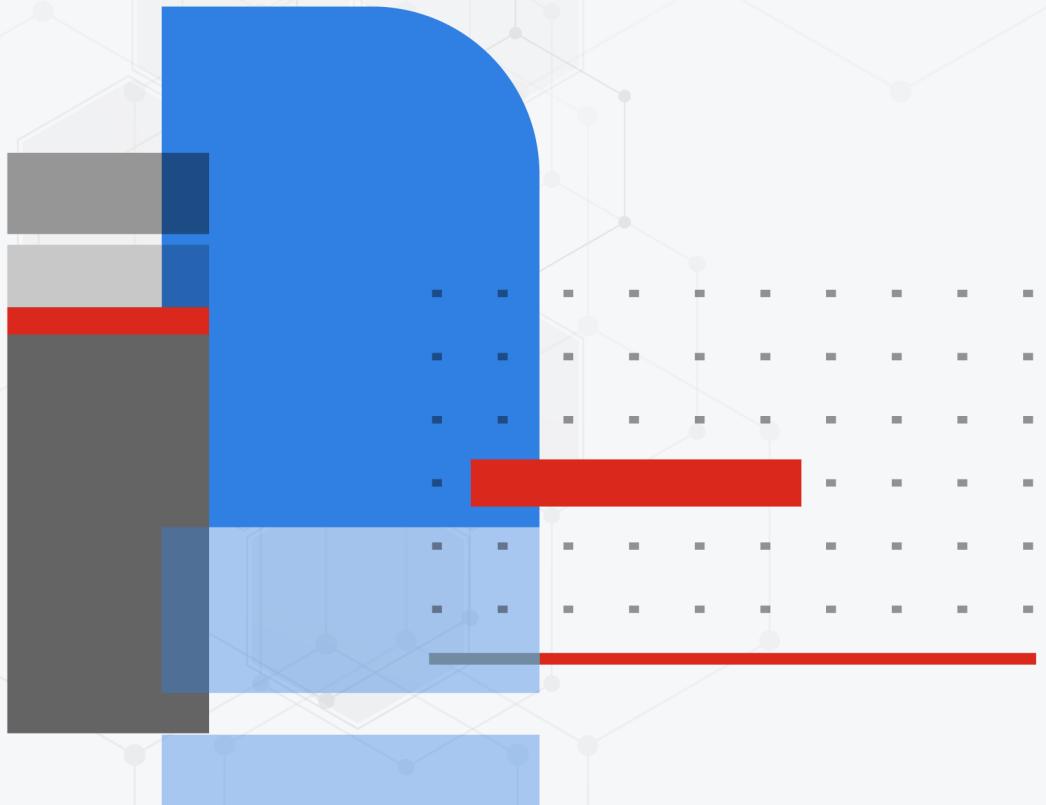




# Release Notes

FortiManager Cloud 7.6.2



**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)



July 8, 2025

FortiManager Cloud 7.6.2 Release Notes

02-762-1108600-20250708

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>FortiManager Cloud 7.6.2 release</b>	<b>5</b>
<b>Special Notices</b>	<b>6</b>
<b>Upgrade information</b>	<b>7</b>
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
<b>Resolved issues</b>	<b>12</b>
AP Manager	12
Device Manager	12
FortiSwitch Manager	13
Others	14
Policy and Objects	14
Script	16
System Settings	17
Common Vulnerabilities and Exposures	17
<b>Known issues</b>	<b>18</b>
New known issues	18
Existing known issues	18
AP Manager	18
Device Manager	18
Others	19
Policy & Objects	19
Script	20
<b>Limitations of FortiManager Cloud</b>	<b>21</b>

# Change log

Date	Change Description
2024-12-23	Initial release.
2024-12-24	Updated <a href="#">Limitations of FortiManager Cloud on page 21</a> .
2025-01-16	Updated <a href="#">Resolved issues on page 12</a> .
2025-02-25	Updated <a href="#">Limitations of FortiManager Cloud on page 21</a> .
2025-07-08	Updated <a href="#">Resolved issues on page 12</a> .

