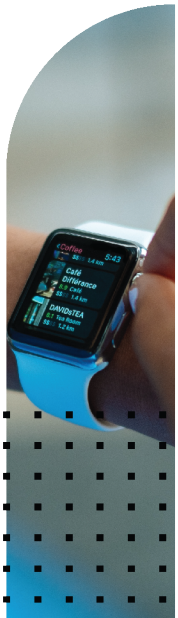
Release Notes

FortiManager Cloud 7.2.10



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 19, 2022
FortiManager Cloud 7.2.10 Release Notes
02-721-843127-20220919

TABLE OF CONTENTS

Change log

Date	Change Description
2025-03-06	Initial release.
2025-03-10	Updated Resolved issues on page 13.
2025-10-14	Updated Resolved issues on page 13

FortiManager Cloud 7.2.10 release

This document provides information about FortiManager Cloud version 7.2.10 build 6359.

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 7.2.10.

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 7.2.10 by using the FortiManager Cloud & Service portal. Secondary users can upgrade FortiManager Cloud firmware to 7.2.10 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.

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.

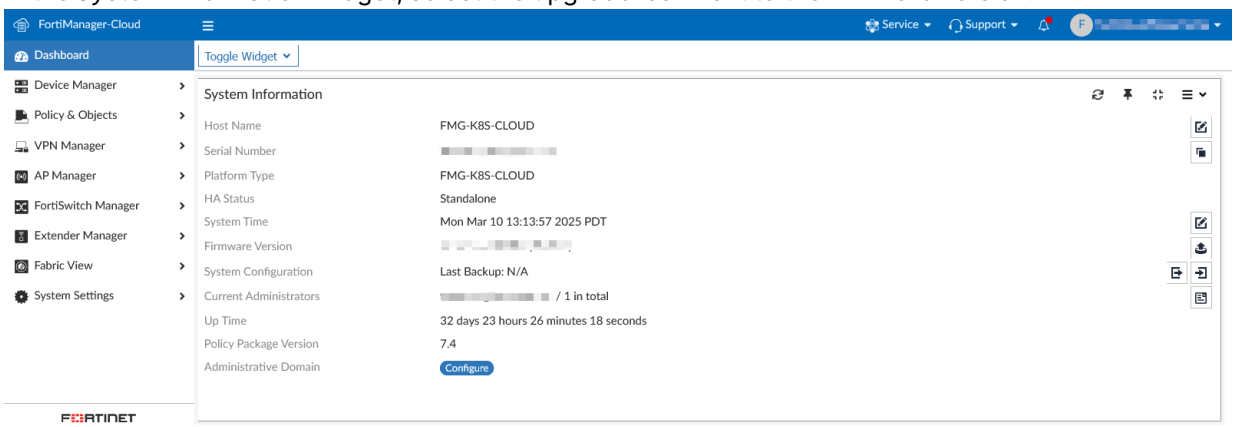
   

   The *Later* option for *Upgrade Time* is only available for one week after the firmware is released.
4. Click *OK* to perform or schedule the upgrade.

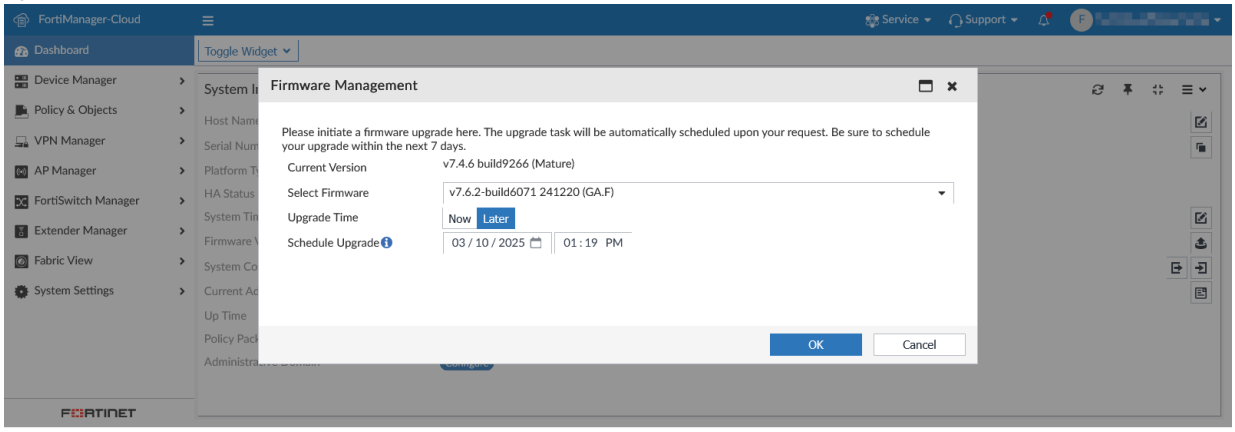
To upgrade FortiManager Cloud firmware:

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.

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.

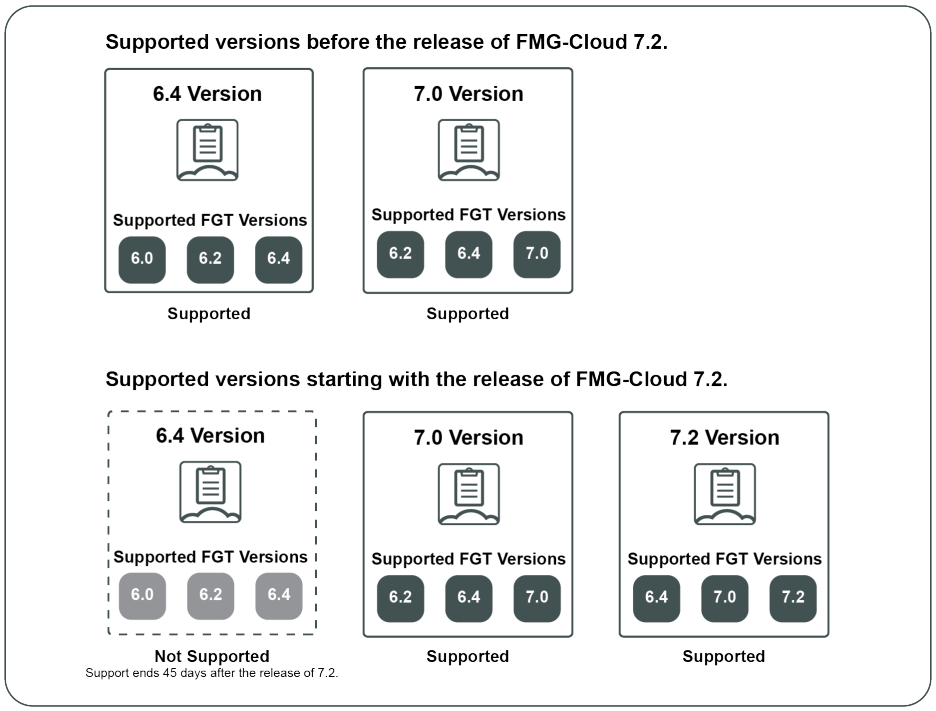
Each FortiManager Cloud major release version is able to manage FortiGate devices for its current version and the two previous versions. For example:

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.

