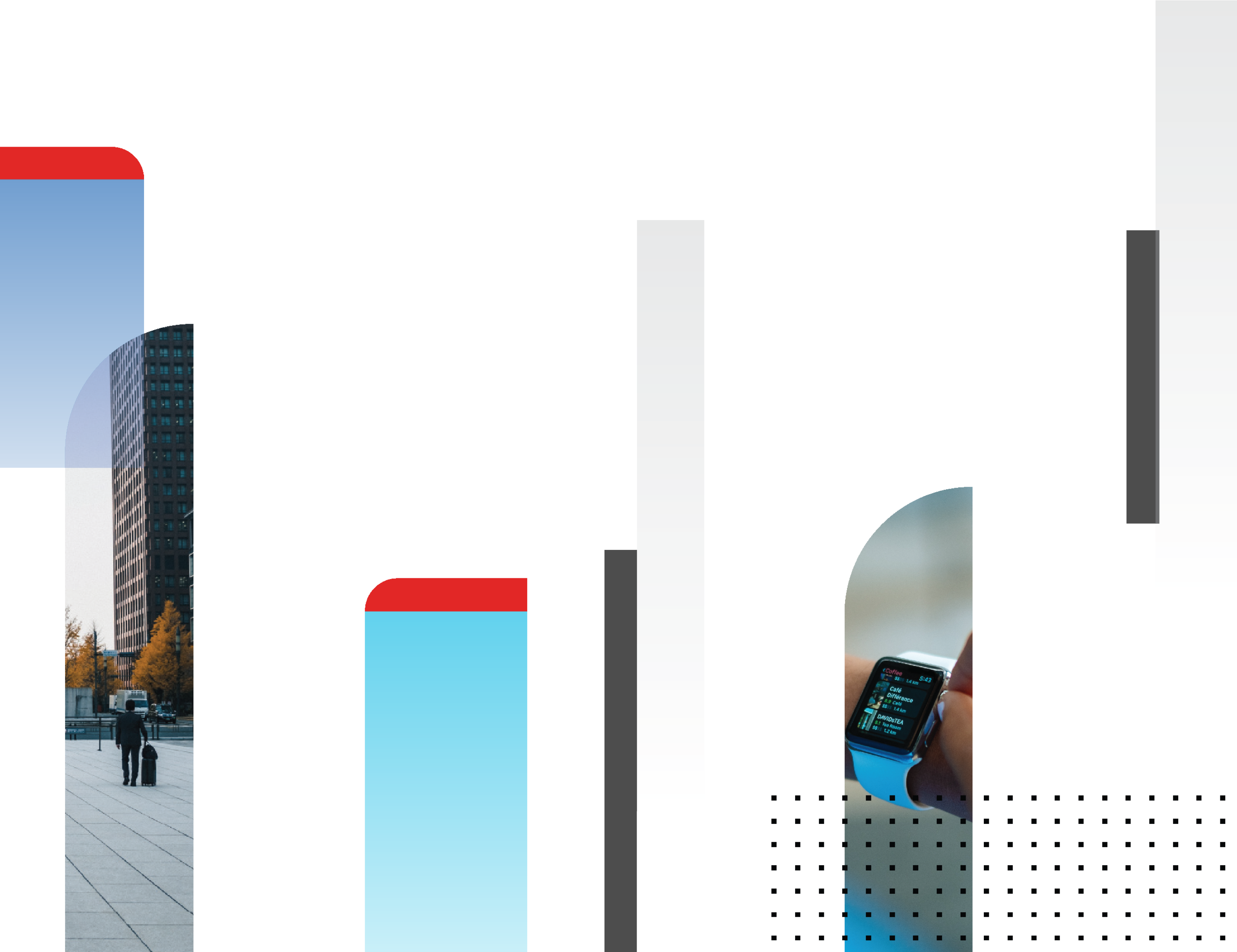
Release Notes

FortiClient EMS 7.0.2



FORTINET®

October 25, 2021
FortiClient EMS 7.0.2 Release Notes
04-702-744819-20211025

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 7.0.2 build 123:

- Special notices on page 6
- What's new on page 8
- Upgrading on page 9
- Resolved issues on page 12
- Known issues on page 14

For information about FortiClient EMS, see the *FortiClient EMS 7.0.2 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 7.0.2 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 7.0.2, 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 adds an improvement to endpoint security that impacts compatibility between FortiClient and EMS, and the recommended upgrade path. The FortiClient 7.0.2 installer is not available on FortiGuard Distribution Servers (FDS). To use the FortiClient 7.0.2 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 7.0.2, 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 will no longer be able to connect to the EMS.

What's new

EMS 7.0.2 adds an improvement to endpoint security to follow industry standards. See Endpoint security improvement.

Upgrading

Upgrading from previous EMS versions

You must upgrade EMS to 7.0.2 before upgrading FortiClient.

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*.

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 7.0.2 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 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 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

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

License

Bug ID	Description
741560	Licenses for all tenants are retracted.

Upgrade

Bug ID	Description
722394	Upgrading EMS fails on Windows Server Core.
740785	Upgrading EMS fails due to duplicate key found for the object name `'dbo.forti_product_info'`.
742359	Upgrading EMS fails due to `'FCM.dbo.admin_user_old_passwords'` column not allowing nulls.

Zero Trust tagging

Bug ID	Description
740581	Cannot manage Zero Trust Network Access policy.

