FortiClient EMS - Release Notes

Version 6.4.7

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/training-certification

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

November 25, 2021
FortiClient EMS 6.4.7 Release Notes
04-647-758984-20211125

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 6.4.7 build 1714:

For information about FortiClient EMS, see the *FortiClient EMS 6.4.7 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 6.4.7 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

Endpoint security improvement

EMS 6.4.7 adds an improvement to endpoint security that impacts compatibility between FortiClient and EMS, and the recommended upgrade path. The FortiClient 6.4.7 installer is available on FortiGuard Distribution Servers (FDS). EMS 6.4.7 can retrieve FortiClient 6.4.7 from FDS. Older versions of EMS 6.4 will not be able to download FortiClient 6.4.7 from the FDS.. See Endpoint security improvement.

If the EMS server certificate is invalid, and FortiClient is upgraded to 6.4.7, by default, FortiClient displays a warning message on the GUI when trying to connect to the EMS. The end user should click *allow* to complete the connection. FortiClient does not connect to the EMS if the end user selects *deny*. If the end user selects *deny*, FortiClient retries connecting to the EMS after a system reboot. The same warning message displays while trying to connect to the EMS. The end user should click *allow* to complete the connection.

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 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 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 6.4.7, unless you have configured a per-tunnel configuration in EMS.

What's new

For information about what's new in FortiClient EMS 6.4.7, see the *FortiClient & FortiClient EMS 6.4 New Features*.

Upgrading

Upgrading from previous EMS versions

You must upgrade EMS to 6.4.7 before upgrading FortiClient.

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*.

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 6.4.7 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 6.4.7. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Deployment

Bug ID	Description
698222	LDAP organization units do not show correctly in *Edit Groups* of deployment package wizard.
719855	Incompatible FortiClient custom installers cause all deployment packages to be unviewable in the GUI.
725298	EMS upgrade removes FortiClient installers.
731440	Creating a deployment package zip file takes a long time.
739705	Deployment issue with FortiClient (macOS).
754104	Changing FortiClient version in a deployment package does not generate new installer ID.

Endpoint management

Bug ID	Description
671073	Improve endpoint modification management behavior.
697136	EMS cannot connect to LDAP server.
721644	*Mark as Uninstalled* action should be unavailable for managed endpoints.
722445	Endpoint shows up as online when it is not currently connected to EMS.
724616	Domain synchronization fails with *The distinguished name contains invalid syntax.* error.
736098	EMS shows *not latest AV signature version system* event.
738000	EMS shows duplicate entry for domain-joined machine after reimaging.
742731	EMS does not show vulnerability events for endpoints.
757059	Active Directory synchronization fails with NullReferenceException after synchronizing a container with no parent GUID.
746746,723902	LDAP sync issue after upgrading EMS.

Endpoint policy and profile

Bug ID	Description
697911	Synchronized updates from imported FortiGate Web Filter profile do not synchronize to FortiClient.
698632	Removable media access rule does not work.
714479	Antiexploit exceptions do not work.
722093	Chromebook profile converts to normal profile after XML editing without saving.
723465	Profile does not synchronize IPsec VPN phase 2 configuration to FortiClient.
724453	*Prompt for Certificate* does not set the correct XML setting. Setting the GUI option to false sets it to true in the backend.
727769	*Sort by Policy Name Filter* is broken.

Upgrade

Bug ID	Description
719991	EMS with remote SQL database fails to upgrade.
726610	Zero Trust tagging rule does not work after EMS upgrade.
742359	Upgrade fails with *FCM.dbo.admin_user_old_passwords; column does not allow nulls*.

GUI

Bug ID	Description
659389	Enabling Windows operating system (OS) widget on dashboard stalls the GUI.
690188	User cannot enable or disable *EMS Settings* > *Show FortiGate Server List* by clicking the *Save* button once.
714580	Sandbox Events *View Detail* and *Download PDF report* buttons do not work.
724642	EMS does not show any users/administrators.
736591	Vulnerabilities detected on FortiClient do not match the record on EMS.
740763	FortiOS API optimization.
742168	*Administrators* page is empty after importing user from LDAP server.

