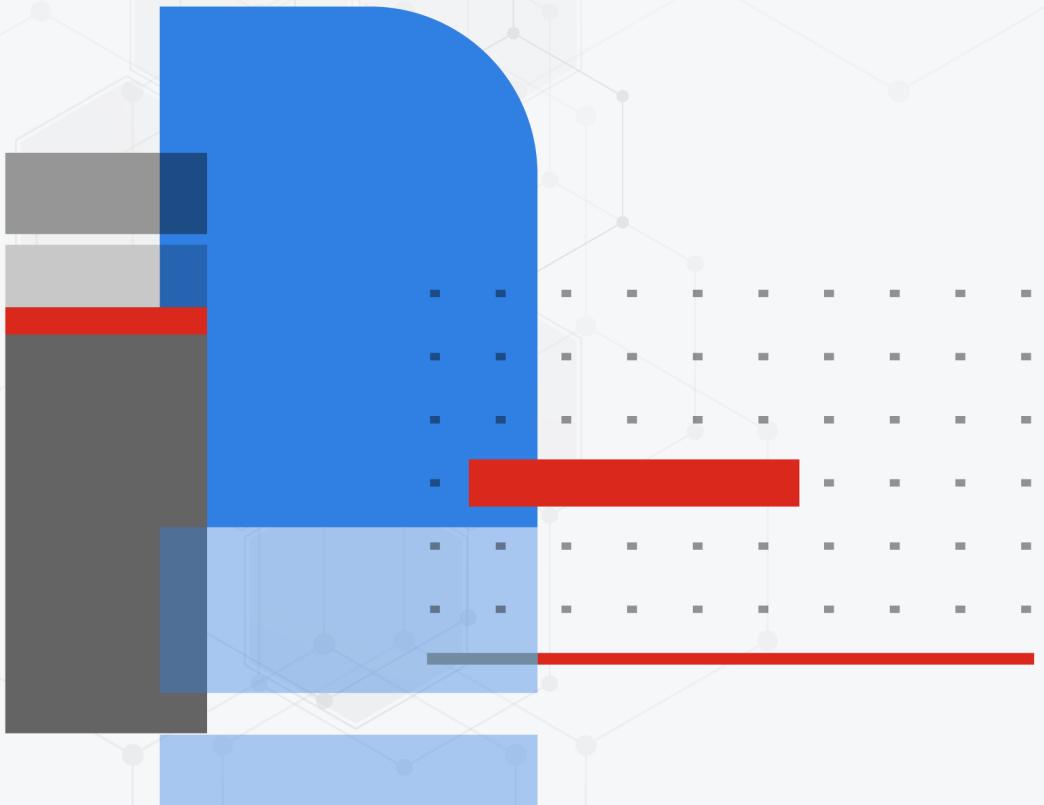




Release Notes

FortiManager Cloud 7.4.7



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 7.4.7 Release Notes

02-721-843127-20220919

TABLE OF CONTENTS

Change log	4
FortiManager Cloud 7.4.7 release	5
Special Notices	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	10
Language support	11
Resolved issues	12
AP Manager	12
Device Manager	12
FortiSwitch Manager	15
Others	15
Policy and Objects	16
Script	18
Services	19
System Settings	19
VPN Manager	19
Common Vulnerabilities and Exposures	20
Known issues	21
New known issues	21
Existing known issues	21
AP Manager	21
Device Manager	21
Others	22
Policy & Objects	23
Limitations of FortiManager Cloud	24

Change log

Date	Change Description
2025-06-16	Initial release of FortiManager Cloud 7.4.7.
2025-06-26	Updated Resolved issues on page 12 and Known issues on page 21 .
2025-07-08	Updated Resolved issues on page 12 .

FortiManager Cloud 7.4.7 release

This document provides information about FortiManager Cloud version 7.4.7 build 6767.



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 7.4.7.

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 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.

