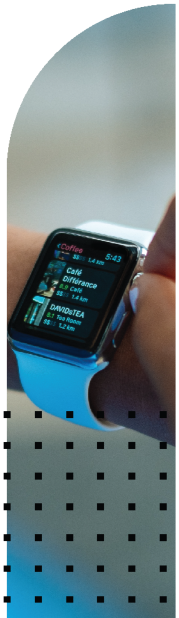
Release Notes

FortiManager Cloud 7.2.11



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 7.2.11 Release Notes
02-721-843127-20220919

TABLE OF CONTENTS

Change log

Date	Change Description
2025-10-02	Initial release.
2026-01-15	Updated Limitations of FortiManager Cloud on page 20.

FortiManager Cloud 7.2.11 release

This document provides information about FortiManager Cloud version 7.2.11 build 7233.

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 7.2.11.

Shell access has been suspended

Shell access has been suspended in FortiManager Cloud 7.2.7.

Upgrade information

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

Primary users can upgrade FortiManager Cloud firmware to 7.2.11 by using the FortiManager Cloud & Service portal. Secondary users can upgrade FortiManager Cloud firmware to 7.2.11 by entering the instance and going to the *System Settings* module.

To keep FortiManager Cloud secure and up to date, it is recommended that you upgrade your 7.2 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 9.

FortiManager Cloud supports FortiOS versions 6.4, 7.0 and 7.2. You must upgrade all managed FortiGates to FortiOS version 6.4.4 or later.

To upgrade firmware from the notification drawer:

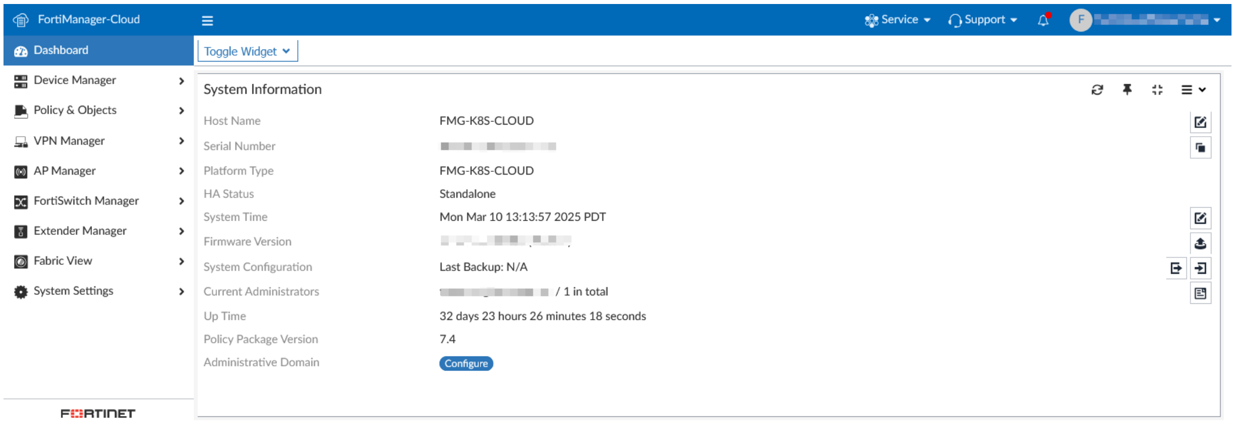
1. Go to FortiManager Cloud (https://fortimanager.forticloud.com/), and use your FortiCloud account credentials to log in. An administrator with *Super_User* permissions is required to perform the upgrade.
2. Expand the notification drawer to view information about available firmware upgrades.
3. Click *Upgrade Firmware* to update the firmware immediately or to schedule upgrade of the firmware for a later date.
   Alternatively, you can access firmware upgrade options from the FortiManager Cloud Dashboard.

   The *Later* option for *Upgrade Time* is only available for one week after the firmware is released.
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.

