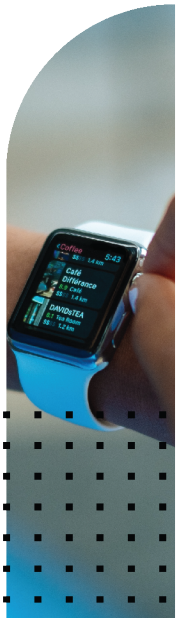
Release Notes

FortiManager Cloud 7.2.5



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

September 19, 2022
FortiManager Cloud 7.2.5 Release Notes
02-721-843127-20220919

TABLE OF CONTENTS

Change log

Date	Change Description
2023-04-08	Initial release.
2024-05-01	Updated Limitations of FortiManager Cloud on page 23.
2024-12-24	Updated Limitations of FortiManager Cloud on page 23.

FortiManager Cloud 7.2.5 release

This document provides information about FortiManager Cloud version 7.2.5 build 5066.

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 7.2.5.

FortiManager Cloud 6.4 support

Starting with the release of FortiManager Cloud 7.2.1, version 6.4.x will no longer be supported, and users must upgrade their FortiManager Cloud versions to 7.0 or 7.2 before November 25th, 2022. After this period passes, you will not be able to access your FortiManager Cloud instance until you have completed the upgrade. See FortiManager Cloud version support on page 8.

Upgrade information

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

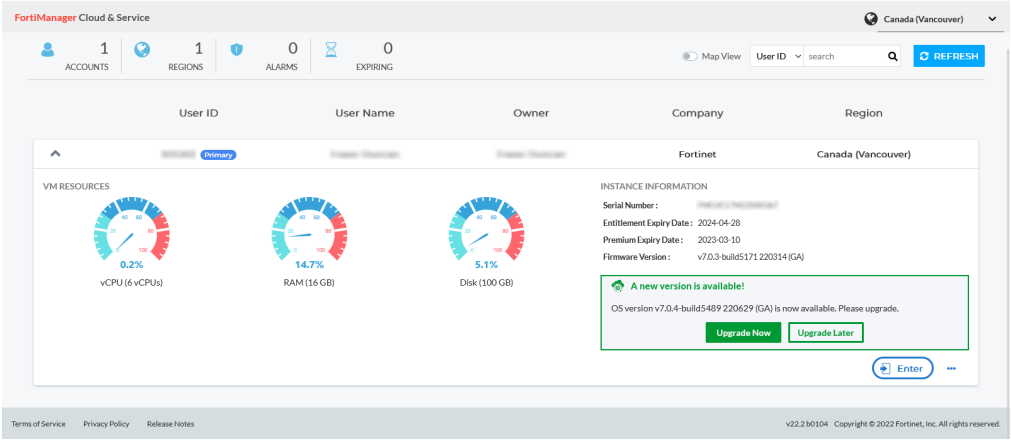
Primary users can upgrade FortiManager Cloud firmware to 7.2.5 by using the FortiManager Cloud & Service portal. Secondary users can upgrade FortiManager Cloud firmware to 7.2.5 by entering the instance and going to the *System Settings* module.

For FortiManager Cloud deployments on 7.2, you have two weeks to upgrade the FortiManager Cloud firmware to 7.2.5 after it is released. If you take no action, you can no longer access FortiManager Cloud. The *Enter* button is grayed out until you upgrade to the required firmware.

FortiManager Cloud supports FortiOS versions 6.4, 7.0 and 7.2. You must upgrade all managed FortiGates to FortiOS version 6.4.4 or later.

To upgrade firmware from the portal:

1. Go to FortiCloud (https://support.fortinet.com/), and use your FortiCloud account credentials to log in.
   The FortiCloud portal is displayed.
2. From the *Services* menu, select *FortiManager Cloud* under *Cloud Management*.
   The FortiManager Cloud & Service portal is displayed. An alert icon appears next your account when a new version of firmware is available.
3. Expand your account.
4. Click *Upgrade Now* to update the firmware immediately, or click *Upgrade Later* to schedule upgrade of the firmware for a later date.



The *Upgrade Later* option is only available for two weeks after the firmware is released.

5. Click *OK*.
6. Click *Enter* to open FortiManager Cloud.

Downgrading to previous firmware versions

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

FortiManager Cloud version support

FortiManager Cloud supports two major release versions.

