



FortiClient EMS - Release Notes

Version 6.0.5

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, 2019

FortiClient EMS 6.0.5 Release Notes

04-605-533964-20190807

TABLE OF CONTENTS

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

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 Chrome OS. FortiClient EMS runs on a Microsoft Windows server.

This document provides the following information for FortiClient EMS 6.0.5 build 0182:

- Introduction
 - [Supported platforms on page 4](#)
 - [System requirements on page 4](#)
 - [Endpoint requirements on page 5](#)
 - [Supported web browsers on page 5](#)
 - [Licensing and installation on page 5](#)
- [Upgrading on page 6](#)
- [Resolved issues on page 7](#)
- [Known issues on page 9](#)

For information about FortiClient EMS, see the *FortiClient EMS 6.0.5 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 6.0.5, 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 6.0.5 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 6.0.5 supports upgrading from the following EMS versions:

- 6.0.0 and later
- 1.2.4 and later

Downgrading to previous versions

Downgrading FortiClient EMS 6.0.5 to previous EMS versions is not supported.

Resolved issues

The following issues have been fixed in version 6.0.5. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Endpoint management

Bug ID	Description
451007	Log registration events.
506548	Vulnerability Scan results not displayed on EMS.
522995	Hiding any feature (except Application Firewall) causes FortiClient to report the feature as <i>Installed</i> and not <i>Enabled</i> .
525500	An upgraded EMS 6.0.3 will not show new Vulnerability events as reported by endpoints after a scan is done.
533673	FortiClient endpoints Anti Virus/Web Filter/Sandbox/Firewall events not shown in <i>Endpoints</i> screen.

Install and upgrade

Bug ID	Description
529261	Error observed after EMS upgrade.
529975	Upgrading EMS does not clear errors and check if they come back.
535933	Duplicate records showing after EMS upgrade.

FortiClient deployment

Bug ID	Description
524705	Enabling <i>Deployment</i> displays <i>Turning on Deployment disables Auto Patch</i> in <i>System Settings</i> when Auto Patch does not exist

Domain management

Bug ID	Description
532242	AdDaemon terminated due to an unhandled exception.

Other

Bug ID	Description
490387	Email alerts not sending (test does).
527976	Query to load 50 endpoints takes around two minutes every time.
534549	Email alerts fail to send - Python error <i>Failed to check email alerts: invalid group reference 3 at position 17</i>

Known issues

The following issues have been identified in version 6.0.5. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Endpoint profiles

Bug ID	Description
501822	FortiClient failed to sync with updated EMS profile that was imported from FortiGate (fcconfig.exe crash).
533651	Importing web filters with multiple local categories.
533889	EMS does not import Allowed websites when they are defined in Local Categories on the FortiGate.

Endpoint management

Bug ID	Description
523213	FortiClient EMS's <i>Endpoint Alerts</i> widget not reporting current endpoint protection status correctly.
523242	Inconsistencies in endpoint and endpoint group sorting.
528220	<i>Anti Virus</i> tab is enabled on endpoint profiles when APT is added to installer.
533299	Domain PCs not showing up in EMS 6.0.4 under Domain computers.

FortiClient deployment

Bug ID	Description
449330	Verifying FortiClient installer downloads during deployment from EMS.
510932	Profile deployment issue (endpoint profile with about 100 VPN tunnels).

Install and upgrade

Bug ID	Description
525851	Installer created in EMS should have an option to embed a preconfigured profile.

Other

Bug ID	Description
470172	EMS proxy settings not working for FDS updates.
482404	Clearing logs via GUI is incomplete.

Change log

Date	Change Description
2019-01-31	Initial release.
2019-02-21	Removed 523957 from Known issues on page 9 .
2019-08-07	Updated Endpoint requirements on page 5 .



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.