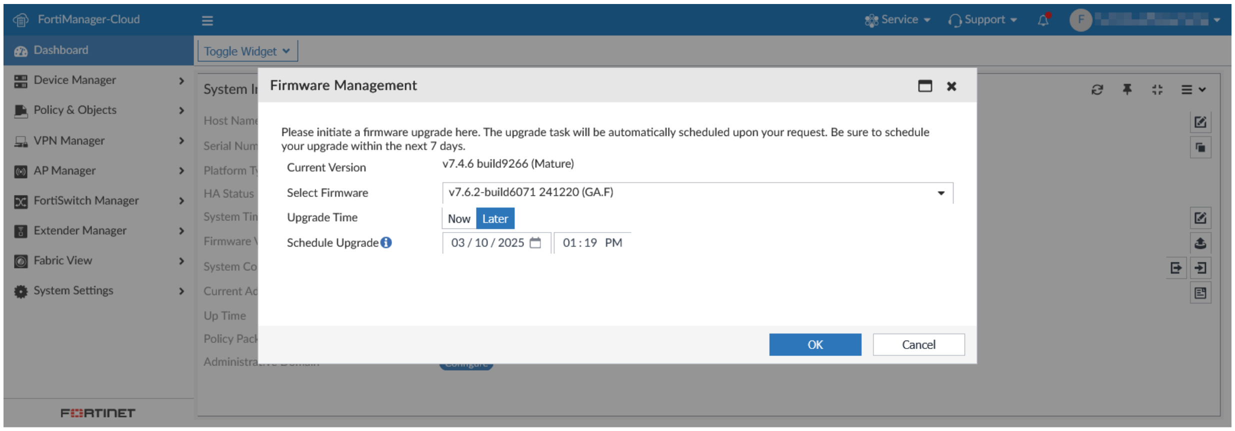
3. In the *System Information* widget, select the upgrade icon next to the firmware version.



System Information

Host Name	FMG-K8S-CLOUD
Serial Number	[redacted]
Platform Type	FMG-K8S-CLOUD
HA Status	Standalone
System Time	Mon Mar 10 13:13:57 2025 PDT
Firmware Version	[redacted]
System Configuration	Last Backup: N/A
Current Administrators	[redacted] / 1 in total
Up Time	32 days 23 hours 26 minutes 18 seconds
Policy Package Version	7.4
Administrative Domain	Configure

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



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	v7.6.2-build6071 241220 (GA.F)
Upgrade Time	Now [✓ Later]
Schedule Upgrade	03 / 10 / 2025 01 : 19 PM

OK Cancel

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

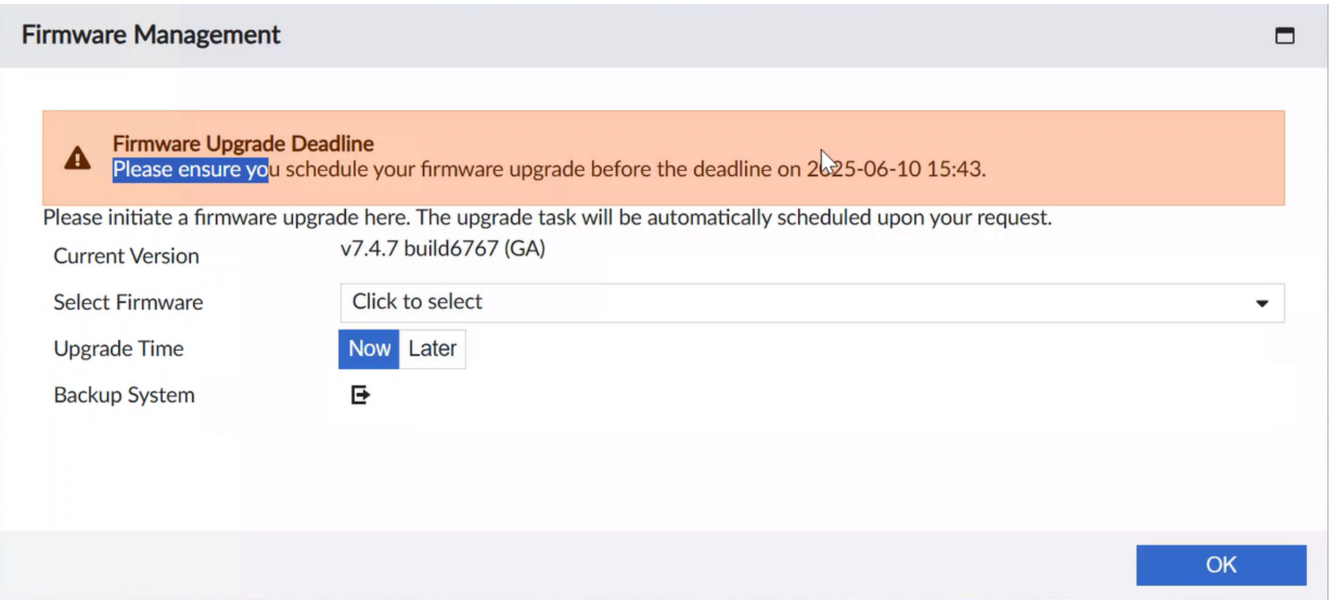
When upgrading FortiManager Cloud between major/minor versions, you must first upgrade to the latest patch release for the current version and any intermediate versions.

