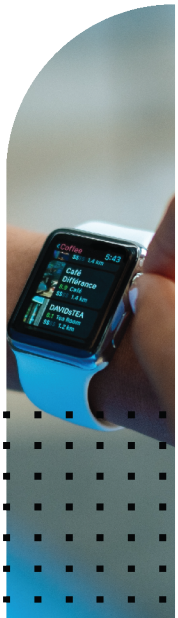
Release Notes

FortiClient EMS 7.0.7



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

August 31, 2022
FortiClient EMS 7.0.7 Release Notes
04-707-832530-20220831

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 7.0.7 build 0398:

For information about FortiClient EMS, see the *FortiClient EMS 7.0.7 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 10 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 7.0.7 GUI:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Internet Explorer is not recommended. You may need to enable remote access from the FortiClient EMS GUI. See To enable remote access to FortiClient EMS.

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 Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise.

Split tunnel

In EMS 7.0.7, 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, change the configuration to per-tunnel.

What's new

For information about what's new in FortiClient EMS 7.0.7, see the FortiClient & FortiClient EMS 7.0 New Features Guide.

Upgrading

Upgrading from previous EMS versions

You must first upgrade EMS to 7.0.3 or a later version before upgrading FortiClient from 7.0.2 or an earlier version.

Follow the upgrade procedure that *FortiClient and FortiClient EMS Upgrade Paths* outlines.

With the endpoint security improvement feature, you must consider backward compatibility issues 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 7.0.7 product integration and support information:

Server operating systems	• Windows Server 2022 • Windows Server 2019 • 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 Although EMS supports the listed FortiAnalyzer versions, confirming the compatibility between your FortiAnalyzer and FortiClient versions is recommended. Otherwise, not all features may be available. See the FortiClient Release Notes. When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.0.5, use FortiClient 7.0.5.
FortiClient (Linux)	If *Use SSL certificate for Endpoint Control* is enabled on EMS, EMS supports the following FortiClient (Linux) versions: • 7.0.2 and later • 6.4.7 and later If *Use SSL certificate for Endpoint Control* is disabled on EMS, EMS supports the following FortiClient (Linux) versions: • 7.0.0 and later • 6.4.0 and later
FortiClient (macOS)	If *Use SSL certificate for Endpoint Control* is enabled on EMS, EMS supports the following FortiClient (macOS) versions: • 7.0.2 and later • 6.4.7 and later If *Use SSL certificate for Endpoint Control* is disabled on EMS, EMS supports the following FortiClient (macOS) versions: • 7.0.0 and later • 6.4.0 and later

FortiClient (Windows)	If *Use SSL certificate for Endpoint Control* is enabled on EMS, EMS supports the following FortiClient (Windows) versions: • 7.0.2 and later • 6.4.7 and later If *Use SSL certificate for Endpoint Control* is disabled on EMS, EMS supports the following FortiClient (Windows) versions: • 7.0.0 and later • 6.4.0 and later
FortiOS	• 7.0.0 and later (for zero trust network access, 7.0.6 or later is recommended) • 6.4.0 and later
FortiSandbox	• 4.2.0 and later (for detailed reports on files that FortiSandbox has detected) • 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 7.0.7. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

License

Bug ID	Description
821767	FortiClient Cloud license expiry error.

System Settings

Bug ID	Description
823701	FortiClient Cloud does not allow enabling *Enforce User Verification*.

Endpoint management

Bug ID	Description
772402	EMS does not move endpoint to correct workgroup based on installer ID after deploying FortiClient from EMS.
780630	EMS does not fully update Active Directory schema.
807741	*All Groups* view shows incorrect endpoint count.
813513	Administrator cannot download or view Sandbox malware report.
821704	EMS always reports device state as managed in verified and unverified user table even after FortiClient unregisters from EMS.
825673	EMS clears all entries after upgrade and does not allow traffic for some users.
827269	Policy is out of sync when moving endpoints using group assignment rules.

Endpoint policy and profile

Bug ID	Description
799062	FortiClient does not send Web Filter traffic logs to FortiAnalyzer.
810123	EMS VPN before logon does not appear with fresh FortiClient installation.
811199	FortiGate to EMS Web Filter profile synchronization misbehaves for Chromebook profiles.
816362	Web Filter profile synced from FortiManager does not allow enabling *Allow websites when rating error occurs*.
817291	EMS cannot import Web Filter options such as safe search and *Allow websites when rating error occurs* from FortiManager.
823595	For a newly created profile, `<invalid_cert_action>` should be set to warning by default when EMS applies a valid certificate.

