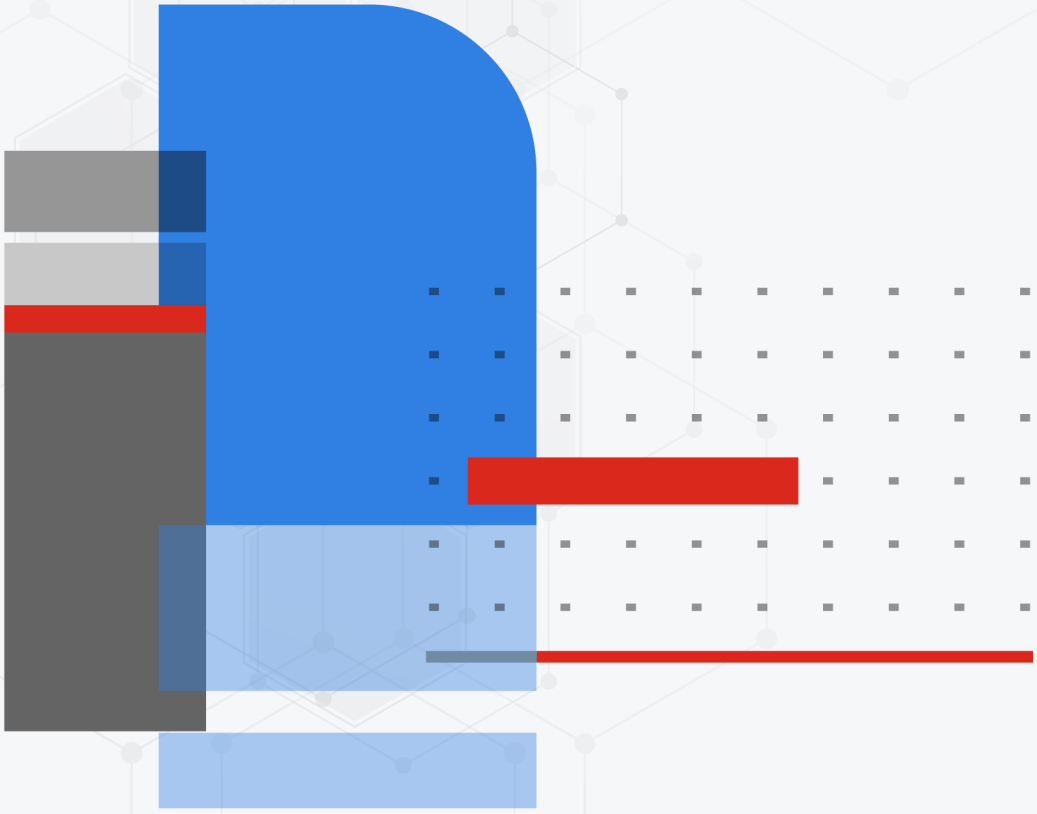
Release Notes

FortiClient EMS 7.4.5



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

January 23, 2026
FortiClient EMS 7.4.5 Release Notes
04-745-1208452-20260123

TABLE OF CONTENTS

Change log

Date	Change description
2025-12-11	Initial release.
2025-12-16	Updated Resolved issues on page 17.
2026-01-13	Updated Resolved issues on page 17.
2026-01-19	Updated Product integration and support on page 15.
2026-01-23	Updated Existing known issues on page 21.

Introduction

FortiClient Endpoint Management Server (EMS) is a Linux-based system that manages FortiClient installations on the following FortiClient platforms:

- Microsoft Windows
- macOS
- Linux
- Android OS
- Apple iOS
- ChromeOS and ChromeOS Flex

This document provides the following information for FortiClient EMS 7.4.5 build 2111.M:

For information about FortiClient EMS, see the *FortiClient EMS 7.4.5 Administration Guide*.

Fortinet uses the following version number format:

<Major version number>.<minor version number>.<patch number>.<build number>

Example: 7.4.5.2111.M

Release Notes correspond to a certain version and build number of the product.

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 15 for FortiClient version support information.

Supported web browsers

The latest version of the following web browsers can be used to connect remotely to the FortiClient EMS 7.4.5 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

Changes to compatibility with FortiManager 7.4 and 7.6

EMS 7.4.5 drops support for FortiManager 7.4.0-7.4.8 and 7.6.0-7.6.4 due to the communication protocol upgrade from HTTP/1.0 to HTTP/2. Unlike HTTP/1.x, the new HTTP/2 replies do not include a traditional "200 OK" text response and cannot be interpreted by those FortiManager versions.

Web filter profile import limitation

FortiClient EMS 7.4.0-7.4.5 do not support importing web filter profiles from FortiOS 7.6.4 or later.

Entra ID integration support limitation

FortiClient EMS supports Entra ID integration with Azure commercial subscription only. Azure Government (e.g. GCC, GCC High, GCC DoD) is not supported.