# FortiManager Cloud 7.6.2 release

This document provides information about FortiManager Cloud version 7.6.2 build 6070.



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 7.6.2.

There are no special notices for this release.

# 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.

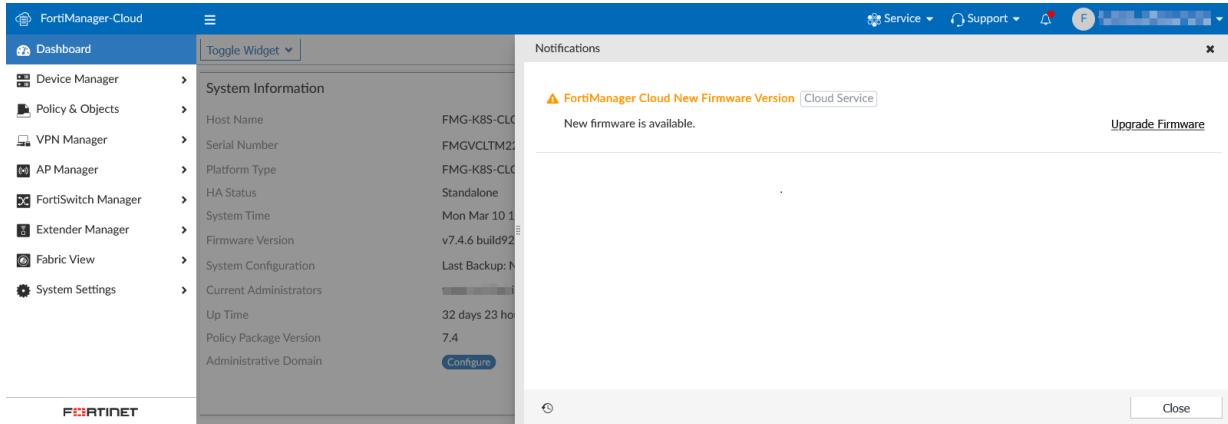
An email will be sent to notify you when an upgrade is mandatory. After receiving the notification, you will have 14 days to complete the upgrade.



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.

Alternatively, you can access firmware upgrade options from the FortiManager Cloud *Dashboard > System Information* widget.



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 from the System Information widget:

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.

# Product integration and support

FortiManager Cloud version 7.6.2 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](#)

## Web browser support

FortiManager Cloud version 7.6.2 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 7.6.2 supports the following FortiOS versions:

- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 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 7.6.2 supports the same FortiGate models as FortiManager 7.6.2.

For a list of supported FortiGate models, see the [FortiManager 7.6.2 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*.

# Resolved issues

The following issues have been fixed in 7.6.2. To inquire about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
955558	FortiManager Cloud unsets the Protected Management Frame (PMF) setting when the SSID security mode is configured to OWE-enabled in the AP Manager.
1040365	FortiManager Cloud is generating false vulnerability reports for certain FortiAPs: <ul style="list-style-type: none"><li>• U431F</li><li>• U231F</li></ul>
1041445	The AP attributes do not automatically update in the AP Manager.
1050466	The 802.11ax-5g AP profile is missing for all FAPs that support WiFi 6.
1060238	FortiManager Cloud is attempting to unset the FortiAP's name.
1076200	Policy install fails due to FortiManager Cloud installs unexpected changes related to "<wifi_intf> address".

## Device Manager

Bug ID	Description
796842	Failed to reload the configuration due to the "datasrc invalid" error message.
952422	IPsec templates created by SDWAN Overlay does not create tunnels for all the underlay interfaces.
963025	When using the static route template, the "SD-WAN Zone" does not appear under the Interface column.
1003899	FortiManager Cloud generates a VPN certificate that is not accepted by the FIPS-enabled FortiGate devices.
1020257	Packet Capture feature for managed FortiGates does not work; it starts but immediately stops.

