



# FortiClient EMS - Release Notes

Version 6.2.1

**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/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

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



July 31, 2019

FortiClient EMS 6.2.1 Release Notes

04-621-563660-20190731

# 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
<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>
License management	10
GUI	10
Dashboard	10
Endpoint management	10
Profile and policy management	11
Install and upgrade	11
FortiClient deployment	12
EMS administration	12
Systems Settings	12
Other	12
<b>Known issues</b>	<b>13</b>
License management	13
GUI	13
Dashboard	13
Endpoint management	13
Profile and policy management	14
FortiClient deployment	14
EMS administration	14
System Settings	15
<b>Change log</b>	<b>16</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 6.2.1 build 0780:

- [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 6.2.1 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 6.2.1 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](#).

## 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 Enterprise instead of SQL Server Express, which is installed with EMS by default. Otherwise, you may experience database deadlocks. See the [FortiClient EMS Administration Guide](#).

# What's new

For information about what's new in FortiClient EMS 6.2.1, see the [FortiClient & FortiClient EMS 6.2.1 New Features Guide](#).

# Upgrading

## Upgrading from previous EMS versions

FortiClient EMS supports upgrading from previous EMS versions as outlined in [FortiClient and FortiClient EMS Upgrade Paths](#). After upgrading from FortiClient EMS 6.0, you cannot make changes to the FortiClient Enterprise Management Server license. Increasing the number of managed endpoints requires you to purchase a new FortiClient Security Fabric Agent license.

## Downgrading to previous versions

Downgrading FortiClient EMS 6.2.1 to previous EMS versions is not supported.



# Product integration and support

The following table lists version 6.2.1 product integration and support information:

<b>Server operating systems</b>	<ul style="list-style-type: none"><li>• Windows Server 2012 R2</li><li>• Windows Server 2016</li><li>• Windows Server 2019</li></ul>
<b>Minimum system requirements</b>	<ul style="list-style-type: none"><li>• 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)</li><li>• 4 GB RAM (8 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 required during installation</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>FortiClient (Linux)</b>	<ul style="list-style-type: none"><li>• 6.2.0 and later</li><li>• 6.0.0 and later</li></ul>
<b>FortiClient (macOS)</b>	<ul style="list-style-type: none"><li>• 6.2.0 and later</li><li>• 6.0.1 and later</li></ul>
<b>FortiClient (Windows)</b>	<ul style="list-style-type: none"><li>• 6.2.0 and later</li><li>• 6.0.0 and later</li></ul>
<b>FortiOS</b>	<ul style="list-style-type: none"><li>• 6.2.0 and later</li><li>• 6.0.0 and later</li></ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"><li>• 3.1.0 and later for detailed reports on files that FortiSandbox has detected</li><li>• 3.0.0 and later</li><li>• 2.5.0 and later</li></ul>

## Resolved issues

The following issues have been fixed in version 6.2.1. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

### License management

Bug ID	Description
552411	HTTP error shows when trying to log in to FortiCare.

### GUI

Bug ID	Description
563559	Cyrillic usernames sent by FortiClient breaks EMS GUI.

### Dashboard

Bug ID	Description
550699	EMS Dashboard and <i>Add Profile</i> pages do not load on Mozilla Firefox and Edge.

### Endpoint management

Bug ID	Description
466871	EMS shows duplicate device if a hostname has more than 15 characters.
541404	EMS does not send an FSSO update message to FortiOS when FortiClient deregisters by EMS or by itself.
543389	fctlog fails to upload when larger than 1 M.
547634	Inconsistent events between EMS and FortiClient.

Bug ID	Description
550692	FcmDaemon crashes with large number of endpoints.
552735	Web Filter event count on EMS is not correct.
553225	EMS fails to sync with Active Directory (AD).
553316	EMS does not report the correct OS version for domain PC after upgrading the OS on the endpoint.
553839	FortiClient reports EMS as not reachable after EMS server is woken up from sleeping.
554474	EMS does not update the endpoint OU when changing it from the domain controller.
554656	EMS does not send the new login information to FortiOS after changing the IP address on FortiClient.
555216	Unable to assign endpoint policy to domain OUs and groups.
555419	EMS blocks users who belong to AD group with "&" in the name.
556752	EMS does not show event details in GUI.
561542	EMS ignores MicroFortiGuard/FortiManager server settings for software/signature updates.
565930	EMS fails to delete domain.

