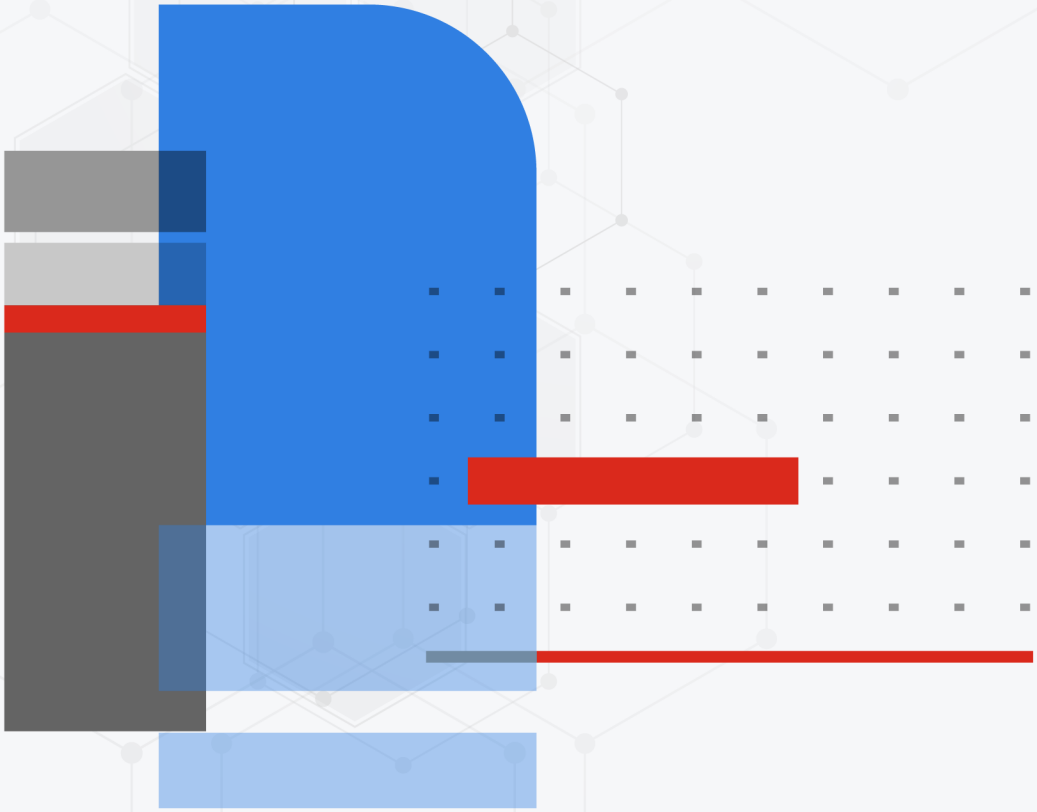
Release Notes

FortiManager Cloud 7.6.7 R1



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

June 12, 2026
FortiManager Cloud 7.6.7 R1 Release Notes
02-767-1289506-20260612

TABLE OF CONTENTS

Change log

Date	Change Description
2026-06-09	Initial release.
2026-06-12	Updated Resolved issues on page 12.

FortiManager Cloud 7.6.7 R1 release

This document provides information about FortiManager Cloud version 7.6.7 R1 (KVM build 3737 and K8S build 6183).

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 7.6.7 R1.

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 chose 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.

