



FortiClient EMS - Release Notes

Version 6.4.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 27, 2020

FortiClient EMS 6.4.0 Release Notes

04-640-626303-20200827

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
What's new	7
Upgrading	8
Upgrading from previous EMS versions	8
Downgrading to previous versions	8
Product integration and support	9
Resolved issues	10
AD domain	10
Administration	10
Group assignment	10
Endpoints	11
Endpoint policy and profile	11
Cloud	11
Deployment	11
GUI	12
Other	12
Known issues	13
Administration	13
Deployment	13
Endpoints	13
Endpoint policy and profile	14
AD domains	14
EMS API	14
Other	14
Change log	15

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, and Chrome OS. FortiClient EMS runs on a Microsoft Windows server.

This document provides the following information for FortiClient EMS 6.4.0 build 1429:

- [Special notices on page 6](#)
- [What's new on page 7](#)
- [Upgrading on page 8](#)
- [Resolved issues on page 10](#)
- [Known issues on page 13](#)

For information about FortiClient EMS, see the [FortiClient EMS 6.4.0 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 9](#) 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 6.4.0 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 version of VC 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 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](#).

What's new

For information about what's new in FortiClient EMS 6.4.0, see the [FortiClient & FortiClient EMS 6.4.0 New Features](#).

Upgrading

Upgrading from previous EMS versions

FortiClient EMS supports direct upgrade from EMS 6.2. To upgrade older EMS versions, follow the upgrade procedure outlined in [FortiClient and FortiClient EMS Upgrade Paths](#).

Downgrading to previous versions

FortiClient EMS does not support downgrading to previous EMS versions.

Product integration and support

The following table lists version 6.4.0 product integration and support information:

Server operating systems	<ul style="list-style-type: none">• Windows Server 2019• Windows Server 2016• Windows Server 2012 R2
Minimum system requirements	<ul style="list-style-type: none">• 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)• 4 GB RAM (8 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 will also try 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>
FortiClient (Linux)	<ul style="list-style-type: none">• 6.4.0• 6.2.0 and later
FortiClient (macOS)	<ul style="list-style-type: none">• 6.4.0• 6.2.0 and later
FortiClient (Windows)	<ul style="list-style-type: none">• 6.4.0• 6.2.0 and later
FortiOS	<ul style="list-style-type: none">• 6.4.0• 6.2.0 and later
FortiSandbox	<ul style="list-style-type: none">• 3.2.0 (for detailed reports on files that FortiSandbox has detected)• 3.1.0 and later (for detailed reports on files that FortiSandbox has detected)• 3.0.0 and later• 2.5.0 and later



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

Resolved issues

The following issues have been fixed in version 6.4.0. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

AD domain

Bug ID	Description
590620	AD workstation shows under <i>Workgroups > All endpoints</i> .
601478	Syncing AD subdomain with empty distinguished name causes LDAP referral error.
607705	EMS policy is not being applied to sub-containers.

Administration

Bug ID	Description
581552	Admin role permission updates.
599429	Diagnostic tool takes a long time to export event logs.
599933	FortiCloud region list is null.
601549	Administrator can add invalid user server configuration.
604438	User server concatenates the subdomain to root domain.

Group assignment

Bug ID	Description
589524	Unable to run group assignment rules to add 8000+ FortiClient endpoints to a workgroup.
598321	Group assignment rule throws an uncaught TypeError when a group is not selected.

Endpoints

Bug ID	Description
599710	Web Filter logs are garbled in FortiClient EMS.
607717	Installer keeps EMS registration password in plain text.
611733	Switching profiles on a Chromebook policy does not apply to endpoints.
617254	EMS fails to enable diagnostic log for USB and Web Filter.

Endpoint policy and profile

Bug ID	Description
578138	You cannot change EMS policy priority from EMS console.
583974	Policy screen requires you to click <i>Save</i> twice to save updated on-net detection rules.
585385	Cannot import profiles from FortiGate/FortiManager in EMS console.
608140	EMS should allow using imported FortiGate Web Filter profile as Chromebook Web Filter profile.

Cloud

Bug ID	Description
604742	FortiClient connected to FortiClient Cloud shows no vulnerability feature.
606618	FCEMS update daemon restarts continuously in FortiClient Cloud.

Deployment

Bug ID	Description
579422	FortiClient deployment is stuck showing <i>Install Error</i> .

GUI

Bug ID	Description
589823	Hide <i>Software Update</i> option from GUI.
612239	Low screen resolution prevents EMS from displaying all event tabs correctly.

Other

Bug ID	Description
539561	Error message from an incomplete API call shows sensitive/critical information.
553323	EMS Apache logs fill up server storage.
579693	EMS host verification rule for vulnerability should be specified differently.
597423	FortiGate reports <i>error -3: EMS REST API</i> when adding EMS in Security Fabric.
616350	EMS does not check FortiSandbox user permission for RPC JSON API function.

Known issues

The following issues have been identified in version 6.4.0. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Administration

Bug ID	Description
596653	EMS does not generate email notification for out-of-date AV signatures.
611069	EMS does not import the certificate chain from a PFX file.
624207	Trial license shows incorrect number of seats in the GUI module.
624810	Profile log settings show settings for all features when only partial features are enabled in EMS.

Deployment

Bug ID	Description
639631	Unable to configure feature selection for deployment packages.
639676	No configuration when installing FortiClient 6.4.0 using MSI and MST.

Endpoints

Bug ID	Description
596933	EMS shows another user avatar when no user is logged in.
609466	EMS endpoints event counter is not correct.
610892	Loading next 50 items in Software Inventory does not work.
614763	Customized block page reverts to default after upgrade.
614823	Vulnerability scan events do not show in EMS.

Endpoint policy and profile

Bug ID	Description
619635	EMS should not allow user to change Web Filter category action setting when it is synced from FortiGate or FortiManager.
621687	<i>Enable Web Browser Plugin</i> for Web Filter setting does not display properly.
628978	EMS fails to update FortiClient avatar after registration.

AD domains

Bug ID	Description
576108	Active Directory (AD) distinguished name parsing problems.
600069	EMS does not reflect change in domain structure when endpoint moves to a different organizational unit in AD.
600379	EMS domain stops syncing.
614582	GUI does not load if syncing or deleting domain.

EMS API

Bug ID	Description
630602	Unable to display FortiClient record on FortiGate when connected to EMS using EMS API.

Other

Bug ID	Description
596403	FcmDaemon causes high CPU usage.
630903	Remote database installation fails with <i>Provider cannot be found</i> error.

Change log

Date	Change Description
2020-05-12	Initial release.
2020-05-25	Added 630602 to Known issues on page 13 .
2020-08-10	Added 639631 and 639676 to Known issues on page 13 .
2020-08-13	Updated Licensing and installation on page 5 .
2020-08-17	Updated Product integration and support on page 9 .
2020-08-27	Updated Product integration and support on page 9 .



FORTINET®



Copyright© 2020 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.