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.



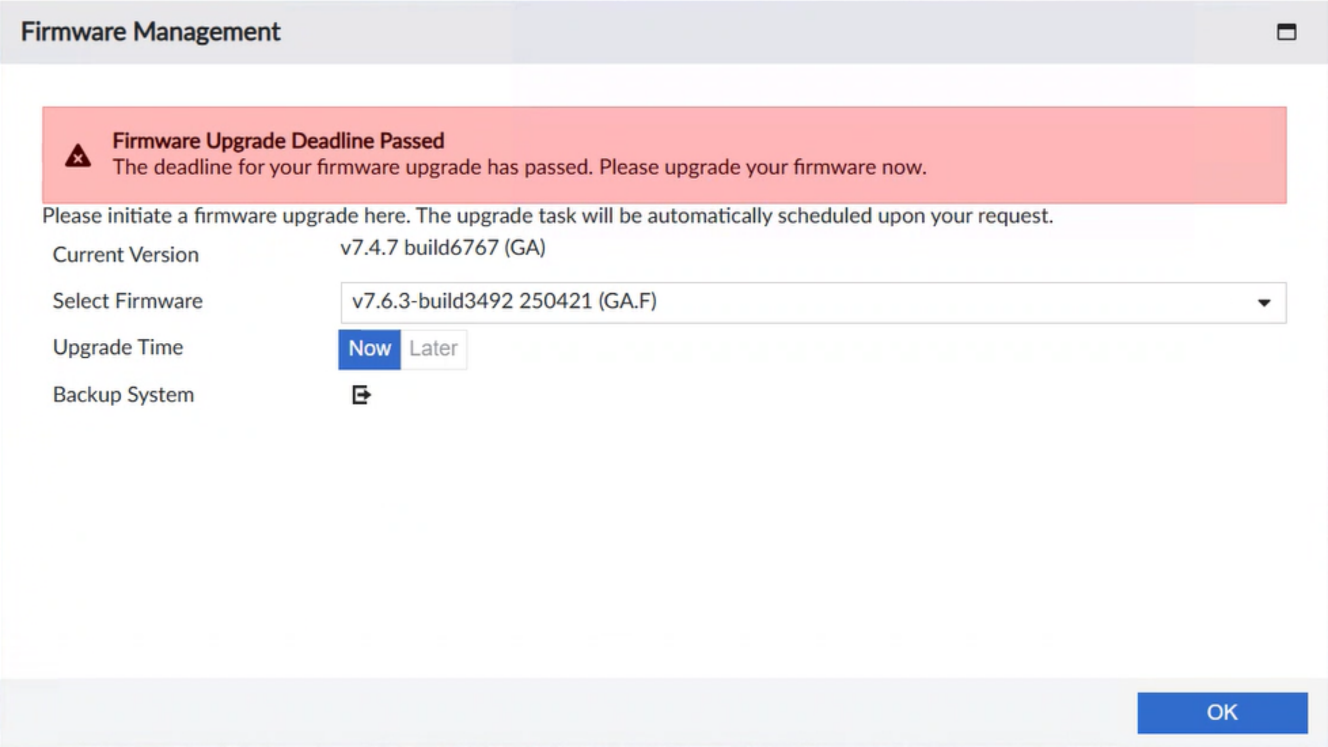
Firmware Management

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



Firmware Management

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.

FortiManager Cloud version support

FortiManager Cloud supports two major release versions.