Split tunnel

In EMS 7.4.5, 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.

FortiGuard Web Filtering category v10 update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency websites. To use the new categories, customers must upgrade their Fortinet products to one of the following versions:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.8 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS: https://support.fortinet.com/Information/Bulletin.aspx

What's new

For information about what's new in FortiClient EMS 7.4.5, see the FortiClient & FortiClient EMS 7.4 New Features Guide.

Installation information

Firmware images and tools

The following files are available in the firmware image file folder:

File	Description
forticlientems_ 7.4.5.2111.M.amd64.bin	FortiClient EMS installer for x86-64 processor.
forticlientems_ 7.4.5.2111.M.arm64.bin	FortiClient EMS installer for ARM64 processor.
forticlientems_7.4.5.2111.M_ migration_tool.zip	FortiClient EMS migration tool.
forticlientems_7.4.5.2111.M_ postgres-ha.tar.gz	PostgreSQL (Postgres) Docker container for EMS high availability.
forticlientems_7.4.5.2111.M_ postgresql15.tar.gz	Postgres Docker container for EMS installation with remote database.
FortiClientEMSADConnector.msi	Active Directory (AD) connector, which acts as a proxy between the AD server and EMS.
FORTINET-FORTICLIENTEMS-build2111.M.mib	MIB file. Your SNMP manager requires this information to monitor EMS settings and receive traps from the EMS SNMP agent.

The following tools and files are available in the forticlientems_7.4.5.2111.M_migration_tool.zip file:

File	Description
migration.exe	Migration tool.
migration.config	Migration tool config file.

VM Images

The following EMS VM images are available to deploy in virtual environment:

File	Description
forticlientems_ vm.7.4.5.2111.M.ova.zip	VMware vSphere - ESXi Hypervisor

File	Description
forticlientems_vm.7.4.5.2111.M.qcow2.zip	Linux KVM (Kernel-based virtual machines)
forticlientems_vm.7.4.5.2111.M.vhdx.zip	Microsoft Hyper-V
forticlientems_vm.7.4.5.2111.M.vmdk.zip	Oracle VirtualBox

Upgrading

Upgrading from previous EMS versions

See Upgrading EMS in the *EMS Administration Guide* for details.

Upgrade endpoints running older FortiClient versions

EMS 7.4.5 only supports FortiClient 7.4, 7.2, and 7.0. You must first upgrade older FortiClient versions to 7.0.7 or newer before upgrading EMS to 7.4.5.

Endpoint security improvement

With the endpoint security improvement feature, there are backward compatibility issues to consider while planning upgrades. See Recommended upgrade path.

Legacy Licenses

EMS 7.4.5 does not support legacy 158 licenses, which were in use before 2021 and have reached end-of-life. Following is a list of discontinued SKUs:

- FC1-15-EMS01-158-02-DD
- FC1-15-EMS02-158-02-DD

If you attempt an upgrade to EMS 7.4.5 with the legacy 158 licenses, the EMS installer displays an error message: *Legacy license is not supported after upgrade*. The EMS upgrade does not proceed.

EMS 7.4.5 does not support the following legacy licenses:

- 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-EMS03-298-01-DD
- FC2-15-EMS03-298-01-DD
- FC1-15-EMS01-299-01-DD
- FC2-15-EMS01-299-01-DD

- FC3-15-EMS01-299-01-DD

You may use the EMS migration tool to migrate your Windows Server-based EMS 7.2 to the Linux-based EMS 7.4. If you attempt to migrate EMS 7.2 using a legacy license to EMS 7.4 using the migration tool, the migration tool aborts the process and displays `Current EMS Windows license is not supported in EMS Linux, migration is aborted`.

Downgrading to previous versions

FortiClient EMS does not support downgrading to previous EMS versions.

Product integration and support

The following table lists version 7.4.5 product integration and support information:

Server operating systems	• Ubuntu 22.04/24.04 LTS Server and Desktop—Minimal Ubuntu is not recommended as it may lack some packages required by EMS. • Red Hat Enterprise Linux 9 • CentOS Stream 9
Minimum system requirements	• 2.0 GHz 64-bit processor, six virtual CPUs • 12 GB RAM • 80 GB free hard disk • Gigabit (10/100/1000baseT) Ethernet adapter • Internet access is recommended, but optional, during installation. EMS also tries to download information about FortiClient signature updates from FortiGuard. • ext4 file system Fortinet recommends that you install only FortiClient EMS and the default services on the Linux server and no other additional applications.
FortiOS	• 7.6.0 and later—For FortiOS 7.6.3 and later versions, see SSL VPN tunnel mode replaced with IPsec VPN. • 7.4.0 and later
FortiClient (Windows)	• 7.4.0 and later • 7.2.0 and later
FortiClient (macOS)	• 7.4.0 and later • 7.2.0 and later
FortiClient (Linux)	• 7.4.0 and later • 7.2.0 and later
FortiClient iOS and Android	• 7.4.0 and later
FortiAnalyzer	• 7.6.0 and later • 7.4.0 and later
FortiManager	• 7.6.5 and later • 7.4.9 and later  EMS 7.4.5 does not support FortiManager 7.4.0-7.4.8 and 7.6.0-7.6.4 due to the communication protocol upgrade from HTTP/1.0 to HTTP/2. See Changes to compatibility with FortiManager 7.4 and 7.6 on page 8 for more details.
FortiAuthenticator	• 8.0.0 and later • 6.6.0 and later • 6.5.0 and later

