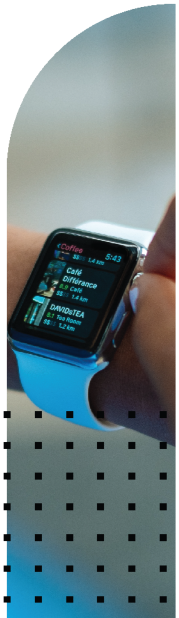
Release Notes

FortiClient EMS 7.0.3



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/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®

February 28, 2022
FortiClient EMS 7.0.3 Release Notes
04-703-766524-20220228

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 7.0.3 build 0229:

- Special notices on page 7
- What's new on page 9
- Upgrading on page 10
- Resolved issues on page 13
- Known issues on page 19

For information about FortiClient EMS, see the *FortiClient EMS 7.0.3 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 11 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 7.0.3 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 7.0.3, 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.

Endpoint security improvement

EMS 7.0.2 introduced an improvement to endpoint security that impacts compatibility between FortiClient and EMS, and the recommended upgrade path. The FortiClient 7.0.3 installer is not available on FortiGuard Distribution Servers (FDS). To use the FortiClient 7.0.3 installer, you must download it from Customer Service & Support. See Endpoint security improvement.

If *Use SSL certificate for Endpoint Control* is disabled, EMS displays a popup that the SSL certificate is not secure even if the SSL certificate is publicly signed and trusted. The banner also displays the same message.

If the EMS server certificate is invalid, and FortiClient is upgraded to 7.0.3, 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.

When the new *Use SSL certificate for Endpoint Control* option is enabled and EMS is using a valid server certificate, FortiClient 7.0.1 and older versions, or 6.4.6 and older, will no longer be able to connect to the EMS.

What's new

For information about what's new in FortiClient (Windows) 7.0.3, see the FortiClient & FortiClient EMS 7.0 New Features Guide.

Upgrading

Upgrading from previous EMS versions

You must upgrade EMS to 7.0.3 before upgrading FortiClient.

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 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 7.0.3 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 • 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 7.0.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

License

Bug ID	Description
733182	License alert continues after uploading license.
741560	License for all tenants are retracted.
744018	EMS displays wrong license expiration alert.

Configuration

Bug ID	Description
725469	EMS uses reply-to email address as from email address when sending email.
748476	FortiClient Cloud SMTP test fails to send notification email with Microsoft.

Endpoint management

Bug ID	Description
671073	Improve endpoint modification management behavior.
731705	LDAP sync error that an item with the same key has already been added.
738000	Domain-joined machine shows duplicate entry on EMS after reimaging.
741242	The FortiGate FortiClient widget cannot show avatar for entries.
741773	Maximum amount of license seats used per tenant causes FortiClient to lose Application Firewall and Malware Protection tabs.
743155	Issue after installing Microsoft KB5003542.
754794	Domain sync fails with *Invalid Device data: invalid character* error.

Bug ID	Description
757059	Sync fails with NullReferenceException after synchronizing a container with no parentGUID.
767522	Domain sync fails with *Invalid char ',' at the start of attribute type.* on EMS upgraded from 6.2.

Endpoint policy and profile

Bug ID	Description
598733	EMS profile fails to update Sandbox exclusion folder and filelist.
614445	Add option for a default tab to GUI and XML.
693230	FortiClient GUI does not display *Save username* option for IPsec VPN tunnel.
737592	EMS overwrites XML configuration.
739218	EMS GUI does not update removable media access XML settings.
742325	Endpoint cannot access URLs when URL is set as part of simple expression exclusion list in EMS Web Filter.
746469	Creating SSL VPN tunnel manually with XML does not pass the certificate check details to the main XML configuration.
749784	Descriptions on the FortiGuard webpage and the Web Filter category in EMS differ.
751718	Web Filter syncing misbehavior between FortiManager/FortiGate, EMS, and FortiClient.
770648	Web Filter profile imported from FortiGate differs from actual profile in FortiOS.
774890	FortiClient does not receive updated profile after syncing the imported Web Filter profile on EMS.

Install and upgrade

Bug ID	Description
719991	EMS with remote SQL database fails to upgrade.
722394	Upgrading EMS fails on Windows Server Core.
740581	EMS cannot manage Zero Trust Network Access (ZTNA) policy.
740785	Upgrading EMS fails due to duplicate key found for the object name `'dbo.forti_product_info'`.
742359	Upgrade fails with *'FCM.dbo.admin_user_old_passwords'; column does not allow nulls* error.
742843	Missing `<warn_invalid_server_certificate>` value crashes GUI after upgrade.

