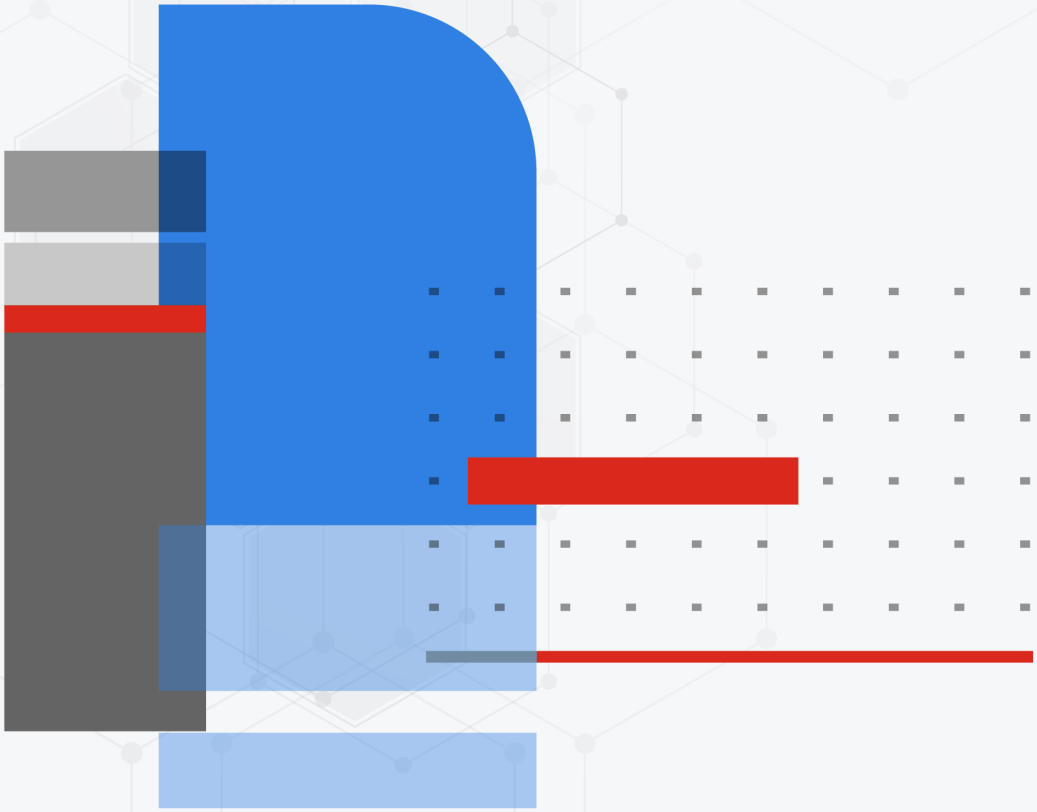
Release Notes

FortiManager Cloud 7.6.5



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

January 15, 2026
FortiManager Cloud 7.6.5 Release Notes
02-765-1237032-20260115

TABLE OF CONTENTS

Change log **4**
FortiManager Cloud 7.6.5 release **5**
Special Notices **6**
FortiAI for FortiManager Cloud 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 11
Language support 11
Outbound connectivity from FortiManager Cloud 11
Resolved issues **12**
AP Manager 12
Device Manager 12
FortiSwitch Manager 13
Global ADOM 13
Others 13
Policy and Objects 14
System Settings 15
Known issues **16**
New known issues 16
Existing known issues 16
AP Manager 16
Device Manager 16
Others 17
Policy and Objects 18
System Settings 18
Limitations of FortiManager Cloud **19**

Change log

Date	Change Description
2025-12-15	Initial release.
2026-01-15	Updated Limitations of FortiManager Cloud on page 19.

FortiManager Cloud 7.6.5 release

This document provides information about FortiManager Cloud version 7.6.5 build 3653.

The recommended minimum screen resolution for the FortiManager Cloud GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.6.5.

There are no special notices for this release.

