



# Release Notes

FortiManager Cloud 7.4.8



**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](mailto:techdoc@fortinet.com)



September 19, 2022

FortiManager Cloud 7.4.8 Release Notes

02-721-843127-20220919

# TABLE OF CONTENTS

<b>Change log</b> .....	<b>4</b>
<b>FortiManager Cloud 7.4.8 release</b> .....	<b>5</b>
<b>Special Notices</b> .....	<b>6</b>
Device database enters an incorrect state .....	6
<b>Upgrade information</b> .....	<b>7</b>
FortiManager Cloud upgrade path .....	8
Mandatory upgrades .....	8
Downgrading to previous firmware versions .....	9
<b>Product integration and support</b> .....	<b>10</b>
Web browser support .....	10
FortiOS support .....	10
FortiGate model support .....	10
Language support .....	11
Outbound connectivity from FortiManager Cloud .....	11
<b>Resolved issues</b> .....	<b>12</b>
AP Manager .....	12
Device Manager .....	12
FortiSwitch Manager .....	13
Global ADOM .....	13
Others .....	13
Policy and Objects .....	14
Services .....	15
System Settings .....	15
VPN Manager .....	15
<b>Known issues</b> .....	<b>16</b>
New known issues .....	16
AP Manager .....	16
Others .....	16
Policy and Objects .....	16
Existing known issues .....	17
AP Manager .....	17
Device Manager .....	17
Others .....	18
Policy and Objects .....	18
Services .....	19
<b>Limitations of FortiManager Cloud</b> .....	<b>20</b>

# Change log

Date	Change Description
2025-10-14	Initial release of FortiManager Cloud 7.4.8.
2026-01-02	Updated <a href="#">Special Notices</a> on page 6.
2026-01-15	Updated <a href="#">Limitations of FortiManager Cloud</a> on page 20.

# FortiManager Cloud 7.4.8 release

This document provides information about FortiManager Cloud version 7.4.8 build 6113.

---



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 7.4.8.

## Device database enters an incorrect state

The device database in FortiManager Cloud 7.4.8 may enter into an incorrect state. When this occurs, the following symptoms may be observed:

- Copy errors for valid objects during the install process, such as "datasrc invalid. detail: copy datasrc failed, attr [attribute\_name] value[object\_name]".
- Integrity check failures when running "diagnose pm2 check-integrity device".
- Unexpected configuration loss during the *Install Device Settings* operation. Some configuration elements may be deleted, such as firewall policies.

The following workaround is available. If you continue to experience issues, please contact Fortinet Support.

### **Workaround:**

- Run integrity check "diagnose pm2 check-integrity device" and identify device with error.
- Retrieve config from device to fix the error.

# Upgrade information

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

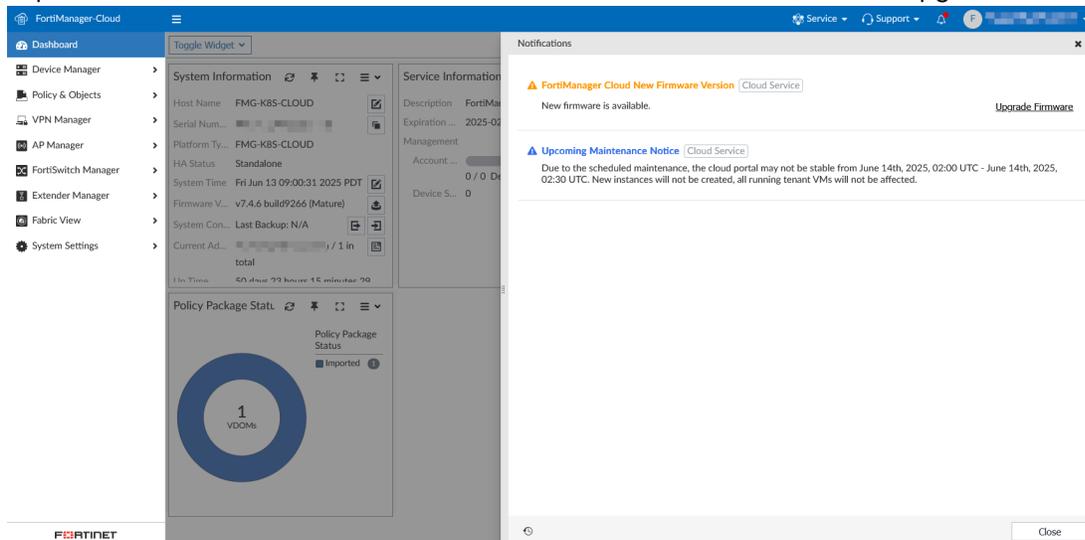
An email will be sent to notify you when an upgrade is mandatory. After receiving the notification, you will have 14 days to complete the upgrade. See [Mandatory upgrades on page 8](#)



