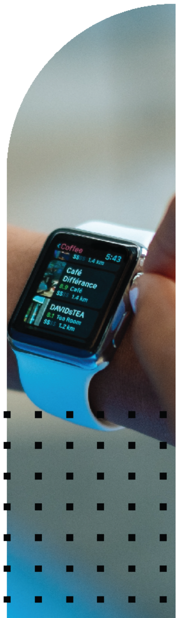
Release Notes

FortiClient EMS 7.0.6



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

FORTINET®

July 07, 2022
FortiClient EMS 7.0.6 Release Notes
04-706-805991-20220707

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 7.0.6 build 0358:

- Special notices on page 7
- What's new on page 8
- Upgrading on page 9
- Resolved issues on page 12
- Known issues on page 17

For information about FortiClient EMS, see the *FortiClient EMS 7.0.6 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 7.0.6 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 *FortiClient EMS Administration Guide*.

Split tunnel

In EMS 7.0.6, 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.

Sending Web Filter logs to FortiAnalyzer

Due to an issue where FortiClient (Windows) does not send Web Filter logs to FortiAnalyzer, EMS has removed the four `default wanacc shield scheduler configd` settings after saving the system profile from the GUI.

Until this issue is resolved, for FortiClient to send traffic logs to FortiAnalyzer, ensure to configure the following settings:

- Enable the log event setting for the scheduler in the EMS *System Settings* profile: `<log_events>...,scheduler,...</log_events>`. Scheduler log events include all events with `subtype="system"` in the log definition file defined in each CM build, for example: `https://info.fortinet.com/files/FortiClient/v7.00/images/build0238/fct_log_def_7.0.5.0238.xml`.
- Enable the `webfilter log_all_urls` setting. When `log_all_urls` is enabled, FortiClient logs all traffic URLs, including passthrough traffic for all features, such as Web Filter, VPN, antivirus, and so on.

What's new

For information about what's new in FortiClient EMS 7.0.6, 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.

FortiClient EMS supports direct upgrade from EMS 6.2, 6.4, and 7.0. To upgrade older EMS versions, follow the upgrade procedure outlined in *FortiClient and FortiClient EMS Upgrade Paths*.

With the 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 7.0.6 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.
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 7.0.6. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

License

Bug ID	Description
773490	FcmMonitor.exe daemon crash stops FCEMS_Monitor service.
813359	*This configuration would disable all features in one or more policies* error displays when updating EMS fully qualified domain name.

Logs

Bug ID	Description
650993	EMS does not provide a way to clean uploaded FortiClient logs and diagnostic logs that EMS requested.

Remote Access

Bug ID	Description
779580	The endpoint record list shows the SSL VPN client's real IP address, as opposed to the expected dynamic IP address from the VPN pool.

System Settings

Bug ID	Description
801164	Email alert does not work with multiple recipients when using Amazon Simple Email Service.

Endpoint management

Bug ID	Description
771128	LDAP UnicodeDecodeError occurs while adding domain.
789330	API error 400 occurs while filtering or sorting checksum field for Sandbox events.
800052	EMS shows duplicate entries for domain- joined endpoints under same organizational unit in Active Directory.
806599	FortiClient and devices get partially deleted from the database.

Endpoint policy and profile

Bug ID	Description
786109	Testing Sandbox connection fails with several development tool errors.
796028	Scheduled synchronizations for imported profiles do not update endpoint policy.
797556	User cannot enable *Exclude Files from Trusted Sources* in a Sandbox profile.
798386	EMS falsely correlates some FortiAnalyzer settings.
800424	Endpoint control does not show invalid certificate action element in XML.
803391	SSL VPN tunnel profile incorrectly parses 6.4 certificates.

Install and upgrade

Bug ID	Description
789986	TLS 1.0 is enabled on port 443 after update.
792179	User cannot access FortiClient Cloud GUI after upgrade.
798556	Upgrade fails due to invalid object name *dbo.logs_raw*.

FortiGuard Outbreak Alerts

Bug ID	Description
773928	Only default site lists FortiGuard outbreak detection rules.

Fabric devices

Bug ID	Description
815026	FortiSoC API connection is down on FortiAnalyzer.

HA

Bug ID	Description
811710	Backup fails when secondary replica becomes primary in always on availability environment.

GUI

Bug ID	Description
632427	Software Inventory filter and sort actions in heading do not work.
800867	Disclaimer message adds extra new lines after first linebreak on GUI saves.

Deployment and installers

Bug ID	Description
793847	Timestamp server requirement for software package code signing certificate use.
805428	EMS does not deploy and displays *Error creating IP_Port_path*.

Deployment and installers

Bug ID	Description
788008	Installer displays *Server encountered an error, please try again* error after upgrade.

Zero Trust tagging

Bug ID	Description
803023	Vulnerable device tag displays when vulnerability is excluded.
811933	When SSL or IPsec VPN client disconnects from tunnel, the resolved IP address in firewall dynamic ems-tag table keeps the same IP address.