## Resolved issues

---

Bug ID	Description
1034355	When assigning a provisioning template with Admin Settings configuration, FortiManager Cloud changes the hostname of the device.
1039591	The Link Status entries are blank under the Interfaces >>> Network.
1041440	Some FortiGate platforms (FGT-40F and FGT-60F) does not support the "ip-managed-by-fortiipam" and FortiGate refuses to take the configuration from FortiManager Cloud; hence users will be experiencing the install error.
1050126	Setting up a FortiGate-HA with ZTP fails because the FortiLink is not deleted during the "HA config pushed to FGT" process.
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".
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 configuration.
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.
1075747	SD-WAN Monitor does not display the members under the SD-WAN Rules (Map View or Table View). This issue is most likely to occur when "priority-zone" is configured.
1080414	CSV import fails to set metadata variables due to old header format ("name").
1099824	FortiManager may push the ICAP and WAF profile configurations to low-end FortiGate models that do not support these features, potentially causing installation failures.

## FortiSwitch Manager

Bug ID	Description
1040428	FortiSwitch diagnostics tools do not display the cable test diagnose results, device information on Ports, and update Registration status.
1053220	Unable to delete FortiSwitches when central management is enabled for FortiSwitch.

## Resolved issues

---

Bug ID	Description
1060242	Unable to change the FortiSwitch name from the <i>FortiSwitch Manager</i> .
1075021	Users with the "admin profile" rights cannot access the "FortiSwitch Manger".

## 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.
1015890	Unable to upgrade ADOM from v6.4 to v7.0 due to "switch-controller traffic-policy" error.
1055417	Unable to upgrade the firmware version of the FortiGates in HA cluster by using the firmware template when HA is in-sync status. The failure to upgrade FortiGate HA cluster firmware is caused by a crash in "dmserver" daemon.
1058185	FortiProxy policies not imported if the policies have either internet service or IPv6 used in the source or destination.
1062128	After upgrading to the latest available build, the FortiManager Cloud GUI displays the warning message: "A new firmware version is available".
1071064	Unable to upgrade the ADOMs.
1078947	Repeatedly testing the URL rating on FortiManager Cloud (diagnose fmupdate test fgd-url-rating...) may cause the "fgdsvr daemon" to crash.

## Policy and Objects

Bug ID	Description
843716	FortiManager Cloud tries to unset url-map for TCP forwarding ZTNA virtual server.
963536	The policy package feature "Export to Excel" is not functioning.
969923	The "View Mode" button, which is used to check the interface in Pair View, is missing in the Firewall Policy under Policy Packages.

Bug ID	Description
971610	FortiManager Cloud does not able to import the Central SNAT, DNAT, DOS, local-in, and traffic shaping policies.
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.
986256	When creating the application list on the FortiManager Cloud, if the Category ID is set to 33 or 34, the installation does not display any errors. However, these invalid categories cannot be set on the FortiGate. Consequently, the assigned application list entry will be created without a specific category and will default to the "block" action. This behavior may cause network interruptions.
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.
1004056	The installation may encounter an error related to Syntax support for the "ssh-enc-algo" command.
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.
1013948	After upgrading to FortiManager Cloud versions 7.2.5 or 7.4.3, the installation preview may hang. However, the installation process itself can be completed successfully.
1014035	Video filter profile config is not getting pushed completely from FortiManager Cloud to FortiGate.
1025012	Configuring the SSL/SSH inspection profile may result in the following error: "The server certificate replacement mode cannot support category exemptions."
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.
1029921	Under the "Web Application Firewall" security profiles, users are unable to disable the signatures through the GUI.
1039766	The Firewall Policy Lookup feature does not display the list of source interfaces for FortiGates.
1040160	When installing policy to a FortiGate that uses FortiSandbox inline scanning on an AV profile, FortiManager Cloud unsets the configuration on install.
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".

