

Release Notes

FortiClient EMS 7.2.9



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



May 28, 2025

FortiClient EMS 7.2.9 Release Notes

04-729-1140136-20250528

TABLE OF CONTENTS

Introduction	4
Endpoint requirements	4
Supported web browsers	5
Licensing and installation	5
Special notices	6
Microsoft Visual C++ installation	6
SQL Server Standard or Enterprise with 5000 or more endpoints	6
Split tunnel	6
SAML logins	6
FortiGuard Web Filtering category v10 update	7
DNS updates when using ZTNA	7
What's new	8
Upgrading	9
Upgrading from previous EMS versions	9
Microsoft SQL Express 2022 update	9
Downgrading to previous versions	10
Product integration and support	11
Resolved issues	13
Endpoint control	13
Endpoint management	13
License	14
Quarantine management	14
System Settings	14
Upgrade	14
ZTNA connection rules	15
Known issues	16
New known issues	16
Endpoint management	16
HA	16
Upgrade	17
Existing known issues	17
Numbering conventions	18
Change log	19

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 7.2.9 build 1193:

- [Special notices on page 6](#)
- [What's new on page 8](#)
- [Upgrading on page 9](#)
- [Product integration and support on page 11](#)
- [Resolved issues on page 13](#)
- [Known issues on page 16](#)

For information about FortiClient EMS, see the [FortiClient EMS 7.2.9 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 7.2.9 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 a newer version is 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 2022. See [Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise](#).

Split tunnel

In EMS 7.2.9, 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), EMS does not support configuring dynamic DNS (DDNS) updates as *Secure only*.

What's new

For information about what's new in FortiClient EMS 7.2.9, see the [FortiClient & FortiClient EMS 7.2 New Features Guide](#).

Upgrading

Upgrading from previous EMS versions



EMS 7.2.9 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 7.2.9.

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 7.2.9 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 7.2.9 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 7.2.9 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 7.2.9.

Microsoft SQL Express 2022 update

Included with EMS 7.2.9, Fortinet updated the Microsoft SQL Express version from 2017 to 2022. During the upgrade to EMS 7.2.9, the Microsoft SQL Server 2022 installer may fail to execute properly, causing the entire upgrade to fail. This issue is being reported externally to Fortinet in the [Microsoft community](#). You may attempt to manually install components one by one to complete a successful upgrade. The following provides steps to perform the install, assuming a starting EMS version of 7.2.4, 7.2.5, or 7.2.6:

To upgrade EMS to 7.2.9 manually:

1. If you are running a EMS as a virtual machine (VM), take a snapshot of the VM.
2. Manually download and install Microsoft Visual C++ Redistributable (x86 and x64) from one of the following and reboot the server:
 - https://aka.ms/vs/17/release/vc_redist.x86.exe
 - https://aka.ms/vs/17/release/vc_redist.x64.exe
3. Manually download and install Microsoft OLE DB or ODBC Driver for SQL Server from one of the following and reboot the server:
 - ODBC 17.10.6.1: <https://go.microsoft.com/fwlink/?linkid=2266337>
 - OLE DB 18.7.4: <https://go.microsoft.com/fwlink/?linkid=2278907>

Confirm access to the EMS GUI and the connected FortiClient endpoints.

4. Download [Microsoft SQL Server 2022 Express](#).
5. Run the *Microsoft SQL Express 2022 installer* > *Download Media* > *Express Advanced* > *Set the download location* > *Download*. A file of around 500 MB is downloaded.
6. Launch the downloaded installer from step 5. During the install, select *Upgrade from a previous version of SQL* > *Next* > *Accept the license* > *Next*. In *Select Instance*, ensure that EMS is detected and selected. Click *Next*, then wait 10-20 minutes for the upgrade to complete. When complete, reboot the server and confirm access to the EMS GUI and the connected FortiClient endpoints.
7. (Optional but recommended) Create another VM snapshot.
8. Run the EMS 7.2.9 installer as administrator to perform the upgrade. The upgrade skips the database upgrade or install phase and proceeds directly to upgrade EMS to 7.2.9. Confirm access to the EMS GUI and the connected FortiClient endpoints.
9. Reboot the server. Confirm access to the EMS GUI and the connected FortiClient endpoints.

Downgrading to previous versions

FortiClient EMS does not support downgrading to previous EMS versions.

