

# FortiClient EMS - Release Notes

Version 6.2.0

**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)



August 19, 2019

FortiClient EMS 6.2.0 Release Notes

04-620-530292-20190819

# TABLE OF CONTENTS

<b>Introduction</b> .....	<b>4</b>
Endpoint requirements .....	4
Supported web browsers .....	4
Licensing and installation .....	4
<b>Special notices</b> .....	<b>5</b>
FortiClient EMS Microsoft Visual C++ installation .....	5
SQL Server Enterprise with 5000 or more endpoints .....	5
<b>What's new</b> .....	<b>6</b>
<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>9</b>
<b>Known issues</b> .....	<b>12</b>
<b>Change log</b> .....	<b>14</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 the following FortiClient platforms: Microsoft Windows, macOS, Linux, and Chrome OS. FortiClient EMS runs on a Microsoft Windows server.

This document provides the following information for FortiClient EMS 6.2.0 build 0727:

- [Special notices on page 5](#)
- [What's new on page 6](#)
- [Upgrading on page 7](#)
- [Resolved issues on page 9](#)
- [Known issues on page 12](#)

For information about FortiClient EMS, see the [FortiClient EMS 6.2.0 Administration Guide](#).

## Endpoint requirements

The following FortiClient platforms are supported:

- FortiClient for Microsoft Windows
- FortiClient for macOS
- FortiClient for Linux
- 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 6.2.0 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 6.2.0, see the [FortiClient & FortiClient EMS 6.2.0 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 6.2.0 to previous EMS versions is not supported.

# Product integration and support

The following table lists version 6.2.0 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 6.2.0. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Bug ID	Description
413419	FortiClient and EMS should prevent installation and upgrade to unsupported OS versions.
454697	EMS should have an option to find which endpoint groups the profile is assigned to.
482404	Clearing logs through the GUI fails to fully remove all logs.
490387	EMS fails to send email alerts after upgrading.
501822	FortiClient fails to sync an updated EMS profile that was imported from the FortiGate.
506548	Vulnerability scan results may fail to display on EMS.
510491	Endpoint details may fail to open when clicking a hostname.
510932	Attempting to deploy a profile with many tunnels may fail.
513214	Setting the deployment time too close to the current time may cause deployment issues.
515911	<i>Software Inventory &gt; Applications</i> incorrectly shows Cyrillic characters.
516143	EMS displays an error when trying to sync with FortiSandbox 2.3.3.
516628	FortiGate profile changes cause continuous profile update messages on FortiClient.
517306	Uninstallation does not work on new registration.
518863	EMS should display the file hash in messages on the <i>Antivirus Events</i> and <i>Sandbox Events</i> tabs.
519257	SQL error results when adding a URL longer than 255 characters to the Web Filter exclusion list.
519442	After assigning a non-default profile to a group, icon disappears from group after reloading or logging into EMS.
519502	Upgrading attempts to insert the value <code>NULL</code> into column <code>display_antivirus</code> .
519568	Upgrading EMS results in the profile to lose the IPsec preshared key.
519806	EMS fails to import devices from a domain.
520276	Changes to a profile assigned to a domain root or all groups causes all endpoints to become out-of-sync.
521053	EMS does not retrieve LDAP information until after manual sync when <i>System Settings &gt; Log &gt; Level</i> is set to <i>Debug</i> .
521188	EMS does not allow uploading profiles.
521365	EMS fails to clear medium vulnerabilities even though they are cleared from the endpoint side.
521505	Random files fill up the EMS log folder, causing the server to run out of space.