## Resolved issues

---

Bug ID	Description
1057228	Importing the SDN Objects, with multiple tags, will addmultiple entries listed as SDN objects; when clients add anything into the filters section ,browser immediately redirects to an error page showing: " Oops! Sorry, an unexpected error has occurred "
1066617	Unable to create the IP address object type wildcard, the following error message is displayed: "Invalid IP netmask".
1066638	In 7.4 ADOM, installation to 7.6 FortiGates may unset firewall service tcp-portrange (if a firewall policy references a firewall service).
1068736	Best Quality SDWAN rules installation may fail with the following error message: "Commit failed: Bad health check name".
1070800	FortiManager Cloud is attempting to install the "cli-cmd-audit" command on a FortiGate (FortiGate-101E and FortiGate-2000E) running version 7.2.8, which does not support this command, leading to an installation error.
1071226	Policy Lookup is not showing result as highlighted when the sections are not expended.
1072354	FortiManager Cloud may attempt to install "ssl-ssh-profile" settings to "quic" objects. However, this syntax might not be supported on smaller FortiGate hardware platforms, particularly those with 2GB of RAM, such as the 60F/61F models.
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.
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".
1086603	Unable to create local-in policy with ISDB objects

## 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
1005098	Verification of the LDAP Server through the LDAP Browser may display an "Operation Error" message.
1027547	In certain cases, the License Status on FortiManager Cloud may be incorrectly displayed as "Expired" despite the license being active in the account.
1047252	Incorrect warning message displayed in FortiManager Cloud GUI during upgrade from Feature build to Mature build.
1060943	FGFM Tunnel does not automatically come back online after disabling the "Offline Mode".

## Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1102080	FortiManager Cloud7.6.2 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2024-50566</li></ul>
1086927	FortiManager Cloud7.6.2 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2025-24474</li></ul>

# 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 7.6.2.

## Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.6.2.

### AP Manager

Bug ID	Description
1086946	The FortiAP upgrade via FortiManager may fail (on FGT 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
974925	The NTP Server setting may not display the correct configuration. This issue might occur on managed devices running FortiOS version 7.4.2 or higher. <b>Workaround:</b> Edit NTP server setting under CLI configuration.
980362	The Firmware Version column in <i>Device Manager</i> incorrectly shows "Upgrading"

Bug ID	Description
	FortiGate from V1 to V2" even after a successful upgrade has been completed.
995919	Cannot config system password-policy expire-day for FortiGates.
1004220	The SD-WAN Overlay template creates route-map names that exceed the 35-character limit.
1062545	When using the backslash "\" in the preshared key of IPSEC settings, the install may fail.
1086303	An installation error may occur when binding and installing the created VLAN interface to the software switch due to ip-managed-by-fortiipam. No issues have been observed with the installation of VLAN interfaces or physical interfaces. <b>Workaround:</b> Use a script (CLI template) on device database on FMG to unset "ip-managed-by-fortiipam" under wan interface (every time before installation), and then install the configuration.

## Others

Bug ID	Description
830592	Upgrade of ADOM type FortiProxy is not supported.
1080463	An admin with access to a specific ADOM can view the database and clone objects to another ADOM, even if they do not have direct access to it.
1106312	The Table View and Device History sections under the SD-WAN Manager's Network tab do not properly display all detailed information, such as Interfaces, Link Mode, and other relevant data. (This issue was initially reported in relation to FGT 7.6.1)

## Policy & Objects

Bug ID	Description
971065	When the number of Custom Internet Services exceeds 256, installation fails due to this limitation.
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).
1077964	After ZTNA server real server address type changes from FQDN to IP, the policy installation may fail; FortiManager Cloud pushes ZTNA server config with wrong order.

## Script

Bug ID	Description
1085374	FortiManager Cloud does not support exporting the TCL scripts via CLI.

# 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><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></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>• 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>• Fabric Management: Fabric Management is not supported on FortiManager Cloud.</li></ul>



The FortiManager Cloud portal does not support IAM user groups.

---



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

Copyright© 2025 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.