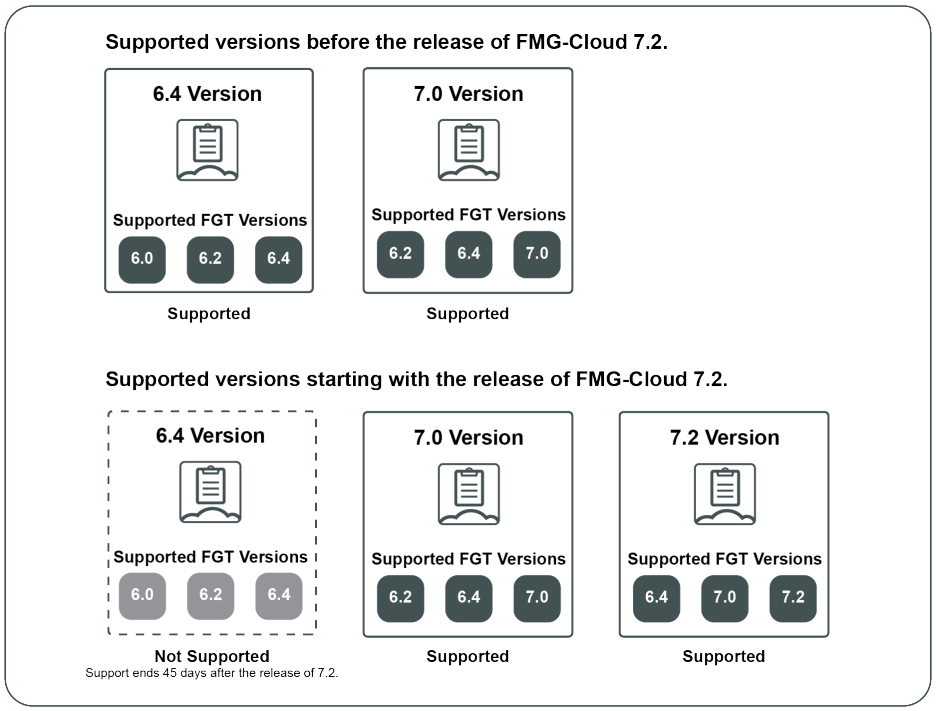
Each FortiManager Cloud major release version is able to manage FortiGate devices for its current version and the two previous versions. For example:

FMG-Cloud version	Managed FortiGate version
FortiManager Cloud 7.0	7.0, 6.4, and 6.2.
FortiManager Cloud 7.2	7.2, 7.0, and 6.4.

When a new major version is released, the lowest previously supported version becomes unsupported and will be phased out within 45 days. You can use this time to schedule an upgrade to a higher version.

With the release of FortiManager Cloud 7.2.1, the supported major versions are 7.2 and 7.0. FortiManager Cloud 6.4 is no longer supported.

The image below shows the supported FortiManager Cloud major release versions before and after the release of FortiManager Cloud 7.2.1, as well the FortiGate versions that can be managed.



Upgrading from FortiManager Cloud 6.4

Customers using FortiManager Cloud 6.4 must update their version to 7.0 or 7.2 within 45 days.

Depending on the managed FortiGate devices' current version, you may be required to upgrade the FortiManager Cloud ADOM and FortiGate device's version as part of the upgrade process.

See the table below to determine what action is required based on your FortiManager Cloud and FortiGate device version.

FMG-Cloud Version	FGT Version	Required Upgrade Procedure
6.4	6.0	You must upgrade FMG-Cloud to 7.0. Your ADOM and managed FGT device versions must first be updated to a minimum of version 6.2. See the upgrade procedure below.
	6.2 6.4	You must upgrade to FMG-Cloud 7.0. You are not required to upgrade your ADOM and FGT device versons as FMG-Cloud 7.0 supports 6.2 and 6.4 devices.
7.0	6.2 6.4 7.0	Upgrading to FMG-Cloud 7.2 is not immediately required. Upgrading to the latest version of FMG-Cloud is recommended as a best practice.