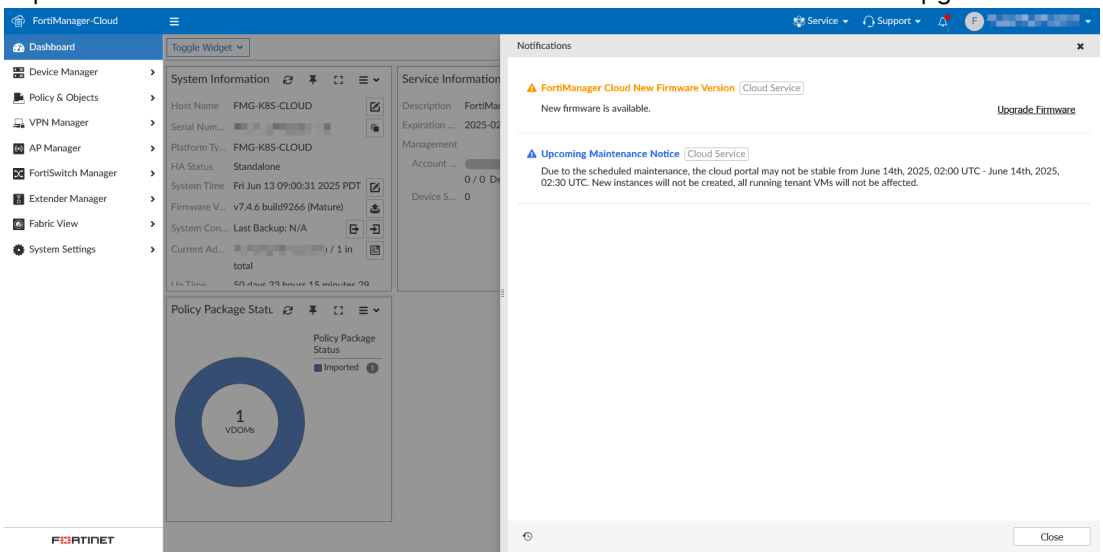
To keep FortiManager Cloud secure and up to date, it is recommended that you upgrade your 7.6 release to the latest release build.

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

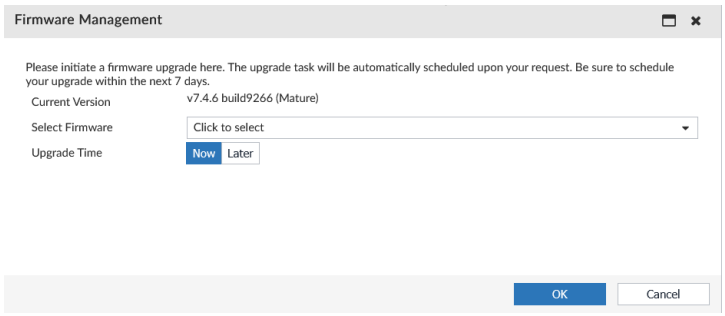
FortiManager Cloud supports FortiOS versions 7.6, 7.4, and 7.2. You must upgrade all managed FortiGates to FortiOS version 7.2 or later.

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.

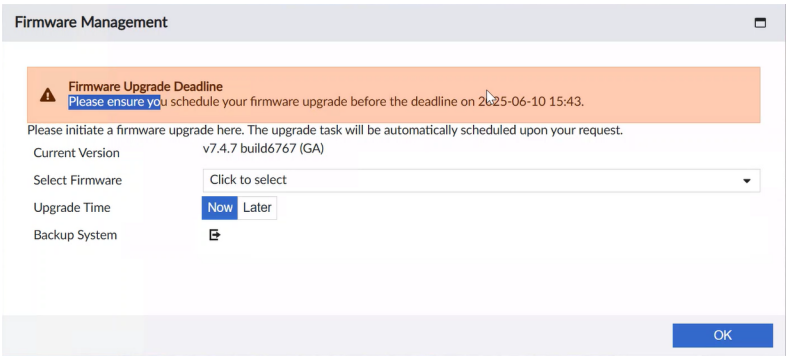
For example, in order to upgrade FortiManager Cloud from version 7.2.x to 7.6.x, you must first upgrade to the latest 7.2 patch version, followed by the latest 7.4 patch version, before finally upgrading to the target 7.6.x release.

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.