Bug ID	Description
750165	EMS installer changes SQL Server TCP port settings and breaks SQL Server.
766910	EMS install service account password length.

Vulnerability Scan

Bug ID	Description
736591	Vulnerabilities detected on FortiClient do not match the record on EMS.
742731	EMS shows no vulnerability events for endpoints.

Multitenancy

Bug ID	Description
745774	After enabling multitenancy, EMS is stuck in the loop of creating the database for that site.
747039	EMS cannot create or show sites.
751261	EMS cannot delete specific users in multitenancy mode.

Dashboard

Bug ID	Description
724870	Dashboard widgets do not display Linux servers.

GUI

Bug ID	Description
742168	Administrators page is empty after importing LDAP user.
744187	Add export function in *Software Inventory* page.

Performance

Bug ID	Description
739326	Server disk I/O high with FcmUpdateDaemon.exe.
740763	FortiOS API optimization containing hotfix.

Deployment and installers

Bug ID	Description
731440	EMS takes a long time to create deployment package zip file.
732414	Editing and saving deployment package changes the download link.
745652	EMS deployment configuration installs to excluded endpoints for managed deployment.

Zero Trust tagging

Bug ID	Description
722030	FortiGate cannot get endpoint record information from EMS.
726911	FortiClient GUI does not show tags.
728318	ZTNA tags sync to FortiOS is delayed.
745443	Change in HostVerification.cpp for Monterey support - Zero Trust Rule for macOS 12.0 Monterey.

Endpoint control

Bug ID	Description
734893	Software inventory does not update to reflect application removed from endpoint.
749083	FortiClient (Windows) Telemetry connection keeps connecting and disconnecting to EMS after upgrade.

Administration

Bug ID	Description
736521	EMS does not remember role when editing an administrator.
741624	LDAP administrators cannot authenticate when New Technology LAN Manager is disabled and Kerberos is unused.
741673	LDAP user is locked out after changing password due to binding requests from EMS.

Fabric devices

Bug ID	Description
682639	EMS does not update Fabric Devices status after authorizing the FortiGate.
744403	EMS sends updates that system information has changed to FortiGate when data has not changed.

Logs

Bug ID	Description
736098	EMS shows *not latest AV signature version* system event.

Other

Bug ID	Description
706816	Chromebook port connection should report HTTP strict transport security.
741085	FcmDaemon crashes after a few minutes.

Common Vulnerabilities and Exposures

Bug ID	Description
721744	FortiClient EMS 7.0.3 is no longer vulnerable to the following CVE Reference:

Bug ID	Description
	• CVE-2021-41028 Visit https://fortiguard.com/psirt for more information.
746418, 751517	FortiClient EMS 7.0.3 is no longer vulnerable to the following CVE Reference: • CVE-2021-3711 Visit https://fortiguard.com/psirt for more information.
752422	FortiClient EMS 7.0.3 is no longer vulnerable to the following CVE References: • CVE-2021-42013 • CVE-2021-41773 Visit https://fortiguard.com/psirt for more information.
724244	FortiClient EMS 7.0.3 is no longer vulnerable to the following CVE References: • CVE-2021-30641 • CVE-2020-35452 • CVE-2021-26691 • CVE-2021-26690 • CVE-2020-13950 • CVE-2020-13938 • CVE-2019-17567 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in version 7.0.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Dashboard

Bug ID	Description
774663	EMS changes dashboard status widgets settings after user refreshes EMS status page.
781654	EMS does not remove dashboard outbreak alerts when endpoint disconnects.
786159	Vulnerability Scan widget is not showing the correct number when first loaded.

Endpoint management

Bug ID	Description
738831	Multitenancy custom site group assignment rules *Run Rules Now* does not work.
756675	Total endpoint count increases on vulnerability dashboard when clicking *Total Vulnerabilities*.
760816	Group assignment rules based on IP addresses do not work when using split tunnel.
770290	All Groups does not show endpoints in a subgroup.
770364	Disable third-party features for non-Windows endpoints.
772402	EMS does not move endpoint to correct workgroup based on installer ID after deploying FortiClient from EMS.
785186	Users are not removed from policy after deleting the domain.
786196	LDAP fails to sync specific security groups in AD.

