



# FortiClient EMS - Release Notes

Version 6.4.4

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<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>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



June 02, 2021

FortiClient EMS 6.4.4 Release Notes

04-644-717035-20210602

# TABLE OF CONTENTS

<b>Introduction</b>	<b>4</b>
Endpoint requirements	4
Supported web browsers	4
Licensing and installation	5
<b>Special notices</b>	<b>6</b>
FortiClient EMS Microsoft Visual C++ installation	6
SQL Server Enterprise with 5000 or more endpoints	6
Split tunnel	6
<b>What's new</b>	<b>7</b>
<b>Upgrading</b>	<b>8</b>
Upgrading from previous EMS versions	8
Downgrading to previous versions	8
<b>Product integration and support</b>	<b>9</b>
<b>Resolved issues</b>	<b>10</b>
Deployment	10
Endpoint management	10
Endpoint policy and profile	10
GUI	11
Dashboard	11
Software Inventory	11
Zero Trust tags	12
Other	12
Common Vulnerabilities and Exposures	12
<b>Known issues</b>	<b>13</b>
Multitenancy	13
Dashboard	13
Endpoint management	13
Endpoint policy and profile	14
Installation and upgrade	14
Deployment	14
GUI	15
Performance	15
Chromebook	15
Zero Trust tags	15
System Settings	16
Other	16
<b>Change log</b>	<b>17</b>

# 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 6.4.4 build 1658:

- [Special notices on page 6](#)
- [What's new on page 7](#)
- [Upgrading on page 8](#)
- [Resolved issues on page 10](#)
- [Known issues on page 13](#)

For information about FortiClient EMS, see the [FortiClient EMS 6.4.4 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 9](#) 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 6.4.4 GUI:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Internet Explorer is not recommended. Remote access may need to be enabled from the FortiClient EMS GUI.

## 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 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

A split tunnel configuration that functioned in FortiClient (Windows) 6.4.1 no longer works after upgrading to 6.4.4, unless you have configured a per-tunnel configuration in EMS.

## What's new

For information about what's new in FortiClient EMS 6.4.4, see the [FortiClient & FortiClient EMS 6.4 New Features](#).

# Upgrading

## Upgrading from previous EMS versions

FortiClient EMS supports direct upgrade from EMS 6.2. To upgrade older EMS versions, follow the upgrade procedure outlined in [FortiClient and FortiClient EMS Upgrade Paths](#).

## Downgrading to previous versions

FortiClient EMS does not support downgrading to previous EMS versions.



# Product integration and support

The following table lists version 6.4.4 product integration and support information:

<b>Server operating systems</b>	<ul style="list-style-type: none"><li>• Windows Server 2019. On Windows Server 2019, preinstalling Microsoft ODBC Driver 17 for SQL Server (x64) is necessary.</li><li>• Windows Server 2016</li><li>• Windows Server 2012 R2</li></ul>
<b>Minimum system requirements</b>	<ul style="list-style-type: none"><li>• 2.0 GHz 64-bit processor, six virtual CPUs (6 vCPU)</li><li>• 8 GB RAM (10 GB RAM or more is recommended)</li><li>• 40 GB free hard disk</li><li>• Gigabit (10/100/1000baseT) Ethernet adapter</li><li>• Internet access is recommended, but optional, during installation. SQL Server may require some dependencies to be downloaded over the Internet. EMS will also try to download information about FortiClient signature updates from FortiGuard.</li></ul> <p>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.</p> <p>Suggested host system hardware configurations for FortiClient EMS depend on the number of endpoints FortiClient EMS is managing. See <a href="#">Management capacity</a>.</p>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 7.0.0 and later</li><li>• 6.4.0 and later</li></ul>
<b>FortiClient (Linux)</b>	<ul style="list-style-type: none"><li>• 6.4.0 and later</li><li>• 6.2.0 and later</li></ul>
<b>FortiClient (macOS)</b>	<ul style="list-style-type: none"><li>• 6.4.0 and later</li><li>• 6.2.0 and later</li></ul>
<b>FortiClient (Windows)</b>	<ul style="list-style-type: none"><li>• 6.4.0 and later</li><li>• 6.2.0 and later</li></ul>
<b>FortiOS</b>	<ul style="list-style-type: none"><li>• 6.4.0 and later</li><li>• 6.2.0 and later</li></ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"><li>• 4.0.0 and later</li><li>• 3.2.0 and later</li><li>• 3.1.0 and later</li></ul>



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

# Resolved issues

The following issues have been fixed in version 6.4.4. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

## Deployment

Bug ID	Description
680808	Reset deployment button is missing.
706524	Duplicated repackager processes and high CPU usage.
709419	Special characters in <code>assignable_installers</code> folder name triggers <code>fcprepaker</code> to run continuously.

## Endpoint management

Bug ID	Description
694580	After applying old trial license, EMS allows more than three endpoints to register.
696729	After trying a few times with the connection key, the migrate option stops working.
700058	FortiClient is still registered after license grace period.
707249	EMS disconnects/deregisters FortiClient randomly overnight with unstable connection.
715320	FortiClient fails to update state when FortiClient Cloud is unreachable.
717074	<i>Devices &gt; Host</i> is incomplete.

