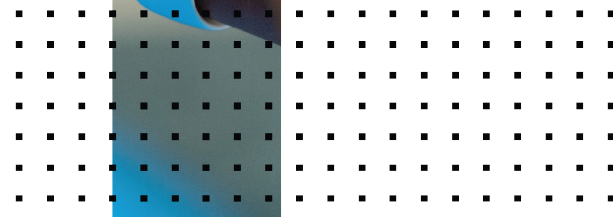


Release Notes

FortiClient EMS 7.0.4



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



April 27, 2022

FortiClient EMS 7.0.4 Release Notes

04-704-766524-20220427

TABLE OF CONTENTS

Introduction	5
Endpoint requirements	5
Supported web browsers	6
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
What's new	8
Upgrading	9
Upgrading from previous EMS versions	9
Downgrading to previous versions	9
Product integration and support	10
Resolved issues	12
Endpoint management	12
Endpoint policy and profile	12
Install and upgrade	12
GUI	12
Deployment and installers	13
Zero Trust tagging	13
Endpoint control	13
Administration	13
Zero Trust telemetry	13
Common Vulnerabilities and Exposures	14
Known issues	15
Dashboard	15
Endpoint management	15
Endpoint policy and profile	15
License	16
Installation and upgrade	16
Zero Trust tagging	16
Deployment and installers	17
System Settings	17
Chromebook	17
Administration	17
Performance	17
FortiGuard Outbreak Alert	18
Configuration	18
Endpoint control	18
GUI	18

Malware Protection and Sandbox	19
Web Filter and plugin	19
Other	19
Change log	20

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
- Chrome OS

FortiClient EMS runs on a Microsoft Windows server.

This document provides the following information for FortiClient EMS 7.0.4 build 0276:

- [Special notices on page 7](#)
- [What's new on page 8](#)
- [Upgrading on page 9](#)
- [Product integration and support on page 10](#)
- [Resolved issues on page 12](#)
- [Known issues on page 15](#)

For information about FortiClient EMS, see the [FortiClient EMS 7.0.4 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 7.0.4 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 [Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise](#).

Split tunnel

In EMS 7.0.4, 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.

What's new

For information about what's new in FortiClient EMS 7.0.4, 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 7.0.4 product integration and support information:

Server operating systems	<ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016• Windows Server 2012 R2
Minimum system requirements	<ul style="list-style-type: none">• 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. <p>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.</p>
FortiAnalyzer	<ul style="list-style-type: none">• 7.0.0 and later• 6.4.0 and later <p>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.</p>
FortiClient (Linux)	<p>If <i>Use SSL certificate for Endpoint Control</i> is enabled on EMS, EMS supports the following FortiClient (Linux) versions:</p> <ul style="list-style-type: none">• 7.0.2 and later• 6.4.7 and later <p>If <i>Use SSL certificate for Endpoint Control</i> is disabled on EMS, EMS supports the following FortiClient (Linux) versions:</p> <ul style="list-style-type: none">• 7.0.0 and later• 6.4.0 and later
FortiClient (macOS)	<p>If <i>Use SSL certificate for Endpoint Control</i> is enabled on EMS, EMS supports the following FortiClient (macOS) versions:</p> <ul style="list-style-type: none">• 7.0.2 and later• 6.4.7 and later <p>If <i>Use SSL certificate for Endpoint Control</i> is disabled on EMS, EMS supports the following FortiClient (macOS) versions:</p> <ul style="list-style-type: none">• 7.0.0 and later• 6.4.0 and later
FortiClient (Windows)	<p>If <i>Use SSL certificate for Endpoint Control</i> is enabled on EMS, EMS supports the following FortiClient (Windows) versions:</p>

- 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 7.0.4. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Endpoint management

Bug ID	Description
756675	Total endpoint count increases in vulnerability dashboard when clicking <i>Total Vulnerabilities</i> .
779309	Domain synchronization fails.

Endpoint policy and profile

Bug ID	Description
694471	FortiClient EMS has issue importing Web Filter profiles from FortiGate after upgrading FortiOS from 6.2.8.
770648	Web Filter profile imported from FortiGate differs from the actual profile on FortiGate.
787732	Enabling <i>Hide User Information</i> enables <i>Hide System Tray Icon</i> . Disabling <i>Hide User Information</i> disables <i>Hide System Tray Icon</i> .