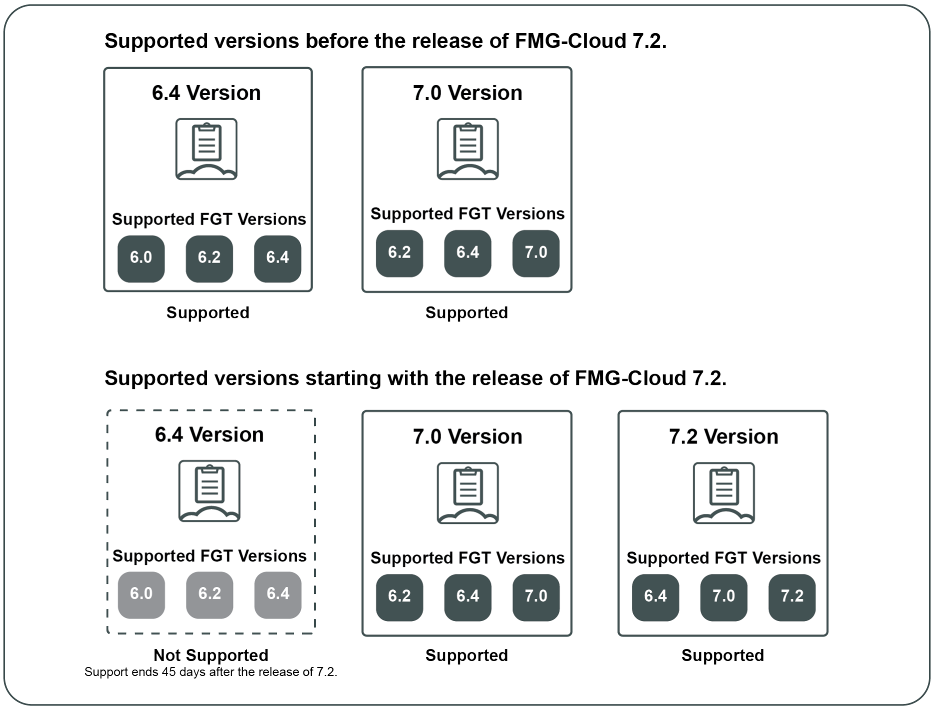
Each FortiManager Cloud major release version is able to manage FortiGate devices for its current version and the two previous versions. For example:

FMG-Cloud version	Managed FortiGate version
FortiManager Cloud 7.0	7.0, 6.4, and 6.2.
FortiManager Cloud 7.2	7.2, 7.0, and 6.4.

When a new major version is released, the lowest previously supported version becomes unsupported and will be phased out within 45 days. You can use this time to schedule an upgrade to a higher version.

With the release of FortiManager Cloud 7.2.1, the supported major versions are 7.2 and 7.0. FortiManager Cloud 6.4 is no longer supported.

The image below shows the supported FortiManager Cloud major release versions before and after the release of FortiManager Cloud 7.2.1, as well the FortiGate versions that can be managed.