Endpoint policy and profile

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

Bug ID	Description
776391	Chromebook user effective profile does not show all profiles assigned.
777067	EMS does not import Web Filter profiles from FortiOS if login banners are enabled.
777957	EMS assigns the wrong profile to an endpoint.
778724	Disabling *Exclude Selected Applications from Vulnerability Compliance Check* and saving does not work if an application is added.
779275	Disabling keyword scanning on search engines has no effect.
779337	EMS always sets safe search level to moderate for Bing and Yahoo searches.
783380	API error while updating OS version Zero Trust tagging rule for Android/iOS.

EMS policy and profile

Bug ID	Description
785652	The network drive scan setting from EMS profile is broken.
786109	EMS test Sandbox connection failed with several Development Tool Error.
786161	Manage policies page has an issue with filtering on name or assigned groups.

Installation and upgrade

Bug ID	Description
754722	Uninstall deployment from EMS does not work on FortiClient 6.4.6.
756267	User cannot delete custom installer with name that includes a space.
785991	Anti-Virus Display value is incorrect on import.
786146	Missing FortiClient EMS 6.4.7 Endpoint info after upgrading EMS from 6.4.7 to 7.0.3.229.

Zero Trust tagging

Bug ID	Description
763868	EMS cannot identify domain/local users if they have the same username.
772022	Tagging fails when endpoint meets tagging rules.

Bug ID	Description
773928	EMS only lists FortiGuard outbreak detection rules in default site.
776439	EMS is missing OS version 12 for Android in Zero Trust tagging rules.
781381	EMS is missing new CentOS Linux distributions in Zero Trust tagging rules.
781590	EMS does not send all tag definitions to all FortiGates when some tags are not applied to any endpoints.

Deployment and installers

Bug ID	Description
714496	FortiClient Cloud upgrade keeps installer on instance and causes space to run out on disk.
754722	Uninstall deployment from EMS does not work on FortiClient 6.4.6.
773672	Disabling installer ID in FortiClient installer does not take effect.

Administration

Bug ID	Description
728424	Administrator with *Manage custom groups* permission cannot create or delete custom groups.
765261	EMS does not disable request for diagnostic log for mobile devices.
773674	EMS fails to work properly when user tries to start new database backup when previous backup still in progress.
781379	Adding classification tags is not disabled for viewing roles.

Fabric devices

Bug ID	Description
741546	FortiGate automatically deauthorizes and disconnects websocket with EMS 20 to 25 minutes after authorization.
785102	EMS should show FortiGate version under Fabric devices.
785606	When a client is deregistered from EMS GUI, the classification importance tag assigned to it will get deleted after some time.
793362	EMS connector does not authorize FortiGate with fingerprint.

Configuration

Bug ID	Description
745913	SMTP configuration fails authentication.

Endpoint control

Bug ID	Description
770610	IndexError: list index out of range at `/api/v1/invitation/index/`.
779267	FortiClient does not receive the updated profile and does not sync.
786160	Profile syncing status issue in "Manage Policies" page.

GUI

Bug ID	Description
551109	Add trusted sources list and logos to tooltip.
767469	EMS marks many endpoints as not installed after upgrade.
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.
771237	EMS ZTNA rules table must display more setting fields.
779249	EMS with ZTNA license allows user to enable and configure Sandbox Cloud feature.

Vulnerability Scan

Bug ID	Description
725170	EMS does not show FortiClient-detected vulnerabilities.
740041	Vulnerability logging with filepath and applications.

Zero Trust Telemetry

Bug ID	Description
763957	FortiClient prompts for telemetry key when administrator changed telemetry key on EMS.

Endpoint security

Bug ID	Description
783287	Let's Encrypt ACME certificate request fails due to port 80 on autotest system.
777546	Regenerating ACME certificate option does not appear after adding, deleting, or editing a site.
784554	Importing ACME Certificate in EMS Settings gets an error.

Performance

Bug ID	Description
760665	EMS is unstable with 100 FortiGates.

Other

Bug ID	Description
752052	EMS does not sending alert emails.
759986	Handle SMTP message size limit.
786181	EMS is not sending EMS and endpoint alert emails.

Change log

Date	Change Description
2022-03-31	Initial release.

www.fortinet.com