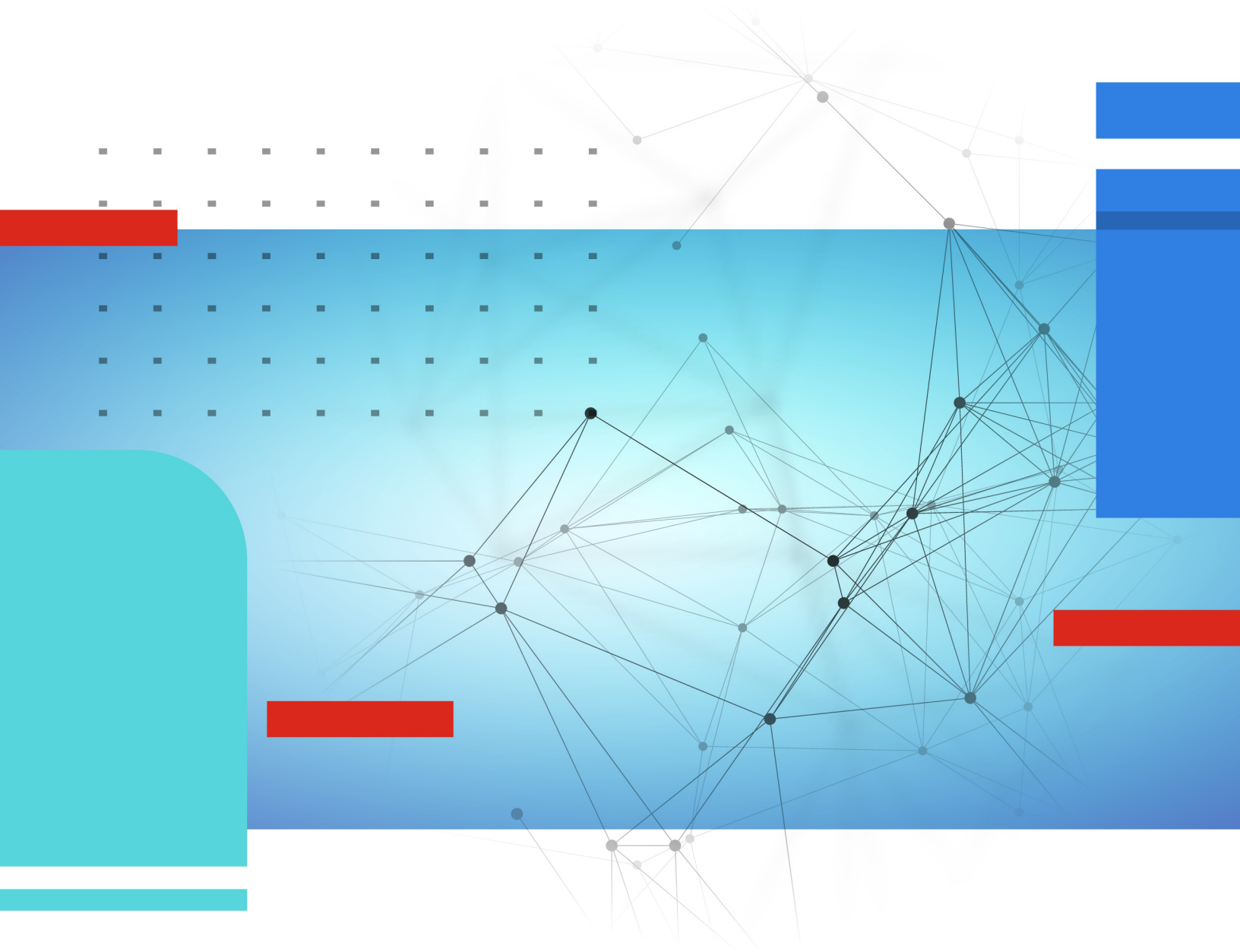
Release Notes

FortiManager Cloud 7.4.11



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 7.4.11 Release Notes
02-721-843127-20220919

TABLE OF CONTENTS

Change log **4**
FortiManager Cloud 7.4.11 release **5**
Special Notices **6**
Device database enters an incorrect state 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 10
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
Services 15
VPN Manager 15
Known issues **16**
New known issues 16
Existing known issues 16
AP Manager 16
Device Manager 16
Others 17
Policy and Objects 17
Services 18
Limitations of FortiManager Cloud **19**

Change log

Date	Change Description
2026-05-13	Initial release of FortiManager Cloud 7.4.11.

