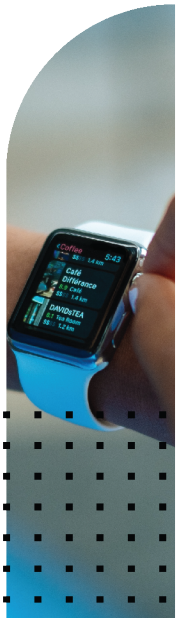
Release Notes

FortiClient EMS 7.0.1



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

August 10, 2021
FortiClient EMS 7.0.1 Release Notes
04-701-729348-20210810

TABLE OF CONTENTS

Introduction **5**
Endpoint requirements 5
Supported web browsers 5
Licensing and installation 6
Special notices **7**
FortiClient EMS Microsoft Visual C++ installation 7
SQL Server Standard or Enterprise with 5000 or more endpoints 7
Split tunnel 7
Upgrading **8**
Upgrading from previous EMS versions 8
Downgrading to previous versions 8
Product integration and support **9**
Resolved issues **10**
Dashboard 10
Deployment and installers 10
Settings 10
Endpoint management 11
Endpoint policy and profile 11
Upgrade 12
Multitenancy 12
Chromebook management 12
GUI 12
Zero Trust tagging 12
Administration 13
Other 13
Known issues **14**
Multitenancy 14
Dashboard 14
Endpoint management 14
Endpoint policy and profile 15
Installation and upgrade 15
Zero Trust Network Access 15
Deployment and installers 15
System Settings 16
Software Inventory 16
Administration 16
Fabric devices 16
Performance 17
Zero Trust tagging 17
Other 17

Change log **18**

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 7.0.1 build 103:

- Special notices on page 7
- What's New on page 1
- Upgrading on page 8
- Resolved issues on page 10
- Known issues on page 14

For information about FortiClient EMS, see the *FortiClient EMS 7.0.1 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 7.0.1 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 Standard or 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

In EMS 7.0.0, 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, ensure that you change the configuration to per-tunnel.

Upgrading

Upgrading from previous EMS versions

FortiClient EMS supports direct upgrade from EMS 6.2 and 6.4. 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 7.0.1 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, 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 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	• 7.0.0 and later • 6.4.0 and later
FortiClient (Linux)	• 7.0.0 and later • 6.4.0 and later
FortiClient (macOS)	• 7.0.0 and later • 6.4.0 and later
FortiClient (Windows)	• 7.0.0 and later • 6.4.0 and later
FortiOS	• 7.0.0 and later • 6.4.0 and later
FortiSandbox	• 4.0.0 and later (for detailed reports on files that FortiSandbox has detected) • 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 7.0.1. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Dashboard

Bug ID	Description
718122	License capacity cannot be below the number of active endpoints error in EMS with multitenancy enabled.

Deployment and installers

Bug ID	Description
665974	EMS fails to create deployment package from FortiGuard Distribution Server (FDS).
698222	LDAP organization units (OU) do not show correctly in *Edit Groups* of deployment package wizard.
708686	EMS allows deletion of FortiClient installer assigned to deployment policy when deleting corresponding invitation code.
719705	User cannot create FortiClient installer package.
721647	FortiClient and EMS should prevent installation and upgrade to unsupported OS versions.

Settings

Bug ID	Description
718276	The VCM engine is missing for Windows.

Endpoint management

Bug ID	Description
677247	When Active Directory (AD) domain is added, EMS shows multiple records of same domain.
687927	AD sync issues with EMS.
696869	LDAP sync cannot import some endpoints and endpoints appear in *Other Endpoints* group after manual install.
697136	EMS cannot connect to LDAP server.
698825	EMS cannot import same OU from AD server when more than ten sites are enabled.
705254	On-premise EMS invitation use count number keeps increasing when the same endpoint unregisters and reregisters.
705500	EMS should filter FortiClient version that does not support invitation code.
712466	*Individual* should toggled on instead of *Bulk* in the edit page of an individual code.
716353	*Real-Time Protection Enabled* does not show in green.
722445	Endpoints show up as online when they are not currently connected.
724616	Domain sync fails with *The distinguished name contains invalid syntax.* error.

Endpoint policy and profile

Bug ID	Description
573037	EMS provides no information regarding real-time protection (RTP) status.
670774	Error while importing Web Filter profiles from FortiGate.
690321	EMS does not update the endpoint policy when user changes groups.
697911	Synced updates from imported FortiGate Web Filter profile do not sync to FortiClient.
698632	Removable Media Access rule does not work.
716989	FortiClient does not block security category not blocked when RTP is enabled but Web Filter is disabled.
722093	Chromebook profile convert to normal profile after XML editing without saving.
723465	Profiles do not sync IPsec VPN phase 2 configuration to FortiClient.
724453	*Prompt for Certificate* option does not set the correct XML setting.
727769	*Sort by Policy Name* is broken.