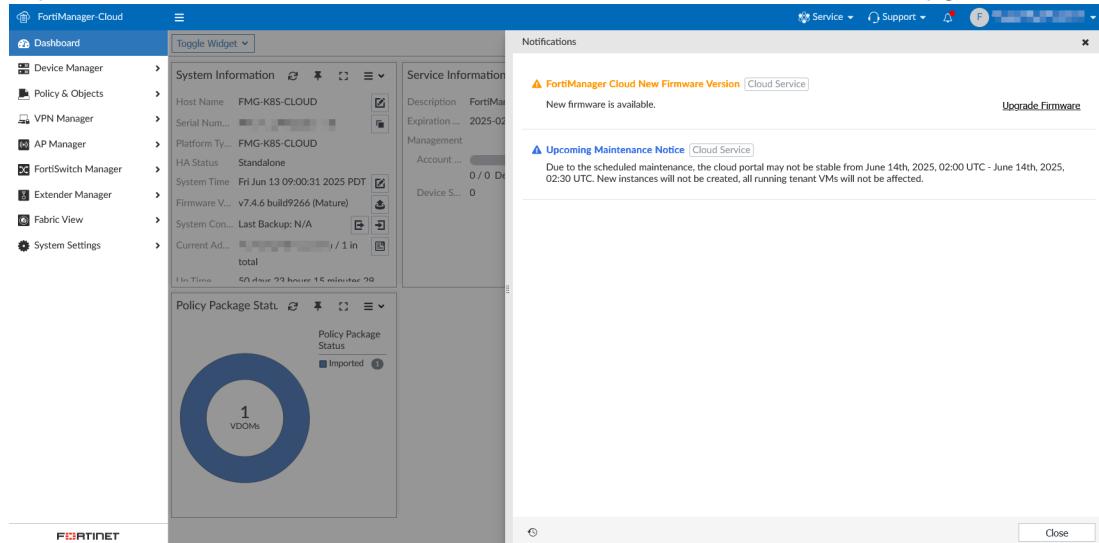
An email will be sent to notify you when an upgrade is mandatory. After receiving the notification, you will have 14 days to complete the upgrade. See [Mandatory upgrades on page 8](#)



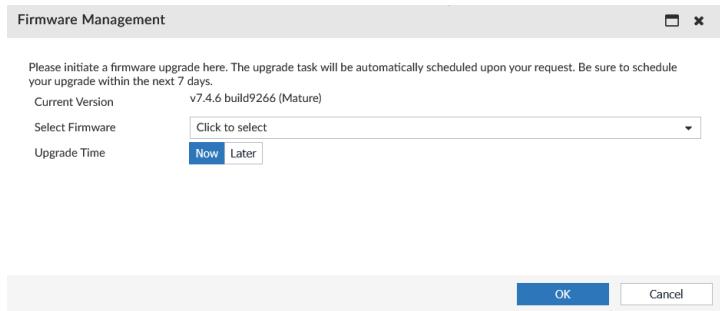
FortiManager Cloud supports FortiOS versions 7.4, 7.2, and 7.0. You must upgrade all managed FortiGates to FortiOS version 7.0 or later.

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.



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.

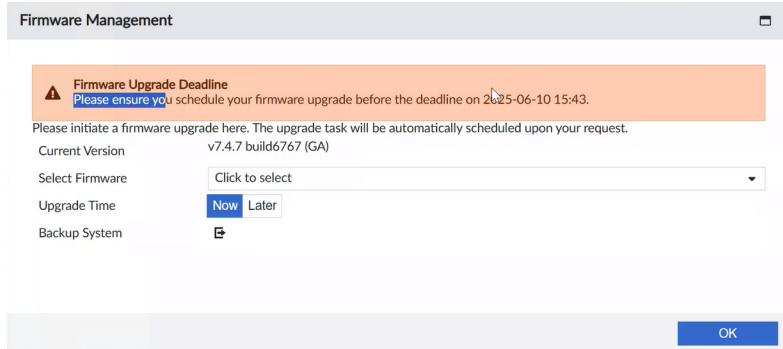
The FortiManager Cloud firmware version selection menu only displays the next eligible version that your instance can be upgraded to in the path. In the example above, the 7.4 firmware would not be displayed as an option until you have updated to the latest available 7.2 patch version.