FortiManager Cloud 7.4.11 release

This document provides information about FortiManager Cloud version 7.4.11 build 6175.

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 7.4.11.

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 chose 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.

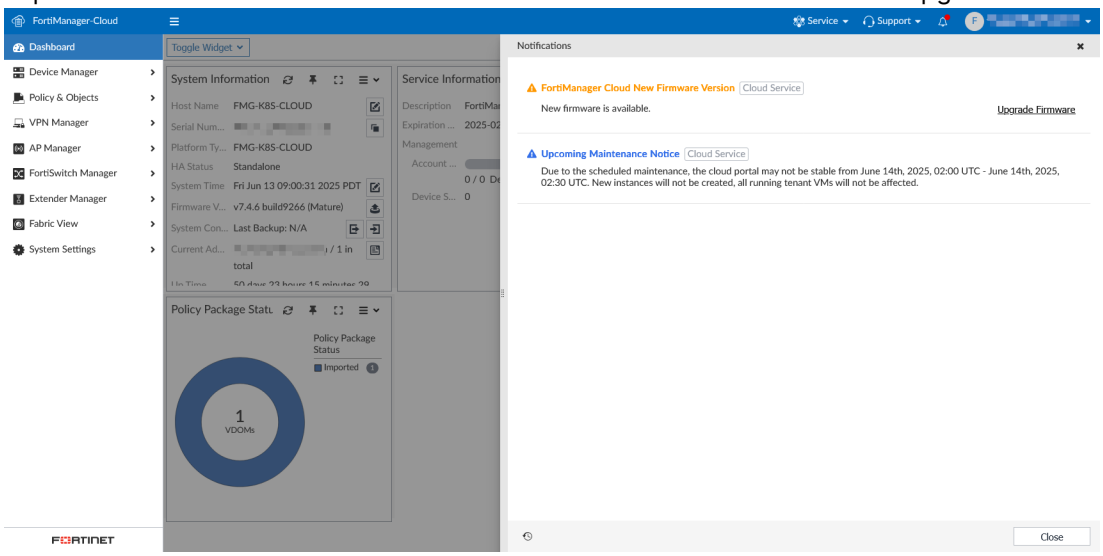
To keep FortiManager Cloud secure and up to date, it is recommended that you upgrade your 7.4 release to the latest release build.

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

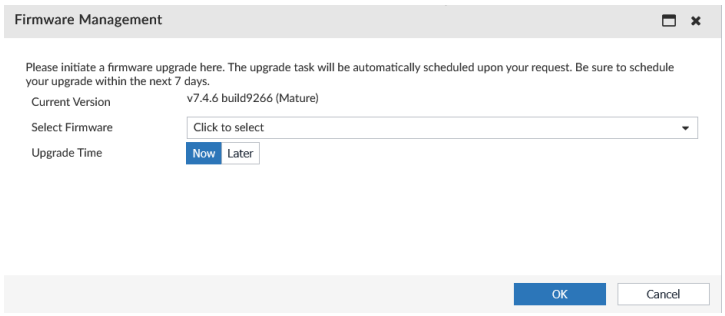
FortiManager Cloud supports FortiOS versions 7.4, 7.2, and 7.0. You must upgrade all managed FortiGates to FortiOS version 7.0 or later.

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.

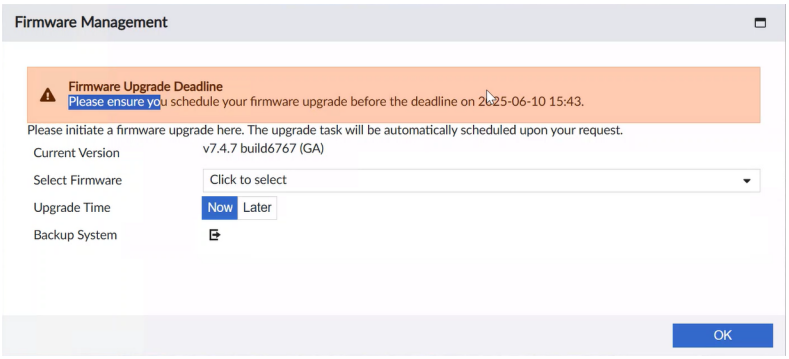
For example, in order to upgrade FortiManager Cloud from version 7.2.x to 7.6.x, you must first upgrade to the latest 7.2 patch version, followed by the latest 7.4 patch version, before finally upgrading to the target 7.6.x release.