Upgrade

Bug ID	Description
710176	Long AD endpoint groups do not appear under *Manage Policies* after upgrade.
716938	LDAP sync issue after upgrading EMS to 7.0.0.
723902	LDAP sync issue after upgrading EMS to 6.4.4.

Multitenancy

Bug ID	Description
721823	Deployment status always shows as *Endpoint Notified* in EMS GUI.

Chromebook management

Bug ID	Description
714739	Devtools reports *Unable to retrieve word signature from EMS* error.

GUI

Bug ID	Description
710355	*System Information* widget does not display on Chromebook dashboard, but does in *Manage Dashboard Widgets* list.
719783	GUI hides EMS alerts.

Zero Trust tagging

Bug ID	Description
639955	EMS should allow custom user input values for OS rule validation.
726610	Zero Trust tagging rule does not work after upgrade.

Administration

Bug ID	Description
714167	Local EMS user with custom role does not see details relating to FortiClient features under endpoint list.
721644	*Mark as uninstalled* action should not be available for managed endpoints.

Other

Bug ID	Description
700616	EMS should fully stop supporting FortiGate server list.
704222	Remove EMS FSSO settings.
715878	Online installer cannot get EMS installed from production FDS.
716408	Failures to update ISDB signature errors are shown on FCM task logs .
716967	EMS shows *Missing site information* error.
721026	FCMDaemon.exe crash after upgrade.

Known issues

The following issues have been identified in version 7.0.1. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Multitenancy

Bug ID	Description
722144	FortiClient cannot connect with non-default site after deleting non-default site and recreating it.

Dashboard

Bug ID	Description
716126	FortiSASE SIA instance uses Next Generation Endpoint Security licenses.
724870	Linux servers do not display in dashboard widgets.
733182	License tag alert continues after user uploads license.
735750	Exceeded max allowed requests in last hour when syncing license in EMS.

Endpoint management

Bug ID	Description
705010	EMS shows endpoints with incorrect username.
718651	FortiClient Cloud invitation email must be updated.
725170	Vulnerabilities that FortiClent has detected do not show in EMS.

Endpoint policy and profile

Bug ID	Description
598733	EMS profile fails to update Sandbox exclusion folder and files list.
697971	EMS fails to import profiles.
708985	*Exclude Selected Applications from Vulnerability Compliance Check* gives error when adding an application.
720348	VPN settings hides *Show "Always Up" Option* when *Auto Connect Only When Off-Fabric* option is enabled.
731716	Application name link to FortiGuard under *Application Firewall* > *Application Signatures* does not work.

Installation and upgrade

Bug ID	Description
724743	Upgrade reassigns devices to the default group.

Zero Trust Network Access

Bug ID	Description
734924	FortiClient EMS should not allow duplicate ZTNA TCP connection rule name.

Deployment and installers

Bug ID	Description
700462	FortiClient download URL refresh button fails to get new IP address.
725061	User cannot create new installer after deleting the old one on FortiClient Cloud.
726720	Deployment packages install FortiClient without deployment settings.
729978	EMS fails to create deployment package that include Windows and macOS images.
731440	EMS takes a long time to create deployment package zip file.
732414	Editing and saving deployment package changes the download link.

Bug ID	Description
734307	Deployment status always shows endpoint notified for 32-bit OS.

System Settings

Bug ID	Description
731659	EMS and endpoint alerts do not work.

Software Inventory

Bug ID	Description
734893	Software Inventory does not update for application removed from endpoint.

Administration

Bug ID	Description
728424	Administrator with *Manage custom groups* permission cannot create or delete custom groups.

Fabric devices

Bug ID	Description
682639	EMS never updates Fabric Devices state after authorizing the FortiGate.
703319	ZTNA Linux endpoint is not tagged when connected via SSL VPN to FortiGate.
708672	FortiGate can only show one FortiClient (latest connected via SSL VPN) in endpoint record list and only this FortiClient gets dynamic address.
718145	Endpoint record entries disappear from FortiGate when using EMS tags.
722030	FortiGate cannot get endpoint record information from EMS and FortiOS.
722178	FortiGate cannot get notification from EMS when EMS creates new ZTNA tag or deletes the old one.

Bug ID	Description
728318	EMS ZTNA tags sync to FortiGate is delayed.
733645	Fabric connection error.

Performance

Bug ID	Description
707316	FcmDaemon.exe uses all available memory.

Zero Trust tagging

Bug ID	Description
731074	Importing the same JSON file for Zero Trust tags twice introduces duplicated tags.
731780	*Zero Trust Tag Monitor* page displays endpoints that match FortiGuard outbreak alert rules.
732430	Zero Trust tagging rules for Active Directory (AD) groups should only list AD user groups.
735272	ZTNA rules should support NOT operation in logic.

Other

Bug ID	Description
705517	*Cannot insert duplicate key row in object* error in FcmDaemon log.
712215	FortiClient refuses to connect to FortiClient Cloud with error that EMS is unreachable.
716838	User cannot access on-premise EMS console.

Change log

Date	Change Description
2021-08-10	Initial release.

www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.