Install and upgrade

Bug ID	Description
788031	Upgrading EMS 7.0.2 to 7.0.3 fails.

GUI

Bug ID	Description
551109	FortiClient EMS should have a trusted sources list and logs as a tooltip.

Deployment and installers

Bug ID	Description
788008	Installer displays <i>Server encountered an error, please try again</i> error after upgrade.

Zero Trust tagging

Bug ID	Description
789881	The <i>fct_tags</i> table does not update its <i>update_time</i> when the <i>Devices_ip_mac_list</i> table is updated for /tags API.
791318	EMS deletes <i>all_registered_clients</i> tags when endpoint goes offline.
797595	EMS does not use <i>route_type</i> of 2 in comparisons.

Endpoint control

Bug ID	Description
769878	EMS cannot delete all unused applications from Software Inventory.

Administration

Bug ID	Description
774596	Domain users cannot log in into EMS.

Zero Trust telemetry

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

Common Vulnerabilities and Exposures

Bug ID	Description
771996	FortiClient EMS 7.0.4 is no longer vulnerable to the following CVE References: <ul style="list-style-type: none">• CVE-2021-44790• CVE-2021-44224 Visit https://fortiguard.com/psirt for more information.
791741	FortiClient EMS 7.0.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2022-0778 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in version 7.0.4. 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.
780630	EMS Active Directory schema does not fully update on EMS.
785186	EMS does not remove user from policy after deleting the domain.
789330	API displays error 400 while filtering/sorting checksum field for Sandbox events.
792652	EMS cannot delete domain.
794153	Importing domain with certificate has issues.
821704	EMS reports device state 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 <code><nat_alive_freq></code> value.
766445	EMS enables or disables profile feature for all policies that use the defined profile.
768768	You can simultaneously configure Security Risk category under AntiVirus protection and Web Filter, which causes conflicts.

Bug ID	Description
777067	EMS does not import Web Filter profiles from FortiOS if login banners are enabled.
783386	Web Filter profile imported from FortiOS shows as enabled in the GUI but disabled in XML.
786109	Testing Sandbox connection fails with dev tool errors.
789344	You can configure <code><candc_enabled></code> tag on both the Malware Protection and Application Firewall profiles in XML.
792793	Quick Scan option does not work in GUI when trying to set scheduled scan.
797556	User cannot enable <i>Exclude Files from Trusted Sources</i> in <i>Endpoint Profiles > Sandbox Detection</i> .
798386	EMS falsely correlates some FortiAnalyzer settings.
823595	For a newly created profile, the invalid certificate action should be set to warning by default when EMS applies a valid certificate.

License

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

Installation and upgrade

Bug ID	Description
754722	Uninstall deployment from EMS does not work on FortiClient 6.4.6.
798556	Upgrade from 6.4.7 to 7.0.3 fails with invalid object name 'dbo.lags_raw' error.

Zero Trust tagging

Bug ID	Description
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.

Deployment and installers

Bug ID	Description
666289	EMS does not report correct deployment package state.
773672	Disabling installer ID in FortiClient installer does not take effect.

System Settings

Bug ID	Description
753951	EMS does not recognize disabling <i>Use FortiManager for client software/signature updates > Failover</i> .
784554	EMS displays error while importing ACME certificate.

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.
786722	Site administrator cannot delete admin user account.

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.

FortiGuard Outbreak Alert

Bug ID	Description
773928	EMS only lists FortiGuard outbreak detection rules in default site.

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.
777546	Regenerating ACME certificate option does not appear after adding, deleting, or editing a site.
779652	IPsec VPN shows offline status in FortiGate endpoint record list and fails to resolve VPN IP address to EMS tag firewall dynamic address.
783838	Custom messages for stop and reevaluation do not reflect on the preview GUI.
800451	Zero Trust tag for on-Fabric rule type applies when endpoint is off-Fabric.

GUI

Bug ID	Description
632427	Software Inventory filter and sorting action in heading does not work.
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.
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.
774880	You can import the same Zero Trust tagging rules multiple times by clicking the <i>Import</i> button multiple times.

Bug ID	Description
793313	Detailed deployment states list does not fit in window.
800867	Disclaimer message adds extra new lines after first line break on GUI saves.

Malware Protection and Sandbox

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

Web Filter and plugin

Bug ID	Description
793017	Web Filter disconnects an application's underlying connection.

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
2022-04-27	Initial release.



www.fortinet.com

Copyright© 2024 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.