FortiAI for FortiManager Cloud

FortiManager Cloud supports FortiAi with the following licenses:

- FC1-10-MVCLD-1118-01-DD: Support FortiAI for instances managing 10 devices/vdoms
- FC2-10-MVCLD-1118-01-DD: Support FortiAI for instances managing 100 devices/vdoms
- FC3-10-MVCLD-1118-01-DD: Support FortiAI for instances managing 1000 devices/vdoms

Upgrade information

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

Administrators can perform firmware upgrades from within the FortiManager Cloud *Dashboard* or notification drawer.

An administrator with *Super_User* permissions is required to perform the upgrade.

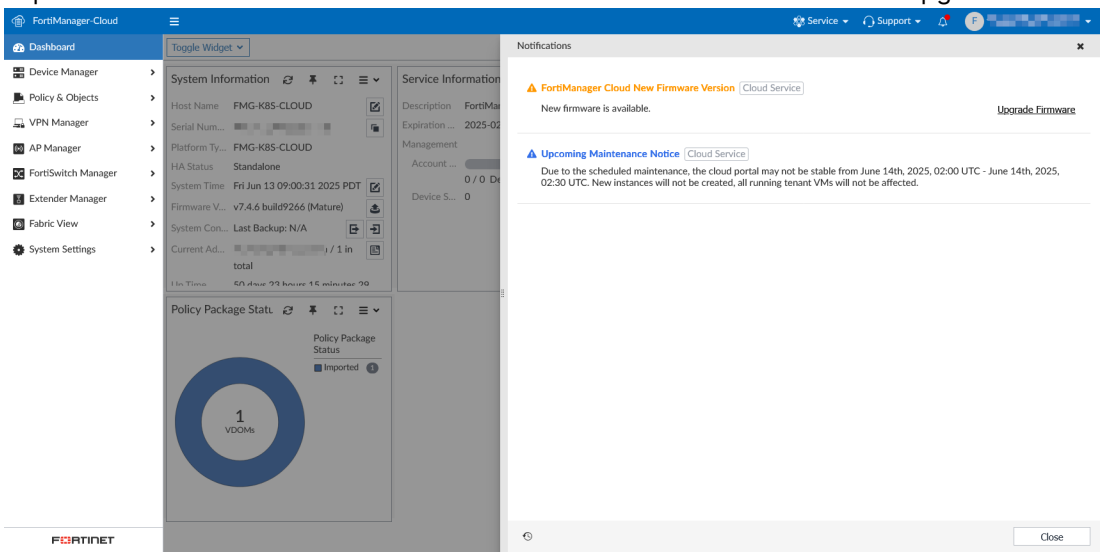
To keep FortiManager Cloud secure and up to date, it is recommended that you upgrade your 7.6 release to the latest release build.

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

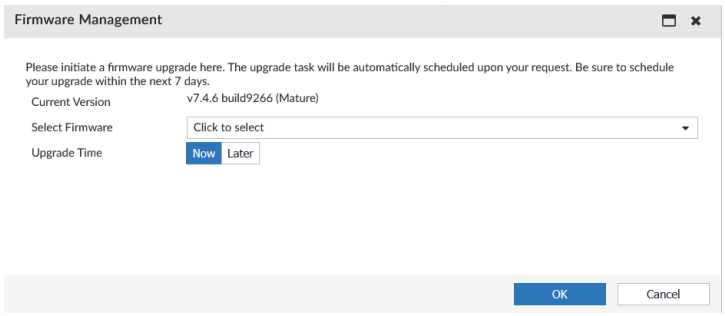
FortiManager Cloud supports FortiOS versions 7.6, 7.4, and 7.2. You must upgrade all managed FortiGates to FortiOS version 7.2 or later.

To upgrade firmware from the notification drawer:

1. Go to FortiManager Cloud (https://fortimanager.forticloud.com/), and use your FortiCloud account credentials to log in. An administrator with *Super_User* permissions is required to perform the upgrade.
2. Expand the notification drawer to view information about available firmware upgrades.