Bug ID	Description
521511	EMS fails to load some endpoints in AD.
522069	EMS fails to show FortiClient endpoint in the correct location on the GUI.
522995	Hiding any feature except Application Firewall causes FortiClient to report the feature as installed and not enabled.
523461	EMS prevents applying the correct EMS profile to users moved to a new OU in AD.
524705	Enabling the <i>Deployment</i> tab displays <i>Turning on Deployment disables Auto Patch in System Settings</i> when Auto Patch does not exist.
524756	EMS should not download or keep unused installers.
525500	After upgrading, EMS does not show new Vulnerability events as reported by endpoints after a scan.
525851	An installer created in EMS should have an option to embed a preconfigured profile.
528218	Endpoint alerts on the dashboard load slowly.
528220	The <i>Malware Protection</i> tab is enabled on endpoint profiles when APT is added to the installer.
528482	Deployment status is stuck at <i>Endpoint Notified</i> .
529035	EMS FortiClient installer component breaks after changing the FDS server in the hosts file.
529975	Upgrading EMS does not clear errors or check if they recur.
530566	FortiSandbox admin user and password are missing.
530646	Clicking on <i>Others</i> from <i>Current Vulnerabilities Summary</i> does not load with the vulnerabilities list.
530781	Manually installing vulnerabilities should not be selectable on the <i>Vulnerability events</i> list.
533651	EMS should be able to import web filters with multiple local categories.
533889	EMS does not import allowed websites when they are defined in local categories on the FortiGate.
535404	The <i>Show Dashboard Banner</i> feature should be removed from the GUI.
536329	Duplicate records show after EMS upgrade.
536680	Changing the action for application signatures in EMS does not work in Firefox.
536983	Filtering on an endpoint tag may fail.
537453	EMS may display an error when creating an administrative user.
537745	EMS blocks the endpoint after enabling it from management.
539387	SSL VPN autodial does not work when using the domain name to register to EMS.
540168	EMS is unable to create a FortiClient installer.
541017	EMS cannot set the DN as the local ID for IPsec VPN profile configuration.
541085	Vulnerability count for endpoints on EMS is incorrect.

Bug ID	Description
541150	EMS fails to delete a custom workgroup.
541269	EMS displays an error when uploading a profile from FortiClient 6.0.4.
542903	FortiClient repackager should be updated to correctly embed the EMS IP address.
542930	Software Inventory does not show any software in its list.
543017	EMS shows the Cloud Based Malware Outbreak Detection feature for a macOS-only deployment package.
543151	By default, installing EMS should enable a firewall inbound rule to allow inbound traffic for TCP port 8000.
543252	Links in the <i>Fabric Device Monitor</i> table fail to work.
543703	EMS still shows Sandbox as Windows-only when creating a macOS installer.
543717	Backing up and restoring EMS fails to restore custom installers.
544049	Registered Windows devices fail to show on registered EMS.
544062	Newly added domain fails to display on <i>Domains</i> .
544407	When importing an AD with many devices, EMS does not respond if trying to register a large number of FortiClient endpoints.
545489	EMS is unable to import an AD domain.
546116	EMS shows the wrong table for the <i>Endpoint Connection</i> widget link.
546143	EMS cannot import devices from an AD with a large number of computers.
546338	EMS displays an error when adding a whitelist and restoring files.
546681	EMS fails to start AV scan actions for a workgroup.
547626	Importing a domain using its distinguished name fails.
547629	<i>Add Signatures</i> description textbox on the <i>Application Firewall</i> tab of endpoint profiles is empty.
547638	The <code>&lt;config use_https_rating_server&gt;</code> XML element should be added.
547713	FortiClient cannot connect to EMS when the user is a member of many groups with names 20 characters long.
547899	FortiClient fails to send Sandbox events to EMS when using a physical Sandbox.
548470	Admin roles are missing if clicking them on the EMS GUI.
548725	Sandbox event process tree does not display properly.
548781	LDAP user login does not work.
548782	You cannot import EMS profiles from a previous build.
549211	EMS should change tab visibility when you enable a feature.
549480	EMS deployment package is missing APT and Cloud Malware Scan features for Windows.
549881	Importing profiles from FortiOS 6.0.2 or 6.0.4 fails.