## Endpoint policy and profile

Bug ID	Description
689709	<i>Enforce Acceptance of Disclaimer Message</i> setting for one VPN tunnel affects all other VPN tunnels.
693278	<i>Send Software Inventory</i> setting does not consume EPP license seat.
694565	<i>Vulnerability Scan &gt; Disable Automatic Patching for These Applications</i> setting reverts to

Bug ID	Description
	being disabled from enabled if administrator opens XML file.
694732	<i>Test Connection</i> button for Sandbox appliance fails to work.
695086	EMS does not allow disabling Web Filter when Chromebook management is disabled.
709560	Importing FortiGate profile fails on <code>youtube-restrict</code> error.

## GUI

Bug ID	Description
642359	Console reports <i>Failed to load URL https://localhost/signin with error ERR_CONNECTION_RESET (-101)</i> after installation.

## Dashboard

Bug ID	Description
659389	<i>Dashboard &gt; Widget &gt; Windows Operating System</i> stalls the GUI.
697036	After upgrading to 6.4.3, the License Information widget on the Dashboard may incorrectly show the Next Generation Endpoint Security License status as unlicensed even though the EPP license is active and working. This is a display issue and the EPP feature will continue to work on a licensed EMS.
716353	Real-time protection (RTP) Enabled does not show in green.
716989	Security category is not blocked when RTP is enabled but Web Filter is disabled.

## Software Inventory

Bug ID	Description
711389	Administrator cannot see software inventory on EMS sent by FortiClient running on Ubuntu 20.04.2.

## Zero Trust tags

Bug ID	Description
716092	EMS fails to delete custom classification tag.
711797	FortiOS fails to display Zero Trust tag for running process.

## Other

Bug ID	Description
668389	FcmChromebookDaemon.exe crashes with FortiClient Cloud.
684313	FcmUpdateDaemon crashes.
693667	Deadlocked on spUpdateIPList.
715878	EMS online installer cannot install EMS from production FortiGuard Distribution Server.

## Common Vulnerabilities and Exposures

Bug ID	Description
685625	FortiClient EMS 6.4.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2020-1971</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.

## Known issues

The following issues have been identified in version 6.4.4. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

### Multitenancy

Bug ID	Description
647465	Some Chromebook settings should be per site and not global.
678899	Persisting LDAP configuration in multitenancy global/default/non-default administration users.
698825	EMS cannot import same organizational unit from Active Directory server when more than ten sites are enabled with default sync interval.
722144	FortiClient cannot connect to non-default site after EMS administrator deletes non-default site and recreates it.

### Dashboard

Bug ID	Description
673587	Running out of license alerts should not apply for global EMS with multitenancy enabled.
716126	FortiSASE SIA instance uses Next-Generation Endpoint Security licenses.

### Endpoint management

Bug ID	Description
649002	Sync fails when adding device with more than 256 characters in distinguished name.
697136	EMS cannot connect to LDAP server.
697620	LDAP sync fails with <i>A local error occurred.</i> error.
698222	LDAP OUs do not show correctly in <i>Edit Groups</i> of deployment package wizard.
712215	FortiClient cannot reach FortiClient Cloud (query timeout expired { <code>call spInsertClientEvents(?)</code> }).

Bug ID	Description
712466	The <i>Individual</i> button should be highlighted instead of the Bulk one in the edit page of an individual code.

## Endpoint policy and profile

Bug ID	Description
697911	Synced updates from imported FortiGate Web Filter profile do not sync to FortiClient.
706321	EMS does not sync FortiGate profile settings at scheduled interval if not logged into EMS console.
714479	Exceptions do not work for antiexploit module.

## Installation and upgrade

Bug ID	Description
712709	After upgrade, license dashboard shows Zero Trust Network Agent (ZTNA) as unlicensed.

## Deployment

Bug ID	Description
666289	EMS should report correct deployment package state.
700462	FortiClient download URL refresh button fails to get new IP address and GUI console shows error 400.
704026	FortiClient Cloud shows error 404 when trying to delete deployment package.
709569	Changing the patch level for a FortiClient installer package does not trigger FortiClient update on endpoint.

## GUI

Bug ID	Description
684209	GUI is inaccessible after uploading SSL certificate.
698698	Endpoints panel Total button shows inconsistent number of endpoints.
705010	EMS shows endpoints with incorrect username.

## Performance

Bug ID	Description
692351	<code>update FortiClients check Config_checksum=? where id=?</code> deadlock seen on <code>fcmdaemon</code> .
707316	FcmDaemon.exe uses all available memory.

## Chromebook

Bug ID	Description
706816	Chromebook port connection should report HTTP Strict Transport Security.

## Zero Trust tags

Bug ID	Description
703319	FortiClient EMS does not tag ZTNA Linux endpoint when connected via SSL VPN to FortiGate.
708672	FortiGate only can show one latest SSL VPN FortiClient in endpoint record list and only this FortiClient receives dynamic address.
714533	User cannot add multiple rules for same Zero Trust tag.

## System Settings

Bug ID	Description
594739	Autodetect control issues detect STARTTLS.
718276	The VCM engine is missing for Windows.

## Other

Bug ID	Description
695370	"NoneType" object is not subscriptable error when logging into FortiClient Cloud.
697354	EMS password fields do not check for caps lock status.
705517	<i>Cannot insert duplicate key row in object 'dbo.FortiClients' with unique index '. The duplicate key value is (x) on FcmDaemon.</i>



## Change log

Date	Change Description
2021-06-02	Initial release.



**FORTINET®**



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.