The following upgrade procedure explains the process of upgrading your FortiManager Cloud 6.4 version to 7.0 when you are managing FortiGate devices on version 6.0.x. For all other scenarios, please follow the standard upgrade instructions: Upgrade information on page 7

To upgrade FortiManager Cloud 6.4 with managed FOS 6.0 devices:

1. Upgrade your FortiOS device version from 6.0 to 6.2.
2. Upgrade your ADOM version in FortiManager Cloud from 6.0 to 6.2.
   For more information, see the *Updating the ADOM version* in the FortiManager Cloud Deployment guide.
3. Upgrade FortiManager Cloud instance from 6.4 to 7.0.
   See Upgrade information on page 7 for more information on how to upgrade your FortiManager Cloud version using the cloud portal.
4. Optionally, you can choose to further upgrade your device and ADOM version as needed.
   For example if you wish to upgrade to FortiManager Cloud 7.2.1, you must first upgrade your device and ADOM version to a minimum of 6.4.

Product integration and support

FortiManager Cloud version 7.2.5 supports the following items:

Web browser support

FortiManager Cloud version 7.2.5 supports the following web browsers:

- Microsoft Edge version 110.0.1587.57 (64-bit)
- Mozilla Firefox version 110 (64-bit)
- Google Chrome version 110.0.5481.104 (64-bit)

FortiOS support

FortiManager Cloud version 7.2.5 supports the following FortiOS versions:

- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 to 6.4.10

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

FortiGate model support

FortiManager Cloud version 7.2.5 supports the same FortiGate models as FortiManager 7.2.5. FortiGate models must be on FortiOS 6.4.4 or later.

For a list of supported FortiGate models, see the *FortiManager 7.2.5 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)	✓	✓
Japanese	✓	✓
Korean	✓	✓
Spanish	✓	✓

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 7.2.5. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
736930	FortiManager Cloud is unable to efficiently display rogue AP lists for FortiGates with a high volume of rogue APs.
861941	FortiManager Cloud attempts to install "`arrp-profile`" even if "`darrp`" is disabled.
906061	It takes a significant amount of time to assign a profile to each FortiAPs.
974444	DNS server for SSIDs gets resets after Importing AP Profile.
982548	FortiGate configuration install may fail with a reason "Need to unset channel list in radio-1 first."
1002043	*AP Manager* view does not show SSIDs and Radio Channels.

Device Manager

Bug ID	Description
723720	The "`strong-crypto`" feature change under the CLI configuration cannot be installed to FortiGate.
777693	Provisioning templates change meta data's values.
778131	FortiManager Cloud did not support the per device mapping for user SAML configurations.
811104	Import policy package fails after installing web-proxy through CLI configurations
838462	Adding device using "Add Model HA Cluster" feature failed as FortiManager Cloud does not allow "virtual switch interfaces" being used as "heartbeat interfaces".
871334 973064	Installation to FortiGate with NP7 Acceleration feature enabled might fail when FortiManager Cloud attempted to modify the QoS settings. Changing the "`default-qos-type`" to values other than its default may result in a FortiGate reboot (FOS Behavior).
880934	FortiManager Cloud reverts Syslog mode settings on local FortiGates (when FortiGates are in FIPS mode).

Bug ID	Description
902577	The status of the FortiLink split-interface radio button under FortiManager Cloud's *Device Manager* does not match the configuration in FortiGates.
920394	Installation failed due to the incorrect install order during ZTP.
923808	Even with the "`set dhcp-relay-request-all-server enable`" option enabled, FortiManager Cloud does not keep the DHCP server & relay configurations on the same interface.
935586	When managed devices go down/appear offline, not all FGFM tunnels are automatically recovered by FortiManager Cloud.
936168	Unable to assign Device Group to the Firmware Template.
936544	When importing CLI Templates, GUI displays a blank page.
939804	Creating/Modifying the IPSEC Phase1 Interface Mode might trigger the following error message: "The string contains XSS vulnerability characters." This ONLY occurs when `devid = ''`. **Workaround**: Manually removing the value `''` from `dev-id`.
949546	When zones have identical names except for case, only 1 of the zones may be visible in *Device Manager*.
949612	The SD-WAN monitor table-view takes too long to load/display information.
952404	FortiManager Cloud cannot install the Static Route config under the Provisioning Template due to a static route template error after upgrading to FortiManager Cloud 7.2.4/7.4.1.
954610	FortiManager Cloud does not show objects under the "named address" options in IPsec VPN Phase 2 definitions.
956920	Monitor Health Check graphs return incomplete or no value.
961447	After upgrading FortiManager Cloud (VMs & FortiManager Cloud Cloud) to versions 7.2.4 or 7.4.1, devices may not be able to be retrieved or refreshed. **Workarounds**: A) Reduce the license use (delete one device). B) Request/purchase a license upgrade. C) On the already managed FortiGates that need to be retrieved, run: `diag fdsm cfg-upload <comment>` D) When adding a new FortiGate to the last license seat, it will initially fail on the retrieve step, but the device is added to DVM and within about 120 seconds an auto-retrieve is triggered and the first revision of the new device is created normally.
966118	FortiManager Cloud tries to purge all entries under table "`system global split-port-mode`" for its System Template .
967611	*Device Manager* interface link status is blank for various Interface type (Tunnel, Aggregate, VDOM Link, Software Switch).
969542	Sometimes IPsec Tunnel Template displaying "Response with errors" message when editing the template.