## Profile and policy management

Bug ID	Description
547207	Clicking <i>Duplicate tunnel</i> , then saving causes the original tunnel to disappear.
554974	<i>Sync Now</i> button for EMS profiles does not confirm synchronization of imported profiles.

## Install and upgrade

Bug ID	Description
552214	EMS fails to connect using remote SQL server with specific port after successful installation.
555693	Cannot correctly upgrade EMS to customized installation folder.
557167	Standalone upgrade from 6.0.5 to 6.2 on Windows changes the EMS IP address to the FortiGate IP address.
569324	Upgrade from EMS 6.2.0 fails.

## FortiClient deployment

Bug ID	Description
510549	EMS tries to deploy FortiClient to Linux endpoints.
554496	EMS deployment status is stuck on <i>Pending Deployment</i> .
563456	EMS fails to deploy FortiClient to the endpoint.

## EMS administration

Bug ID	Description
547103	LDAPS does not work for <i>Endpoints &gt; Domains</i> or <i>User Servers</i> .
554494	Backing up the EMS database does not work.
558559	Database backup file from EMS fails to restore properly.
560677	EMS does not bind to AD if you use the server's hostname.
560706	EMS fails to sync with LDAP and gives errors.
562552	Database restore on EMS fails.

## Systems Settings

Bug ID	Description
562886	EMS fails to save System Settings configuration.

## Other

Bug ID	Description
564332	EMS process crashes frequently.

# Known issues

The following issues have been identified in version 6.2.1. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

## License management

Bug ID	Description
568413	License info is cutoff in license info windows.

## GUI

Bug ID	Description
565986	Edge browser is missing expiry date for invitation code.

## Dashboard

Bug ID	Description
549380	EMS does not preserve Dashboard widget order.

## Endpoint management

Bug ID	Description
539028	No cloud based malware scan events for the endpoint when Sandbox feature is disabled in the profile.
543354	Endpoints show in EMS as unscanned.
546107	FortiClient misses telemetry EMS list when FortiClient is unregistered.
547726	Domain computer shows under <i>Workgroups &gt; All endpoints</i> .

Bug ID	Description
549212	Domain import fails when using a remote SQL server.
550165	EMS misses cloud malware protection feature state.
551474	With always-up enabled and disclaimer enforced, disclaimer acceptance box always pops up when the network goes up or down.
552884	Client receives configuration update every time it reconnects to EMS.
562914	EMS reports error when importing a domain using the hostname.

## Profile and policy management

Bug ID	Description
535324	FortiClient fails to receive <fail_over_server> setting from EMS profile.
544641	Importing a profile with an individual schedule does not create a schedule.
546404	Unable to delete Chromebook profiles.
564932	Profile imported to EMS loses log upload settings on the <i>System Settings</i> tab.
565304	Profile sync issue between FortiOS and EMS.

## FortiClient deployment

Bug ID	Description
552101	EMS reports endpoint notified state after EMS deploys FortiClient successfully.
555904	EMS pushes FortiClient package from previous deployment profile to endpoints when EMS tries to deploy FortiClient with XML configuration profile.
564681	EMS fails to deploy to some endpoints.

## EMS administration

Bug ID	Description
524088	FortiClient EMS cannot add AD server certificate.
546221	EMS sends duplicated email alerts.

Bug ID	Description
546357	Host Verification page does not alert user while creating rule with custom role with view-only access.
549229	FCEMS_Server starts or stops very slowly with remote SQL server setup.
549723	EMS does not retrieve the user server distinguished name if a user edits the user server.
564084	<i>Allow Inactive Days</i> feature does not lock out users that have not logged in during the period configured.
568282	Unable to log in to EMS with LDAP credentials after upgrade.

## System Settings

Bug ID	Description
470172	EMS proxy settings do not work for FDS updates.
549060	Listen on IP refresh does not list new IP address.

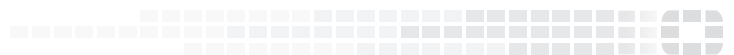
## Change log

Date	Change Description
2019-07-18	Initial release.
2019-07-31	Updated <a href="#">Product integration and support on page 9</a> .





**FORTINET®**



Copyright© 2019 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.