3. Click *Upgrade Firmware* to update the firmware immediately or to schedule upgrade of the firmware for a later date.



4. Click *OK* to perform or schedule the upgrade.

To upgrade firmware from the Dashboard:

1. Log in to your FortiManager Cloud instance.
2. Go to *Dashboard* in the tree menu.
3. In the *System Information* widget, select the upgrade icon next to the firmware version.
   The *Firmware Management* dialog appears. The current firmware version is displayed along with upgrade options.
4. In the *Select Firmware* field, choose an available firmware version.
5. In the *Upgrade Time* choose *Now* or *Later*.
   - *Now*: Begin the upgrade immediately.
   - *Later*: Schedule the upgrade for a later time.
6. Click *OK*. The upgrade will be completed based on the selected options.

FortiManager Cloud upgrade path

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

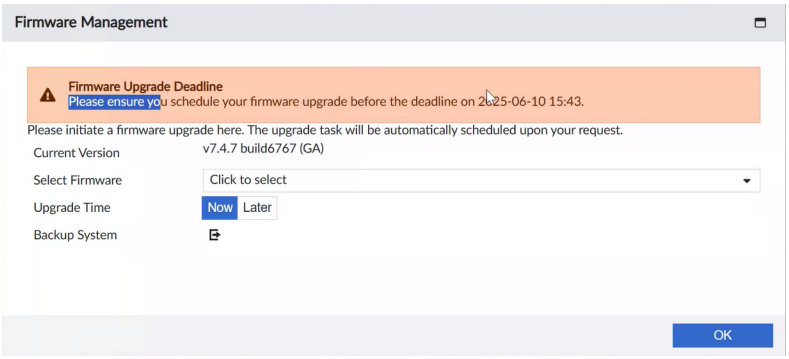
For example, in order to upgrade FortiManager Cloud from version 7.2.x to 7.6.x, you must first upgrade to the latest 7.2 patch version, followed by the latest 7.4 patch version, before finally upgrading to the target 7.6.x release.

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

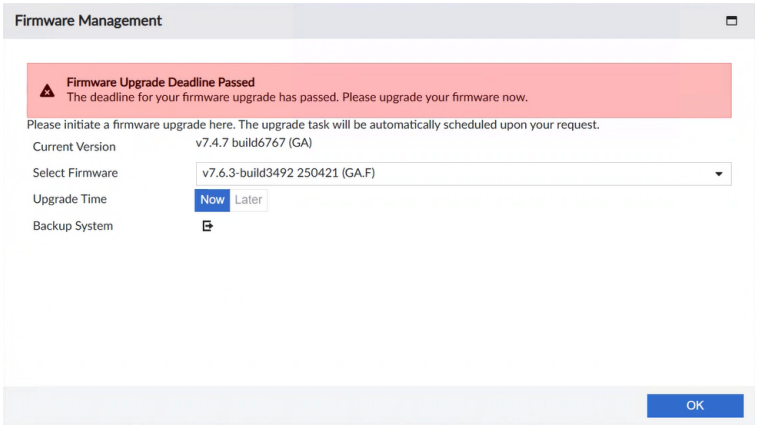
Mandatory upgrades

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

version. You can choose to upgrade immediately or schedule the upgrade for a later time. This dialog cannot be bypassed.



After the deadline has passed, you can still connect to your instance's GUI to see the *Firmware Management* dialog window, however, you will only have the option to upgrade immediately. This dialog cannot be bypassed and you will not be able to access your instance until the upgrade is completed.



Downgrading to previous firmware versions

Downgrade to previous versions of FortiManager Cloud firmware is not supported.

Product integration and support

FortiManager Cloud version 7.6.5 supports the following items:

- Web browser support on page 10
- FortiOS support on page 10
- FortiGate model support on page 11
- Language support on page 11
- Outbound connectivity from FortiManager Cloud on page 11

Web browser support

FortiManager Cloud version 7.6.5 supports the following web browsers:

- Microsoft Edge 114
- Mozilla Firefox version 96
- Google Chrome version 114

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiManager Cloud version 7.6.5 supports the following FortiOS versions:

- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

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

FortiGate model support

FortiManager Cloud version 7.6.5 supports the same FortiGate models as FortiManager 7.6.5.

For a list of supported FortiGate models, see the *FortiManager 7.6.5 Release Notes* on the Document Library.