Install and upgrade

Bug ID	Description
824303	EMS upgrade breaks Malware Protection profiles with XML error.

Fabric devices

Bug ID	Description
824210	EMS shows error when handling incoming FortiGate gateway information `/api/v1/fgt/gateway_details/gateway_mac`.

HA

Bug ID	Description
816314	Restoring database does not restore EMS configuration/settings in always on availability environment.

Deployment and installers

Bug ID	Description
814700	FIPS feature is gone after manual upgrade with FIPS-enabled installer that EMS created.

Zero Trust tagging

Bug ID	Description
821700	Dynamic firewall list on FortiGate does not list FortiClient endpoints.
823801	EMS does not dynamically remove CVE zero trust tag after FortiClient patches related vulnerabilities.
827300	Endpoint does not get correct zero trust network access tag.

Endpoint control

Bug ID	Description
825559	FortiClient fails to register with EMS when *Enforce invitation-only registration for* is enabled.

Performance

Bug ID	Description
812927	FCEMS_Das keeps restarting.

Vulnerability Scan

Bug ID	Description
740041	Vulnerability logging does not include filepath and applications.

Other

Bug ID	Description
814515	Int overflow on spInsertClientQuarantineFiles.

Common Vulnerabilities and Exposures

Bug ID	Description
792536	FortiClient EMS 7.0.7 is no longer vulnerable to the following CVE References: • CVE-2022-22720 • CVE-2022-22719 • CVE-2022-22721 • CVE-2022-23943 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in version 7.0.7. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Multitenancy

Bug ID	Description
745854	Super administrators convert to site administrators after enabling multitenancy.
777642	Global site does not list FortiCloud license- and account-related logs.
816600	Non-default site database does not update EMS serial number after new license upload.
820803	License distribution modal shows incorrect information.

Dashboard

Bug ID	Description
781654	EMS does not remove dashboard outbreak alerts when endpoint disconnects.
817485	Drilldown on macOS vulnerability includes unrelated vulnerabilities.

Endpoint management

Bug ID	Description
691790	EMS should not allow downloading requested diagnostic result for FortiClient (Linux).
760816	Group assignment rules based on IP addresses do not work when using split tunnel.
770364	EMS does not disable third party features for non-Windows endpoints.
785186	EMS does not remove user from policy after deleting the domain.
786738	Anti-Ransomware Events tab is visible after disabling the feature in Feature Select.
792447	EMS fails to show zero trust network access (ZTNA) feature in endpoint details enabled/disabled features section.

Bug ID	Description
792652	EMS cannot delete domain.
803887	GUI does not show assigned installer for fresh domain machine during deployment.
808266	Dashboard widget has incorrect results for endpoints with Windows operating systems.
819196	The multipart identifiers `cs.software_id` and `cs.is_missing` cannot be bound.
831359	Forensics Analysis Download Report option opens the report instead of downloading it.
834228	EMS reports endpoint vulnerability when Vulnerability Scan is not installed on the endpoint.

Endpoint policy and profile

Bug ID	Description
466124	User cannot change `<nat_alive_freq>` value.
766445	EMS enables or disables profile feature for all policies that use the defined profile.
826013	Setting Vulnerability Scan patch status to *Not* does not work.
826940	EMS does not save `<temp_whitelist_timeout>` in an endpoint profile.
833819	Backing up configuration files on FortiClient Cloud results in import errors.

License

Bug ID	Description
823690	EMS includes Removable Media Access feature when using ZTNA user-based license.
827875	Non-default site's License information page shows irrelevant license information.
828944	EMS does not show *A new license has been detected...* if synced with FortiCloud account.

Install and upgrade

Bug ID	Description
820546	EMS disables *New EMS Version is available for deployment* EMS alert after upgrade.
829631	Administrator cannot disable *Delete Timeout* option.

Zero Trust tagging

Bug ID	Description
712522	FortiGate does not receive some endpoint tags from EMS after upgrading.
765375	User in Active Directory Group Zero Trust Network Access rule does not identify domains.
810778	FortiClient tag information is not shared equally to connected FortiGate Fabric devices.
815736	EMS fails to apply NOT for On-Fabric Status rule while creating a new tag.
832328	EMS tags endpoint with threat ID rule after clearing firewall events.