Mandatory upgrades

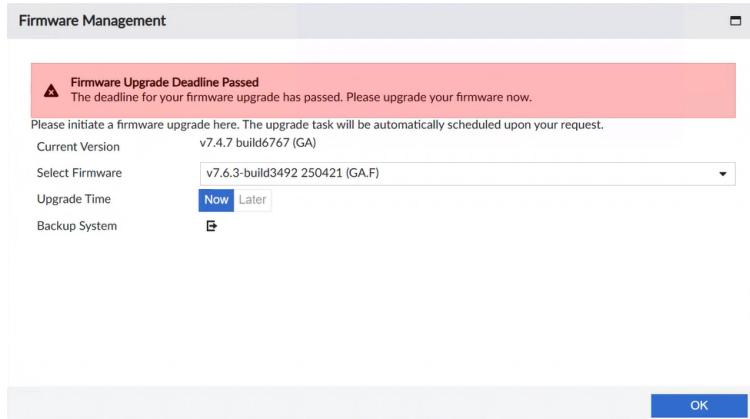
When a firmware upgrade is mandatory, a *Firmware Management* dialog window will appear when you access your instance. This dialog provides details about the upgrade deadline and options for upgrading your firmware

Upgrade information

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 7.4.7 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](#)

Web browser support

FortiManager Cloud version 7.4.7 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 7.4.7 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 7.4.7 supports the same FortiGate models as FortiManager 7.4.7.

For a list of supported FortiGate models, see the [FortiManager 7.4.7 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*.

Resolved issues

The following issues have been fixed in 7.4.7. To inquire about a particular bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
1041445	The AP attributes do not automatically update in the <i>AP Manager</i> .
1050466	The 802.11ax-5g AP profile is missing for all FortiAPs that support WiFi 6.
1083224	FortiManager Cloud attempts to install 'port1-mode > bridge-to-wan' when 'Override LAN Port' is enabled and 'LAN Port Bridge' is set to 'Bridge to LAN'.

Device Manager

Bug ID	Description
932579	Assigning a BGP template is purging the previously existing BGP config from the target FortiGates
992550	Unable to remove the trusted host for a FortiGate admins under the Device DB from the FortiManager Cloud's GUI.
995919	Cannot config system password-policy expire-day for FortiGates.
1000101	FortiManager Cloud fails to retrieve certificates that were directly imported into the FortiGate. As a result, FortiManager Cloudrepeatedly attempts to push a CSR, leading to installation status conflicts.
1004220	The SD-WAN Overlay template creates route-map names that exceed the 35-character limit.
1021789	The FortiManager Cloud SD-WAN widget's health check status is not functioning as expected.
1039127	Unable to edit the Logs settings under the device management.
1041265	While using a <i>Device Blueprint</i> to apply a pre-run cli template and creating model devices via CSV import, the pre-run does not show applied in <i>Device Manager</i> .

Bug ID	Description
1041440	Some FortiGate platform (FGT-40F & FGT-60F) does not support the <code>ip-managed-by-fortiipam</code> and FortiGate refuses to take the configuration from FortiManager Cloud; hence users will be experiencing the install error.
1053194	If the <code>system interface speed</code> attribute is changed from the FortiManager Cloud, it may potentially cause an installation failure. Modifying the " <code>system interface speed</code> " is not currently supported on the FortiManager Cloud and must be done on the FortiGate side.
1063635	FortiManager Cloud does not support the FortiWiFi-80F-2R-3G4G-DSL.
1063835	FortiManager Cloud ZTP installation to FortiGate versions 7.2.8 and lower may fail due to differing default <code>ssh-kex-algo</code> settings between FortiManager Cloud and FortiGate.
1063850	FortiManager Cloud is attempting to install a "PRIVATE KEY" with every installation, even after retrieving the config.
1071249	Under <i>Device Manager > Monitors > SD-WAN Monitor</i> , there are some missing data on widgets Bandwidth Overview and Traffic Growth.
1073479	Install preview does not function properly.
1075052	Occasionally, installations may fail on FortiGates in HA mode due to a "Serial number does NOT match" error. This can happen if the HA device's serial number on FortiManager Cloud does not immediately update after a failover.
1079654	Firewall address entries are incorrectly generated when creating a bridge/mesh-type SSID.
1080414	CSV import fails to set metadata variables due to old header format ("name").
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.
1085385	Importing SD-WAN configuration previously completed on a FortiGate as a provisioning template in FortiManager Cloud returns "Response format error" message
1086303	An installation error may occur when binding and installing the created VLAN interface to the software switch due to <code>ip-managed-by-fortiipam</code> . No issues have been observed with the installation of VLAN interfaces or physical interfaces.
1089102	Metadata variable value cannot be emptied (value deleted) after a value has been set via <i>Edit Variable Mapping</i> for a model device.
1090340	Deleting at least 1 VPN IPsec tunnel from the IPSEC Templates purging other vpn phase2-interfaces which are using the same template
1094451	If the <i>Timezone</i> field in the <i>System Template</i> is left blank, FortiManager Cloud may apply its default timezone and overwrite the existing timezone on the FortiGates.
1099270	Unable to upgrade of FortiGate HA devices via Firmware Templates.
1103166	Installation wizard might stuck at 50% if the device has Jinja CLI template assigned.