Language support

The following table lists FortiManager Cloud language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French	✓	✓
Japanese	✓	✓
Korean	✓	✓
Spanish	✓	✓
Portuguese		✓

To change the FortiManager Cloud language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Outbound connectivity from FortiManager Cloud

FortiManager Cloud supports initiating outbound traffic to supported external services such as public cloud connectors (for example, AWS, Azure) and on-premises systems (for example, Cisco ISE) when these endpoints are reachable over the public Internet.

For more information, see External Connectors in the FortiManager Administration Guide.

Resolved issues

The following issues have been fixed in 7.6.5. To inquire about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
1173274	FortiManager is trying to enable ddscan when it is not enabled on ADOM db, device db, and AP Manager profile.
1174004	After FortiManager Cloud's upgrade, FortiManager may suggest to "`set ddscan enable`" during the first installation, and this may create some issue on FortiAPs connected to the FortiGate.
1178251	FortiManager is attempting to unset the auth-cert on the wireless-controller VAP during every installation.
1198357	*AP Manager* encounters issues with central AP management because some channels may not be supported.
1204035	FAP-231K is not supported by FortiManager.

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.
1102790	FortiManager pushes the `unset auto-connect` command to `config system lte-modem`, where the default value is disabled on FortiOS but still enabled on FortiManager.
1152287	HA group-id not inherited from CSV file or from pre-run script.
1155534	An error occurs when disabling the IP Range Managed by IPAM option on the VLAN interface.
1173182	CLI Template Installation Fails with error message "SSID rename not allowed".
1176785	Getting error while importing certificate 'no write permission to do this operation'.
1188313	The Device Asset Identity Center displays an incorrect last-seen time, and the hardware information should remain consistent with the FortiGate.

Bug ID	Description
1198163	When installing an SD-WAN static route via a template, the push fails with a duplicated route error.
1201252	The static route template triggers duplicate-route errors during installation because duplicate routes, including those using blackhole interfaces, are not allowed.
1202695	FGT90G/91G Gen2 are not supported in Device Model.
1208974	Device count is not correct.
1215090	Unable to retrieve correct setting of device-identification in system interface.
1219062	"sla-compare-method" still available on SDWAN rules when load balance is enabled.

FortiSwitch Manager

Bug ID	Description
1193285	When changing the name of a FortiSwitch from *FortiSwitch Manager*, the next Installation will reset the ports configuration of the switch to default configuration.

Global ADOM

Bug ID	Description
1182076	Renamed global objects are not reflected with their new names in associated policies.
1183101	Not able to delete firewall objects from the global database after upgrading FortiManager from 7.2 (7.2.10) to 7.4 (7.4.7).

Others

Bug ID	Description
1077126	The FortiExtender API connection status is returning incorrect value for the FortiExtender device when in an "unknown" state.
1099773	FortiExtender Page 'Data Usage' value does not display the updated values.
1146320	After creating the SSID and assigning it to the FortiExtender profile, the configuration is not

Bug ID	Description
	pushing to the FortiGate, resulting in an installation failure.
1158842	The FortiManager Cloud dashboard FortiGuard license status does not display the same data as shown on the FortiGuard page.
1177268	FortiFirewall License Validation fails on FortiManager configured as Local FDS.
1199504	When Workspace is in Workflow mode, the fmg-admin may observe "You have no write permission to do this operation" error message when attempting to modify an interface.
1201751	Unable to add managed FortiAnalyzer to FortiManager Cloud.
1211261	Users might experience "Attempting to reconnect" messages every few minutes while logged in to the GUI.
1217951	FortiManager Cloud may not recognize the 1000F serial number as valid for applying the corresponding Device Blueprint, preventing the CSV file from being loaded.
1224258	The new EMS version (7.4.5) has upgraded its communication protocol from HTTP/1.0 to HTTP/2. Unlike HTTP/1.x, HTTP/2 does not return a traditional 200 OK text response, so older FortiManager Cloud versions that expect this format cannot interpret the new HTTP/2 replies. Because of this, older FortiManager Cloud builds will not be compatible with the latest EMS version.

