FORTINET

Release Notes

FortiClient EMS 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

October 09, 2024
FortiClient EMS 7.2.5 Release Notes
04-725-1045778-20241009

TABLE OF CONTENTS

Introduction

FortiClient Endpoint Management Server (EMS) is a system intended to be used to manage FortiClient installations. It uses the Endpoint Control protocol and supports all FortiClient platforms:

- Microsoft Windows
- macOS
- Linux
- Android OS
- Apple iOS
- Chrome OS

FortiClient EMS runs on a Microsoft Windows server.

This document provides the following information for FortiClient EMS 7.2.5 build 1061:

For information about FortiClient EMS, see the *FortiClient EMS 7.2.5 Administration Guide*.

Endpoint requirements

The following FortiClient platforms are supported:

- FortiClient for Microsoft Windows
- FortiClient for macOS
- FortiClient for Linux
- FortiClient for Android OS
- FortiClient for iOS
- FortiClient for Chromebooks

See Product integration and support on page 11 for FortiClient version support information.

FortiClient is supported on multiple Microsoft Windows, macOS, and Linux platforms. EMS supports all such platforms as endpoints.

Supported web browsers

The latest version of the following web browsers can be used to connect remotely to the FortiClient EMS 7.2.5 GUI:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Internet Explorer is not recommended. You may need to enable remote access from the FortiClient EMS GUI. See To enable remote access to FortiClient EMS.

Licensing and installation

For information on licensing and installing FortiClient EMS, see the *FortiClient EMS Administration Guide*.

Ensuring that all installed software, including EMS and SQL Server, is up-to-date, is considered best practice.

Special notices

Microsoft Visual C++ installation

The EMS installation includes installation of Microsoft Visual C++ (VC) 2015. If the server already has a newer version of VC installed, the installation fails. See VC++ 2015 Redistributable installation returns error 1638 when newer version already installed.

If you have a VC version installed on your server that is newer than 2015, uninstall VC before installing EMS.

SQL Server Standard or Enterprise with 5000 or more endpoints

When managing more than 5000 endpoints, install SQL Server Standard or Enterprise instead of SQL Server Express, which the EMS installation also installs by default. Otherwise, you may experience database deadlocks. The minimum SQL Server version that FortiClient EMS supports is 2017. See Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise.

Split tunnel

In EMS 7.2.5, you configure application split tunnel using per-tunnel configuration, not a global configuration. If you are upgrading from an older version that uses the global application split tunnel configuration, change the configuration to per-tunnel.

SAML logins

Upon initial SAML single sign on account login, EMS creates a standard administrator for this user in *Administration* > *Admin Users*. A standard administrator has permissions to modify endpoints, policies, and settings. Having the EMS super administrator manually assign the proper role to the newly created login is recommended.

FortiGuard Web Filtering Category v10 Update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency websites. To use the new categories, customers must upgrade their Fortinet products to one of the versions below:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.8 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Read the following CSB for more information to caveats on the usage in FortiManager and FortiOS:
https://support.fortinet.com/Information/Bulletin.aspx

DNS updates when using ZTNA

When using zero trust network access (ZTNA), configuring dynamic DNS (DDNS) updates as *Secure only* is not supported.

What's new

For information about what's new in FortiClient EMS 7.2.5, see the FortiClient & FortiClient EMS 7.2 New Features Guide.

Upgrading

Upgrading from previous EMS versions

EMS 7.2.5 only supports FortiClient 7.2 and 7.0. You must first upgrade older FortiClient versions to 7.0.2 or newer before upgrading EMS to 7.2.5.

FortiClient EMS supports direct upgrade from EMS 6.2, 6.4, and 7.0. To upgrade older EMS versions, follow the upgrade procedure in *FortiClient and FortiClient EMS Upgrade Paths*.

With the endpoint security improvement feature, there are backward compatibility issues to consider while planning upgrades. See Recommended upgrade path.

