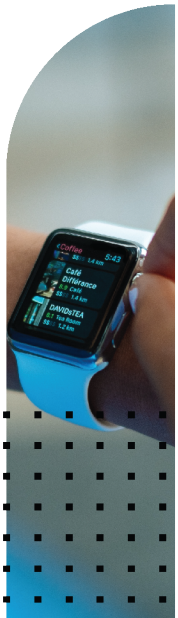
Release Notes

FortiManager Cloud 7.2.8 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

September 19, 2022
FortiManager Cloud 7.2.8 R1 Release Notes
02-721-843127-20220919

TABLE OF CONTENTS

Change log

Date	Change Description
2024-10-18	Initial release.
2024-11-08	Updated Known Issues on page 14.
2024-12-12	Initial release of 7.2.8 R1.
2024-12-24	Updated Limitations of FortiManager Cloud on page 18.
2025-01-16	Updated Resolved issues on page 13.

FortiManager Cloud 7.2.8 R1 release

This document provides information about FortiManager Cloud version 7.2.8 R1 build 6018.

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 7.2.8 R1.

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.

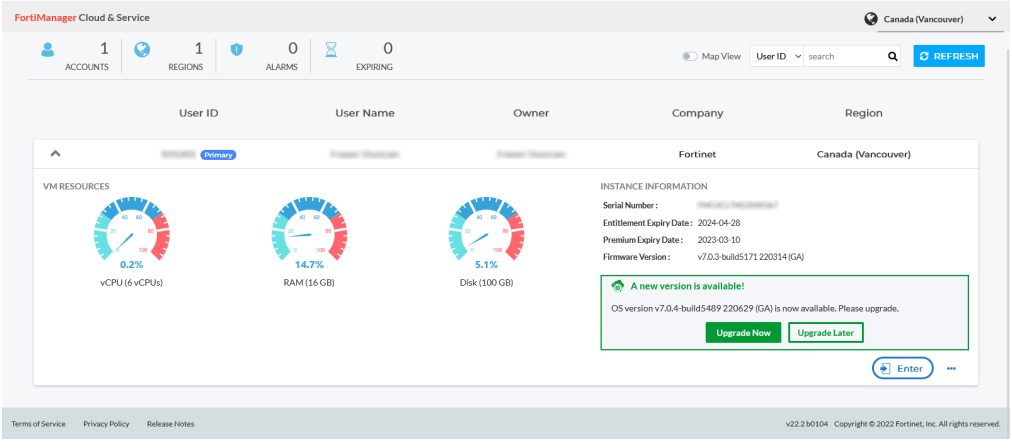
Primary users can upgrade FortiManager Cloud firmware to 7.2.8 R1 by using the FortiManager Cloud & Service portal. Secondary users can upgrade FortiManager Cloud firmware to 7.2.8 R1 by entering the instance and going to the *System Settings* module.

For FortiManager Cloud deployments on 7.2, you have two weeks to upgrade the FortiManager Cloud firmware to 7.2.8 R1 after it is released. If you take no action, you can no longer access FortiManager Cloud. The *Enter* button is grayed out until you upgrade to the required firmware.

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 portal:

1. Go to FortiCloud (https://support.fortinet.com/), and use your FortiCloud account credentials to log in.
   The FortiCloud portal is displayed.
2. From the *Services* menu, select *FortiManager Cloud* under *Cloud Management*.
   The FortiManager Cloud & Service portal is displayed. An alert icon appears next your account when a new version of firmware is available.
3. Expand your account.
4. Click *Upgrade Now* to update the firmware immediately, or click *Upgrade Later* to schedule upgrade of the firmware for a later date.



The *Upgrade Later* option is only available for two weeks after the firmware is released.

5. Click *OK*.
6. Click *Enter* to open FortiManager Cloud.

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.

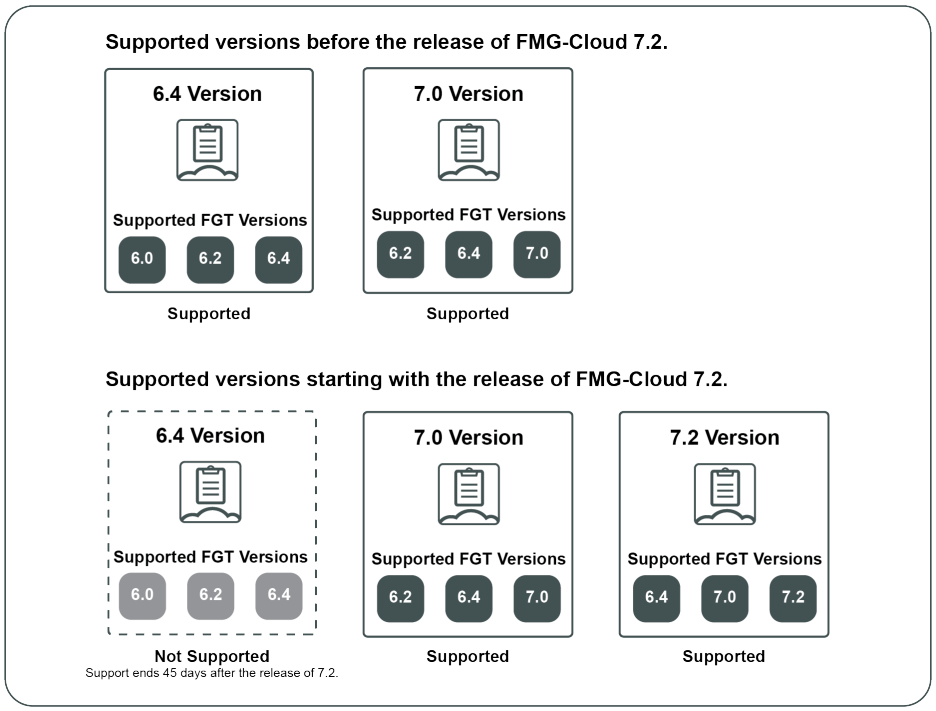
Each FortiManager Cloud major release version is able to manage FortiGate devices for its current version and the two previous versions. For example:

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 7.2.8 R1 supports the following items:

Web browser support

FortiManager Cloud version 7.2.8 R1 supports the following web browsers:

- Microsoft Edge version 110.0.1587.57 (64-bit)
- Mozilla Firefox version 110 (64-bit)
- Google Chrome version 110.0.5481.104 (64-bit)

FortiOS support

FortiManager Cloud version 7.2.8 R1 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 7.2.8 R1 supports the same FortiGate models as FortiManager 7.2.8 R1. 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*.

Resolved issues

The following issues have been fixed in FortiManager Cloud version 7.2.8 R1. To inquire about a particular bug, please contact Customer Service & Support.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1086790	FortiManager Cloud 7.2.8 R1 is no longer vulnerable to the following CVE Reference: • CVE-2024-47575
1102080	FortiManager Cloud 7.2.8 R1 is no longer vulnerable to the following CVE Reference: • CVE-2024-50566

Known Issues

Known issues are organized into the following categories:

- New known issues on page 14
- Existing known issues on page 14

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 7.2.8 R1.

Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.2.8 R1.

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.
1040365	FortiManager Cloud is generating false vulnerability reports for certain FortiAPs: • U431F • U231F
1076200	Policy install fails due to FortiManager Cloud installs unexpected changes related to "<wifi_ intf> address". **Workaround**: Create a CLI template with all subnet addresses and assign to device.
1081136	FortiManager Cloud is trying to delete and create ssid interface subnet address after upgrade.
1082873	FortiManager Cloud keeps creating and deleting the VAP interface address with every install.
1083312	Unable to remove Address Object Matching Subnet of SSID interface.

Device Manager

Bug ID	Description
894948	FortiManager Cloud fails to push the FortiAnalyzer override settings to the FortiGate.
973365	FortiManager Cloud does not display the IP addresses of FortiGate interfaces configured with DHCP addressing mode. **Workaround**: Disable Addressing Mode from DHCP to Manual in FortiManager Cloud Device DB, then Retrieve from FortiGate and IP will be updated successfully.
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.
1024552	SD-WAN Monitor (Map View) and Network Monitor SD-WAN (on device DB) keep loading indefinitely.
1030685	Unable to export metadata variables if the metadata's per-device-mapping value is empty.
1062545	When using the backslash "\" in the preshared key of IPSEC settings, the install may fail.
1063835	FortiManager Cloud ZTP installation to FortiGate versions 7.2.8 and lower may fail due to differing default "`ssh-kex-algo`" settings between FortiManager Cloud and FortiGate.
1070943	Unable to upgrade the devices via Device Group Upgrade Firmware feature. **Workaround**: Upgrade devices individually by using the "Device Firmware Upgrade" feature or Create New Firmware Template for single devices or device groups and use the "Assign to Devices/Groups" feature.

Others

Bug ID	Description
703585	FortiManager Cloud may return 'Connection aborted' error with JSON API request.
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. **Workaround**: Disabling the disk check on fmupdate before the upgrade.

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"`

Bug ID	Description
	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" > save. It can be deleted after that. Once ADOM upgraded, new g-default is created.

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 this limitation.
1004929	FortiManager Cloud removes the Web Filter Profile from the Profile Group for Policy-Based FortiGates. **Workaround**: Use individual profiles in the policy instead of the profile group.
1005161	The policy package status changes for all devices even when an address object is opened and saved without any modifications. This issue is particularly observed in objects utilizing the per-device mapping feature.
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).
1037861	ADOM versions (7.0 & 7.2) do nothave "ie-allow-list" option available to create GTP object.
1076659	When policy package configured with policy block, installation to 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.
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".

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.

System Settings

Bug ID	Description
825319	FortiManager Cloud fails to promote a FortiGate HA member (running on firmware 7.2.0 to 7.2.4) to the Primary.

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's configuration prior to the workaround. Perform the following command to check & repair the FortiManager Cloud's configuration database. `diagnose cdb check policy-packages <adom>` After running this command, FortiManager Cloud 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.
		• 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