Bug ID	Description
1103304	OSPF passive interface settings cannot be set via <i>Device settings > Router > OSPF</i> .
1110780	FortiManager Cloud does not allow creating the local-in policy with SD-WAN zone.
1111432	In a BGP template Neighbor Range, set <code>max-neighbor-num 0</code> is not accepted by the GUI.
1115014	FortiManager Cloud fails to install SSID configuration in FortiGate when captive portal is enabled with error "Must set selected-usergroups"
1119280	Firmware Template assignment does not work properly.
1122481	When an FortiGate HA failover occurs, making any changes to the SD-WAN configuration on the FortiGate HA may cause FortiManager Cloud to attempt to purge the firewall policies on the device during the installation (Install Device Settings (only)).
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.
1124431	Installation failure due to 'sslvpn os check' syntax error.
1126321	When creating a VLAN with "LAN" Role, an object is created even if "Create Address Object Matching Subnet" is disabled.
1128094	After upgrading to v7.2.10, the entries under Network Monitor > Routing (Static & Dynamic) no longer appear.
1129574	Unable to restrict Firmware upgrade via Admin Profile.
1136080	Starting from version 7.2.11, FortiGate 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 FortiGate, which may result in an installation failure.
1148864	During provisioning, if multiple scripts attempt to modify the aggregate interface, the database installation fails with the following error: [attribute "vdom" check error - runtime error -2: Virtual domain must be same as virtual domain () for all aggregate/redundant interfaces] This issue occurs only with aggregate interfaces.
1152564	Unable to edit route-map due to the following error "rule/2/set-priority is out of range (property: set-priority)".
1153376	If devices are added to FortiManager Cloud after SD-WAN is enabled, then Traffic Shaping/SD-WAN may display No Data or No Records Found. If the user enables SD-WAN after the device is already managed by FortiManager Cloud, there should be no issue.

FortiSwitch Manager

Bug ID	Description
1026433	When navigating to <i>FortiSwitch Manager > FSW VLAN > "BUILD-VLAN"</i> and enabling the DHCP Server, the Advanced options are missing the <i>filename</i> field.
1077058	IPv4 allow access for VLAN interface over Per-Device Mapping cannot be set.
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.
1110598	Unable to add per device mapping config for FortiSwitch VLAN.
1153287	The maximum number of managed FortiSwitches on FortiManager Cloud does not match with the maximum number of managed FortiSwitches by FortiGate, resulting in a copy failure error during installation to FortiGates.

Others

Bug ID	Description
1003711	During the FortiGate HA upgrade, both the primary and secondary FortiGates may reboot simultaneously, which can disrupt the network. This issue is more likely to occur in FortiGates that require disk checks, leading to longer boot times.
1009848	Support ISE distributed deployment: PAN/MnT Nodes up to 2, Pxgrid Nodes up to 4.
1025366	FortiManager Cloud does not support the FortiExtender SSID
1052341	Not able to select Address type MAC in SD-WAN rule source address.
1065593	Not able upgrade ADOM.
1075449	Intermittent connection issues have been reported randomly when the FortiManager Cloud manages 1000+ FortiGates.
1081941	When UTM-Profile gets added to a FortiProxy policy, FortiManager Cloud generates invalid config.
1089725	Progressively slower GUI performance caused by increasing memory usage of the "init" daemon.
1091375	When the install is waiting for a session, it neither updates nor completes the task.
1111686	FortiManager Cloud's GUI may crash with the error "Oops! Sorry, an unexpected error has occurred." when downloading a backup or accessing the <i>Last Script Run</i> option

