 10
- FortiOS support on page 10
- FortiGate model support on page 10
- Language support on page 11
- Outbound connectivity from FortiManager Cloud on page 11

Web browser support

FortiManager Cloud version 7.4.10 supports the following web browsers:

- Google Chrome version 135
- Microsoft Edge version 135
- Mozilla Firefox 138

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

FortiOS support

FortiManager Cloud version 7.4.10 supports the following FortiOS versions:

- 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 7.4.10 supports the same FortiGate models as FortiManager 7.4.10.

For a list of supported FortiGate models, see the *FortiManager 7.4.10 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

The following issues have been fixed in 7.4.10. To inquire about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
1198357	*AP Manager* encounters issues with central AP management because some channels may not be supported.
1204035	FAP-231K is not supported by FortiManager.

Device Manager

Bug ID	Description
970157	FortiManager is attempting to install SNMP configurations that are not supported by the FortiGate VM, such as power-supply-failure, temperature-high, and voltage-alert.
1164358	Device config - dhcp server - address range missing netmask logic in subnet.
1173681	Virtual-wan-link interface is not displayed on Static Route page.
1202467	ADOM 7.4 converts SD-WAN rules route-tags into empty route-tag address objects, breaking compatibility with FortiOS 7.2 devices.
1202695	The FGT90G/91G Gen2 are not supported in Device Model.
1208974	Device count is not correct.
1219062	"sla-compare-method" is still available on SDWAN rules when load balance is enabled.

Others

Bug ID	Description
1077126	The FortiExtender API connection status is returning incorrect value for the FortiExtender device when in an "unknown" state.
1099773	FortiExtender Page 'Data Usage' value does not display the updated values.
1146320	After creating the SSID and assigning it to the FortiExtender profile, the configuration is not pushing to the FortiGate, resulting in an installation failure.
1211261	Users might experiencing Attempting to reconnect messages every few minutes while logged in to the GUI.
1217951	FortiManager may not recognize the 1000F serial number as valid for applying the corresponding Device Blueprint, preventing the CSV file from being loaded.
1224258	In FortiClient EMS 7.4.5, the communication protocol has been upgraded from HTTP/1.0 to HTTP/2. Unlike HTTP/1.x, HTTP/2 does not return a traditional "200 OK" text response, so previous versions of FortiManager that expect this format cannot interpret the new HTTP/2 replies. Because of this, versions prior to FortiManager 7.4.9 and 7.6.5 are not compatible with the EMS version 7.4.5 and later.
1224460	After the upgrade, policy installation fails with a normalized interface error. The issue appears to be related to dynamic mapping validation failures.
1228166	Running "`diagnose dvm check-integrity`" on already corrupt DB may cause unintended behavior.

Policy and Objects

Bug ID	Description
1083504	FortiManager attempts to configure the service in the ISDB6 policy (IPv6), but FortiOS rejects it, causing the installation to fail.
1101351	Unable to create ZTNA Server with SAML SSO Server.
1139663	When using the Install Object(s) function after renaming an object, FortiManager pushes the old object name to the firewall policy.
1156437	No interface mapping listed when importing config for a device (device mapping undefined).
1160047	Application control category "GenAI" is missing in FortiManager, but present in FortiGate.
1169058	Installation might fail to these devices "FGT/FWF-30G/31G" due to some unsupported syntax.

