Release Notes

FortiManager Cloud 7.4.5 R1

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

TABLE OF CONTENTS

Change log

Date	Change Description
2024-10-18	Initial release.
2024-12-12	Initial release of 7.4.5 R1.
2024-12-24	Updated Limitations of FortiManager Cloud on page 15.
2025-01-16	Updated Resolved issues on page 10.

FortiManager Cloud 7.4.5 R1 release

This document provides information about FortiManager Cloud version 7.4.5 R1 build 6017.

	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 7.4.5 R1.

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.

	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.
	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. Alternatively, you can access firmware upgrade options from the FortiManager Cloud Dashboard.

	The *Later* option for *Upgrade Time* is only available for one week after the firmware is released.

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

Downgrading to previous firmware versions

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

Product integration and support

FortiManager Cloud version 7.4.5 R1 supports the following items:

Web browser support

FortiManager Cloud version 7.4.5 R1 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 7.4.5 R1 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 7.4.5 R1 supports the same FortiGate models as FortiManager 7.4.5.

For a list of supported FortiGate models, see the *FortiManager 7.4.5 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*.

Resolved issues

The following issues have been fixed in 7.4.5 R1. To inquire about a particular bug, please contact Customer Service & Support.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1086790	FortiManager Cloud 7.4.5 R1 is no longer vulnerable to the following CVE Reference: • CVE-2024-47575
1102080	FortiManager Cloud7.4.5 R1 is no longer vulnerable to the following CVE Reference: • CVE-2024-50566

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 7.4.5 R1.

Existing known issues

The following issues have been identified in a previous version of FortiManager Cloud and remain in FortiManager Cloud 7.4.5 R1.

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.
1041445	The AP attributes do not automatically update in the *AP Manager*.
1062154	Due to a syntax mismatch between FortiGates and FortiManager Clouds for FortiAPs, installation may fail. Currently, FortiManager Cloud v7.4.3 with ADOM 7.4 only supports the FortiAP syntax of the latest FortiGates version 7.4.4.
1076200	Policy install fails due to FortiManager Cloud installs unexpected changes related to "<wifi_ intf> address". **Workaround**: Create a CLI template with all subnet addresses and assign to device.
1081136	FortiManager Cloud is trying to delete and create ssid interface subnet address after upgrade.

Device Manager

Bug ID	Description
952422	IPsec templates created by SDWAN Overlay does not create tunnels for all the underlay interfaces.
973365	FortiManager Cloud does not display the IP addresses of FortiGate interfaces configured with DHCP addressing mode. **Workaround**: Disable Addressing Mode from DHCP to Manual in FortiManager Cloud Device DB, then retrieve from FortiGate and IP will be updated successfully.
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. **Workaround**: Edit NTP server setting under CLI configuration.
1004220	The SD-WAN Overlay template creates route-map names that exceed the 35-character limit.
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.
1070943	Unable to upgrade the devices through the Device Group Upgrade Firmware feature. **Workaround**: Upgrade devices individually by using the "Device Firmware Upgrade" feature or Create New Firmware Template for single devices or device groups and use the "Assign to Devices/Groups" feature.
1074717	An error might be observed when the SD-WAN template health check name contains a space, displaying the following message: "Bad health check name...".
1075747	SD-WAN Monitor does not display the members under the SD-WAN Rules (Map View or Table View).
1080414	CSV import fails to set metadata variables due to old header format ("name").

Others

Bug ID	Description
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. **Workaround**: Disabling thedisk check on fmupdate before the upgarde.
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".

Bug ID	Description
	Workaround:
	Run the following script against the ADOM DB:
| | ```
config webfilter profile
    edit "g-default"
        config web
            unset urlfilter-table
        end
    next
end
``` |
1019784	ADOM Upgrade from 7.0 to 7.2 fails with the "Fail(errno=0):invalid value" error message.
1029677	Unable to upgrade ADOM from v6.4 to v7.0 due to global scope error in webfilter profile.
	Workaround:
	Rename the "`g-default`" to "`g-test`" > save. It can be deleted after that. Once ADOM upgraded, new g-default is created.

Policy & Objects

Bug ID	Description
845022	SDN Connector failed to import objects from VMware VSphere.
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.
	Workaround:
	Disable the option under advance option in Firewall Rule.
998850	Modification to Policy with install target does not update the policy package status.
	Workaround:
	Remove the Installation Target and re-add to the policy which will trigger Policy Package Modification and the install preview will also show the changes made.
1029921	Under the "Web Application Firewall" security profiles, users are unable to disable the signatures through the GUI.
1074686	FortiManager Cloud fails to import NAC policies.
	Workaround:
	Manually create the NAC policy in the policy package and then install.
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.
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".

System Settings

Bug ID	Description
825319	FortiManager Cloud fails to promote a FortiGate HA member (running on firmware 7.2.0 to 7.2.4) to the Primary.

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: • ADOMs cannot be created. • Advanced ADOM mode is not supported.

Feature	Feature available?	Details of limitations and unsupported features
		- 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.

The FortiManager Cloud portal does not support IAM user groups.

FÜRTINET®