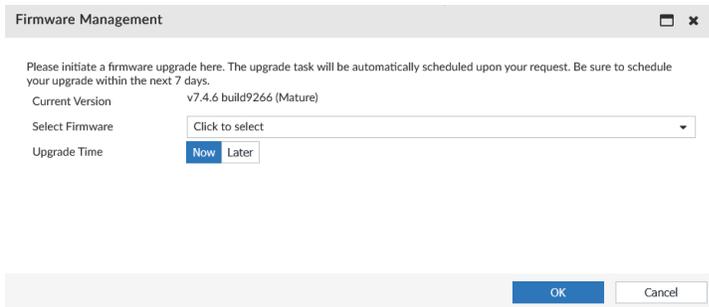
FortiManager Cloud supports FortiOS versions 7.4, 7.2, and 7.0. You must upgrade all managed FortiGates to FortiOS version 7.0 or later.

## 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.

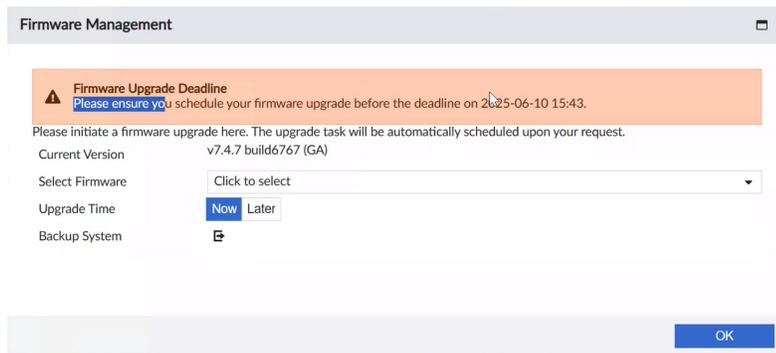
For example, in order to upgrade FortiManager Cloud from version 7.2.x to 7.6.x, you must first upgrade to the latest 7.2 patch version, followed by the latest 7.4 patch version, before finally upgrading to the target 7.6.x release.

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

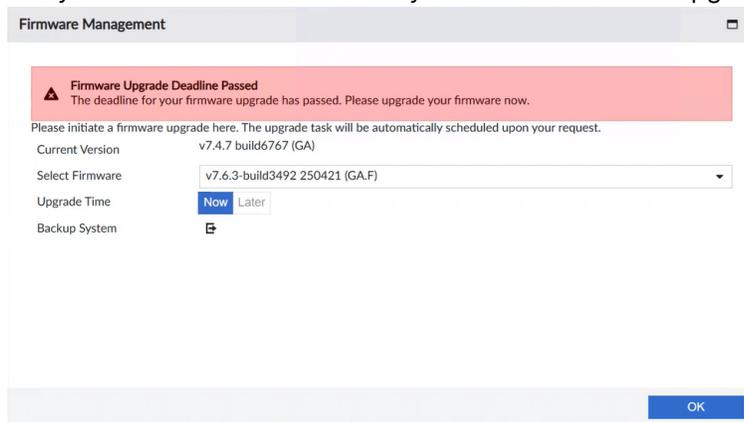
When a firmware upgrade is mandatory, a *Firmware Management* dialog window will appear when you access your instance. This dialog provides details about the upgrade deadline and options for upgrading your firmware