Policy and Objects

Bug ID	Description
1083504	FortiManager Cloud attempts to configure the service in the ISDB6 policy (IPv6), but FortiOS rejects it, causing the installation to fail.
1139663	When using the Install Object(s) function after renaming an object, FortiManager pushes the old object name to the firewall policy.
1156437	No interface mapping listed when importing config for a device (device mapping undefined).
1169058	Installation might fail to these devices "FGT/FWF-30G/31G" due to some unsupported syntax.
1170381	Unable to create new section "*Add Section*" in policy after upgrading FortiManager Cloud while using interface pair view mode. Operation "*Add Section*" triggers nothing. Field "`label`" or "`global-label`" are empty.
1174618	After importing the policies and objects from the FortiGate, even though the FortiManager Cloud settings were selected, the configuration status for all FortiGates changed to Modified.
1181585	"Where Used" feature does not function.
1185738	During the auto-linking process, FortiManager Cloud attempts to push a policy package

Bug ID	Description
	containing Internet-Service based rules, but the FortiGates outdated ISDB causes the installation to fail.
1196308	EMS server security posture tags are not fully synchronized with FortiManager Cloud; ZTNA tags comment are missing.
1198075	Upon any modification, policy installation will result in attempt to purge dns-database even though no changes are made to dns database.
1211860	Existing Objects shown as "Not found" in "Where Used".
1212118	Reinstalling policy packages for more than three devices may cause the Application Security Console to crash.
1215309	Installation hang when pushing configurations to firewall groups.
1215349	FortiManager may delete policies or settings during device installation due to concurrent database interactions from tasks like auto-updates, policy installs, or HA-related updates running simultaneously.
1218648	The Alternative Resources setting under AWS connector is not pushed to FortiGate.

System Settings

Bug ID	Description
1086386	Unable to save changes for SNMP users in FortiManager Cloud if more than one notification host is configured.

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 7.6.5.

Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.6.5.

AP Manager

Bug ID	Description
1086946	The FortiAP upgrade via FortiManager may fail (on FortiGate 7.6.1). The process could stop at the controller_download_image step or experience a prolonged stall, eventually resulting in a timeout.

Device Manager

Bug ID	Description
980362	The *Firmware Version* column in *Device Manager* incorrectly shows 'Upgrading FortiGate from V1 to V2' even after a successful upgrade has been completed.
1028515	The Greenwich time zone on FortiGate is not supported on the FortiManager Cloud.
1112389	*FortiView* and *Log View* fail to display logs when FortiAnalyzer is configured as a managed device in FortiManager.

Bug ID	Description
1136080	Starting from version 7.2.11, FortiGate devices use a different password type for the administrator's password field. FortiManager versions released before this change cannot verify the administrator password when installing to a FortiGate, which may result in an installation failure.
1136726	Enabling the Power Supply Failure option in an SNMP v2 configuration applied via a System Template results in the following installation error: "multi-option(power-blade-down) not exist".

Others

Bug ID	Description
1203535	FortiManager Cloud does not support the `diagnose fdsm fap-fsw-contract-download` request, so the fgdhttpd daemon rejects FortiGate attempts to retrieve FortiAP/FortiSwitch registration status.

1217534	During an upgrade of a FortiGate-HA cluster via FortiManager Cloud, if the disk-check feature is enabled, it may cause all cluster members to reboot simultaneously. This can result in an unexpected traffic interruption.
	Workaround:
	To prevent this issue, disable the disk check before performing the upgrade:
	`config fmupdate fwm-setting`
	`  set check-fgt-disk disable`
	`end`