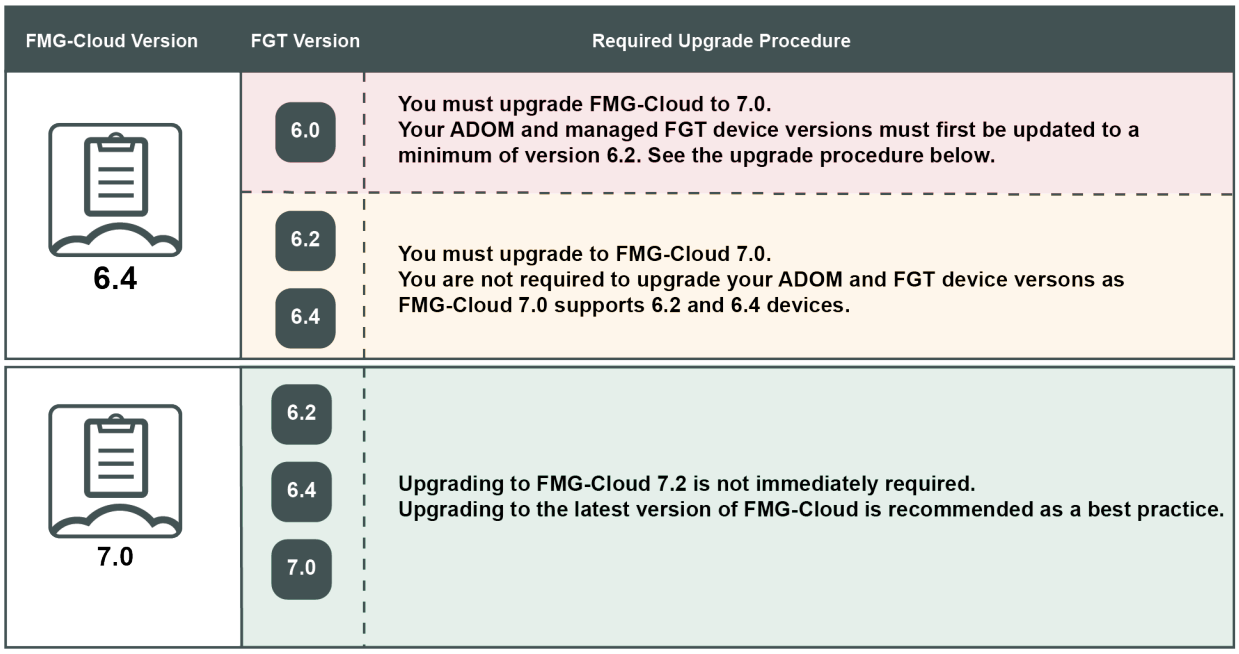


Upgrading from FortiManager Cloud 6.4

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.



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 7.2.10 supports the following items:

Web browser support

FortiManager Cloud version 7.2.10 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 7.2.10 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 7.2.10 supports the same FortiGate models as FortiManager 7.2.10. 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 7.2.10. To inquire about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
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".

Device Manager

Bug ID	Description
973365	FortiManager Cloud does not display the IP addresses of FortiGate interfaces configured with DHCP addressing mode.
1015138	Unable to edit interface with dhcp reservation.
1030685	Unable to export metadata variables if the metadata's per-device-mapping value is empty.
1050126	Setting up a FortiGate-HA with ZTP fails because the FortiLink is not deleted during the "HA config pushed to FGT" process.
1051889	When downloading the FortiGate config through *Device Manager > Managed Devices > Device Configuration DB*, the downloaded file contains line breaks in middle of commands, which prevents it to be installed on FortiGate.
1053194	If the "`system interface speed`" attribute is changed from the FortiManager Cloud, it may potentially cause an installation failure. Modifying the "`system interface speed`" 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".

Bug ID	Description
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.
1063850	FortiManager Cloud is attempting to install a "PRIVATE KEY" with every installation, even after retrieving the config.
1067706	Metadata variables cannot be used in the firewall address objects.
1070943	Unable to upgrade the devices via Device Group Upgrade Firmware feature.
1074717	An error might be observed when the SD-WAN template health check name contains a space, displaying the following message: "Bad health check name...".
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.

FortiSwitch Manager

Bug ID	Description
1061315	Device DB FortiLink config changes when authorizing or deauthorizing FortiSwitch from either *FortiSwitch Manager* or local FortiGate.