# Known issues

The following issues have been identified in version 6.2.0. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Bug ID	Description
470172	EMS proxy settings do not work for FDS updates.
489370	Email alerts are incomplete for AV events.
498338	EMS fails to update the mdare engine.
521116	EMS fails to back up a database as initiated from the EMS GUI if the Microsoft SQL Server is on a remote computer.
523263	FortiClient should verify installer downloads.
524864	FortiClient sends wrong most recent Vulnerability Scan time to EMS.
532143	User-defined extensions are not synced to FortiClient EMS in FortiSandbox.
533299	Domain PCs do not show up in EMS under <i>Endpoints &gt; Domains</i> .
536697	Applications loaded always shows the same number.
538009	EMS fails to clean up uploaded files that have failed to complete.
542672	The list of policies in the left navigation section should be removed.
543354	Endpoints in EMS show as unscanned.
543563	EMS does not send alert emails until the server reboots.
543999	Deployment package may not be accessible from secondary/standby server if the primary server is down.
544379	EMS has issues with importing and exporting profile from files.
544641	Importing profiles for individual schedules does not create a schedule.
544964	EMS calculates expiry status based on browser time instead of server time.
544988	EMS provides information about where EMS-created installer is being used.
545681	EMS should open all links in endpoint status page in-place.
545874	Vulnerability events cannot be cleared.
546058	EMS reports the password as not secure after EMS user refreshes the page.
546097	EMS welcome page always displays for each EMS login.
546107	FortiClient is missing the Telemetry EMS list when FortiClient is unregistered.
546221	EMS sends duplicate email alerts.

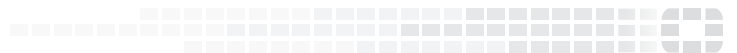
Bug ID	Description
546357	<i>Compliance Verification</i> does not alert user when creating a rule with custom role with view-only access.
546404	EMS is unable to delete Chromebook profiles.
547207	After clicking <i>Duplicate Tunnel</i> and saving the endpoint profile, the original tunnel disappears.
547376	EMS should enable <i>Allow duplicate FortiClient registrations by assigning them new UIDs</i> by default.
547627	EMS allows API-based import of duplicate domains.
547634	FortiClient and EMS may show an inconsistent number of events, such as the number of websites that web filtering has blocked.
547877	Profiles imported from FortiGate/FortiManager with individual sync do not get proper configuration.
548401	EMS features should match license type.
549024	Verification rules GUI collapses when clicking a rule.
549060	<i>Listen on IP Refresh</i> does not list new IP address.
549198	Using the <i>Clear now</i> button for the <i>Clear logs older than</i> option may fail.
549229	FCEMS_Server starts or stops very slow on remote SQL server setup.
549325	FortiCare support account window shows previous error if opened twice during the same session.
549380	EMS does not preserve Dashboard widget order.
549594	FortiClient cannot get upgrade notifications if running on Windows 8.1.
549721	In <i>Quarantine Management &gt; Files</i> , the hyperlink for a threat fails to take you to FortiSandbox and FortiGuard.
549723	EMS does not retrieve the user server DN if user edits the user server.
549786	When RTP is disabled, RTP hides other settings that are supposed to be independent of RTP.
549790	Endpoint <i>Summary</i> details do not show host verification tags.
549794	EMS should sort <i>Top 10 Vulnerabilities</i> by number of hosts.
550082	EMS fails to update onnet/offnet state.
550126	Linux avatars may appear larger than normal on the <i>Endpoints</i> page.
550164	EMS displays an error when viewing Sandbox events with a Sandbox appliance profile configured.
550252	Saving an XML configuration generates a crash.
550286	FortiGate sub-menu items show without any profile under them.
550296	FortiClient 6.2.0 and FortiOS 6.2.0 do not support the Compliance Enforcement from the FortiGate. This feature still is available for FortiClient 6.0 and FortiOS 6.0.
550300	CA certificates imported from a FortiGate unit incorrectly are mixed with local certificates after import.

# Change log

Date	Change Description
2019-04-16	Initial release.
2019-05-23	Updated <a href="#">Product integration and support on page 8</a> .
2019-06-25	Removed FortiClient for Android OS and FortiClient for iOS from <a href="#">Endpoint requirements on page 4</a> .
2019-07-31	Updated <a href="#">Product integration and support on page 8</a> .
2019-08-19	Added 550296 to <a href="#">Known issues on page 12</a> .



**FORTINET**<sup>®</sup>



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.