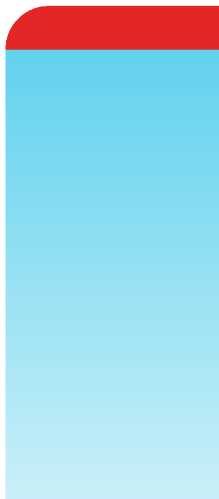


# Release Notes

## FortiClient EMS 7.0.13



**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](mailto:techdoc@fortinet.com)



July 02, 2024

FortiClient EMS 7.0.13 Release Notes

04-7013-1042623-20240702

# 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 VC installation .....	6
SQL Server Standard or Enterprise with 5000 or more endpoints .....	6
Split tunnel .....	6
SAML logins .....	6
<b>Upgrading</b> .....	<b>7</b>
Upgrading from previous EMS versions .....	7
Downgrading to previous versions .....	7
<b>Product integration and support</b> .....	<b>8</b>
<b>Resolved issues</b> .....	<b>10</b>
Endpoint management .....	10
Endpoint policy and profile .....	10
Malware Protection and Sandbox .....	10
Onboarding .....	10
Common Vulnerabilities and Exposures .....	11
<b>Known issues</b> .....	<b>12</b>
New known issues .....	12
Existing known issues .....	13
Administration .....	13
Deployment and installers .....	13
Endpoint management .....	13
Endpoint policy and profile .....	13
Fabric devices .....	14
GUI .....	14
Logs .....	14
Multitenancy .....	14
System Settings .....	14
Upgrade .....	14
Quarantine management .....	15
Zero Trust tagging .....	15
<b>Change log</b> .....	<b>16</b>

# 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 7.0.13 build 0588:

- [Special notices on page 6](#)
- [Upgrading on page 7](#)
- [Product integration and support on page 8](#)
- [Resolved issues on page 10](#)
- [Existing known issues on page 13](#)

For information about FortiClient EMS, see the [FortiClient EMS 7.0.13 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 7.0.13 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 VC 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 7.0.13, 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 7.0.13 product integration and support information:

<b>Server operating systems</b>	<ul style="list-style-type: none"><li>• Windows Server 2022</li><li>• Windows Server 2019</li><li>• Windows Server 2016</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 also tries 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>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li><li>• 7.0.0 and later</li></ul> <p>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 <a href="#">FortiClient Release Notes</a>.</p>
<b>FortiClient (Linux)</b>	<p>If <i>Use SSL certificate for Endpoint Control</i> is enabled on EMS, EMS supports the following FortiClient (Linux) versions:</p> <ul style="list-style-type: none"><li>• 7.0.2 and later</li><li>• 6.4.7 and later</li></ul> <p>If <i>Use SSL certificate for Endpoint Control</i> is disabled on EMS, EMS supports the following FortiClient (Linux) versions:</p> <ul style="list-style-type: none"><li>• 7.0.0 and later</li><li>• 6.4.0 and later</li></ul>
<b>FortiClient (macOS)</b>	<p>If <i>Use SSL certificate for Endpoint Control</i> is enabled on EMS, EMS supports the following FortiClient (macOS) versions:</p> <ul style="list-style-type: none"><li>• 7.0.2 and later</li><li>• 6.4.7 and later</li></ul> <p>If <i>Use SSL certificate for Endpoint Control</i> is disabled on EMS, EMS supports the following FortiClient (macOS) versions:</p> <ul style="list-style-type: none"><li>• 7.0.0 and later</li><li>• 6.4.0 and later</li></ul>
<b>FortiClient (Windows)</b>	<p>If <i>Use SSL certificate for Endpoint Control</i> is enabled on EMS, EMS supports the following FortiClient (Windows) versions:</p>



- 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 7.0.13. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

### Endpoint management

Bug ID	Description
1026086	FortiClient 7.0.2 (macOS and Windows) cannot connect to EMS.

### Endpoint policy and profile

Bug ID	Description
1010671	EMS does not allow configuring on-net public IP rule to use subnets.

### Malware Protection and Sandbox

Bug ID	Description
992576	User cannot download Sandbox PDF report due to error: <i>PDF report can't be downloaded. DATA_NOT_EXIST</i> .

### Onboarding

Bug ID	Description
1005122	FortiClient Telemetry user authentication fails with <i>Authentication is blocked</i> .

## Common Vulnerabilities and Exposures

Bug ID	Description
1024586	FortiClient EMS 7.0.13 is no longer vulnerable to the following CVE References: <ul style="list-style-type: none"><li>• CVE-2024-33508</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.

## Known issues

Known issues are organized into the following categories:

- [New known issues on page 12](#)
- [Existing known issues on page 13](#)

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 7.0.13.

## Existing known issues

The following issues have been identified in a previous version of FortiClient EMS and remain in FortiClient EMS 7.0.13.

### Administration

Bug ID	Description
678899	LDAP configuration is persistent in EMS multitenancy global/default/non-default administration users.

### 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 management

Bug ID	Description
831108	User cannot download PDF report of Cloud Sandbox events on EMS.
836134	Inverse selection with ! does not work for deployment package, profile, and features under <i>All Endpoints</i> view.
845739	EMS shows VMware clones with duplicated UUIDs.
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 <i>Not</i> does not work.
826940	EMS does not save <code>&lt;temp_whitelist_timeout&gt;</code> in an endpoint profile.

---

## 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 <i>NaN used of X</i> when no license is in use.
929410	Admin page has delay with LDAP accounts.

## Logs

Bug ID	Description
856952	FortiClient EMS requires improvements and to add missing update daemon logs.

## 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 <i>Delete Timeout</i> option.

## Upgrade

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

---

## Quarantine management

Bug ID	Description
956891	FortiClient does not download EMS allowlist file, preventing file restore from <i>Quarantine Management</i> .

## Zero Trust tagging

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

# Change log

Date	Change description
2024-07-02	Initial release.





[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.