FortiClient EMS - Release Notes

Version 6.4.3

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://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 18, 2021
FortiClient EMS 6.4.3 Release Notes
04-643-690106-20210318

TABLE OF CONTENTS

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 6.4.3 build 1600:

- Special notices on page 6
- Upgrading on page 7
- Resolved issues on page 9
- Known issues on page 13

For information about FortiClient EMS, see the *FortiClient EMS 6.4.3 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 6.4.3 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 the *FortiClient EMS Administration Guide*.

Split tunnel

A split tunnel configuration that functioned in FortiClient (Windows) 6.4.1 no longer works after upgrading to 6.4.3, unless you have configured a per-tunnel configuration in EMS.

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*.

FortiClient EMS 6.4.3 GA supports upgrade from FortiClient EMS 6.4.3 RC1 and RC2.

Downgrading to previous versions

FortiClient EMS does not support downgrading to previous EMS versions.

Product integration and support

The following table lists version 6.4.3 product integration and support information:

Server operating systems	• 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, four virtual CPUs (4 vCPU) • 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. 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	• 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	• 3.2.0 and later (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 6.4.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Deployment

Bug ID	Description
690949	Deployment gets stuck on protocol schedule created.

License management

Bug ID	Description
666925	Freshly installed EMS reports global site is using all license seats.
675005	EMS reassigns all license seats to the default site after manually syncing license.
685471	EMS should not return no licenses available when it cannot read licenses.

Endpoint management

Bug ID	Description
668851	EMS fails to display IP address for endpoints when they are moved from a workgroup to an LDAP domain organizational unit (OU).
674145	IPsec VPN tunnel that EMS pushed does not work properly.
678542	User identity and social network zero trust tags do not work.
682739	Endpoint summary displays scheduled time with value "invalid date" when user modifies the installation schedule.
686304	EMS does not show list of endpoints under All endpoints.
688061	EMS shows duplicate device in endpoint list if a hostname has more than 15 characters.
689379	Profile is not updated if a workstation is moved to a different organizational unit (OU) in Active Directory (AD) and there is no domain user associated with the device.
691002	Excluding an endpoint from management fails to work.

Endpoint policy and profile

Bug ID	Description
678922	Endpoint policy takes several minutes to save.
684377	Policy with empty groups does not take preference over default policy.
686311	Endpoint policies disappear if assigned to OU with \ character in name.
688993	*Enable Web Browser Plugin* is disabled on profile *Web Filter* tab when syncing Web Filter profile from FortiOS or FortiManager.

Upgrade

Bug ID	Description
690845	EMS fails to login after upgrade from previous GA build.

GUI

Bug ID	Description
647531	No site information for telemetry server list.
663742	FortiClient installers default directory allows access to list of installers from all sites.
688213	Browser console throws exception when deleting a Google domain.

FortiClient Cloud

Bug ID	Description
585763	User cannot log in to FortiClient Cloud if they used the same browser used for logging into on-premise EMS.

AD domains

Bug ID	Description
647407	Computers deleted from Active Directory domain still show in EMS endpoint list.
686147	LDAP sync errors for computers moved into custom groups under domain.

Administration

Bug ID	Description
673178	Settings Administrator user role has SAML SSO setting available but no permissions to it.
674276	Display EMS FSSO Settings only in global settings when multitenancy is enabled.
682286	SMTP server settings show optional fields as required.
689060	User cannot save Chromebook system settings.
689251	Database restore from older EMS version removes SSL certificate in EMS settings.
689971	Update *Add User* control in FortiClient Cloud user interface.

System

Bug ID	Description
634581	FortiClient EMS session cookie does not expire after logout.
664087	EMS duplicate key in object"dbo.group_container".
669746	Converting the nvarchar value "FW" to data type int fails.
685012	spUpdateIPlist() and spUpdateAvatar() deadlocks generated on fcmdaemon.
685565	Deadlocks on FCM daemon cause FortiClient to have all features removed.
685974	FcmDaemon crashes when multitenancy is enabled.

Other

Bug ID	Description
683512	macOS Big Sur reported version.

Bug ID	Description
673375	EMS fails to configure HID class for removable media access.
682708	Login banner is disabled after EMS upgrade.

Common Vulnerabilities and Exposures

Bug ID	Description
685625	FortiClient EMS 6.4.3 is no longer vulnerable to the following CVE Reference: • CVE-2020-1971 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in version 6.4.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Endpoint management

Bug ID	Description
686308	User-based policy does not work assigned to security user groups.
689682	Device in Zero Trust Tag Monitor shows future timestamp.
690890	Endpoint search only shows the first 50 results.

GUI

Bug ID	Description
614445	Add option for a default tab to GUI and XML.
678471	Group assignment rules do not work automatically for installer ID.
684209	GUI is inaccessible after uploading SSL certificate.

Administration

Bug ID	Description
677679	EMS sends duplicate email alerts.
688708	User cannot back up EMS database after enabling multitenancy.

AD domains

Bug ID	Description
576108	Distinguished name (DN) parsing problems.
608500	AD groups do not show syncing to AD server.
649002	AD sync fails when adding device with more than 256 characters in DN.
668190	Endpoint does not show in domain OU.
677247	EMS shows multiple records of same domain when AD domain is added.
681244	Saving a Zero Trust Tagging rule in GUI is inconsistent for AD Group and User Identity rule types.
682159	EMS shows empty Security Groups when LDAP query reaches value (MaxValRange) limit.
686211	Endpoint registered to EMS is moved into original OU from custom domain group.

FortiClient Cloud

Bug ID	Description
680940	FortiClient Cloud does not accurately record the IP addresses of the EMS administrators that log in.

License management

Bug ID	Description
697036	After upgrading to 6.4.3, the License Information widget on the Dashboard may incorrectly show the Next Generation Endpoint Security License status as unlicensed even though the EPP license is active and working. This is a display issue and the EPP feature will continue to work on a licensed EMS.

Other

Bug ID	Description
681744	FortiOS fails to set up Security Fabric connector with EMS after upgrade. Workaround: When EMS reaches this broken state, you must do one of the following:

Bug ID	Description
	- Reupload the certificate. Reuploading the certificate causes the certificate to be saved in server.crt and correctly applied. - Delete the user certificate from the GUI. This causes EMS to use the FortiCare certificate, making the configuration match what it was prior to the upgrade. You should only see this issue when upgrading from 6.4.1 to a later 6.4 version. Upgrading from 6.4.2 to 6.4.3 should result in the correct certificate being applied.
687815	Changing FQDN deletes files in EMS installation directory.

Change log

Date	Change Description
2021-02-09	Initial release.
2021-02-16	Updated Known issues on page 13.
2021-02-17	Added 697036 to Known issues on page 13.
2021-02-19	Updated 681744 in Known issues on page 13.
2021-03-18	Added Split tunnel on page 6.