Bug ID	Description
	under <i>Device Database</i> .
1113799	Unable to upgrade the FortiAP or FortiSwitch from FortiManager Cloud.
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 FortiManager Cloud 7.4.6 Release Notes.
1119279	Event log for object is generating thousands of Wifi Events.
1124007	'OK' button does not save the settings; Navigate to Device Manager > Device & Groups > Right click on FortiGate > Firmware upgrade > Schedule > Custom > Define time > Press OK.
1125382	When EMS is added as a Fabric Connector to these FortiGates from FortiManager Cloud, all devices appear under FortiManager Cloud-managed devices, but only the primary FortiGates serial number is displayed.
1136765	The PxGrid connector should support Fully Qualified Domain Names (FQDN).
1142559	When attempting to upload the firmware image from FortiGuard, FortiManager Cloud returns the following error "Code: -1, Invalid image". This issue has primarily been observed on FortiGate hardware platforms running special build firmware versions, where the image contains an encrypted MBR such as on the FortiGateRugged-70G-5G-Dual, FortiGateRugged-70G, FortiGateRugged-50G-5G, FortiWiFi-70G models.
1147636	Universal connector card on <i>Fabric View</i> page is missing under <i>Fabric View > Endpoint/Identity connectors</i> .

Policy and Objects

Bug ID	Description
706809	Policy Checkexport does not have the last hit count details anymore.
968149	Unable to export policy package to CSV.
969923	The <i>View Mode</i> button, which is used to check the interface in Pair View, is missing in the Firewall Policy under Policy Packages.
991720	FortiManager Cloud still has an option to enable the <code>match-vip</code> through the policy package for "allow" policies. However, this is not supported anymore on the FortiGates.
1011220	FortiManager Cloud constantly changes the UUID of some objects.
1025012	Configuring the SSL/SSH inspection profile may result in the following error: "The server certificate replacement mode cannot support category exemptions."

Bug ID	Description
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).
1047850	Error occurs when modifying any route maps: "Cannot save route maps: rule/[id]/set-priority: out of range...".
1054707	FortiManager Cloud try to install "unset qos-policy" and installation fails.
1057228	Importing the SDN Objects, with multiple tags, will addmultiple entries listed as SDN objects; when clients add anything into the filters section, browser immediately redirects to an error page showing: "Oops! Sorry, an unexpected error has occurred".
1070800	FortiManager Cloud is attempting to install the <code>cli-cmd-audit</code> command on a FortiGate running version 7.2.8, which does not support this command, leading to an installation error.
1073463	Installation is failed with error "VIP entry cannot be moved when central-nat is disabled."
1076659	When policy package configured with policy block, installationto multiple devices may have copy fail errors if combined length of the Policy Block name and Policy name is greater than 35 characters and if the total number of such policies exceeds 1000.
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.
1078598	Unable to import policy due to issues related to the protocol-options feature.
1079037	The <code>internet-service-id</code> attribute is configurable in the FortiManager Cloud, whereas this attribute cannot be modified on the FortiGate.
1079128	ZTNA Server Per-Device Mapping may display a copy error failure if a new per-device mapping is created without specifying the object interface.
1079678	FortiManager Cloud does not provide any warning when there is a "deny all" policy in the middle of a Policy Package. This can be still seen on the "task monitor".
1082548	Address type FQDN is missing DNS resolve domain name function feature.
1086603	Unable to create local-in policy with ISDB objects.
1086705	Multicast policy table Log column shows wrong info and right click update does not work properly.
1092581	FortiManager Cloud cannot modify <code>rat-timeout-profile</code> in Policy Packages.
1097885	Action column is missing in policy package for security policy when NGFW Mode set to policy-based.
1101436	The <code>sni-server-cert-check</code> cannot be disabled on SSL-SSH inspection profile for "ftps", "pop3s", and "smtps".
1101919	Changes to a Virtual IP global settings are not applied when a per-device mapping exists.

Resolved issues

Bug ID	Description
1106646	When attempting to configure a local-in policy on FortiManager Cloud using ISDB objects as the source, the following error is encountered: "Attribute 'srcaddr' MUST be set when internet-service-src-name is set"
1108159	IP address list for an ISDB object differ between FortiManager Cloud and managed FortiGate while both devices have installed the same ISDB definitions.
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.
1112917	Unable to set or update a security profile group on a policy directly in the firewall or proxy policy view.
1113129	FortiManager Cloud is treating <code>implicit-deny local-in</code> policy incorrectly, denying any traffic.
1114832	Any addition/modification in Application and Filter Overrides for Application profile doesn't show up in the install preview.
1116489	The revision history time stamps for custom profiles are all showing the same.
1119299	Installation fails due to syntax compatibility issues between FortiManager Cloud and FortiGate version 7.2.10. Specifically, the issue occurs when FortiManager Cloud attempts to unset the <code>servercert</code> in the <code>vpn ssl</code> settings.
1130475	FortiManager Cloud starts appending an ID to the global-label associated with policies. This can cause a problem if global labels are being used to group policies together.
1131552	Import fails due to an invalid remote certificate, even though the certificate is available on the FortiGate.
1133553	Unused policy tool showing <code>No hit count report</code> for this policy package message when policy block is added to policy package.
1134276	Installation of "config system ddns" configuration fails.
1139220	FortiManager Cloud does not prevent users to mix ISDB and destination addresses.