Product integration and support

The following table lists version 7.2.9 product integration and support information:

Server operating systems	<ul style="list-style-type: none">• Windows Server 2025• Windows Server 2022
Minimum system requirements	<ul style="list-style-type: none">• 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. <p>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.</p>
FortiAnalyzer	<ul style="list-style-type: none">• 7.4.0 and later• 7.2.0 and later• 7.0.0 and later <p>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.</p>
FortiAuthenticator	<ul style="list-style-type: none">• 6.6.0 and later• 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)	<ul style="list-style-type: none">• 7.2.0 and later• 7.0.2 and later
FortiClient (macOS)	<ul style="list-style-type: none">• 7.2.0 and later• 7.0.2 and later
FortiClient (Windows)	<ul style="list-style-type: none">• 7.2.0 and later• 7.0.2 and later
FortiManager	<ul style="list-style-type: none">• 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 7.2.9. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Endpoint control

Bug ID	Description
1111238	Active Directory (AD) sync fails to update database sync object tables: <i>error deleting devices: invalid character 'F' after object key:value pair.</i>

Endpoint management

Bug ID	Description
1076058	Under <i>Administration > Authentication Servers</i> , you must edit the username and remove domain\ (or @domain) to authenticate via NTLM instead of Kerberos.
1109725	Administrators with custom admin roles cannot move endpoints between groups due to the missing <i>Move to</i> tab.
1110507	EMS does not use Kerberos authentication for LDAP and uses NTLM.
1112618	EMS fails to recognize endpoint as Microsoft Entra ID-joined devices and puts endpoint in workgroup instead of Entra ID group.
1116613	Invalid characters in filter by distinguished name causes LDAP result code 201 filter compile error.
1116767	Error: <i>mssql: Cannot insert duplicate key row in object 'dbo.Devices' with unique index 'uq_devices_guid' occurs.</i>
1116781	Error occurs when syncing LDAP after updating EMS.
1117228	LDAP sync fails due to long UPN char: <i>error: mssql: The data for table*valued parameter "@updated" doesn't conform.</i>
1118444	LDAPS sync error occurs: <i>spUpdateDomainUsers on 'uq_users_uid_name_sid_saml_id_auth_type_upn_domain_id'.</i>
1139290	EMS AD sync intermittently fails with bind parameter and Kerberos errors.

License

Bug ID	Description
1111045	Notification for expiring license shows even when new license has been uploaded.

Quarantine management

Bug ID	Description
1126306	Duplicate hosts display in <i>Quarantine Management</i> when selecting <i>Display by Host</i> .

System Settings

Bug ID	Description
1082865	When configuring SMTP server authentication over STARTTLS, EMS does not accept configuration with or without username and password.

Upgrade

Bug ID	Description
995790	During device upgrade check, duplicate Android devices are mistaken as duplicates and deleted.
1074319	Upgrade fails when EMS is installed in non-default folder.
1135642	You cannot upgrade EMS from before a version earlier than 7.0.8 to 7.2.7 or later.

ZTNA connection rules

Bug ID	Description
1103786	EMS does not support of underscore on zero trust network access (ZTNA) destinations.
1115649	You cannot delete leftover ZTNA application catalog entries when EMS is part of a high availability cluster and connected to FortiGate.
1118615	Adding ZTNA rules in ZTNA destination profile automatically creates a manually created ZTNA application in application catalog.
1133163	EMS fails to create ZTNA application due to long FQDN.

Known issues

Known issues are organized into the following categories:

- [New known issues on page 16](#)
- [Existing known issues on page 17](#)

To inquire about a particular bug or to report a bug, contact [Customer Service & Support](#).

New known issues

The following issues have been identified in version 7.2.9.

Endpoint management

Bug ID	Description
1135123	EMS cannot add LDAP administrator and import user or device from domain, with <i>Invalid idp guid</i> error.
1139723	LDAP sync needs improvement to reduce the number of binds.
1148779	EMS has following LDAP sync error: <code>uq_users_uid_name_sid_saml_id_auth_type_upn_domain_id</code> .
1149494	EMS gives internal error when FortiClient connects to it.
1151701	Chromebook constantly shuts down.

HA

Bug ID	Description
1146646	EMS high availability (HA) reports license sync error despite valid hardware ID and product registration.

Upgrade

Bug ID	Description
1139102	Error occurs when syncing LDAP after upgrading EMS to 7.2.8.

Existing known issues

No existing issues remain in EMS 7.2.9.

Numbering conventions

Fortinet uses the following version number format:

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

Example: 7.2.9.15

- 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
2025-04-08	Initial release.
2025-04-21	Added License on page 14.
2025-05-28	Updated New known issues on page 16.



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.