FortiClient Cloud

Bug ID	Description
731201	FortiClient Cloud clients lose connection.
733271	Invalid object name `dbo.cloud_settings` when sending global email alerts on FortiClient Cloud.
748476	FortiClient Cloud SMTP test fails to send notification email with Microsoft.

Dashboard

Bug ID	Description
724870	Linux servers do not display in dashboard widgets.

Multitenancy

Bug ID	Description
718122	*License capacity cannot be below the number of active endpoints. Please disconnect some endpoints first* error.
721823	Deployment status always shows as *Endpoint Notified*.
741560	Licenses for all endpoints are retracted.
745774	After enabling multitenancy, EMS is stuck in the loop of creating the database for that site.

Zero Trust tags

Bug ID	Description
708386	Zero trust tag should not automatically add Google account when user specified is selected after saving.
727199	OS tag rule for macOS 12 Monterey.
745234	Zero Trust tags do not list Windows 11 in OS versions.

Other

Bug ID	Description
718276	VCM engine is missing for Windows.
720394	FCMChromebookDaemon crashes.
727078	impipsdb.exe process crashes.
727945	FortiClientEndpointManagementServer.exe crashes when launched on Windows Server 2016 Standard.
735949	Domain administrator credentials used in deployment can be seen in HTTP GET request response.
739326	FcmUpdateDaemon.exe high disk I/O.

Common Vulnerabilities and Exposures

Bug ID	Description
746418	FortiClient EMS 6.4.7 is no longer vulnerable to the following CVE Reference: • CVE-2021-3711 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in version 6.4.7. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Multitenancy

Bug ID	Description
722144	FortiClient cannot connect to non-default site after EMS administrator deletes non-default site and recreates it.

Dashboard

Bug ID	Description
717433	Patching a vulnerability for a specific endpoint patches it on other endpoints.
725170	EMS does not show vulnerabilities detected on FortiClient.
737139	Endpoint connection widget reports fewer endpoints.
759776	EMS does not remove vulnerability events after successful patch.

Endpoint management

Bug ID	Description
705010	EMS shows endpoints with incorrect username.

Endpoint policy and profile

Bug ID	Description
720348	EMS hides *Show "Always Up"* when *Auto Connect Only When Off-Fabric* is enabled in VPN settings.

Bug ID	Description
737592	EMS overwrites XML configuration.
746469	Creating an SSL VPN tunnel manually with XML does not pass the certificate check details to the main XML configuration.
750022	Real-time protection *Delete* option does not delete file nor prompt for virus detection.
751718	FortiManager/FortiGate Web Filter syncing misbehavior.

Administration

Bug ID	Description
702712	*Cannot enumerate AD Domain until email alert is sent for previous error* warning errors in EMS logs.

Fabric Devices

Bug ID	Description
682639	EMS does not update its Fabric Devices state after authorizing a FortiGate.
708672	FortiGate can only show one latest SSL VPN FortiClient in endpoint record list and only this FortiClient receives dynamic address.
718145	Endpoint record entries disappear from FortiOS when using EMS tags.
731548	EMS does not update FortiGate when FortiClient disconnects from EMS.

Zero Trust tags

Bug ID	Description
705411	Active Directory group Zero Trust tagging rule gives inconsistent results.
743765	Zero Trust tag does not save value.

System Settings

Bug ID	Description
700462	FortiClient download URL refresh button fails to get new IP address and GUI console shows error 400.
729499	EMS sends *Endpoints failing to update AV signatures* and *AV Out-of-Date* email notifications.
745913	SMTP configuration fails authentication.
752052	EMS does not send alert emails.

Change log

Date	Change Description
2021-11-25	Initial release.