EMS 7.2.5 does not support legacy 158 licenses, which were in use before 2021 and have reached end-of-life. Following is a list of discontinued SKUs:

- FC1-15-EMS01-158-02-DD
- FC1-15-EMS02-158-02-DD

If you attempt an upgrade to EMS 7.2.5 with the legacy 158 licenses, the EMS installer displays an error message: "Legacy license is not supported after upgrade". The EMS upgrade does not proceed.

EMS 7.2.5 supports the following legacy Fabric Agent licenses to help customers with migration:

- FCX-15-EMS01-297-01-DD
- FCX-15-EMS01-298-01-DD
- FCX-15-EMS01-299-01-DD

You do not need to convert the aforementioned Fabric Agent licenses to upgrade to EMS 7.2.5.

Downgrading to previous versions

FortiClient EMS does not support downgrading to previous EMS versions.

Product integration and support

The following table lists version 7.2.5 product integration and support information:

Server operating systems	• Windows Server 2022 • Windows Server 2019
Minimum system requirements	• 2.0 GHz 64-bit processor, six virtual CPUs • 8 GB RAM (10 GB RAM or more is recommended) • 40 GB free hard disk • Gigabit (10/100/1000baseT) Ethernet adapter • Internet access is recommended, but optional, during installation. SQL Server may require some dependencies to be downloaded over the internet. EMS also tries to download information about FortiClient signature updates from FortiGuard. You should only install FortiClient EMS and the default services for the operating system on the server. You should not install additional services on the same server as FortiClient EMS.
FortiAnalyzer	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later Although EMS supports the listed FortiAnalyzer versions, confirming the compatibility between your FortiAnalyzer and FortiClient versions is recommended. Otherwise, not all features may be available. See the FortiClient Release Notes.
FortiAuthenticator	• 6.5.0 and later • 6.4.0 and later • 6.3.0 and later • 6.2.0 and later • 6.1.0 and later • 6.0.0 and later
FortiClient (Linux)	• 7.2.0 and later • 7.0.2 and later
FortiClient (macOS)	• 7.2.0 and later • 7.0.2 and later
FortiClient (Windows)	• 7.2.0 and later • 7.0.2 and later
FortiManager	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiOS	• 7.4.0 and later • 7.2.0 and later

	• 7.0.0 and later (for zero trust network access, 7.0.6 or later is recommended) • 6.4.0 and later
FortiSandbox	• 4.4.0 and later • 4.2.0 and later • 4.0.0 and later • 3.2.0 and later

Installing and running EMS on a domain controller is not supported.

Resolved issues

The following issues have been fixed in version 7.2.5. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Administration

Bug ID	Description
1036509	EMS does not log administrator out of GUI based on the configured inactivity timeout when specific widgets are added.

Install and upgrade

Bug ID	Description
985789	After upgrade to FortiClient Cloud 7.2.2, user cannot sync domain.
1010309	AD sync does not work since upgrade from EMS 7.2.3.

Dashboard

Bug ID	Description
974187	Number of endpoints under *Out of Sync* in EMS dashboard differ from out of sync endpoints under *Endpoints* pane.
976000	FortiClient version widget sort order is incorrect due to string comparison.
978588	EMS widgets in the dashboard never update.

Endpoint management

Bug ID	Description
917374	The invitation code count does not decrease when endpoints are deleted from EMS.

