FortiClient EMS - Release Notes

Version 6.4.8

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

March 30, 2022
FortiClient EMS 6.4.8 Release Notes
04-648-789527-20220330

TABLE OF CONTENTS

Introduction **4**
Endpoint requirements 4
Supported web browsers 4
Licensing and installation 5
Special notices **6**
FortiClient EMS Microsoft Visual C++ installation 6
SQL Server Enterprise with 5000 or more endpoints 6
Split tunnel 6
Upgrading **7**
Upgrading from previous EMS versions 7
Downgrading to previous versions 7
Product integration and support **8**
Resolved issues **9**
Endpoint control 9
Endpoint management 9
Endpoint policy and profile 9
Install and upgrade 9
GUI 10
Multitenancy 10
Zero Trust tags 10
Known issues **11**
Administration 11
Endpoint control 11
Endpoint management 11
Endpoint policy and profile 12
Installation and upgrade 12
Remote access 12
Vulnerability Scan 12
Web Filter 12
Zero Trust Telemetry 13
Other 13
Change log **14**

Introduction

FortiClient Endpoint Management Server (EMS) is a system intended to be used to manage installations of FortiClient. 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 6.4.8 build 1753:

- Special notices on page 6
- Upgrading on page 7
- Product integration and support on page 8
- Resolved issues on page 9
- Known issues on page 11

For information about FortiClient EMS, see the *FortiClient EMS 6.4.8 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 8 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 6.4.8 GUI:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Internet Explorer is not recommended. Remote access may need to be enabled from the FortiClient EMS GUI.

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

FortiClient EMS 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 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 6.4.8, 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.

Upgrading

Upgrading from previous EMS versions

You must upgrade EMS to 6.4.8 before upgrading FortiClient.

FortiClient EMS supports direct upgrade from EMS 6.2. To upgrade older EMS versions, follow the upgrade procedure that *FortiClient and FortiClient EMS Upgrade Paths* outlines.

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

Downgrading to previous versions

FortiClient EMS does not support downgrading to previous EMS versions.

Product integration and support

The following table lists version 6.4.8 product integration and support information:

Server operating systems	• Windows Server 2022 • Windows Server 2019. On Windows Server 2019, preinstalling Microsoft ODBC Driver 17 for SQL Server (x64) is necessary. • Windows Server 2016 • Windows Server 2012 R2
Minimum system requirements	• 2.0 GHz 64-bit processor, six virtual CPUs (6 vCPU) • 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	• 7.0.0 and later • 6.4.0 and later
FortiClient (Linux)	• 6.4.0 and later • 6.2.0 and later
FortiClient (macOS)	• 6.4.0 and later • 6.2.0 and later
FortiClient (Windows)	• 6.4.0 and later • 6.2.0 and later
FortiOS	• 6.4.0 and later • 6.2.0 and later
FortiSandbox	• 4.0.0 and later • 3.2.0 and later • 3.1.0 and later

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

Resolved issues

The following issues have been fixed in version 6.4.8. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
771940	FortiClient Cloud is down and does not let user log in until instance is rebooted.

Endpoint management

Bug ID	Description
779309	Domain synchronization fails.

Endpoint policy and profile

Bug ID	Description
774890	FortiClient does not receive updated profile after syncing the imported Web Filter profile on EMS.

Install and upgrade

Bug ID	Description
719991	EMS with remote SQL database fails to upgrade.
766910	EMS install service account password length.

GUI

Bug ID	Description
632427	Software Inventory filter and sorting action in heading does not work.

Multitenancy

Bug ID	Description
770119	FortiClient EMS does not move licenses between sites.

Zero Trust tags

Bug ID	Description
731548	EMS does not update FortiGate when FortiClient disconnects from EMS.

Known issues

The following issues have been identified in version 6.4.8. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Administration

Bug ID	Description
745854	Superadministrators convert to site administrators after enabling multitenancy.
764149	When EMS tries to sync its license from FortiCloud, there is an API error.

Endpoint control

Bug ID	Description
764664	FortiClient falls out of sync with EMS.

Endpoint management

Bug ID	Description
680577	EMS shows limited additional user information for Active Directory endpoint.
691790	EMS allows user to download requested diagnostic result for FortiClient (Linux).
717433	Patching a vulnerability for a specific endpoint patches it on other endpoints.
724865	EMS displays duplicate Android endpoints.
764999	EMS lists FortiClient versions in its official installer list that the FortiGuard distribution server blocks EMS from downloading.
770364	EMS does not support displaying third-party feature details for non-Windows endpoints, but displays that section in endpoint details.

Endpoint policy and profile

Bug ID	Description
777067	EMS does not import Web Filter profiles from FortiGate if login banners are enabled.

Installation and upgrade

Bug ID	Description
754722	Uninstall deployment from EMS does not work on FortiClient 6.4.6.
756267	User cannot delete a custom installer if its name includes a space.

Remote access

Bug ID	Description
790404	FortiClient GUI is missing SAML button.

Vulnerability Scan

Bug ID	Description
740041	EMS does not clearly display the filepath and applications associated with vulnerabilities for centralized management.

Web Filter

Bug ID	Description
793017	Web Filter disconnects an application's underlying connection.

Zero Trust Telemetry

Bug ID	Description
763957	FortiClient prompts for Telemetry key when Telemetry key changes on EMS.

Other

Bug ID	Description
650993	EMS does not provide a way to clean uploaded FortiClient logs and diagnostic logs that EMS requests.

Change log

Date	Change description
2022-03-30	Initial release.

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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 General Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.