1196043	Failed to create *Event Handlers* or *Reports* on FortiManager when a Fortinet Fabric Connection is established on FortiAnalyzer to connect to the FortiManager device. **Workaround**: Go back to the specific ADOM on FortiAnalyzer and create the *Event Handlers* or *Reports* there. After synchronization, the new entries should become available on FortiManager.
1149980	FortiManager attempts to install a config to FortiProxy may result in the removal of physical ports. This can occur randomly and originates from the FortiProxy side, due to syntax support compatibility issues. A fix is planned for the next FortiProxy release.
1230277	If the ADOM in an earlier FortiManager Cloud version contains DLP dictionary entries named `fg-*`, which are reserved in FortiManager Cloud 7.6, the upgrade from ADOM 7.4 to 7.6 will fail. The upgrade process attempts to copy these reserved-name objects, but ADOM 7.6 does not allow them to be created or modified.
1126662	In an FortiGate HA setup running on the public cloud platform, the FortiManager attempts to install changes on static routes, which may cause routes to be deleted after an HA failover.
1185269	The local log syslog feature `set facility` is not functioning properly.
1081121	The syslog server is unable to receive FortiManager event logs when the reliable option is

Bug ID	Description
	enabled.
1105387	The upgrade task failed when the FortiManager attempted to send the image to the FortiGates. The image file transfer between FortiManager and FortiGate appeared to fail over the FGFM tunnel. FortiManager timed out and was unable to retrieve the FortiGate version (first observed in FortiGate version 7.6.1). **Workaround**: Enable option "Let Device Download Firmware From FortiGuard" in FortiManager side.
1143100	Unable to add physical FortiProxy to FortiManager.

Policy and Objects

Bug ID	Description
1101351	Unable to create ZTNA Server with SAML SSO Server.
1160047	Application control category "GenAI" is missing in FortiManager, but present in FortiGate. **Workaround**: Copy a FortiGate application list (Applist) from the CLI that includes Category 36, and insert it into a CLI template in FortiManager. Assign CLI template to FortiGate.
1171027	NAT64 policy and CNAT cannot be created or modified in FortiManager Cloud.
1189177	The FortiManager configuration attempted to change the order of custom service objects, but this returned an "Unknown action 0" error.
1200063	Failed to update EMS tags from EMS cloud server on FortiManager v7.6.x.
1209756	Policy package installation fails for FGT-30G due to SSL VPN settings not supported by this FortiGate model.

System Settings

Bug ID	Description
1158131	The GUI permits configuring the management port to a port number already in use, resulting in loss of access to the GUI.

Limitations of FortiManager Cloud

This section lists the features currently unavailable in FortiManager Cloud.

Feature	Feature available?	Details of limitations and unsupported features
Dashboard	Yes	• *System Resources*, *Unit Operation*, *Alert Message Console*, and *FortiGuard License Status* widgets are unavailable. • The *Service Information* widget replaces the *License Information* widget.
Device Manager	Yes	• Add Device: • Cannot discover a new device, but can add a model device. • 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. • Remote access to managed FortiGate: Remote FortiGate GUI access is not supported by FortiManager Cloud. Remote access to FortiGate using SSH is supported.
Policy & Objects	Yes	• Because Fortinet cannot host LDAP servers for customers, FortiManager Cloud can only connect to a remote LDAP server on the Internet. You can use NAT with a VIP.
AP Manager	Yes	
VPN Manager	Yes	
Fabric View	Yes	
FortiGuard	Not applicable	• FortiManager Cloud does not provide the FortiGuard update service because managed devices can update directly from FortiGuard Cloud.
FortiSwitch Manager	Yes	
System Settings	Yes	• License Information: Available with FortiManager Cloud entitlement information only. • Administrator: The FortiCloud user ID is the administrator's user name. Additional administrators cannot be added directly from FortiManager Cloud. • Trusted Hosts: Not supported. • Create Clone: Create Clone option is unavailable. • Profile: Available for configuring profiles for Cloud IAM users with custom permissions to FortiManager Cloud. • ADOM:

Feature	Feature available?	Details of limitations and unsupported features
		• ADOMs cannot be created. • Advanced ADOM mode is not supported. • Enabling FortiAnalyzer: FortiAnalyzer Features cannot be enabled from FortiManager Cloud. • Remote Authentication Server: Remote Authentication Server is unavailable. • SAML SSO: SAML SSO unavailable. • HA: HA unavailable. • SNMP monitoring tool is not supported. • Fabric Management: Fabric Management is not supported on FortiManager Cloud. • Pre-login banners are not supported.

The FortiManager Cloud portal does not support IAM user groups.

www.fortinet.com