FORTINET

Release Notes

FortiClient EMS 7.4.4

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

TABLE OF CONTENTS

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
- Chrome OS

This document provides the following information for FortiClient EMS 7.4.4 build 2034.F:

- Special notices on page 7
- What's new on page 8
- Installation information on page 9
- Upgrading on page 11
- Product integration and support on page 13
- Resolved issues on page 15
- Known issues on page 20

For information about FortiClient EMS, see the *FortiClient EMS 7.4.4 Administration Guide*.

Fortinet uses the following version number format:

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

Example: 7.4.4.2034.F

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 13 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 7.4.4 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

Split tunnel

In EMS 7.4.4, 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, 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 7.4.4, 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_ 7.4.4.2034.F.amd64.bin	FortiClient EMS installer for x86-64 processor.
forticlientems_ 7.4.4.2034.F.arm64.bin	FortiClient EMS installer for ARM64 processor.
forticlientems_7.4.4.2034.F_ migration_tool.zip	FortiClient EMS migration tool.
forticlientems_7.4.4.2034.F_ postgres-ha.tar.gz	PostgreSQL (Postgres) Docker container for EMS high availability.
forticlientems_7.4.4.2034.F_ 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.

The following tools and files are available in the forticlientems_7.4.4.2034.F_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.7.4.4.2034.F.ova.zip	VMware vSphere - ESXi Hypervisor

File	Description
forticlientems_ vm.7.4.4.2034.F.qcow2.zip	Linux KVM (Kernel-based virtual machines)
forticlientems_ vm.7.4.4.2034.F.vhdx.zip	Microsoft Hyper-V
forticlientems_ vm.7.4.4.2034.F.vmdk.zip	Oracle VirtualBox

Upgrading

Upgrading from previous EMS versions

Upgrade endpoints running older FortiClient versions

EMS 7.4.4 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 7.4.4.

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 7.4.4 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 7.4.4 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 7.4.4 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 7.4.4 product integration and support information:

Server operating systems	• Ubuntu 22.04 LTS Server and Desktop • Ubuntu 24.04 LTS Server and Desktop • 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 • 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
FortiClient (Windows)	• 7.4.0 and later • 7.2.0 and later • 7.0.2 and later
FortiClient (macOS)	• 7.4.0 and later • 7.2.0 and later • 7.0.2 and later
FortiClient (Linux)	• 7.4.0 and later • 7.2.0 and later • 7.0.2 and later
FortiAnalyzer	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiManager	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later

FortiAuthenticator	• 6.6.0 and later • 6.5.0 and later • 6.4.0 and later • 6.3.0 and later
FortiSandbox	• 4.4.0 and later • 4.2.0 and later • 4.0.0 and later

Resolved issues

The following issues have been fixed in version 7.4.4. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Administration

Bug ID	Description
1138296	Admins with *Manage Invitations* permission cannot create invitations in EMS 7.4 due to an unexpected error.

Endpoint Management

Bug ID	Description
1095972	Local ad connector stuck at 1%.
1111936	Higher maximum limit for EMS license timeout setting.
1117228	LDAP sync fails due to long UPN char with the following error: *error: mssql: The data for table*valued parameter "@updated" doesn't conform*.
1119648	EMS is showing SAM user name instead of UPN name for endpoints logged in with Azure account.
1135123	Unable to add LDAP admin and unable to import user/device from domain with the following error: *Invalid idp guid*.
1139290	EMS AD sync intermittently fails with bind parameter and Kerberos errors.
1139723	LDAP sync improvement: reduce number of binds.
1142865	EMS Cloud AD connector randomly goes offline and then comes online again.
1148779	(FortiClient EMS Windows) LDAP sync error "*uq_users_uid_name_sid_saml_id_auth_type_upn_domain_id*".
1150306	Endpoints cannot be returned to original group after being moved to a custom group.
1150641	Ad connector gets stuck after LDAP connection timeout.
1152075	GUI inconsistency in reporting the sync progress for LOCAL AD domain.

Bug ID	Description
1166665	LDAP sync fails due to special characters in user data.

Endpoint Policy and Profile

Bug ID	Description
1112386	EMS does not apply Azure user-group policies intermittently.
1136465	Error syncing web filter profile from FortiManager.
1142846	ZTNA application import enables UDP while the enable_udp option is set to FALSE.
1159904	Azure AD group-based policy assignments are not being applied: endpoints are receiving the default policy.