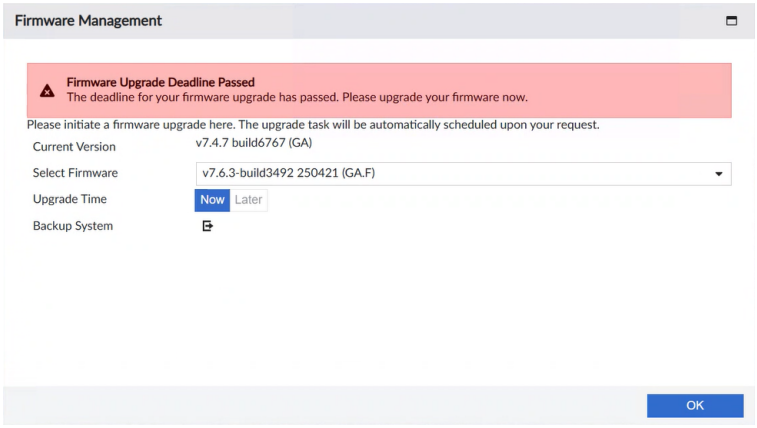
Mandatory upgrades

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.



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 7.6.7 R1 supports the following items:

Web browser support

FortiManager Cloud version 7.6.7 R1 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 7.6.7 R1 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 7.6.7 R1 supports the same FortiGate models as FortiManager 7.6.7.

For a list of supported FortiGate models, see the *FortiManager 7.6.7 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 7.6.7 R1.

AP Manager

Bug ID	Description
1239191	When SSID configured with per-device mapping, during the installation, the FortiManager will report error: Commit failed: ssid fortinet is used by vap.
1239368	Duplicate SSID occurs when accented character is used at the end of the SSID name.
1286849	A GUI freeze may occur when making changes to FortiAP Profiles under AP Manager Operational Profiles.

Device Manager

Bug ID	Description
894948	FortiManager fails to push the FortiAnalyzer override settings to the FortiGate.
895994	When using the 'where used' feature in Phase 2 quick mode selector, objects do not appear, and they can be removed.
1001557	Metadata variables are not supported for the "XAUTH" field in IPsec tunnel provisioning templates.
1015138	Unable to edit interface with dhcp reservation.
1028515	The Greenwich time zone on FortiGate does not supported on the FortiManager.
1189821	Failure to add FortiAnalyzer occurs when using the HA cluster's virtual IP in FortiManager.
1191558	Changes to SD-WAN performance SLA values are not reflected in the device database or the install preview when the detect-mode is set to remote.
1194361	Installation fails when device description contains single quote characters.
1204427	Script log results do not display logs from the most recent script execution; only logs from previous executions are shown.
1215217	The install preview does not load if a device in the device group is offline, but it works fine if all the devices are online.

Bug ID	Description
1224965	Device identification is disabled when changing interface role from LAN to undefined.
1244586	Installation failure occurs when unsetting the "`allow-traffic-redirect`" under the system global.
1246821	FortiManager retrieve may fail when an admins remote-group exists only in the root VDOM and the VDOM order starts with a non-root VDOM, causing invalid reference detection during device addition.
1247501	Installation error occurs when using metadata variables on IP range field in system template.
1251613	Registration of FortiGate-VM64-KVM as Device model to FortiManager may fail due to incorrect platform identification.
1254998	Incorrect Interface Syntax Selection for FGT90G/91G Gen1/Gen2 During Model Device (ZTP) Creation has been observed.
1269401	Performing device deletion may appear very slow. While the deletion process is still ongoing, clients performing policy package installation tasks may experience delays before the task starts or completes. This behavior has been observed in some cases where FortiManager manages more than 6,000 device groups.

FortiSwitch Manager

Bug ID	Description
1118271	FortiSwitch Device information is not displayed when FortiSwitch version is 7.4.3.
1227473	FortiManager attempts to install set poe-status disable on FortiSwitch ports that already have PoE disabled. The issue persists and reoccurs after configuration installation and synchronization.
1244165	When centrally managing switches via FortiManager Cloud, the "Switch-id" is limited to 16 characters. Configuring a hostname exceeding this limit triggers the error: "Switch-id: Value too long."
1246204	Firmware upgrade tasks stall when multiple upgrades for the same FortiSwitch are run concurrently.
1268279	Deleting custom-command from FortiSwitch Manager template is not deleting it from device.

