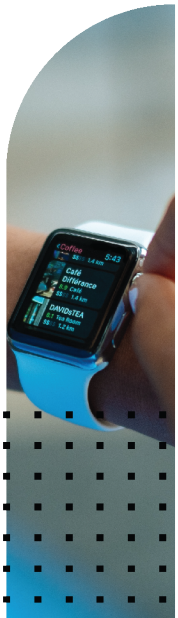
Release Notes

FortiClient EMS 7.0.12



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 04, 2024
FortiClient EMS 7.0.12 Release Notes
04-7012-1012266-20240404

TABLE OF CONTENTS

Introduction **4**
Endpoint requirements 4
Supported web browsers 4
Licensing and installation 5
Special notices **6**
FortiClient EMS Microsoft Visual C++ installation 6
SQL Server Standard or Enterprise with 5000 or more endpoints 6
Split tunnel 6
SAML logins 6
Upgrading **7**
Upgrading from previous EMS versions 7
Downgrading to previous versions 7
Product integration and support **8**
Resolved issues **10**
Endpoint management 10
Zero Trust tags 10
Known issues **11**
Administration 11
Deployment and installers 11
Endpoint control 11
Endpoint management 12
Endpoint policy and profile 12
Endpoint security 12
Fabric devices 12
GUI 13
License 13
Multitenancy 13
System Settings 13
Upgrade 13
Logs 14
Quarantine management 14
Zero Trust tagging 14
ZTNA connection rules 14
Change log **15**

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 7.0.12 build 0585:

- Special notices on page 6
- Upgrading on page 7
- Product integration and support on page 8
- Resolved issues on page 10
- Known issues on page 11

For information about FortiClient EMS, see the FortiClient EMS 7.0.12 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 8 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 7.0.12 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 VC version installed, the installation fails. See VC++ 2015 Redistributable installation returns error 1638 when newer version already installed.

If you have a VC version 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 7.0.12, 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.

SAML logins

Upon initial SAML single sign on account login, EMS creates a standard administrator for this user in *Administration* > *Admin Users*. A standard administrator has permissions to modify endpoints, policies, and settings. Having the EMS super administrator manually assign the proper role to the newly created login is recommended.

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 7.0.12 product integration and support information:

Server operating systems	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016
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	• 7.4.0 and later • 7.2.0 and later • 7.0.0 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	• 7.4.0 and later • 7.2.0 and later • 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 • 4.0.0 and later • 3.2.0 and later • 3.1.0 and later

Installing and running EMS on a domain controller is not supported.

Resolved issues

The following issues have been fixed in version 7.0.12. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Endpoint management

Bug ID	Description
974761	LDAP sync has issue: *Cannot insert duplicate key in object 'dbo.FortiClients_users'.*
995512	EMS fails to delete domain and shows server error message.

Zero Trust tags

Bug ID	Description
991962	Zero trust network access policies fail to apply to matched endpoints.

Known issues

The following issues have been identified in version 7.0.12. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Administration

Bug ID	Description
678899	LDAP configuration is persistent in EMS multitenancy global/default/non-default administration users.
828490	EMS fails to update email address from personal information from FortiClient.
924646	*Your permissions might have been updated* message displays on endpoints with vulnerability/antivirus scan request with endpoint administrator.

Deployment and installers

Bug ID	Description
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.
847870	FortiClient Cloud does not include packaged installer when sending email invitation.
878308	Next scheduled scan displays incorrect date.

Endpoint control

Bug ID	Description
863131	GUI does not show or shows inconsistent quarantine files.
928110	FortiClient clones share the same UID after using removeFCTID.exe with Ctrix MCS.

Endpoint management

Bug ID	Description
831108	User cannot download PDF report of Cloud Sandbox events on EMS.
831359	Forensics analysis *Download Report* option opens the report instead of downloading it.
836134	Inverse selection with ! does not work for deployment package, profile, and features under *All Endpoints* view.
845739	EMS shows VMware clones with duplicated UUIDs.
861603	Cloud Sandbox scan event details are not visible.
904348	FortiClient and EMS detect encryption status as not enabled when only one hard disk has encryption (Bitlocker) enabled.

Endpoint policy and profile

Bug ID	Description
826013	Setting Vulnerability Scan patch status to *Not* does not work.
826940	EMS does not save `<temp_whitelist_timeout>` in an endpoint profile.
989640	FortiClient does not follow EMS profile after EMS updates *Feature Select* settings.

Endpoint security

Bug ID	Description
960595	Some FortiClient endpoints cannot reach FortiClient Cloud.

Fabric devices

Bug ID	Description
850144	FortiClient Cloud connection fails/breaks during HA failover.

GUI

Bug ID	Description
819205	License widget shows Forensic license as *NaN used of X* when no license is in use.
929410	Admin page has delay with LDAP accounts.

License

Bug ID	Description
868174	EMS shows features for future license.

Multitenancy

Bug ID	Description
816600	Non-default site database does not update EMS serial number after new license upload.

System Settings

Bug ID	Description
807340	EMS tries to connect to FortiGuard Anycast server on port 8000.
829631	User cannot disable *Delete Timeout* option.

Upgrade

Bug ID	Description
918021	EMS cannot enforce user verification after upgrade from 6.4.8.

Logs

Bug ID	Description
856952	EMS is missing update daemon logs.

Quarantine management

Bug ID	Description
956891	FortiClient does not download EMS allowlist file, preventing file restore from *Quarantine Management*.

Zero Trust tagging

Bug ID	Description
843774	EMS ZTNA Monitor shows VPN connected IP address when IP address range matches with LAN IP address.

ZTNA connection rules

Bug ID	Description
838317	ZTNA status display should be updated in Endpoint Details.

Change log

Date	Change description
2024-04-04	Initial release.

www.fortinet.com