Release Notes

FortiClient EMS 7.2.0

TABLE OF CONTENTS

Introduction

FortiClient Endpoint Management Server (EMS) is a system intended to be used to manage FortiClient installations. 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 7.2.0 build 0689:

For information about FortiClient EMS, see the *FortiClient EMS 7.2.0 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 7.2.0 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

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 Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise.

Split tunnel

In EMS 7.2.0, 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.

What's new

For information about what's new in FortiClient EMS 7.2.0, see the FortiClient & FortiClient EMS 7.2 New Features Guide.

Upgrading

Upgrading from previous EMS versions

> EMS 7.2.0 only supports FortiClient 7.2 and 7.0. You must first upgrade older FortiClient versions to 7.0.7 or newer before upgrading EMS to 7.2.0.

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.

EMS 7.2.0 does not support legacy Fabric Agent licenses, which were in use before 2021 and have reached end-of-life (EOL). Following is a list of discontinued SKUs:

- FC1-15-EMS01-297-01-DD
- FC2-15-EMS01-297-01-DD
- FC3-15-EMS01-297-01-DD
- FC4-15-EMS01-297-01-DD
- FC1-15-EMS03-297-01-DD
- FC2-15-EMS03-297-01-DD
- FC1-15-EMS01-158-02-DD
- FC1-15-EMS02-158-02-DD

If you have the Fabric Agent licenses, you must convert the license to a different license type using the Fortinet Customer & Service Support portal before proceeding with EMS upgrade to 7.2.0. See Upgrading from an earlier FortiClient EMS version for details.

If you attempt an upgrade to EMS 7.2.0 with the legacy licenses, the EMS installer displays an error message: "Legacy Fabric Agent license is not supported after upgrade". The EMS upgrade does not proceed.

Downgrading to previous versions

FortiClient EMS does not support downgrading to previous EMS versions.

Product integration and support

The following table lists version 7.2.0 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 • 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	• 7.2.0 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. When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.2.0, use FortiClient 7.2.0.
FortiAuthenticator	• 6.4.0 and later • 6.3.0 and later • 6.2.0 and later • 6.1.0 and later • 6.0.0 and later
FortiClient (Linux)	• 7.2.0 • 7.0.2 and later
FortiClient (macOS)	• 7.2.0 • 7.0.2 and later
FortiClient (Windows)	• 7.2.0 • 7.0.2 and later
FortiManager	• 7.2.0 and later • 7.0.0 and later
FortiOS	• 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

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

Resolved issues

The following issues have been fixed in version 7.2.0. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Administration

Bug ID	Description
678899	LDAP configuration persists in EMS multitenancy global/default/non-default administration users.
853647	EMS displays no administrators found error.
853830	EMS console times out. Inactivity timeout logs off administrator despite EMS activity.
871765	Active Directory (AD) connector fails to start after upgrade from 7.0.7 to 7.2.0 if authentication credential expired.

Dashboard

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

License

Bug ID	Description
818702	Log viewer fails to check for license expiration: type object `'License'` has no attribute `'get'`.
821767	FortiClient Cloud displays license expiry error when license is unexpired.
870207	EMS crashes after user applies incorrect license.

Multitenancy

Bug ID	Description
848558	Non-default site sends `LIC_ED|0|` to FortiClient.
873029	FortiClient shows as disconnected and licenses for all multitenancy sites are removed and returned to global site after upgrading EMS from 7.0.7 to 7.2.0.

Onboarding

Bug ID	Description
819203	Authorized user group name is not full path.
822126	Deleting SAML configuration message shows incorrect active users.
835182	The DELETE statement conflicts with the REFERENCE constraint `fk_Forticlient_Users_Users_machine_user_id`.
866140	Authorized groups do not work with SAML verification.

ZTNA connection rules

Bug ID	Description
832635	Off-fabric FortiClient certificate serial number does not sync to FortiOS.

System Settings

Bug ID	Description
823701	FortiClient Cloud does not allow enabling *Enforce User Verification*.
839677	EMS displays notification: Failed to send email alerts. Please check SMTP server configuration.

Endpoint management

Bug ID	Description
727076	EMS does not process uploaded software inventory.
770364	EMS displays third-party features section for non-Windows endpoints.
801583	EMS shows clients as unprotected if they have third-party antivirus.
808266	EMS has inaccurate dashboard widget results for endpoints with Windows operating systems.
819196	The multipart identifier `cs.software_id` and `cs.is_missing` cannot be bound.
821704	EMS always reports device state as managed in verified and unverified user table even after FortiClient unregisters from EMS.
825673	EMS clears all entries after upgrade and does not allow traffic for some users.
827269	Policy is out of sync when moving endpoints using group assignment rules.
834228	EMS reports endpoint vulnerability when Vulnerability Scan is not installed on endpoint.
835705	Group assignment rules Run Rules Now option does not work.
839300	EMS fails to download PDF report of on-premise FortiSandbox events.
842539	EMS shows endpoints duplicated in multiple groups after EMS upgrade.
846033	EMS displays error during AD sync when an organizational unit's old ancestor is deleted from the domain.