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



The screenshot shows a 'Firmware Management' dialog window. At the top, there is a warning banner with a triangle icon and the text 'Firmware Upgrade Deadline'. Below the banner, it says 'Please ensure you schedule your firmware upgrade before the deadline on 2025-06-10 15:43.' Below this, there is a message: 'Please initiate a firmware upgrade here. The upgrade task will be automatically scheduled upon your request.' The dialog contains several fields: 'Current Version' is 'v7.4.7 build6767 (GA)'; 'Select Firmware' is a dropdown menu with 'Click to select'; 'Upgrade Time' has two buttons, 'Now' and 'Later'; and 'Backup System' has a checkbox. An 'OK' button is at the bottom right.

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.



The screenshot shows the same 'Firmware Management' dialog window, but the warning banner is now red and says 'Firmware Upgrade Deadline Passed'. Below the banner, it says 'The deadline for your firmware upgrade has passed. Please upgrade your firmware now.' The rest of the dialog is the same as in the previous screenshot, but the 'Upgrade Time' buttons are now 'Now' and 'Later', with 'Now' being the selected option.

## Downgrading to previous firmware versions

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

# Product integration and support

FortiManager Cloud version 7.4.8 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](#)
- [Outbound connectivity from FortiManager Cloud on page 11](#)

## Web browser support

FortiManager Cloud version 7.4.8 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 7.4.8 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 7.4.8 supports the same FortiGate models as FortiManager 7.4.8.

For a list of supported FortiGate models, see the [FortiManager 7.4.8 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 7.4.8. To inquire about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
1148572	SSID Per-device-mapping cannot save the dhcp server settings.
1173274	FortiManager Cloud is trying to enable ddscan when it is not enabled on ADOM db, device db, and AP Manager profile
1174004	After FortiManager Cloud upgrade to 7.4.7, FortiManager Cloud may suggest to "set ddscan enable" during the first installation, and this may create some issue on FortiAPs connected to the FortiGate.
1178251	FortiManager Cloud is attempting to unset the auth-cert on the wireless-controller VAP during every installation.

## Device Manager

Bug ID	Description
1094451	If the Timezone field in the System Template is left blank, FortiManager Cloud may apply its default timezone and overwrite the existing timezone on the FortiGates.
1102790	FortiManager Cloud pushes the unset auto-connect command to config system lte-modem, where the default value is disabled on FortiOS but still enabled on FortiManager Cloud.
1119223	FortiManager Cloud erroneously tries to "unset annex" on DSL interface on the FortiGate "FGT-50G-DLS".
1152287	HA group-id not inherited from CSV file or from pre-run script.
1166830	FortiGates may be unexpectedly renamed during policy package installation when deploying to multiple devices (more than 5).
1167436	FortiManager Cloud displays "retrievehaconfail" error when performing retrieve config for FortiGate HA cluster.

Bug ID	Description
1167958 1175207	After upgrading FortiManager to version 7.4.7, /var may fill up with temporary files. This is most likely to happen with high device count (>100) or heavy use of thread feeds. Possible symptoms include FGFM tunnels to FortiGates not coming up or GUI not functioning correctly. The likelihood of /var filling up increases the longer FortiManager runs on 7.4.7
1173182	CLI Template Installation Fails with error message "SSID rename not allowed".

## FortiSwitch Manager

Bug ID	Description
1161320	FortiManager Cloud shows an incomplete FortiSwitch Topology compared with FortiGate.

## Global ADOM

Bug ID	Description
1141123	Installing the Global Header Policy fails with the error: "invalid value", this issue has been observed after upgrading fmg to v7.2.10.
1183101	Not able to delete firewall objects from the global database after upgrading fmg from 7.2 (7.2.10) to 7.4 (7.4.7).