Administration

Bug ID	Description
742168	*Administrators* page is empty after importing user from LDAP server.

Other

Bug ID	Description
711352	Deadlocks on fcm_error logs.
743531	High CPU usage for sqlservr.exe on systems with deployment enabled.

Common Vulnerabilities and Exposures

Bug ID	Description
721744	FortiClient EMS7.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2021-41028 Visit https://fortiguard.com/psirt for more information.
746418, 751517	FortiClient EMS 7.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2021-3711 Visit https://fortiguard.com/psirt for more information.
752422	FortiClient EMS7.0.2 is no longer vulnerable to the following CVE References: • CVE-2021-42013 • CVE-2021-41773 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in version 7.0.2. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Multitenancy

Bug ID	Description
722030	FortiGate cannot get endpoint record information from EMS 7.0 and FortiOS 7.0.
722144	FortiClient cannot connect with non-default site after deleting non-default site and recreating it.
722178	FortiGate cannot get notification from EMS to call host_tag API when EMS creates new Zero Trust Network Access tag or deletes an old one.
750711	With FQDN enabled, URL is incorrect when switching between different sites.
751261	Administrator cannot delete specific users when multitenancy is enabled.
751889	EMS fails to import certificate from local ACME server if managing multiple custom sites.

Dashboard

Bug ID	Description
744018	Dashboard displays wrong license expiration alert.
752664	*Configure License* page details go blank after adding FortiCare account for licensing on EMS.

Endpoint management

Bug ID	Description
705010	EMS shows endpoints with incorrect username.
725170	Vulnerabilities that FortiClient has detected do not show in EMS.
728428	FortiClient Cloud does not have LDAP management option for administrator roles.
737217	EMS and FortiClient (Windows) report different management statuses.

Bug ID	Description
744649	Domain endpoint does not reregister after deleting domain.
748306	*Chromebook Status* drilldown pages do not show all columns if URL is lengthy.
750415	Administrator cannot delete domains.
754794	Domain sync fails with *Invalid Device data: invalid character* error.

Endpoint policy and profile

Bug ID	Description
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.
726911	FortiClient GUI does not show tags.
736179	Profile must add support for using browser as external user agent for SAML SSL VPN.
736997	Testing XML fails with errors found in the following components during parsing: `Sandboxing:'sbcloud'.`
737592	XML configuration becomes overwritten.
739218	Removable media access XML settings are not updated to EMS GUI.
742325	User cannot access URL from endpoint when URLs are set as simple expression exclusion list in EMS Web Filter.
742843	Missing `warn_invalid_server_certificate` value crashes GUI after upgrade.
746469	When creating an SSL VPN tunnel manually with XML, the certificate check details do not get passed to the main XML.
750022	Real-time protection *Delete* option does not delete file or prompt for virus detection.
751718	Web Filter changes from FortiManager or FortiGate sync incorrectly.

Zero Trust tagging

Bug ID	Description
718145	Endpoint record entries disappear from FortiGate when using EMS tags.
743765	Zero Trust tags do not save values.

Deployment and installers

Bug ID	Description
700462	FortiClient download URL refresh button fails to get new IP address.
729978	EMS fails to create deployment package that includes Windows and macOS images.
733322	Wrong configuration in default configuration of FortiClient installer. Registration after deployment fails.
751917	Editing a deployment package results in multiple recreations of the zip file.
756267	Administrator cannot delete custom installer with name that includes a space.
756715	EMS defaults *Invalid Cert Action* to *Warn* for created FortiClient installer. Workaround: EMS administrator to select *Allow* for *Invalid Cert Action* when creating FortiClient installer.

System Settings

Bug ID	Description
755166	Redirect HTTP request to HTTPS does not work.

Administration

Bug ID	Description
737139	Total number of endpoints that EMS shows is less when logged in as a read-only administrator.
744566	SAML SSO user should have restricted permissions by default.

Fabric devices

Bug ID	Description
682639	EMS never updates Fabric Devices state after authorizing the FortiGate.
708672	FortiGate can only show one FortiClient (latest connected via SSL VPN) in endpoint record list and only this FortiClient gets dynamic address.

Bug ID	Description
744403	EMS sends sysinfo changed updates to FortiGate when data has not changed.
753719	Issues on EMS (httpd.exe) with one FortiGate connected.

FortiGuard Outbreak Alert

Bug ID	Description
730007	Add EOAP package version info into FortiGuard Signature Information page.
732130	EMS must differentiate between FortiGuard Outbreak Alert rules and Zero Trust tagging rules when sending them to FortiClient.

System Settings

Bug ID	Description
729499	Endpoints fail to update antivirus (AV) signatures, causing EMS to consistently send AV out-of-date email notifications.
745913	SMTP configuration fails authentication.
751922	After deleting custom certificate, Chromebook port 8443 still holds same certificate.

License management

Bug ID	Description
716126	FortiSASE instance uses next generation endpoint security licenses.
741773	Maximum amount of license seats used per tenant causes FortiClient to lose *Application Firewall* and *Malware Protection* tabs.

Other

Bug ID	Description
702712	Many *Cannot enumerate AD Domain until email alert is sent for previous error* warning errors in EMS logs.

Bug ID	Description
720518	Memory error while compressing data errors in FCM error logs.
747752	Three FOS_Server.exe process restarts on EMS.

Change log

Date	Change Description
2021-10-25	Initial release.

FORTINET®

www.fortinet.com