Endpoint policy and profile

Bug ID	Description
818408	Malware Protection profile antiexploit application list includes applications that FortiClient does not support.
824666	EMS does not send FortiClient status changes via syslog.
832445	Web Filter profiles are mismatched between EMS and FortiGate for cryptomining category.
842084	Profile GUI is blank.
852508	FortiClient blocks all USB sticks after adding revision in Malware Protection profile.

Install and upgrade

Bug ID	Description
828850	Deadlocks on Users and Forticlients_users table.
835824	Upgrade from 7.0.4 to 7.0.6 fails.

FortiGuard Outbreak Alerts

Bug ID	Description
813928	EMS fails to update EOAP signatures: type object `ComplianceVerificationRuleSet` has no attribute `eoap_version`.

Zero Trust telemetry

Bug ID	Description
836156	User cannot access FortiClient Cloud.

HA

Bug ID	Description
809396	EMS generates a generic error on high availability (HA) backup.
832719	EMS shows error while trying to restore backup.

GUI

Bug ID	Description
632427	Software Inventory filter and sort actions in heading do not work.
774880	EMS user can import the same zero trust tagging rules multiple times by clicking *Import* button multiple times.

Deployment and installers

Bug ID	Description
842065	FortiClient cannot connect to EMS after upgrade from 7.0.2 to 7.0.7.
859123	Only FortiClient 7.0.7 appears in installers list. EMS shows no custom installers.

Zero Trust tagging

Bug ID	Description
802599	EMS should calculate zero trust network access (ZTNA) rules.
827300	Endpoint does not get correct zero trust network access tag.
832328	Endpoint is still tagged with threat ID rule after clearing firewall events.
837163	EMS shows hosts with indicators of compromise for Ransomware Evil (REvil) but shows details as *No REvil_IOC_registry_key - Compromised Endpoints (0) Found*.
841675	EMS receives network information but does not send it to FortiGates.
874683	EMS does not tag some endpoints with AD group after disabling *Evaluate on FortiClient* on the rule.
874693	When a rule set has an AD FortiClient-based rule and at least one non-FortiClient rule of any type, the AD rule is not loaded.

Endpoint control

Bug ID	Description
813439	FortiClient registered with EMS IP address does not deregister from EMS when administrator enforces invitation-only registration for all endpoints.
825559	FortiClient fails to register with EMS when *Enforce invitation-only registration for* is enabled.
840199	EMS stops allowing client connections.
848147	EMS sends malformed SAML URL to FortiClient.

Performance

Bug ID	Description
801299	spUpdateIPList and trigger_users_UPDATED errors.

Endpoint security

Bug ID	Description
783287	Let's Encrypt ACME certificate request fails due to port 80 on autotest system.

Other

Bug ID	Description
844330	EMS reports vulnerability to web server dictionary indexing/dictionary directory listing attack.
873218	Multiple FortiClient records share the same token ID.

Common Vulnerabilities and Exposures

Bug ID	Description
766139	FortiClient EMS 7.2.0 is no longer vulnerable to the following CVE References: • CVE-2021-44172 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in version 7.2.0. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Dashboard

Bug ID	Description
817485	Drilldown on macOS vulnerability includes unrelated vulnerabilities.
821570	Vulnerability count on vulnerability widgets does not match the actual number of vulnerabilities.

Endpoint management

Bug ID	Description
786738	Anti-Ransomware Events tab is visible after disabling the feature in Feature Select.
792447	EMS fails to show zero trust network access (ZTNA) feature in endpoint details enabled/disabled features section.
792652	EMS cannot delete domain.
798409	EMS does not display detected paths of vulnerabilities.
823047	After upgrading from 6.4.4 to 7.0.4, FCM Events table grows exponentially.
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	VMware clones in EMS duplicate UUID.
861603	Cloud Sandbox scan event details are not visible.
868104	FortiClient does not reconnect to EMS after deploying 7.2.0 Beta 1 over 7.0.7 GA.
874908	Moving device in workgroup shows error.