Bug ID	Description
1170381	Unable to create new section "Add Section" in policy after upgrade FortiManager to 7.4.7 while using interface pair view mode. Operation "Add Section" triggers nothing. Field "label" or "global-label" are empty.
1171027	NAT64 policy and CNAT cannot be created or modified in FortiManager.
1174618	After importing the policies and objects from the FortiGate, even though the FortiManager settings were selected, the configuration status for all FortiGates changed to Modified.
1185738	During the auto-linking process, FortiManager attempts to push a policy package containing Internet-Service based rules, but the FortiGates outdated ISDB causes the installation to fail.
1189177	The FortiManager configuration attempted to change the order of custom service objects, but this returned an "Unknown action 0" error.
1196308	EMS server security posture tags are not fully synchronized with FortiManager Cloud; ZTNA tags comment are missing.
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.
1211860	Existing Objects shown as "Not found" in "Where Used".
1212118	Reinstalling policy packages for more than three devices may cause the Application Security Console to crash.
1215309	Installation hang when pushing configurations to firewall groups.
1215335	Redundant policy sub-sections are displayed in the UI after the upgrade.
1215349	FortiManager may delete policies or settings during device installation due to concurrent database interactions from tasks like auto-updates, policy installs, or HA-related updates running simultaneously.
1216601	When attempting to merge duplicate objects, a Minified React error is observed.
1218648	Alternative Resources setting under AWS connector is not pushed to FortiGate.
1224598	The Policy Package Diff does not display any differences and throws an error.

System Settings

Bug ID	Description
1086386	Unable to save changes for SNMP users in FortiManager if more than one notification host is configured.

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 7.4.10.

Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.4.10.

AP Manager

Bug ID	Description
1032762	Since FortiOS 7.4.4 now supports the selection of multiple 802.11 protocols and has trimmed the band options, importing FortiOS 7.4.3 AP profiles may result in some bands and channels being un-matched or unset.

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 lower than 7.4.2. **Workaround**: Edit NTP server setting under CLI configuration.
1028515	The Greenwich time zone on FortiGate does not supported on the FortiManager.

Bug ID	Description
1112389	FortiView & LogView fail to display logs when FortiAnalyzer is configured as a managed device in FortiManager.

Others

Bug ID	Description

1019261	Unable to upgrade ADOM from 7.0 to 7.2, due to the error "Do not support urlfilter-table for global scope webfilter profile".
	Workaround:
	Run the following script against the ADOM DB:
	`config webfilter profile`
	`edit "g-default"`
	`config web`
	`unset urlfilter-table`
	`end`
	`next`
	`end`

1217534	During an upgrade of an FortiGate-HA cluster via FortiManager Cloud, if the disk-check 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:
	`config fmupdate fwm-setting`
	`set check-fgt-disk disable`
	`end`

Policy and Objects

Bug ID	Description
845022	SDN Connector failed to import objects from VMware VSphere.
1199272	Imported certificate does not show details.
1217455	FortiManager is not able to retrieve "usergroup" from "Cisco 3.3 Path7 Pxgrid" using FortiManager connector. **Workaround**: Add the appropriate DNS entry under System Settings Network.
1224582	FortiManager tries to delete access-proxy and all ZTNA-related configuration from the firewall.

Services

Bug ID	Description
1167362	Despite having the "`fgfm-deny-unknown`" setting enabled, unauthorized devices might still be appearing in the *Device Manager*.

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	• *System Resources*, *Unit Operation*, *Alert Message Console*, and *FortiGuard License Status* widgets are unavailable. • The *Service Information* widget replaces the *License Information* widget.
Device Manager	Yes	• Add Device: • Cannot discover a new device, but can add a model device. • Add FortiAnalyzer: Cannot add a managed FortiAnalyzer device. • Devices & Groups: The *IP Address* 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	• 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	• FortiManager Cloud does not provide the FortiGuard update service because managed devices can update directly from FortiGuard Cloud.
FortiSwitch Manager	Yes	
System Settings	Yes	• 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
		• ADOMs cannot be created. • Advanced ADOM mode is not supported. • Enabling FortiAnalyzer: FortiAnalyzer Features cannot be enabled from FortiManager Cloud. • Unit Operation: Unit Operation is unavailable. • Remote Authentication Server: Remote Authentication Server is unavailable. • SAML SSO: SAML SSO unavailable. • HA: HA unavailable. • SNMP monitoring tool is not supported. • Pre-login banners are not supported.

The FortiManager Cloud portal does not support IAM user groups.

www.fortinet.com