Global ADOM

Bug ID	Description
1150670	Installation failure occurs when upgrading global ADOM from v7.2 to v7.4 due to gno-inspection settings.
1163223	A global object loses its global status when transferred from a local ADOM to an FortiGate device and then re-imported into another local ADOM, resulting in a duplicate object error.
1177672	When global policy package assignment fails, it may impacts the policy packages on the ADOM.
1201449	Global policy assignment configured with Automatically Install Policies to ADOM Devices may get stuck during deployment.
1232811	Unassigning a Global Policy Package may fail when it is referenced by SSL inspection profiles in the root ADOM.
1244194	Global Policy Block appended to Global Policy Package is not visible under root ADOM PP when assigned.
1245741	The Promote to Global feature for objects created in an ADOM may fail if the object name contains a forward slash (/) character.

Others

Bug ID	Description
1081121	The syslog server is unable to receive FortiManager event logs when the reliable option is enabled.
1179653	The API interface performance in version 7.6 may appear slower compared to previous versions.
1180920	After the installation, an event alert was received indicating that the FGFM tunnel is flapping.
1185269	The local log syslog feature set facility is not functioning properly.
1189184	Copy Policy Package operations may take longer than usual and remain stuck for an extended duration, even for small changes. This issue may occur when FortiOS does not return a response to FGFM requests from FortiManager.
1203535	FortiManager does not support the `diagnose fdsm fap-fsw-contract-download` request, so the fgdhttpd daemon rejects FortiGate attempts to retrieve FortiAP/FortiSwitch registration status.

Bug ID	Description
1210519	Central-management settings are deleted on the primary unit when adding a FortiProxy HA cluster via Device Discover. This issue may occur when the FortiManager ADOM is configured in backup mode and the FortiProxy central-management setting is also set to the backup mode. Refreshing the device may trigger the issue.
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.
1234093	Time discrepancy occurs between formatted and raw logs when using GMT timezone.
1239748	Unable to delete Meta Variables with the following Error: The data is invalid for selected url.
1241163	After upgrading from 7.6.4 or earlier, users may encounter a blank GUI screen upon login if the ADOM flag value (flags) contains an incorrect value.
1241561	ADOM integrity check fails when running `diagnose cdb check adom-integrity`.
1244008	When FortiAnalyzer is added as a managed device in FortiManager Cloud, executing any of the "`diagnose cdb upgrade check`" commands may result in an unexpected behavior in the CLI.
1246091	FortiOS 7.4.10 partially supported by FortiManager 7.6.5/7.6.6. See the FortiManager Cloud 7.6.5/7.6.6 Release Notes for Compatibility Issues.
1247597	FortiManager is unable to sync user information from the pxGrid connector.
1251516	Installation failure occurs when pushing primus HSM (on-premises Hardware Security Module) settings via provisioning templates to FortiProxy.
1252855	ADOM upgrade from 7.4 to 7.6 may fail repeatedly during the dynamic_mapping copy phase with the error message: "unexpected input."
1255147	The fmg-admin is able to click both the text label and the toggle.
1256462	FortiClient fails to pull AV signatures from FortiManager acting as FDS server when receiving UM objects over HTTP.
1257065	FortiGuard subscription status shows unknown when trial license has expired.
1257789	Root ADOM upgrade fails when duplicate policy package names exist within a policy block.
1266515	When importing a custom firewall service definition through a FortiManager script that mixes the set protocol TCP/UDP/SCTP parameter with `set protocol-number <value>`, FortiManager allows the configuration without validation errors.
1268146	An error occurs when upgrading FortiManager due to password length limitations.
1284743	In an FortiGate HA setup running on a public cloud platform and managed by FortiManager Cloud, FortiManager may attempt to install or modify `vdom-exception` configurations, such as static routes. This may lead to issues during a failover event, including routes being deleted or other unexpected behavior.
1240263	FortiManager Cloud discrepancy in device license counts between the CLI and GUI.