## Others

Bug ID	Description
1071646	Formatted Event logs do not display the correct timestamp.
1145473	Upgrading ADOM fails with FortiExtender object errors "Fail (errno=0):invalid value" and "fail: err=-999,The string contains XSS vulnerability characters".
1162845	It is not possible to delete the FortiExtender after performing a Quick Install on the model FortiGate. The FortiExtender can be deleted from Device Manager > Managed FortiGate > CLI Configuration; however, it will still appear in FortiExtender Manager.
1163922	The <i>FortiView</i> tile is missing after adding FortiAnalyzer as a managed device to FortiManager Cloud.

Bug ID	Description
1165254	In both AP Manager and FortiSwitch Manager, the Enforce Firmware Version option does not display the correct data.
1168422	FortiManager Cloud does not properly support the "FortiGate-50G-SFP-POE" platform.
1170281	Not able to create a new VDOM or remove any interfaces from VDOMs when Workspace mode is enabled.
1177051	"retrievehaconffail" error has been observed when performing retrieve config on the FortiManager Cloud GUI.
1188452	Downstream FortiManager Clouds in cascade mode does not download the Webfilter database from the Upstream FortiManager Cloud.

## Policy and Objects

Bug ID	Description
971065	When the number of Custom Internet Services exceeds 256, installation fails due to this limitation.
1011220	FortiManager Cloud constantly changes the UUID of some objects.
1054707	FortiManager Cloud try to install "unset qos-policy" and installation fails.
1078598	Unable to import policy due to issues related to the protocol-options feature.
1087777	During policy installation, FortiManager Cloud tries to delete firewall address object for the SSID interface UUID causing policy package Modifying.
1131041	Not able to create ZTNA Server due to the certificate error.
1142983	In FortiManager, 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.
1152640	When no port setting (empty value) has been set for HTTPS on SSL/SSH Inspection Profile, the installation preview shows error, "https ... Must set at least one port (default port:443) or enable ssl inspect-all".
1157272	When creating a new entry under the Logical Relationship for a DLP dictionary, the Pattern field must be completed only for the applicable entry types; it should remain blank for those that do not require it.
1162327 1113980	Install preview may get stuck if another user is simultaneously pushing an install on a different FortiGate within FortiManager.
1167035	Installation to FortiGates with multiple VDOMs might fail with the following error message: "max entry. object: firewall internet-service-custom. detail: global limit. solution: limit is 512"

Bug ID	Description
1169058	Installation might fail to these devices "FGT/FWF-30G/31G" due to some unsupported syntax.
1171386	Install failure might be observed when pushing proxy-based antivirus profile to FortiGate models FGT-40F and FGT-60F.
1173197	Where Used feature is not working for objects that contain a forward slash (/).
1181585	"Where Used" feature does not function.
1198075	Upon any modification, policy installation will result in attempt to purge dns-database even though no changes are made to dns database.

## Services

Bug ID	Description
1170893	When FortiManager Cloud is acting as Local FortiGaurd Servers, FortiClient applications running on Linux machines are not receiving any signature updates.

## System Settings

Bug ID	Description
1169081	When clicking on the "Approve this request" link in the Workflow mode, following error message can be observed. "Unable to complete action, failed to 'approve'."

## VPN Manager

Bug ID	Description
1166323	The <i>VPN Manager &gt; IPsec VPN Communities</i> page no longer displays correctly the page loads but shows only a blank (white) screen.

# 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

The following issues have been identified in version 7.4.8.

### AP Manager

Bug ID	Description
1204035	FAP-231K is not supported by FortiManager.

### Others

Bug ID	Description
1217534	<p>During an upgrade of an 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.</p> <p><b>Workaround:</b></p> <p>To prevent this issue, disable the disk check before performing the upgrade:</p> <pre>config fmupdate fwm-setting   set check-fgt-disk disable end</pre>

### Policy and Objects

Bug ID	Description
1212118	Reinstalling policy packages for more than three devices may cause the Application Security Console to crash.