Endpoint policy and profile

Bug ID	Description
466124	User cannot change `<nat_alive_freq>` value.
826013	Setting Vulnerability Scan patch status to *Not* does not work.
826940	EMS does not save `<temp_whitelist_timeout>` in an endpoint profile.
833819	Backing up configuration files on FortiClient Cloud results in import errors.
868534	Web Filter profile synced from FortiGate keeps disabled status links in the exception list.

License

Bug ID	Description
823690	EMS includes Removable Media Access feature when using ZTNA user-based license.
827875	Non-default site's License information page shows irrelevant license information.
828944	EMS does not show *A new license has been detected...* if synced with FortiCloud account.
834686	Allocating license to site resets if changes are done to default site license.
846993	Multitenancy-enabled EMS removes license from multiple sites.
868174	EMS shows features for future license.

Multitenancy

Bug ID	Description
777642	Global site does not list FortiCloud license- and account-related logs.
816600	Non-default site database does not update EMS serial number after new license upload.
820803	License distribution modal shows incorrect information.
868478	FortiSASE input field is invisible for future license when the current FortiSASE is deselected in the add/edit site form.

Fabric devices

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

Zero Trust tagging

Bug ID	Description
810778	FortiClient tag information is not shared equally to connected FortiGate Fabric devices.
843774	ZTNA monitor shows VPN connected IP address when IP address range matches with LAN IP address.
875503	Error 400 "Can only enable up to 10 rules set" displays while trying to reenable EMS ZTNA tag.

Deployment and installers

Bug ID	Description
714496	FortiClient Cloud upgrade keeps installer on instance and causes disk to have no space.
764999	EMS does not list FortiClient versions in official installer list if FDS blocks EMS from downloading said versions.
783690	The system does not prompt for reboot after user login.
824936	EMS fails to deploy FortiClient when manually created FortiClient installer is updated.
874652	After updating the FortiClient version on an assignable installer on FortiClient Cloud, the zip file contains installers for both versions.
878308	EMS displays incorrect date for next scheduled scan.

System Settings

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

Bug ID	Description
820889	FortiGuard services setting for FortiManager selector switch shows as disabled after configuring and logging out of EMS.
829631	User cannot disable *Delete Timeout* option.
861109	EMS does not send email alerts for Active Directory events.

Logs

Bug ID	Description
827295	FortiClient cannot connect to FortiClient Cloud.
856952	FortiClient EMS is missing update daemon logs.
871050	EMS does not send FortiClient logon message offline to syslog server (FortiAuthenticator).

Administration

Bug ID	Description
828490	*Permission Denied : Your permissions might have been updated* error message displays for all admin roles.
867746	Deleting large domain quickly fails.

Performance

Bug ID	Description
759729	EMS has possible slow httpd file handle leak.

HA

Bug ID	Description
824066	spHAKeepAlive deadlock causes failover.
860787	With always on high availability (HA) on multitenancy-enabled in multisubnet environment,

Bug ID	Description
	FCEMS_monitor stops and EMS loses all configured license seats.
860903	The \\FCM_Default_Filesync\\ directory increases in size until space is exhausted. This causes the EMS console to change nodes.

ZTNA connection rules

Bug ID	Description
838317	EMS does not update ZTNA status display in endpoint details.
868825	ZTNA service portal does not allow for external browser for SAML authentication.

Endpoint control

Bug ID	Description
857179	EMS sends `FCKARPLY: CONT|0` if DAS cannot access the database.
863131	GUI does not show quarantine files or shows inconsistent ones.

GUI

Bug ID	Description
717433	Patching a vulnerability for a specific endpoint patches it on others.
819205	License widget shows Forensic license as *NaN used of X* when no license is in use.
870219	EMS deployment only shows domain NetBIOS name under endpoint groups.
871491	Deselecting an item from item list removes the deselected item.

Avatar and social login information

Bug ID	Description
830117	EMS fails to update email address from personal information form in FortiClient.

FortiGuard outbreak alert

Bug ID	Description
819025	With multiple sites, EMS fails to display FortiGuard outbreak detection rules downloaded from FortiGuard distribution server (FDS).

FortiClient Cloud API

Bug ID	Description
585763	User cannot log in to FortiClient Cloud if they are using the same browser for login to on-premise EMS. **Workaround**: Clear the browser client cache or use a different browser.
832144	User cannot call APIs in FortiClient Cloud. **Workaround**: Clear the browser client cache or use a different browser.

Other

Bug ID	Description
766163	Browser causes FortiClient Cloud issues.
847870	FortiClient Cloud does not include packaged installer when sending email invitation.
868556	EMS is missing newly added signature information in FortiGuard signature information page.

Change log

Date	Change Description
2023-01-31	Initial release.
2023-04-11	Added SAML logins on page 7.

FEERTINET