Release Notes

FortiClient EMS 7.2.13

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
2026-01-19	Initial release.
2026-02-13	Updated Product integration and support on page 12.

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 7.2.13 build 1268:

- Special notices on page 7
- What's new on page 9
- Upgrading on page 10
- Product integration and support on page 12
- Resolved issues on page 14
- Known issues on page 15

For information about FortiClient EMS, see the *FortiClient EMS 7.2.13 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 12 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 7.2.13 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 7.2.13, 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*.

Entra ID integration support limitation

FortiClient EMS supports Entra ID integration with Azure commercial subscription only. Azure Government (e.g. GCC, GCC High, GCC DoD) is not supported.

Web filter profile import limitation

FortiClient EMS 7.2 does not support importing web filter profiles from FortiOS 7.6.4 or later.

What's new

For information about what's new in FortiClient EMS 7.2.13, see the FortiClient & FortiClient EMS 7.2 New Features Guide.

Upgrading

Upgrading from previous EMS versions

> EMS 7.2.13 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 7.2.13.

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 7.2.13 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 7.2.13 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 7.2.13 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 7.2.13.

Microsoft SQL Express 2022 update

Included with EMS 7.2.13, Fortinet updated the Microsoft SQL Express version from 2017 to 2022. During the upgrade to EMS 7.2.13, 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 7.2.13 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 7.2.13 installer as administrator to perform the upgrade. The upgrade skips the database upgrade or install phase and proceeds directly to upgrade EMS to 7.2.13. 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 7.2.13 product integration and support information:

Server operating systems	• Windows Server 2025 • Windows Server 2022
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	• 6.6.0 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 (Windows/macOS/Linux)	The following FortiClient versions are recommended: • 7.2.0 - 7.2.13 • 7.0.0 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 issue has been fixed in version 7.2.13. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Installation and Upgrade

Bug ID	Description
1167266	Unable to install EMS 7.2.10 on another drive via PowerShell.

Known issues

Known issues are organized into the following categories:

To inquire about a particular bug or to report a bug, contact Customer Service & Support.

New known issues

No new issues have been identified in version 7.2.13.

Existing known issues

The following issues have been identified in a previous version of FortiClient EMS and remains in FortiClient EMS 7.2.13.

Endpoint control

Bug ID	Description
1213829	FortiClient auth-period registry is not reset to 0 after *User Verification Period* is disabled in EMS.

Endpoint policy and profile

Bug ID	Description
1229556	No support for importing web filter profiles from FortiOS 7.6.4 or later.

Numbering conventions

Fortinet uses the following version number format:

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

Example: 7.2.13.15

- 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.