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.

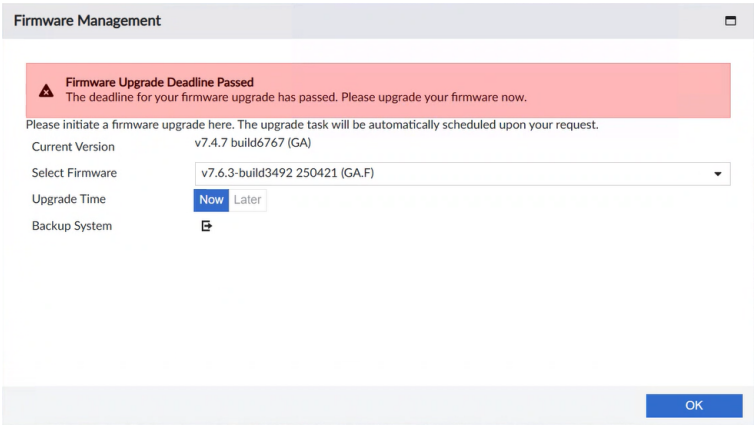
Mandatory upgrades

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 by 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 by 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 7.4.11 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 7.4.11 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 7.4.11 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 7.4.11 supports the same FortiGate models as FortiManager 7.4.11.

For a list of supported FortiGate models, see the *FortiManager 7.4.11 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 7.4.11. To inquire about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
1239368	Duplicate SSID occurs when accented character is used at the end of the SSID name.

Device Manager

Bug ID	Description
1015138	Unable to edit interface with dhcp reservation.
1194361	Installation fails when device description contains single quote characters.
1215090	Unable to retrieve correct setting of device-identification in system interface.
1224965	Device identification is disabled when changing interface role from LAN to undefined.
1246821	FortiManager retrieve may fail when an admins remote-group exists only in the root VDOM and the VDOM order starts with a non-root VDOM, causing invalid reference detection during device addition.
1254998	Incorrect Interface Syntax Selection for FGT90G/91G Gen1/Gen2 During Model Device (ZTP) Creation has been observed.
1269401	Performing device deletion may appear very slow. While the deletion process is still ongoing, clients performing policy package installation tasks may experience delays before the task starts or completes. This behavior has been observed in some cases where FortiManager manages more than 6,000 device groups.

FortiSwitch Manager

Bug ID	Description
1118271	FortiSwitch Device information is not displayed when FortiSwitch version is 7.4.3.
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.
1227473	FortiManager attempts to install set poe-status disable on FortiSwitch ports that already have PoE disabled. The issue persists and reoccurs after configuration installation and synchronization.
1246204	Firmware upgrade tasks stall when multiple upgrades for the same FortiSwitch are run concurrently.
1268279	Deleting custom-command from FortiSwitch Manager template is not deleting it from device.

Global ADOM

Bug ID	Description
1232811	Unassigning a Global Policy Package may fail when it is referenced by SSL inspection profiles in the root ADOM.
1244194	Global Policy Block appended to Global Policy Package is not visible under root ADOM PP when assigned.
1245741	The Promote to Global feature for objects created in an ADOM may fail if the object name contains a forward slash (/) character.

Others

Bug ID	Description
1017440	Import SDN connector failure occurs when special characters are in the username or password
1081121	The syslog server is unable to receive FortiManager event logs when the reliable option is enabled.
1234093	Time discrepancy occurs between formatted and raw logs when using GMT timezone.
1239748	Unable to delete Meta Variables with the following Error: The data is invalid for selected url.

Bug ID	Description
1241561	ADOM integrity check fails when running diagnose cdb check adom-integrity.
1255147	The fmg-admin is able to click both the text label and the toggle.
1256462	FortiClient fails to pull AV signatures from FortiManager acting as FDS server when receiving UM objects over HTTP.
1266515	When importing a custom firewall service definition through a FortiManager script that mixes the set protocol TCP/UDP/SCTP parameter with set protocol-number <value>, FortiManager allows the configuration without validation errors.
1268146	An error occurs when upgrading FortiManager due to password length limitations.