Endpoint control

Bug ID	Description
1140281	Existing HTML files of "send one-way message" using Japanese cannot be previewed due to an error.

Fabric Devices

Bug ID	Description
1142252	FortiGate fails to sync security posture tags from EMS, blocking compliant VPN users.
1169328	The firewall dynamic address table still keeps the IP/MAC even when VPN client is down.

GUI

Bug ID	Description
1153047	EMS vulnerability scan dashboard shows wrong number of affected endpoints.

Onboarding

Bug ID	Description
1126324	Cannot delete SAML configuration.
1139975	AD UPN matching case sensitity for user verification with SAML authentication and domain authorization.
1147712	FortiClient cannot connect to EMS using AD accounts where SAMAccountName differs from UPN.
1163833	EMS Cloud: invitation emails lose installer link after a while.

Other

Bug ID	Description
1107278	Custom port numbers change when migrating from Windows Server-based EMS 7.2 to Linux-based 7.4.

Remote Access

Bug ID	Description
1138981	Dh group 31 is not available in EMS dhgroup: invalid value 31.
1160262	FortiClient continiously attempts to connect to machine prelogon tunnel after user is already logged in.

System Settings

Bug ID	Description
1159054	Tag removal issue for offline endpoints despite auto tag removal being enabled.

Upgrade

Bug ID	Description
1142806	Migrating 7.2.8 to 7.4.3 or upgrade 7.4.1 to 7.4.3 can sometimes fail when running the sqitch script that adds forensic tags.
995790	During the device upgrade check, duplicate Android devices are end up getting mistaken as duplicates and deleted in upgrade.
1195599	- When FortiClient EMS 7.4.3 is installed on Ubuntu 22.04, upgrading Ubuntu to 24.04 will break the EMS database backup and restore function. - FortiClient EMS 7.4.1 may be uninstalled after upgrading the Ubuntu OS from 22.04 to 24.04.

Web Filter and Plugin

Bug ID	Description
1026115	Some web filter categories are not visible on EMS GUI for configuration.
1156273	EMS adds new XML tags to control FortiClient to force user to enabled "Allow in private" when the web filter plugin is enabled.

Zero Trust Network Access (ZTNA) Connection Rules

Bug ID	Description
1057009	EMS GUI page shows "mask must be null or an IPv4 formatted string" error message when creating a ZTNA Destinations profile.
1133163	Failed to create ZTNA application due to long FQDN.

Security Posture Tags

Bug ID	Description
1148269	In HA mode, EMS does not assign tags to the endpoint when connect to EMS after few days.
1152696	EMS 7.4.3 does not assign *User in AD group* tag to macOS endpoints.
1165567	Failure in saving security posture tags for certificate with special character in Issuer CN.

Known issues

Known issues are organized into the following categories:

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

New known issues

The following issues have been identified in version 7.4.4.

Endpoint Management

Bug ID	Description
1127493	EMS displays inaccurate user information for endpoints running on the Windows Server operating system.

Fabric Devices

Bug ID	Description
1150817	No "Delete associated auto-detected ZTNA application data" option when removing a FortiGate from an HA cluster.

FortiGuard Outbreak Detection

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

GUI

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

Zero Trust Network Access (ZTNA) Connection Rules

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.

Security Posture Tags

Bug ID	Description
1176991	Entra ID group is not shown when you hover over an affected endpoint's end user name in the EMS endpoint pane.

Existing known issues

The following issues have been identified in a previous version of FortiClient EMS and remain in FortiClient EMS 7.4.4.

Endpoint management

Bug ID	Description
1116089	User cannot delete custom group with no associated endpoints.
1117228	LDAP sync fails due to long UPN char with the following error: *error: mssql: The data for table*valued parameter "@updated" doesn't conform*.

Bug ID	Description
1117269	Active Directory (AD) sync is slow on FortiClient Cloud with AD connector.

Endpoint policy and profile

Bug ID	Description
1089889	Chromebooks intermittently receive error *Failed to retrieve user profile from FortiClient EMS*.

Other

Bug ID	Description
1107278	Custom port numbers change when migrating from Windows Server-based EMS 7.2 to Linux-based 7.4.

Change log

Date	Change description
2025-09-03	Initial release.

www.fortinet.com