FortiClient EMS - Release Notes

Version 6.2.3

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://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

January 24, 2020
FortiClient EMS 6.2.3 Release Notes
04-623-597454-20200124

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 6.2.3 build 0875:

For information about FortiClient EMS, see the *FortiClient EMS 6.2.3 Administration Guide*.

FortiClient EMS 6.2.3 images will be available for download from FortiGuard starting the week of January 6, 2020. Currently, the images are available for download directly from the Fortinet Support site.

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 6.2.3 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*.

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 is installed with EMS by default. Otherwise, you may experience database deadlocks. The minimum SQL Server version that FortiClient EMS supports is 2014. It is recommended to use SQL Server 2017 or a later version. See the *FortiClient EMS Administration Guide*.

Upgrading

Upgrading from previous EMS versions

FortiClient EMS supports upgrading from previous EMS versions as outlined in *FortiClient and FortiClient EMS Upgrade Paths*. After upgrading from FortiClient EMS 6.0, you cannot make changes to the FortiClient Enterprise Management Server license. Increasing the number of managed endpoints requires you to purchase a new FortiClient Security Fabric Agent license.

Downgrading to previous versions

FortiClient EMS EMS does not support downgrading to previous EMS versions.

Product integration and support

The following table lists version 6.2.3 product integration and support information:

Server operating systems	• Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2
Minimum system requirements	• 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 required during installation 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.
FortiClient (Linux)	• 6.2.0 and later • 6.0.0 and later
FortiClient (macOS)	• 6.2.0 and later • 6.0.1 and later
FortiClient (Windows)	• 6.2.0 and later • 6.0.0 and later
FortiOS	• 6.2.0 and later • 6.0.0 and later
FortiSandbox	• 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 6.2.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

EMS administration

Bug ID	Description
572762	User server LDAP query does not work with specific organizational unit (OU) DN used.

EMS installation and upgrade

Bug ID	Description
573360	Upgrading EMS using a remote SQL server does not work.
577222	Upgrade from 6.0.6 to 6.2.1 fails.
585704	Upgrading results in being unable to log in to EMS.
587602	Non-clean EMS messes up database when importing databases exported from older GA releases.
588172	A Fortinet Security Fabric-only and premium cloud account should not be able to see Cloud Sandbox enabled after upgrade.
588434	Installer package reverts to older version when auto-update option is enabled.
590271	Upgrade fails from duplicate key in *dbo.endpoint_policies*.
591230	Upgrade fails to duplicate key for object name *dbo.ad_groups_users* and index name *uq_ad_groups_users_ids*.

Endpoints

Bug ID	Description
565986	Microsoft Edge misses expiry day for invitation code.
575344	Endpoint OU membership reverts to original OU.

Bug ID	Description
577797	Unquarantine does not work.
579348	*Host Tag Monitor* does not show any devices when complication verification rules are configured.
579436	Incomplete OS information for domain-joined macOS devices.
579700	EMS displays vulnerabilities that require manual patch as scheduled.
588141	FortiClient Cloud with Sandbox-only license asks for Sandbox license to use feature.
591101	Policy shows that it is not synced after syncing with FortiClient.
591730	GUI out-of-sync count differs from the list.
594625	Group assignment rules do not work in FortiClient Cloud.

Endpoint policy and profile

Bug ID	Description
578138	Cannot change policy priority.
582026	EMS pushes disabled on-net subnet detection rules to endpoints.
589304	EMS upgrade wipes all existing policies and newly created policies do not become visible in the GUI.
590103	EMS assigns default profile to OUs after upgrade.

FortiClient deployment

Bug ID	Description
580620	Installer ID is missing on deployment package creation.
580752	Deployment broken on policy without a group is created.
584843	FortiClient Cloud cannot deploy new FortiClient to registered endpoints.

FortiCare

Bug ID	Description
587534	FortiClient Cloud does not update master user permissions after changing the master user in

Bug ID	Description
	FortiCare.
596617	Error 500 while trying to sync with FortiCare account license.
597739	Cannot log in to FortiClient Cloud.
598904	EMS shows wrong license information after EMS deletes FortiCare user account.

GUI

Bug ID	Description
591697	Cloud services region is blank after upgrade, causing EMS to give error when saving profile changes.

Other

Bug ID	Description
579662	Host verification rule for macOS is missing version 10.15 Catalina for OS version.
582957	EMS log reports *Failed to sync FortiSandboxes: 'type' object is not subscriptable* error message.
585162	EMS remote login with Edge does not work.

Known issues

The following issues have been identified in version 6.2.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

EMS administration

Bug ID	Description
563305	Permission denied for user with limited admin role.
577368	Using LDAP users as EMS users causes duplicate `admin_user` records.
581907	*Add User* button goes to the wrong page.
592677	Restore does not work, failing on large backup files.
599859	EMS fails to allow access using admin credentials.

EMS installation and upgrade

Bug ID	Description
470172	EMS proxy settings do not work for FDS updates.
578016	Unable to access EMS after upgrade.
579255	Keeping a deployment package updated to the latest patch is visible for all patches.
592458	Downloading available FortiClient logs does not work after upgrade.
594798	Installer limitation and disk size check.

Endpoints

Bug ID	Description
576108	Distinguished name (DN) parsing problems.
585648	Host verification tags are present in EMS but missing in FortiOS.
587344	EMS Web Filter custom default message shows categorized as unrated URL when FortiGuard is inaccessible.

Bug ID	Description
588212	macOS endpoint in domain shows up in workgroups in EMS.
588710	EMS fails to report combined host verification rule match.
588716	Unable to delete custom group if it is not empty.
590620	Domain computer displays under workgroups.
592450	Selecting *All Endpoints* selects limited endpoints.
595548	FortiClient does not receive a profile from EMS.
598321	Uncaught TypeError arises when group is not selected in group assignment rule.
601239	FortiClient and EMS report different group tags.
601478	Syncing Active Directory (AD) subdomain with empty DN causes LDAP referral error.

Endpoint policy and profile

Bug ID	Description
565304	Profile synchronization between FortiOS and EMS fails if FortiOS admin password changes.
585394	Cannot access previously created endpoint profiles in EMS to make changes.
607235	Unable to import profile from FortiOS in EMS desktop console. Workaround: Use browser connection to EMS.

FortiClient deployment

Bug ID	Description
552883	Endpoint stuck on pending endpoint Telemetry message after AD-based deployment.
579422	Deployment stuck on install error.
588597	EMS reports it failed to delete an invitation being used when deleting a deployment package.
590998	EMS never renotifies clients to download installer.
600823	Installer does not populate firewall tables on remote databases.

Other

Bug ID	Description
553323	EMS Apache logs fill up server storage.
593195	EMS does not report IP address change to FortiOS via FSSO when user changes from wired to wireless.
597508	EMS FSSO reports wrong hostname to FortiOS.
599429	EMS diagnostic tool takes a long time to export event log.
599443	LDAP error.

Change log

Date	Change Description
2019-12-19	Initial release.
2020-01-23	Updated Product integration and support on page 8.
2020-01-24	Added 607235 to Endpoint policy and profile on page 13.