Bug ID	Description
974761	LDAP sync issue *Cannot insert duplicate key in object 'dbo.FortiClients_users'.* occurs.
981669	Enforced onboarding may cause FortiClient on mobile devices to unregister from EMS.
987356	User cannot move endpoints between groups on EMS.
995512	EMS fails to delete domain and shows server error message.
998207	EMS shows some endpoint users as *No User*.
999617	In hybrid Active Directory (AD) environment, devices on EMS have two users (UPN and SAMAccountName).
1010142	When the hostname of an Azure endpoint changes, EMS creates a duplicate entry and cannot manage the endpoint properly.
1010861	EMS LDAP sync error *failed to update database sync object tables* occurs.
1012080	Exported endpoints CSV list shows incorrect remote IP address for some endpoints.
1018643	Incorrect username shows for several endpoints in EMS GUI due to `|` in `USR_NAME`.
1019542	EMS shows wrong username associated with endpoint.
1027417	Incorrectly selected user record.
1027527	Exporting CSV for filtered endpoint list does not work.
1028852	FortiClient Cloud *Endpoints* pane shows *No User* or incorrect username.
1030908	EMS does not display correct username on endpoint information for macOS device.
1032058	EMS displays multiple FortiClients as out-of-sync unless marked as uninstalled.
1034831	EMS fails to run group assignment rule due to *Data Access Server Error, Error: DAS returned error: Internal error* error.
1040963	Social user information processing fails due to `:` in `USR_NAME`.
1056690	Hostname of the endpoint device is blank.

Endpoint policy and profile

Bug ID	Description
868534	Web Filter profile synced from FortiGate keeps disabled status links in the exception list.
976029	EMS sends `REVOKE` when profile changes.

Bug ID	Description
984437	EMS fails to assign Microsoft Entra ID user-based policy.
1002075	EMS does not update assigned policy or deployment package after GAR triggers.
1006059	EMS Azure security groups do not match with users correctly.
1017064	Endpoints do not get the correct profile.
1020480	EMS does not assign device a `group_container_parent`, resulting in no endpoint policy assigned.
1037992	EMS cannot import Web Filter profile from a particular administrative domain in FortiManager.

Fortinet Security Fabric devices

Bug ID	Description
986035	EMS /FortiGate API message change causes EMS to no longer support FortiOS 7.2.
990863	Zero trust network access (ZTNA) tags do not sync correctly between non-default EMS site and FortiGate.
1058260	Due to FortiClient keepalive and tag worker timing, tag notifications can be missed when FortiClient comes online.

Remote Access - SSL VPN

Bug ID	Description
1044769	FortiClient fails to establish VPN connection if it cannot reach the internet until `<disable_internet_check>` is enabled.

Vulnerability Scan

Bug ID	Description
954584	EMS reports endpoint vulnerability when Vulnerability Scan feature is disabled or not installed on endpoint.

Multitenancy

Bug ID	Description
1052268	Site disappears from EMS after renaming.

Onboarding

Bug ID	Description
989006	Azure external user SAML authorization has issue with # character in the name.
997697	EMS denies endpoint registration attempt due to LDAP authentication failure.

Deployment and installers

Bug ID	Description
773672	Disabling installer ID in FortiClient installer does not take effect.
982536	When Entra ID device belongs to two Entra ID groups, deployment policy cannot match the endpoint.
1029510	EMS does not remove deployment checkmark when moving endpoints out of deployment groups.

Zero Trust tagging

Bug ID	Description
1003279	ZTNA AD tag evaluated on EMS does not work as expected with hybrid AD environment.
1008496	AD group zero trust tag rule stops working.
1024820	Deleting ZTNA tags temporarily unassigns other tags.
1037111	Zero Trust tagging rules do not allow for custom operating system versions.
1056225	EMS cannot use domain tag in Azure hybrid domain environment.

Endpoint control

Bug ID	Description
999081	When pushing endpoint certificates EMS also pushes `ZCONF` when that configuration is already up-to-date for the endpoint.
1002476	Disconnecting FortiClient from EMS using password does not work.
1014009	EMS blocks new reimaged renamed device from connecting to EMS when it is not in the endpoint list.

Performance

Bug ID	Description
955037	Searching for an endpoint takes up to five minutes.

Logs

Bug ID	Description
956383	Log files are not rotated based on log settings from the GUI.

Upgrade

Bug ID	Description
990711	Duplicate rule names display in *ZTNA Destination* after upgrading EMS from 7.2.2 to 7.2.3.
993235	After upgrading EMS from 7.2.1 to 7.2.3, FortiClient does not link the IP and MAC address information of the PC to the FortiGate.