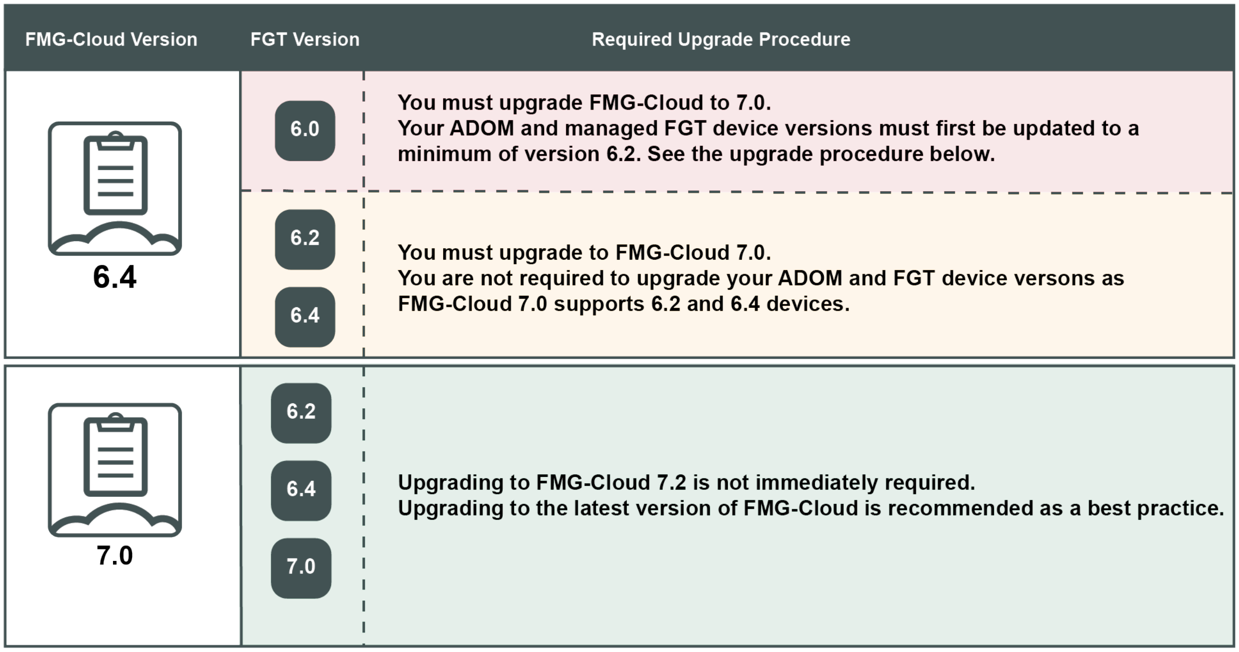


Upgrading from FortiManager Cloud 6.4

Customers using FortiManager Cloud 6.4 must update their version to 7.0 or 7.2 within 45 days.

Depending on the managed FortiGate devices' current version, you may be required to upgrade the FortiManager Cloud ADOM and FortiGate device's version as part of the upgrade process.

See the table below to determine what action is required based on your FortiManager Cloud and FortiGate device version.



FMG-Cloud Version	FGT Version	Required Upgrade Procedure
6.4	6.0	You must upgrade FMG-Cloud to 7.0. Your ADOM and managed FGT device versions must first be updated to a minimum of version 6.2. See the upgrade procedure below.
	6.2 6.4	You must upgrade to FMG-Cloud 7.0. You are not required to upgrade your ADOM and FGT device versons as FMG-Cloud 7.0 supports 6.2 and 6.4 devices.
7.0	6.2 6.4 7.0	Upgrading to FMG-Cloud 7.2 is not immediately required. Upgrading to the latest version of FMG-Cloud is recommended as a best practice.

The following upgrade procedure explains the process of upgrading your FortiManager Cloud 6.4 version to 7.0 when you are managing FortiGate devices on version 6.0.x. For all other scenarios, please follow the standard upgrade instructions: Upgrade information on page 7

To upgrade FortiManager Cloud 6.4 with managed FOS 6.0 devices:

1. Upgrade your FortiOS device version from 6.0 to 6.2.
2. Upgrade your ADOM version in FortiManager Cloud from 6.0 to 6.2.
   For more information, see the *Updating the ADOM version* in the FortiManager Cloud Deployment guide.
3. Upgrade FortiManager Cloud instance from 6.4 to 7.0.
   See Upgrade information on page 7 for more information on how to upgrade your FortiManager Cloud version using the cloud portal.
4. Optionally, you can choose to further upgrade your device and ADOM version as needed.
   For example if you wish to upgrade to FortiManager Cloud 7.2.1, you must first upgrade your device and ADOM version to a minimum of 6.4.

Product integration and support

FortiManager Cloud version 7.2.11 supports the following items:

- Web browser support on page 13
- FortiOS support on page 13
- FortiGate model support on page 13
- Language support on page 14
- Outbound connectivity from FortiManager Cloud on page 14

Web browser support

FortiManager Cloud version 7.2.11 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 7.2.11 supports the following FortiOS versions:

- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 to 6.4.10

For the complete list of supported FortiOS versions including versions with compatibility issues, see the FortiManager Release Notes.

FortiGate model support

FortiManager Cloud version 7.2.11 supports the same FortiGate models as FortiManager 7.2.11. FortiGate models must be on FortiOS 6.4.4 or later.

For a list of supported FortiGate models, see the *FortiManager 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)	✓	✓
Japanese	✓	✓
Korean	✓	✓
Spanish	✓	✓

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 FortiManager Cloud version 7.2.11. To inquire about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
1000101	FortiManager Cloud fails to retrieve certificates that were directly imported into the FortiGate. As a result, FortiManager Cloud repeatedly attempts to push a CSR, leading to installation status conflicts.
1119280	Firmware Template assignment does not work properly.
1122481	When a 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.