Bug ID	Description
969698	FortiManager Cloud allows the creation of an empty service value for Internet Service routes.
975310	Unable to unset interface IP for a VLAN interface in *Device Manager*.
1009883	Unable to set the Radius-Server addresses as FQDN. **Workaround**: Run the script directly on the FortiGate and then retrieve config back to the FortiManager Cloud.

FortiSwitch Manager

Bug ID	Description
940419	When adding FortiSwitch on FortiManager Cloud Error message, "Import error - invalid port number" is displayed.
947651	*Per Device* under the *FortiSwitch Manager* cannot edit FortiSwitch name and GUI returns error "invalid value".
967213	While attempting to deploy a FortiSwitch template to a model device, FortiManager Cloud generates the following error message: "VLAN interface does not match FortiLink."

925188	The per-device mapping for any assigned global objects cannot be modified.
969182	Under the Global ADOM, the assignment of specific policy packages does not function properly.

Others

Bug ID	Description
583349	FortiManager Cloud does not provide support for image upgrades on "ONDEMAND" devices.
796858	Subject Key Identifier extension is missing on FortiManager ADOM CA certificate.
874052	After upgrade ADOM from v7.0 to v7.2, when installing a policy package to FGT-v7.2 device, FortiManager Cloud tries to change "`match-vip`" from "disabled" to "enabled".
875584	FortiManager Cloud cannot upgrade ADOMs to 7.2 due to error, "copy system replacemsg spam.smtp-spam-emailblock". **Workaround**: Delete replacement message "smtp-spam-emailblock" from System Templates.
891253	The firmware upgrade is successful; however, the task line does not get updated for the retrieve action when device names exceed the predefined character limit.

Bug ID	Description
897157	Unexpected changes in existing static routes, created by static route template after upgrade to 7.0.7, 7.2.2, 7.4.0.
900512	FortiManager Cloud ADOM Upgrade fails with the error message, "Peer type cannot be peer when authentication method is pre-share key".
922957	The "`fmgd`" process may crash while loading the ADOM when multiple Policy Packages are locked.
924201	Jinja templates does not identify new variables automatically when a new variable is added.
930305	Firmware template upgrade preview shows incorrect versions for the upgrade.
941203	FortiManager Cloud does not support the use of Certificate Templates to create certificates with a "`range=global`" setting for FortiGates operating in multi-vdom mode.
957433	When creating the FortiManager/FortiAnalyzer docker instances, UUID is missing under the "`diagnose debug vminfo`".
960796	FortiExtenders are not displayed under the *FortiExtender Manager* for all FortiGates.
961155	Event Logs cannot be downloaded via GUI.
963490	Installation fails as FortiManager Cloud attempts to "`set role primary`" feature for the "`lan-extension backhaul`" under the "`extender-controller`"
971122	FortiManager Cloud does not support all authentication types that are supported by FortiOS, leading to a certificate error in the FortiClient EMS connector.
982564	When upgrading the root ADOM, the process might fail with the following error message: "...The string contains XSS vulnerability characters...".