Bug ID	Description
	<p><b>Workaround:</b></p> <ul style="list-style-type: none"> <li>• Just select to install two device at the same time.</li> <li>• Use normal installation process, instead of Re-Install.</li> </ul>
1215349	<p>FortiManager 7.4.8 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.</p> <p><b>Workaround:</b></p> <p>Consider using policy package installations instead of device installations whenever possible. It is recommended to use Installation Preview before committing any changes to FortiGates. If you observe any unexpected actions, run an Integrity Check. If the issue is confirmed, retrieve the device configuration before proceeding.</p>
1217455	<p>FortiManager Cloud is not able to retrieve "usergroup" from "Cisco 3.3 Path7 Pxgrid" using FortiManager Cloud connector.</p> <p><b>Workaround:</b></p> <p>Add the appropriate DNS entry under <i>System Settings &gt; Network</i>.</p>

## Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.4.8.

### AP Manager

Bug ID	Description
1032762	<p>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.</p>

### Device Manager

Bug ID	Description
974925	<p>The NTP Server setting may not display the correct configuration. This issue might occur on managed devices running FortiOS version lower than 7.4.2.</p> <p><b>Workaround:</b></p> <p>Edit NTP server setting under CLI configuration.</p>

Bug ID	Description
980362	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.
1112389	<i>FortiView</i> and <i>Log View</i> fail to display logs when FortiAnalyzer is configured as a managed device in FortiManager Cloud.

## Others

Bug ID	Description
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><b>Workaround:</b></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>
1126662	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.

## Policy and Objects

Bug ID	Description
845022	SDN Connector failed to import objects from VMware vSphere.
1160047	<p>Application control category "GenAI" is missing in FortiManager, but present in FortiGate.</p> <p><b>Workaround:</b></p> <p>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.</p>
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.
1199272	Imported certificate does not show details.

## Services

Bug ID	Description
1167362	Despite having the "fgfm-deny-unknown" setting enabled, unauthorized devices might still be appearing in the <i>Device Manager</i> .

# 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"> <li>• <i>System Resources, Unit Operation, Alert Message Console, and FortiGuard License Status</i> widgets are unavailable.</li> <li>• The <i>Service Information</i> widget replaces the <i>License Information</i> widget.</li> </ul>
Device Manager	Yes	<ul style="list-style-type: none"> <li>• Add Device: <ul style="list-style-type: none"> <li>• Cannot discover a new device, but can add a model device.</li> </ul> </li> <li>• Add FortiAnalyzer: Cannot add a managed FortiAnalyzer device.</li> <li>• Devices &amp; 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.</li> <li>• Remote access to managed FortiGate: Remote FortiGate GUI access is not supported by FortiManager Cloud. Remote access to FortiGate using SSH is supported.</li> </ul>
Policy & Objects	Yes	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
AP Manager	Yes	
VPN Manager	Yes	
Fabric View	Yes	
FortiGuard	Not applicable	<ul style="list-style-type: none"> <li>• FortiManager Cloud does not provide the FortiGuard update service because managed devices can update directly from FortiGuard Cloud.</li> </ul>
FortiSwitch Manager	Yes	
System Settings	Yes	<ul style="list-style-type: none"> <li>• License Information: Available with FortiManager Cloud entitlement information only.</li> <li>• Administrator: The FortiCloud user ID is the administrator's user name. Additional administrators cannot be added directly from FortiManager Cloud.</li> <li>• Trusted Hosts: Not supported.</li> <li>• Create Clone: Create Clone option is unavailable.</li> <li>• Profile: Available for configuring profiles for Cloud IAM users with custom permissions to FortiManager Cloud.</li> <li>• ADOM:</li> </ul>

Feature	Feature available?	Details of limitations and unsupported features
		<ul style="list-style-type: none"><li>• ADOMs cannot be created.</li><li>• Advanced ADOM mode is not supported.</li><li>• Enabling FortiAnalyzer: FortiAnalyzer Features cannot be enabled from FortiManager Cloud.</li><li>• Unit Operation: Unit Operation is unavailable.</li><li>• Remote Authentication Server: Remote Authentication Server is unavailable.</li><li>• SAML SSO: SAML SSO unavailable.</li><li>• HA: HA unavailable.</li><li>• SNMP monitoring tool is not supported.</li><li>• Pre-login banners are not supported.</li></ul>



The FortiManager Cloud portal does not support IAM user groups.

---



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2026 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.