Others

Bug ID	Description
1114809	After upgrading the FMG using the "Upgrade Image via FortiGuard" feature, the FortiManager JSON API login may fail, leading to service disruptions. This issue is important for FortiPortal and other FortiManager API clients.

Policy and Objects

Bug ID	Description
1073463	Installation is failed with error, "VIP entry cannot be moved when central-nat is disabled."
1101436	The "sni-server-cert-check" cannot be disabled on SSL-SSH inspection profile for "ftps" "pop3s" and "smtps".
1113129	FortiManager is treating implicit-deny local-in policy incorrectly, denying any traffic.

Services

Bug ID	Description
1104925	FortiManager Cloud in Cascade mode may fail to display accurate license information/contracts for FortiGate retrieved from the FDS server, as it is not listed in the FortiGate authlist.

VPN Manager

Bug ID	Description
1084696	If users reopen the IPsec Tunnel template and close it without making any changes, FortiManager Cloudmight still display the following error message in the install log: "Error: VPN IPsec phase1-interface psksecret...Minimum psksecret length is 6..."

Known Issues

Known issues are organized into the following categories:

- New known issues on page 17
- Existing known issues on page 17

To inquire about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

New known issues

There are no new issues identified in 7.2.11.

Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.2.11.

AP Manager

Bug ID	Description
1010632	Floor Map shows wrong AP status and does not show the rest of APs when adding a new AP.

Device Manager

Bug ID	Description
894948	FortiManager Cloud fails to push the FortiAnalyzer override settings to the FortiGate.
980362	The Firmware Version column in *Device Manager* incorrectly shows 'Upgrading FortiGate from V1 to V2' even after a successful upgrade has been completed.
1004220	The SD-WAN Overlay template creates route-map names that exceed the 35-character limit.

Others

Bug ID	Description
703585	FortiManager may return 'Connection aborted' error with JSON API request.
968647	On the *Log View* (when FortiAnalyzer is added to FortiManager Cloud) changing time filters, first request always fails but second one is successful. **Workaround:** Use FortiAnalyzer *Log View* to view logs.

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`

1029677	Unable to upgrade ADOM from v6.4 to v7.0 due to global scope error in webfilter profile. **Workaround:** Rename the "g-default" to "g-test" and save. It can be deleted after that. Once ADOM upgraded, new g-default is created.
1052341	Not able to select Address type MAC in SD-WAN rule source address.
1093040	SD-WAN template import failed when meta variable has the default value set.
1142559	When attempting to upload the firmware image from FortiGuard, FortiManager 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.

Policy & Objects

Bug ID	Description
845022	SDN Connector failed to import objects from VMware VSphere.
967271	Installation failed when trying to remove firewall internet-service-name objects.
971065	When the number of Custom Internet Services exceeds 256, installation fails due to

Bug ID	Description
	this limitation.
1029921	Under the "Web Application Firewall" security profiles, users are unable to disable the signatures via GUI.
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).
1054707	FortiManager Cloud tries to install "unset qos-policy" and installation fails.
1131041	Not able to create ZTNA Server due to the certificate error.

VPN Manager

Bug ID	Description
784385	If policy changes are made directly on the FortiGates, the subsequent policy package import creates faulty dynamic mappings for *VPN Manager*. **Workaround:** It is strongly recommended to create a fresh backup of the FortiManager Cloud configuration prior to the workaround. Perform the following command to check & repair the FortiManager Cloud configuration database. `diagnose cdb check policy-packages <adom>` After running this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.
1042701	The traffic view page for the full mesh does not display the FortiGate and the external gateway.

Limitations of FortiManager Cloud

This section lists the features currently unavailable in FortiManager Cloud.

Feature	Feature available?	Details
Device Manager	Yes	• Add Device: ◦ Cannot discover a new device, but can add a model device. ◦ Does not support Azure vWan FortiGate network virtual appliances (NVAs). • 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.
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	
FortiGuard	Not applicable	• FortiManager Cloud does not provide the FortiGuard update service because managed devices can update directly from FortiGuard Cloud.
FortiSwitch Manager	Yes	
Fabric View	Yes	
System Settings	Yes	• License Information: License Information widget unavailable. • 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: Profile option is unavailable. • ADOM: ◦ 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.

Feature	Feature available?	Details
		- 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