Deployment and installers

Bug ID	Description
666289	EMS does not report correct deployment package state.
714496	FortiClient Cloud upgrade keeps installer on instance and causes disk to have no space.
773672	Disabling installer ID in FortiClient installer does not take effect.
764999	EMS does not list FortiClient versions in official installer list if FortiGuard distribution server (FDS) blocks EMS from downloading said versions.
783690	The system does not prompt for reboot after user login.
824936	EMS fails to deploy FortiClient when manually created FortiClient installer is updated.

System Settings

Bug ID	Description
753951	EMS does not recognize disabling *Use FortiManager for client software/signature updates* > *Failover*.
784554	EMS displays error while importing ACME certificate.
794841	Email alerts are not triggered when the number of available licenses is less than 10% of the total.
807340	EMS tries to connect to FortiGuard Anycast server on port 8000.
828490	*Permission Denied : Your permissions might have been updated* error message displays for all admin roles.

Chromebook

Bug ID	Description
777957	EMS assigns the wrong profile.

Administration

Bug ID	Description
678899	Persisting LDAP configuration in multitenancy global/default/non-default administration users.

Performance

Bug ID	Description
731097	Updating or disabling policy assigned to large number of AD endpoints takes long time to process.
759729	Possible slow httpd file handle leak.

HA

Bug ID	Description
809344	High availability (HA) does not start if starting without the database.
809396	EMS on HA backup generates a generic error.

Configuration

Bug ID	Description
745913	SMTP configuration fails authentication.

Endpoint control

Bug ID	Description
776626	FortiClient may fail to get Web Filter custom message when EMS runs in high availability mode.
813439	FortiClient registered with EMS IP address does not deregister from EMS when *Enforce invitation-only registration for* is set to *ALL*.
813531	EMS does not push profile to endpoints if they connect to EMS after enabling the feature under EMS System Settings.
822914	EMS does not have a mechanism to keep the client aware of the new license expiration date.
827200	EMS displays some devices as having no user.
833717	EMS shows endpoints as offline, while endpoints show their own statuses as online.

GUI

Bug ID	Description
717433	Patching a vulnerability for a specific endpoint patches it on others.
731074	Importing the same JSON file for zero trust tagging twice introduces duplicate tags.
767469	EMS marks many endpoints as not installed after upgrading.
774880	You can import the same Zero Trust tagging rules multiple times by clicking the *Import* button multiple times.
793313	Detailed deployment states list does not fit in window.
811774	EMS with Remote Access-only license shows unrelated feature options on GUI.
816151	Toggle for *Use FortiManager for client software/signature updates* appears disabled after enabling the feature.
819205	License widget shows Forensic license as *NaN used of X* when no license is in use.

Malware Protection and Sandbox

Bug ID	Description
793926	FortiShield blocks spoolsv.exe on Citrix virtual machine servers.

License

Bug ID	Description
823458	EMS with Endpoint Protection Platform (EPP)-only license and ZTNA feature enabled reports EPP license as consumed but fails to quarantine endpoint.

Remote access

Bug ID	Description
830899	FortiClient becomes unlicensed while connected to SSL VPN.

Avatar and social login information

Bug ID	Description
830117	EMS fails to update email address from personal information form in FortiClient.

Endpoint security

Bug ID	Description
783287	Let's Encrypt ACME certificate request fails due to port 80 on autotest system.

FortiGuard outbreak alert

Bug ID	Description
813928	EMS retrieves the EOAP signature from FDS but does not show it on the GUI. **Workaround**: Restart fcems services to display all FortiGuard outbreak detection rules on the GUI.
819025	With multiple sites, EMS fails to display FortiGuard outbreak detection rules downloaded from FDS.

Onboarding

Bug ID	Description
819203	Authorized user group name should be full path.
820060	EMS displays same device list with the same login and registration LDAP user on verified user and unverified user tables.
822126	Delete SAML configuration message shows incorrect active users.

FortiClient Cloud API

Bug ID	Description
585763	User cannot log in to FortiClient Cloud if they are using the same browser for login to on-premise EMS. **Workaround**: In FortiClient Cloud 7.0.6 and 7.0.7, you can clear the browser client cache or use a different browser.
832144	User cannot call APIs in FortiClient Cloud. **Workaround**: In FortiClient Cloud 7.0.6 and 7.0.7, you can clear the browser client cache or use a different browser.

Change log

Date	Change Description
2022-08-31	Initial release.

www.fortinet.com

Copyright© 2023 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.