FortiSandbox	• 5.0.0 and later • 4.4.0 and later

Resolved issues

The following issues have been fixed in version 7.4.5. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Installation and Upgrade

Bug ID	Description
1211414	Endpoint profile values revert to previous settings after EMS upgrade from 7.4.3 to 7.4.4.

Deployment and Installers

Bug ID	Description
1203744	Installer assigned to a group of endpoints does not trigger the upgrade as the deployment schedule is not created.

Endpoint Management

Bug ID	Description
1216934	Entra ID sync and deregistration issue.
1179268	Large Entra ID domain import fails.

Endpoint Policy and Profile

Bug ID	Description
1162867	EMS Cloud displays duplicate entries for web filter profiles imported from FortiGate. Deleting one of the duplicated entries results in both being removed.

Bug ID	Description
1176906	After switching from "Manual Set" to "Mode Config" for an IKEv2 tunnel, EMS still pushes the old manually set configuration to FortiClient.
1204095	Entra ID users are not matched against policies and end up matching the default policy.

Fabric and Connectors

Bug ID	Description
1150817	No "Delete associated auto-detected ZTNA application data" option when removing a FortiGate from an HA cluster.
1231061	All destinations configured and synced from the FortiGate are duplicated on the ZTNA Applications Catalog.

HA

Bug ID	Description
1205131	PostgreSQL database failover causes EMS server failover.
1208343	In a setup of EMS HA with Postgres HA, the secondary EMS node appears offline after a failover process of Postgres DB.

License

Bug ID	Description
1206645	Licensing of EMS is failing after the migration from 7.2.10 to 7.4.4.
1222776	VPN gateway is changed in VPN profile after migration or upgrade to EMS 7.4.4.
1217373	FortiFlex license does not have a license grace period. A license accident can cause seats to reset.

Software Inventory

Bug ID	Description
1209075	All software inventory is deleted within 10 minutes of software being reported by FortiClient.

Zero Trust Telemetry (On Boarding)

Bug ID	Description
1195127	EMS login using email fails if the UPN and SAM account name have different naming conventions.

ZTNA TCP/UDP Forwarding

Bug ID	Description
1104178	ZTNA application is missing after being edited on the FortiGate.
1158448	The alias for a ZTNA server disappears from the EMS GUI after you create a new ZTNA server on the FortiGate.
1184219	Auto-detected ZTNA destinations cannot be deleted, even after removal on the FortiGate.

FortiGuard Outbreak

Bug ID	Description
1103367	Outbreak detection rules are tagged/untagged by EMS.

Vulnerabilities and Exposures

FortiClient EMS 7.4.5 is no longer vulnerable to the following CVE reference. Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
1199423	CVE-2025-59922

Known issues

Known issues are organized into the following categories:

- New known issues on page 21
- Existing known issues on page 21

To inquire about a particular bug or to report a bug, contact Customer Service & Support.

New known issues

No new issues have been identified in version 7.4.5.

Existing known issues

The following issues have been identified in a previous version of FortiClient EMS and remain in FortiClient EMS 7.4.5.

Deployment and installers

Bug ID	Description
1247961	EMS deployment to update FortiClient feature sets for the same FortiClient version fails unless the initial deployment was done using the EMS-generated FortiClient EXE installer or the MSI file (rather than the MST file).

Endpoint control

Bug ID	Description
1213829	FortiClient auth-period registry is not reset to 0 after *User Verification Period* is disabled in EMS.
1208862	Entra ID user verification fails if MFA is made compulsory on Entra ID side.

Endpoint management

Bug ID	Description
1127493	EMS displays inaccurate user information for endpoints running on the Windows Server operating system.
1211682	Unable to delete ADDS authentication server when it is not reachable.

Endpoint policy and profile

Bug ID	Description
1089889	Chromebooks intermittently receive error *Failed to retrieve user profile from FortiClient EMS*.
1219573	EMS fails to apply Entra ID policies to Entra ID-joined devices that use an alias domains instead of the primary UPN domain.

GUI

Bug ID	Description
1186739	Back button in endpoint vulnerability details page returns to Dashboard instead of previous page.

www.fortinet.com