Policy and Objects

Bug ID	Description
630648	A FortiManager Cloud instance running on Microsoft Azure is unable to import the SDN connector for a dynamic firewall address and is displaying an error message stating, "wrong input parameter."
696367	Hit count, first used, and last used may not get updated on FortiManager Cloud.
725427	Policy package install skips the policy where destination interface is set as SD-WAN zone and policy is IPSEC policy.
751443	FortiManager Cloud displays policy installation copy failures error when IPsec template gets unassigned.
804160	FortiManager Cloud does not remove "Radius Server" on the FortiGate when it becomes unused.
817289	FortiManager Cloud only accepts IPv6 Compressed Notation format for the *Policy & Objects*.

Bug ID	Description
830640	"Send files to FortiSandbox for inspection" option is being enabled when creating an antivirus profile.
854359	An installation error occurs when FortiManager Cloud attempts to install wildcard FQDN addresses "`mzstatic-apple`" and "`cdn-apple`" within the "`custom-deep-inspection`" SSL-SSH profile.
855073	The "where used" feature (under the Source & Destination objects) incorrectly displays "No Record Found" even when these objects are in use.
875103	Local categories gets purged if used in Profile Mode Security Profiles.
888798	Changing deep inspection ssl-ssh-profile to "`inspect all ports`" may cause installation error.
894597	Default value for "`unsupported-ssl-version`" in ssl-ssh-profile gets modified during the installation.
899226	Unable to create Central SNAT explicit port translations on FortiManager Cloud.
900229	In policy-based policy packaged, application IDs are displayed instead of their names.
901324	Change entries in FortiGuard Category Based Filter table from "*Monitor*" to "*Allow*" cannot be saved.
904751	WebRating overrides can't be deployed or deleted via FortiManager Cloud.
905377	Threat Feeds with name starting with "`g-`" do not get installed to FortiGates without VDOM enabled.
907925	IPS profile/Signature tab is not visible for admins with non-default admin profile.
908353	When ISDB name changed, FortiManager Cloud is not automatically updating the new ISDB object name.
908445	FortiManager Cloud does not display correct edit page for virtual server VIP when edit object in policy table.
917225	FortiManager Cloud is unable to install policy packages to multiple devices due to "security console" crashes.
920983	The policy blocks using a group object do not get updated when the objects within the group are modified.
924680	Policy packages containing geo-based ISDB objects may not be successfully installed to the FortiGates.
924900	Wrong date format is displayed for "*first used*" and "*last used*" column.
938019	Policy Package Status not changed on modification of nested group used in policy block.
939979	After editing authentication-rule/portal mapping, FortiManager Cloud installs unexpected changes to these rules.
942659	Syncing EMS tags from FortiManager Cloud fails when the EMS Connector is configured in multi-site mode.

Bug ID	Description
945632	Modifying the Policy Installation Target does not trigger a status change in the Policy Package when adding an "install on" to a single policy.
945853	FortiManager Cloud doesn't sync previously deleted EMS tags.
948559	Policy blocks doesn't load properly.
949515	Security Policy Installation Verification fails because the "`internet-service-negate`" feature gets enabled every time after modifying the policy.
954399	Cloning Webfilter profiles does not save the FortiGuard Category Based Filter action.
955010	Comments on policies may be cleared when a blank area within the text field is clicked.
957225	ADOM admin users not able to view the managed FortiGate in the policy push wizard
958923	Installing policy packages that utilize an SSL/SSH Inspection profile may fail with the error message, "Server certificate replace mode cannot support category exempt."
959116	The timestamps displayed for 'First/Last Used' under the Hit Count for Firewall Policies within the Policy & Objects section are invalid.
959166	Export to Excel does not work.
959877	The timestamps displayed for "First/Last Used" under the *Hit Count* for Firewall Policies within the *Policy & Objects* section are invalid.
959890	Per-device mapping search for VDOMs is not possible for users.
960660	The Clone Reverse feature is not functioning when the firewall policy includes an Internet service address object.
960778	Installation failed because FortiManager Cloud attempts to remove a static entry, "QuarantinedDevices."
963008	Impossible to merge duplicate objects.
963536	The policy package feature "*Export to Excel*" is not functioning.
965670	Creating a new interface type "`vlan`"; changing VDOM results in the removal of the selected interface.
965719	FortiManager Cloud is unable to enable the log setting for implicit deny rule under the policy package.
972392	Users do not receive a proper warning when creating a firewall address with the IP address "`0.0.0.0/0`."
978814	When attempting to use the "*Export to Excel*" feature under the Firewall Policy with extensive rules, GUI may slow down and become unresponsive for some time.
986262	EMS Cloud tags are not updated on FortiManager Cloud.
1002551	FortiManager Cloud is pushing the web-proxy profile configuration without space between domains.