Endpoint control

Bug ID	Description
792787	Application Firewall blocks RDP connection when it is allowlisted and remote access category is blocked.
800451	Zero Trust tag for on-fabric rule type applies when endpoint is off-fabric.
810462	EMS should ensure that the zero trust network access certificate on FortiClient is synchronized with EMS.

Administration

Bug ID	Description
786722	User cannot delete administrator user account with site administrator profile.

ZTNA connection rules

Bug ID	Description
730459	Serial number of FortiClient certificate in endpoint is incorrect.

Common Vulnerabilities and Exposures

Bug ID	Description
771996	FortiClient EMS 7.0.6 is no longer vulnerable to the following CVE References:

Bug ID	Description
	• CVE-2021-44790 • CVE-2021-44224 Visit https://fortiguard.com/psirt for more information.
791741	FortiClient EMS 7.0.6 is no longer vulnerable to the following CVE Reference: • CVE-2022-0778 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in version 7.0.6. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Dashboard

Bug ID	Description
781654	EMS does not remove dashboard outbreak alerts when endpoint disconnects.

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.
772402	Endpoint does not move to correct workgroup based on installer ID after deploying FortiClient from EMS.
780630	EMS Active Directory schema does not fully update on EMS.
785186	EMS does not remove user from policy after deleting the domain.
792652	EMS cannot delete domain.
803887	GUI does not show assigned installer for fresh domain machine during deployment.
813513	User cannot download or view Sandbox malware report.
821704	EMS reports device as managed in verified and unverified user table after FortiClient is unregistered from EMS.

Endpoint policy and profile

Bug ID	Description
466124	User cannot change `<nat_alive_freq>` value.

Bug ID	Description
766445	EMS enables or disables profile feature for all policies that use the defined profile.
799062	FortiClient does not send Web Filter traffic logs to FortiAnalyzer.
810123	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 *Allow websites when rating error occurs*.
817291	EMS cannot import some Web Filter options, such as safe search and *Allow websites when rating error* occurs from FortiManager.
823595	A newly created profile should have the invalid certificate action set to warning by default when EMS applies a valid certificate.
823685	Imported Web Filter profile from FortiGate or FortiManager changes to allow all categories after enabling *Log User Initiated Traffic* and resynchronizing.

License

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

Multitenancy

Bug ID	Description
745854	Super administrators convert to site administrators after enabling multitenancy.
816600	Non-default site database does not update EMS serial number after uploading new license.

Install and upgrade

Bug ID	Description
820546	EMS disables *New EMS Version is available for deployment* EMS alert after upgrade.
824303	Upgrading to 7.0.6 breaks Malware Protection profiles due to XML error.

Bug ID	Description
	Workaround: Open an existing profile, click the *Advanced* button, then go to the *XML Configuration* tab. Click the *Edit* button, then save it. This resolves the issue and removes the red X from the left window pane.

Zero Trust tagging

Bug ID	Description
712522	FortiGate does not receive some endpoint tags from EMS after upgrading.
726835	FortiGate cannot get the updated VPN IP address in firewall dynamic EMS tag address when FortiClient establishes the VPN tunnel.
765375	User in Active Directory Group Zero Trust Network Access rule does not identify domains.
781590	EMS does not send all tag definitions to all FortiGates if there are no FortiClients that use them.
783287	Let's Encrypt ACME certificate request fails due to port 80 on autotest system.
795202	IP/MAC address information is not present in dynamic address list when establishing SSL VPN.
815736	EMS fails to apply NOT for On-Fabric Status rule while creating a new tag.

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

System Settings

Bug ID	Description
753951	EMS does not recognize disabling *Use FortiManager for client software/signature updates > Failover*.

Bug ID	Description
784554	EMS displays error while importing ACME certificate.
807340	EMS tries to connect to FortiGuard Anycast server on port 8000.
794841	Email alerts are not triggered when the number of available licenses is less than 10% of the total.
753951	EMS does not recognize it when user disables *Use FortiManager for client software/signature updates* > *Failover*.
823701	User cannot enable *Enforce User Verification* on FortiClient Cloud.

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.

EMS 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.
816314	Restoring a database does not restore EMS configuration and settings in always on availability environment.

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.
779652	IPsec VPN shows offline status in FortiGate endpoint record list and fails to resolve VPN IP address to EMS tag firewall dynamic address.
813531	EMS does not push profile to endpoints if they connect to EMS after enabling the feature under EMS System Settings.

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.
770204	When CX changes the invitation link expiry date, the previous invitation link does not work.
771027	FortiClient does not detect virus within large zip file, but detects it when extracted.

Bug ID	Description
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.

Vulnerability Scan

Bug ID	Description
725170	Vulnerabilities detected on FortiClient do not show in EMS.
740041	Vulnerability logging does not have filepath and applications information.

Other

Bug ID	Description
752052	EMS does not sending alert emails.
786181	EMS is not sending EMS and endpoint alert emails.
820060	Verified user and unverified user tables show same device list with the same logins and registered LDAP users.

Change log

Date	Change Description
2022-07-05	Initial release.
2022-07-07	Added 773490 and 810462 to Resolved issues on page 12.

FORTINET®

www.fortinet.com