GUI

Bug ID	Description
987768	*Zero Trust Tag Monitor* page has GUI issues.

Bug ID	Description
987926	Vulnerability Events are not visible on EMS GUI.
1004777	*Invitations* page displays error: *Server encountered an error.*

System Settings

Bug ID	Description
864900	Endpoint alerts send multiple emails for the same alert.
1019744	Signature and new installer download fails when *Enable SSL* is enabled in *FortiGuard Services*.
1045221	EMS fails to renew ACME certificate due to *"Default.fems.fsg-hosting.com": Domain name contains an invalid character* error.

Zero Trust Telemetry

Bug ID	Description
1023404	Classification tags IP address information does not update on FortiGate unless user deletes and readds tag on EMS.

Other

Bug ID	Description
872871	CSV export file is missing some fields.
914170	*Allowlist & Restore* option is missing under *Quarantine Management*.
976654	User cannot restore EMS from backup for same patch with different interim build number.
1019826	When a FortiClient switches VPN IP addresses, EMS receives the new IP address, then drops both connection entries in the database.

Common Vulnerabilities and Exposures

Bug ID	Description
959857	FortiClient EMS 7.2.5 is no longer vulnerable to the following CVE References: • CVE-2024-21753 Visit https://fortiguard.com/psirt for more information.
1024586	FortiClient EMS 7.2.5 is no longer vulnerable to the following CVE References: • CVE-2024-33508 Visit https://fortiguard.com/psirt for more information.

Known issues

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

Administration

Bug ID	Description
980584	Single sign on through AD Federation Services as identity provider does not function due to case-sensitive SAML response.
1064133	API error occurs when trying to download logs from EMS console.

Dashboard

Bug ID	Description
982452	EMS dashboard widgets have issues.

Endpoint management

Bug ID	Description
1067809	FortiClients deregister if domain is deleted.
1068273	Active Directory sync gets stuck at 1% on FortiClient Cloud.

Endpoint policy and profile

Bug ID	Description
1070260	Importing XML files with Remote Access elements changes the format of the on connect/disconnect scripts for VPN tunnels.

Install and upgrade

Bug ID	Description
1071351	Automatic upgrade notification does not display on EMS high availability GUI and primary node is upgraded while doing EMS failover.

System Settings

Bug ID	Description
1034235	FortiClient EMS tries to revoke expired ACME certificate when user clicks *Delete*.
1055766	FortiClient Cloud sends certificate expiry alert when the in-use certificate is not expiring.

GUI

Bug ID	Description
1054915	Performance issues occur when trying to filter endpoints, with each search taking over 40 seconds.

Upgrade

Bug ID	Description
995790	Android devices disappear from endpoints list after EMS upgrade.
1068441	DAS service stops after EMS upgrade to 7.2.4.

Onboarding

Bug ID	Description
1057130	macOS and iPhone endpoints do not stay verified in FortiClient Cloud if hostname changes.

Zero Trust tagging

Bug ID	Description
984598	Packet loss occurs when using firewall policy with ZTNA tags.

ZTNA connection rules

Bug ID	Description
1050090	User has issue accessing remote servers via RDP when they configure ZTNA TAG in firewall policy intermittently.

Other

Bug ID	Description
1040103	FortiClient Cloud delivers endpoint alerts in different time zone.

Numbering conventions

Fortinet uses the following version number format:

<First number>.<Second number>.<Third number>.<Fourth number>

Example: 7.2.5.15

- First number = major version
- Second number = minor version
- Third number = maintenance version
- Fourth number = build version

Release Notes pertain to a certain version of the product. Release Notes are revised as needed.

Change log

Date	Change description
2024-08-29	Initial release.
2024-10-09	Added Numbering conventions on page 23.

www.fortinet.com

Copyright© 2024 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.