



FortiClient EMS - Release Notes

Version 6.0.4

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/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



August 7, 2018

FortiClient EMS 6.0.4 Release Notes

04-604-524554-20190807

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported platforms	5
System requirements	5
Endpoint requirements	6
Supported web browsers	6
Licensing and installation	6
Upgrading	7
Upgrading from previous EMS versions	7
Downgrading to previous versions	7
Resolved Issues	8
Dashboard	8
Endpoint profiles	8
Endpoint management	8
Install and upgrade	9
FortiClient deployment	9
Google domains	9
Domain management	9
Other	10
Known Issues	11
Dashboard	11
Endpoint profiles	11
Endpoint management	11
FortiClient deployment	12
Google domains	12
Other	12

Change Log

Date	Change Description
2018-12-10	Initial release.
2019-08-07	Updated Endpoint requirements on page 6.

Introduction

FortiClient Enterprise 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 ChromeOS. FortiClient EMS runs on a Microsoft Windows server.

This document provides the following information for FortiClient EMS 6.0.4 build 0158:

- Introduction
 - [Supported platforms on page 5](#)
 - [System requirements on page 5](#)
 - [Endpoint requirements on page 6](#)
 - [Supported web browsers on page 6](#)
 - [Licensing and installation on page 6](#)
- [Upgrading on page 7](#)
- [Resolved Issues on page 8](#)
- [Known Issues on page 11](#)

For information about FortiClient EMS, see the *FortiClient EMS 6.0.4 Administration Guide*.

Supported platforms

The EMS server can be installed on the following platforms:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

System requirements

The minimum system requirements are as follows.

- 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)
- 4 GB RAM (8 GB RAM or more is recommended)
- 40 GB free hard disk
- Gigabit (10/100/1000baseT) Ethernet adapter
- Internet access

Internet access is required during installation. This becomes optional once installation is complete. FortiClient EMS accesses the Internet to obtain information about FortiGuard engine and signature updates.



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.

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

The FortiClient version should be 5.4.0 or newer.

When using FortiClient 5.4.1-5.4.5 with FortiClient EMS 6.0.4, FortiClient may fail to establish IPsec VPN connection due to conflicting preshared keys.

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 6.0.4 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*.

Upgrading

Upgrading from previous EMS versions

FortiClient EMS 6.0.4 supports upgrading from the following EMS versions:

- 6.0.0 and later
- 1.2.4 and later

Downgrading to previous versions

Downgrading FortiClient EMS 6.0.4 to previous EMS versions is not supported.

Resolved Issues

The following issues have been fixed in version 6.0.4. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Dashboard

Bug ID	Description
491824	The data in Top 10 Site Categories Distribution is not cleaned up after clicking <i>Clear Chromebook Event</i> from right-click menu.
519381	Widget central number links to an empty or wrong list.

Endpoint profiles

Bug ID	Description
516143	Error displayed when EMS tries to sync with Sandbox 2.3.3.
519058	EMS failed to update settings for Safe Search.
519257	SQL error when adding URL longer than 255 to Web Filter exclusion list.
519442	After assigning a non-default profile to a group, icon disappears from group after reloading/relogin of EMS.
519568	Upgrading EMS from 6.0.2 to 6.0.3 causes the IPsec pre-shared key to be lost in the profile.
521188	Unable to upload profile to EMS..
523003	Cannot save <auth_data>.
526922	Typo error in EMS Server "DNSSCAHCE".

Endpoint management

Bug ID	Description
517234	Admin cannot initiate AV signature update from EMS.
518058	FortiClient failed to import update_action "download_only" value.

Bug ID	Description
521365	EMS 6.0.3 fails to clear medium vulnerabilities even though they are cleared from the endpoint side.
521511	EMS 6.0.3 fails to load some endpoints in Active Directory.
522069	FortiClient EMS 6.0.3 failing to show FortiClient endpoint in correct location in GUI.
523461	A bug on 6.0.3 prevents applying the correct EMS profile to users moved to new OU in AD.
525761	Group assignment tag rule is broken.

Install and upgrade

Bug ID	Description
519502	Upgrade from 1.2.5 to 6.0.3 fails: attempts to insert the value NULL into column 'display_antivirus'.

FortiClient deployment

Bug ID	Description
515731	AD domain computers with names longer than 15 characters do not show up in EMS.
524399	Users not showing in a domain if two domains are added.

Google domains

Bug ID	Description
521716	Chromebook needs to re-import SSL certificate.

Domain management

Bug ID	Description
519806	Cannot import devices from domain.
521053	FortiClient EMS not retrieving LDAP information until after manual sync with Debug level set In System Settings.

Other

Bug ID	Description
490387	Email alerts not sending (test does).
515911	FortiClient EMS console in Software Inventory Application section incorrectly shows Cyrillic characters.
521505	On EMS 6.0.3 random files are filling up the EMS log folder, causing the server to run out of space.
524986	Adding unique service account credentials to EMS specifies "ID" where email address is required.

Known Issues

The following issues have been identified in version 6.0.4. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Dashboard

Bug ID	Description
506598	EMS Dashboard widgets arrangement does not save.

Endpoint profiles

Bug ID	Description
518230	Installer created by EMS should include uninstall action.
524756	EMS should not download or keep unused installers.

Endpoint management

Bug ID	Description
501822	FortiClient failed to sync with updated EMS profile that was imported from FortiGate (fcconfig.exe crash).
505635	FortiClient EMS does not show VPN and Application Firewall events.
506548	Vulnerability Scan results not displayed on EMS.
516628	Profile changes on the FortiGate causing for continuous profile update messages on FortiClient.
522995	Hiding any feature (except Application Firewall) will cause FortiClient to report feature as <i>Installed</i> and not <i>Enabled</i> .
523213	FortiClient EMS's Endpoint Alerts widget not reporting current endpoint protection status correctly.
523957	Domain endpoints showing up in workgroups.
525500	An upgraded EMS 6.0.3 will not show new Vulnerability events as reported by endpoints after

Bug ID	Description
	a scan is done.
527037	Uninstalling FortiClient from EMS let some references on system.

FortiClient deployment

Bug ID	Description
396262	EMS should not retry when credentials are invalid.
413419	FortiClient and EMS server should prevent installation and upgrade to unsupported OS versions.
505294	Installer is not assigned to some endpoints, OS is unknown.
510549	EMS is trying to deploy to Linux.
510932	Profile deployment issue (endpoint profile with about 100 VPN tunnels).
517306	Uninstall did not work on new registration.
524705	Enabling Deployment displays <i>Turning on Deployment disables Auto Patch in System Settings</i> when Auto Patch does not exist.
524864	FortiClient sends wrong most recent Vulnerability Scan time to EMS.

Google domains

Bug ID	Description
519795	User with Google domain management permission is not working.

Other

Bug ID	Description
470172	EMS proxy settings not working for FDS updates.
482404	Clearing logs via GUI is incomplete.
521939	Should update LDAP user drop-down list if user server changed.



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.