Others

Bug ID	Description
998198	When upgrading ADOM, the upgrade process fails with the following error: "invalid value - can not find import template 'XYZ' ".
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.
1020787	ZTP Enforce firmware Version doesn't upgrade the secondary cluster member.
1058185	FortiProxy policies not imported if the policies have either internet service or IPv6 used in the source or destination.
1078947	Repeatedly testing the URL rating on FortiManager Cloud (`diagnose fmupdate test fgd-url-rating`...) may cause the "fgdsvr daemon" to crash.
1081941	When UTM-Profile gets added to a FortiProxy policy FortiManager Cloud generates invalid config.

Policy and Objects

Bug ID	Description
958923	Installing policy packages that utilize an SSL/SSH Inspection profile may fail with the error message "Server certificate replace mode cannot support category exempt."
978136	Occasionally, installation may fail due to an error message, "Waiting for another session", which prevents policies from being installed from FortiManager Cloud. During this issue, the following message may also appear: "Blocked by session id(XYZ) username(n/a)". This issue may be caused by a signal loss between the child and parent security console processes, leading the parent process to continue waiting for a copy result.
983591	In the Firewall section, when attempting to add a note to the policy, the comment window shifts towards the left corner.
991720	FortiManager Cloud still has an option to enable the "match-vip" through the policy package for "allow" policies. However, this is not supported anymore on the FortiGates.
1004929	FortiManager Cloud removes the Web Filter Profile from the Profile Group for Policy-Based FortiGates.
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.
1008413	FortiManager Cloud fails to load IPS signatures in the profile. This may only occur when the number of signatures listed in the profile is larger than 80.
1014025 1087922	While attempting to access the Application Signatures list on FortiManager Cloud, an error message: "a.foreach is not a function" might be displayed.
1029787	The Firewall Policy pane in the FortiManager Cloud GUI may occasionally display both "Standard Security Profiles" (SSL no-inspection and protocol default profiles) and "Security Profile Groups" simultaneously.
1046002	Policy Package status does not display "unknown" status immediately following retrieve.
1055795	During device import via multiple CSV files at same time, some devices were imported successfully, while others encountered errors and had missing metadata variables. Additionally, FortiManager Cloud forced the admin to log out. When attempting to log back in, the following error message appeared: "ADOM not found".
1068736	Best Quality SDWAN rules installation may fail with the following error message: "Commit failed: Bad health check name".
1069285	Using TAB button while creating firewall address object creates error Invalid IP address.
1071226	Policy Lookup is not showing result as highlighted when the sections are not expended.

Bug ID	Description
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.
1079037	The "`internet-service-id`" 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.
1082548	Address type FQDN is missing DNS resolve domain name function feature.

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. InternalNotes: ---------- - The case apparently has been reproduced by ""Olivier Brunori, 2024-06-27 00:47"".
1085374	FortiManager Cloud does not support exporting the TCL scripts via CLI.

Services

Bug ID	Description
1034102	Unable to upgrade FortiGates from FortiManager Cloud due to a "no valid FMWR license" error, despite the FortiGates being licensed. This issue is reported when the "FMG Authorization table" on the FDS server is empty.
1060509	When updating query service packages from the global anycast server (globalupdate.fortinet.net), larger-sized IoTS 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.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1020280	FortiManager Cloud 7.2.10 is no longer vulnerable to the following CVE Reference: • CVE-2024-33504
1103779	FortiManager Cloud 7.2.10 is no longer vulnerable to the following CVE Reference: • CVE-2024-50571

Known Issues

Known issues are organized into the following categories:

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 7.2.10.

Others

Bug ID	Description
1093040	SDWAN template import failed when meta variable has the default value set.

Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.2.10.

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 Cloud may return 'Connection aborted' error with JSON API request.

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

Policy & Objects

Bug ID	Description
971065	When the number of Custom Internet Services exceeds 256, installation fails due to this limitation.

Bug ID	Description
967271	Installation failed when trying to remove firewall internet-service-name objects.
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).
845022	SDN Connector failed to import objects from VMware VSphere.

VPN Manager

Bug ID	Description
784385	If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for VPN manager. **Workaround**: It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to the workaround. Perform the following command to check & repair the FortiManager's 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.

The FortiManager Cloud portal does not support IAM user groups.

www.fortinet.com