Script

Bug ID	Description
931088	Unable to delete VDOMs using the FortiManager Cloud script. Interfaces remain in the device database, causing the installation to fail.
1085374	FortiManager Cloud does not support exporting the TCL scripts via CLI.

Services

Bug ID	Description
1108706	When updating query service packages from the global anycast server (globalupdate.fortinet.net), medium-sized IoT packages may encounter checksum errors. These errors can prevent the proper updating of SPAM and URL databases, potentially impacting the FortiManager Cloud's FortiGuard Services.
1116120	When the FortiGuard Web Filter and Email Filter services are enabled, the usage of the root filesystem ("rootfs") gradually increases until it reaches 100%. This may affect the performance of other functions on the FortiManager Cloud, and it will be more noticeable when the FortiManager Cloud is operating with a smaller memory size.
1138715	FortiManager Cloud does not auto-download the FortiClient signature from FortiGuard.

System Settings

Bug ID	Description
1047252	Incorrect warning message displayed in FortiManager Cloud GUI during upgrade from Feature build to Mature build.
1081463	The encrypted backup file cannot be easily correlated with the backup details, as the date and time are not included.
1088248	When users perform any task, such as installing a policy, the task monitor icon that appears at the top-right of the GUI continuously shows a loading state, and users are unable to view the task progress.
1108205	ADOM lock override does not work even though lock-preempt has been enabled.
1121608	Under the <i>Dashboard > Sessions</i> widget, the number of current sessions presented in FortiManager Cloud does not match the number of sessions in the FortiGate.

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.

Bug ID	Description
1084696	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...".
1090636	Unable to edit VPN community due to the following error message: "vpnmgr/vpntable/: cannot be edited".

Common Vulnerabilities and Exposures

Visit <https://fortiguard.com/psirt> for more information.

Bug ID	CVE references
1086927	FortiManager Cloud7.4.7 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2025-24474

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 7.4.7.

Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.4.7.

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
970157	FortiManager Cloud is attempting to install SNMP configurations that are not supported by the FortiGate VM, such as power-supply-failure, temperature-high, and voltage-alert. Workaround: Create a CLI template for SNMP configuration and assign it to the device(s).

Bug ID	Description
973365	<p>FortiManager Cloud does not display the IP addresses of FortiGate interfaces configured with DHCP addressing mode.</p> <p>Workaround:</p> <p>Disable Addressing Mode from DHCP to Manual in FortiManager Cloud Device DB, then retrieve from FortiGate and IP will be updated successfully.</p>
974925	<p>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.</p> <p>Workaround:</p> <p>Edit NTP server setting under CLI configuration.</p>
980362	<p>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.</p>
1102790	<p>FortiManager Cloud pushes the <code>unset auto-connect</code> command to <code>config system 1te-modem</code>, where the default value is disabled on FortiOS but still enabled on FortiManager Cloud.</p>

Others

Bug ID	Description
1126662	<p>In an 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.</p>
1019261	<p>Unable to upgrade ADOM from 7.0 to 7.2, due to the error "Do not support urlfilter-table for global scope webfilter profile".</p> <p>Workaround:</p> <p>Run the following script against the ADOM DB:</p> <pre> config webfilter profile edit "g-default" config web unset urlfilter-table end next end </pre>
1041706	<p><i>Extender Manager</i> shows the managed Extender as Down even if it is Up and correctly displayed on FortiGate.</p>

Policy & Objects

Bug ID	Description
845022	SDN Connector failed to import objects from VMware VSphere.
971065	When the number of Custom Internet Services exceeds 256, installation fails due to this limitation.
1142983	In FortiManager Cloud, creating a threat feed connector and applying it to multiple VDOMs results in the same UUID being assigned across all instances. This behavior may lead to duplicate UUID issues.

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.• 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.



The FortiManager Cloud portal does not support IAM user groups.



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.