Revision History

Bug ID	Description
513317	FortiManager Cloud may fail to install policy after FortiGate failover on Azure.
894523	Object revision timestamp is taken from previous revision.
904710	Restoring a revision of a policy removes the information of all the SD-WAN rules.

Script

Bug ID	Description
923966	When FortiManager Cloud is operating in Workspace mode, there are no options to save changes after executing a CLI script.
937528	Unable to send DHCP options "`set value`" using CLI template and using Script.

Bug ID	Description
938365	FortiManager Cloud's GUI does not display an option under FortiGuard Settings to support the 7.2 version for FortiClient and FortiMail.
980334	"*Download to Excel*" option on Licensing Status under the FortiGuard does not work.

System Settings

Bug ID	Description
853429	Creating FortiManager Cloud's configuration backup via scp cannot be done.
930200	Unable to change the time and timezone from the GUI.
930449	Testing the syslog server displays the message, "Failed to send a test log to syslog server".
941082	A password prompt is consistently requested with each new login attempt when applying password policies to a local account linked to FortiToken Cloud Mobile for multi-factor authentication (MFA).

VPN Manager

Bug ID	Description
678319	Once "`os-check`" option is enabled, "`os-check-list`" table is not loaded.
897574	Address Objects with Meta Variables do not function correctly when creating Static routes using the *VPN Manager*.
906097	*VPN Manager* IPsec community Phase 2 encryption setting can't be changed to AES256GCM from the GUI.
923221	Provision Template - IPsec Tunnel: cannot Activate IPsec_Fortinet_Recommended; GUI returns error.
942222	The configuration settings for the "`peergroup`" are not being retained properly.

Known Issues

The following issues have been identified in 7.2.5. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
884233	FortiManager Cloud displays the AP critical security vulnerability info even after FortiAPs are being upgraded.
977726	SSID config changes cannot be installed when SSID mode selected as Tunnel under AP.

Device Manager

Bug ID	Description
895994	When using the 'where used' feature in Phase 2 quick mode selector, objects do not appear, and they can be removed.
955058	Changes on Address groups only referenced in phase2 selectors are not installed
961508	*SD-WAN Monitor* table-view does not load.
966546	Unable to disable the"Create Address Object Matching Subnet" feature when the interfaces role is LAN.

Others

Bug ID	Description
703585	FortiManager Cloud may return "Connection aborted" error with JSON API request.
924164	The firmware template status changes to "unknown" after retrieve.

Policy & Objects

Bug ID	Description
718223	Hyperscale firewall EIF shall not be enabled when IP pool with CGN overload configuration is used in a policy.
779363	FortiManager Cloud fails to install analytics-wl-filetype in AV profile to FortiGates.
845022	SDN Connector failed to import objects from VMware VSphere.
980649	"where used" feature disappears when ADOM is unlocked.

Revision History

Bug ID	Description
801614	FortiManager Cloud might display an error message "Failed to create a new revision." for some FortiGates when retrieving their configurations.

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.

VPN Manager

Bug ID	Description
784385	If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for *VPN Manager*. **Workaround**: It is strongly recommended to create a fresh backup of the FortiManager Cloud's configuration prior to the workaround. Perform the following command to check & repair the FortiManager Cloud's configuration database. `diagnose cdb check policy-packages <adom>` After running this command, FortiManager Cloud will remove the invalid mappings of vpnmgr interfaces.

Limitations of FortiManager Cloud

This section lists the features currently unavailable in FortiManager Cloud.

Feature	Feature available?	Details

Device Manager	Yes	• Add Device:
		  • Cannot discover a new device, but can add a model device.
		  • Does not support Azure vWan FortiGate network virtual appliances (NVAs).
		• 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.

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	
FortiGuard	Not applicable	• FortiManager Cloud does not provide the FortiGuard update service because managed devices can update directly from FortiGuard Cloud.
FortiSwitch Manager	Yes	
Fabric View	Yes	

System Settings	Yes	• License Information: License Information widget unavailable.
		• 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: Profile option is unavailable.
		• ADOM:
		  • 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.

The FortiManager Cloud portal does not support IAM user groups.

www.fortinet.com