Policy and Objects

Bug ID	Description
1182465	Installation fails when FortiManager creates a default shaping-profile and binds it to an interface.
1194560	Missing CASB applications occur when FortiManager fetches casb application data without the 'get reserved' option.
1224582	FortiManager tries to delete access-proxy and all ZTNA-related configuration from the firewall.
1227209	Insert above or insert below fails when using ISDB objects in the policies.
1230592	An error condition in the security console occurs when reinstalling a previous policy package after upgrading ADOM from v7.4 to v7.6.
1232760	Permit-stun-host configuration is not applied during installation when NAT is disabled.
1240260	When the Policy Package setting "Policy Offload Level" is set to Default mode, the Copy Policy Validation may fail and display an error log "COMMIT FAIL - invalid value".
1240764	Users may experience slowness when loading large policy packages while switching between Interface Pair views.
1242707	Policy package status does not change to "Out of Sync" on FortiManager when local changes are made on FortiGate.
1247668	Importing firewall policies may fail when adding an FortiGate with a large number of policies (e.g., over 60K).
1255176	Policy package installation may stuck when dynamic mapping member of a "firewall addrgrp" is empty.
1257077	The securityconsole application may crash when performing an installation from a FortiManager 7.4 ADOM to a FortiGate 7.2 device if an address group is referenced in an SD-WAN rule within a template.

Bug ID	Description
1257115	Policy package installation may fail on hardware devices when policy-offload-level is set to default.
1258985	When disabling the HTTPS protocol under "Protocol Port Mapping" of any "SSL/SSH Inspection" profile, FortiManager tries to push the command "unset ports" which is not recognized by the FortiGate. As a result, the error "Must set at least one port or enable ssl inspect-all. ..."is generated during the Policy Package Installation.
1259013	Meta-variable modifiers fail when adding colon to a meta-variable within fields such as address objects.
1270583	Installation fails when FortiManager pushes an invalid limit for policing type shaping-profile.

Services

Bug ID	Description
1180123	FortiManager downloads and pushes full-version objects between FDS and FortiGate, which can result in high traffic usage.

VPN Manager

Bug ID	Description
1262311	In a FortiManager 7.4 ADOM, attempts to create or retrieve SSL VPN web portal settings for FortiOS 7.4 devices may fail due to per-VDOM limit validation errors.

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 7.4.11.

Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.4.11.

AP Manager

Bug ID	Description
1032762	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.
1263157	FortiManager may become unresponsive when upgrading FortiSwitch or FortiAP using a Firmware Template.

Device Manager

Bug ID	Description
974925	The NTP Server setting may not display the correct configuration. This issue might occur on managed devices running FOS version lower than 7.4.2. **Workaround**:

Bug ID	Description
	Edit NTP server setting under CLI configuration.
1028515	The Greenwich time zone on FortiGate does not supported on the FortiManager.
1218573	Invalid config error occurs when running CLI script with metadata variables on Device Database in multi-vdom mode.

Others

Bug ID	Description

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`

1217534	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.
	Workaround:
	To prevent this issue, disable the disk check before performing the upgrade:
	`config fmupdate fwm-setting`
	`set check-fgt-disk disable`
	`end`

Policy and Objects

Bug ID	Description
845022	SDN Connector failed to import objects from VMware VSphere.
1199272	Imported certificate does not show details.
1217455	FortiManager is not able to retrieve "usergroup" from "Cisco 3.3 Path7 Pxgrid" using FortiManager connector. **Workaround**:

Bug ID	Description
	Add the appropriate DNS entry under System Settings Network.

Services

Bug ID	Description
1167362	Despite having the "fgfm-deny-unknown" setting enabled, unauthorized devices might still be appearing in the Device Manager. Please check the Special notice for more details.

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. • Unit Operation: Unit Operation is unavailable. • Remote Authentication Server: Remote Authentication Server is unavailable. • SAML SSO: SAML SSO unavailable. • HA: HA unavailable. • SNMP monitoring tool is not supported. • Pre-login banners are not supported.

The FortiManager Cloud portal does not support IAM user groups.

www.fortinet.com