Policy and Objects

Bug ID	Description
1101351	Unable to create ZTNA Server with SAML SSO Server.
1171027	NAT64 policy and CNAT cannot be created or modified in FortiManager.
1182465	Installation fails when FortiManager creates a default shaping-profile and binds it to an interface.
1189177	The FortiManager configuration attempted to change the order of custom service objects, but this returned an "Unknown action 0" error.
1194560	Missing CASB applications occur when FortiManager fetches casb application data without the 'get reserved' option.
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.
1227209	Insert above or insert below fails when using ISDB objects in the policies.
1232760	Permit-stun-host configuration is not applied during installation when NAT is disabled.
1234646	FortiManager fails to display installation preview info. Preview stays blank with just a special character.
1235065	When loading an ssh cert, there is no password option and encrypted keys are not accepted.
1240260	When the Policy Package setting "Policy Offload Level" is set to Default mode, the Copy Policy Validation may fail and display an error log "COMMIT FAIL - invalid value".
1240764	Users may experience slowness when loading large policy packages while switching between Interface Pair views.
1242292	When configuring ISDB entries through the GUI, the default port value may be incorrectly applied, resulting in inaccurate port assignments within the configuration.
1242707	Policy package status does not change to "Out of Sync" on FortiManager when local changes are made on FortiGate.

1245964	In FortiOS 7.4.10, CLI syntax changes can cause install failures on low-memory (2GB) models when pushing configuration for:
	`web-proxy global proxy-fqdn`
	`firewall ssl-ssh-profile ssh`

Bug ID	Description
	For more details, please review the Special Notices in the FortiManager Cloud 7.6.5/7.6.6 Release Notes.
1247668	Importing firewall policies may fail when adding an FortiGate with a large number of policies (e.g., over 60K).
1249297	Policies disappear from policy block GUI when policy block name contains '/' character.
1252128	Firewall Policy object lists are auto-compressed when more than 3 objects per rule are present.
1255176	Policy package installation may stuck when dynamic mapping member of a "firewall addrgrp" is empty.
1257115	Policy package installation may fail on hardware devices when policy-offload-level is set to default.
1257828	Searching in Policy Packages/Policies with certain keywords may result in an unexpected error.
1258985	When disabling the HTTPS protocol under "Protocol Port Mapping" of any "SSL/SSH Inspection" profile, FortiManager tries to push the command "unset ports" which is not recognized by the FortiGate. As a result, the error "Must set at least one port or enable ssl inspect-all. ..."is generated during the Policy Package Installation.
1265850	When attempting to view "Where Used" for a url-filter list, the GUI continuously loads and does not return any results, even after several minutes.
1270583	Installation fails when FortiManager pushes an invalid limit for policing type shaping-profile.
1287157	GUI may crash when clicking Next in the Import Wizard before the Conflict Configuration table has fully loaded.
1287203	When attempting to view "Where Used" for a Web Content Filter, the GUI continuously loads and does not return any results, even after several minutes.

Revision History

Bug ID	Description
1248791	ADOM revision history may be lost when upgrading the ADOM to version 7.6.

Services

Bug ID	Description
1180123	FortiManager downloads and pushes full-version objects between FDS and FortiGate, which can result in high traffic usage.

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.
1257096	Policy package changes are unavailable to FortiManager Cloud-admins authenticated by Radius with ADOM scope and ext-auth-adom-override enabled.

VPN Manager

Bug ID	Description
1256324	Installation may fail after creating VPN communities of any type.
1262311	In a FortiManager 7.4 ADOM, attempts to create or retrieve SSL VPN web portal settings for FortiOS 7.4 devices may fail due to per-VDOM limit validation errors.

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

The following issues have been identified in version 7.6.7 R1.

Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.6.7 R1.

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.

Others

Bug ID	Description
1196043	Failed to create *Event Handlers* or *Reports* 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 *Event Handlers* or *Reports* there. After synchronization, the new entries should become available on FortiManager.

Bug ID	Description

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
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.
1200063	Failed to update EMS tags from EMS cloud server on FortiManager v7.6.x.

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. • 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: • ADOMs cannot be created.

Feature	Feature available?	Details of limitations and unsupported features
		• 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