

FortiClient EMS - Release Notes

VERSION 1.2.0

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



June 22, 2017

FortiClient EMS 1.2.0 Release Notes

04-120-406927-20170622

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported platforms	5
System Requirements	5
Endpoint Requirements	6
Licensing and installation	6
What's New	7
Customize FortiClient Installer	7
FortiClient for Mac OS X Vulnerability Scan Support	7
One-time pull of existing FortiClient Profile from FortiGate	7
Pre-Login Banner	7
Installer Deployment Improvements	7
Redesigned Endpoints Page	8
Upgrade	9
Upgrading from previous EMS versions	9
Downgrading to previous versions	9
Resolved Issues	10
Known Issues	12

Change Log

Date	Change Description
2017-06-15	Initial release.
2017-06-22	Added note for upgrading from earlier version of FortiClient EMS in "Upgrade" on page 9

Introduction

FortiClient Enterprise Management Server (EMS) is a system intended to be used to manage installations of FortiClient. It uses the same Endpoint Control protocol that was introduced in FortiOS 5.0 and enhanced in FortiOS 5.2. Like FortiOS, EMS supports all FortiClient platforms: Microsoft Windows, Mac OS X, Android OS and Apple iOS. FortiClient EMS does not require a Fortinet device. It runs on a Microsoft Windows server. End users with FortiClient installations could choose to use a FortiGate or the EMS to manage their installations.

This document provides the following information for FortiClient EMS 1.2.0 build 0388:

- [Introduction on page 5](#)
 - [Supported platforms on page 5](#)
 - [System Requirements on page 5](#)
 - [Endpoint Requirements on page 6](#)
 - [Licensing and installation on page 6](#)
- [What's New on page 7](#)
- [Upgrade on page 9](#)
- [Resolved Issues on page 10](#)
- [Known Issues on page 12](#)

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

Supported platforms

The EMS server can be installed on any of the following platforms:

- Microsoft Windows Server 2008 R2 or newer

System Requirements

The minimum system requirement is as follows.

- 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)
- 4 GB RAM (8 GB RAM or better 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 completed. The EMS uses access to the internet to obtain information about FortiGuard engine and signature updates.



You should only install EMS and the default services for the operating system on the server. Additional services should not be installed on the same server as EMS.

Endpoint Requirements

The following FortiClient platforms are supported:

- FortiClient for Microsoft Windows
- FortiClient for Mac OS X
- FortiClient for Android OS
- FortiClient for iOS

The FortiClient version should be 5.6.0 and later.

FortiClient is supported on multiple Microsoft Windows and Mac OS X platforms. The EMS supports all such platforms as endpoints.

Licensing and installation

For information on licensing and installing FortiClient EMS, see the *FortiClient EMS Administration Guide*.

What's New

The core features of the FortiClient EMS 1.2.0 include the following:

Customize FortiClient Installer

EMS can create a FortiClient Installer with any of the following components:

- **SFA**: The Security Fabric Agent provides endpoint telemetry, host vulnerability scanning and remediation; This component is always selected and cannot be de-selected.
- **SAA**: Secure Access Architecture includes SSL VPN and IPSec VPN features. This component is selected by default.
- **APT**: Advanced Persistent Threat Components provides integration with FortiSandbox detection.
- **ASF**: Additional Security Features includes AntiVirus, Webfiltering, Application Firewall, and Single Sign-On mobility agent.

FortiClient for Mac OS X Vulnerability Scan Support

Vulnerability Scan and auto-patching feature is now supported in FortiClient for Mac OS X.

One-time pull of existing FortiClient Profile from FortiGate

FortiClient EMS now supports a one-time pull of an existing FortiClient Profile from FortiGate. The EMS admin can pull an existing FortiClient profile from a FortiGate and modify it before deploying to endpoints.

Pre-Login Banner

The Pre-login Banner feature can be used to display message on the EMS login page before user logs in. The user will need to accept the banner message before they can login.

Installer Deployment Improvements

FortiClient EMS has improved the installer deployment functionality so that more real-time deployment information is visible on EMS. The deployment technique has also been enhanced so it is more reliable and provides a better user experience.

Redesigned Endpoints Page

The Endpoints page in EMS has been redesigned to be more user friendly. Users can clearly see the endpoint installer deployment, profile sync, telemetry connection and compliance status. The device information is better organized so it is easier to access.

Upgrade

Upgrading from previous EMS versions

FortiClient EMS 1.2.0 supports upgrading from EMS 1.0.3 and later 1.0 versions. It is recommended to perform the upgrade on a staging server before upgrading the production server. For details, see the *FortiClient EMS Administration Guide*.

Downgrading to previous versions

Downgrading FortiClient EMS 1.2.0 to previous EMS versions is not supported.

Resolved Issues

The following issues have been fixed in version 1.2.0.

Bug ID	Description
377410	No notification is given when Trial license limit is reached.
379495	Endpoints move to <i>Other Endpoints</i> workgroup after being assigned to a Domain EMS group.
380271	Unable to update FortiClient from EMS server.
384016	Login page displays <i>Unable to reach database. Are you restoring? error message.</i>
385043	EMS still sent old serial number after EMS imports a new license with new a serial number.
385747	Users should not be allowed to login without any permissions.
385974	Email alert not received when new EMS versions are available.
386674	Warning is not hidden when testing/discarding changes.
387391	Endpoint status switches to out-of-sync in a non-deterministic way.
387820	FortiClient and FortiClient EMS does not support Microsoft recommended exclusion methods.
388991	EMS does not work with FortiClient on MacOS as expected (VCM related).
390230	<i>Listen on IP Addresses</i> can only detect one interface.
390373	EMS generates duplicate devices.
391104	EMS displays the <i>Profile Name already exists</i> error message when re-editing a profile right after creating it in <i>Advanced mode</i> .
391603	The error message is hidden when importing a domain with the wrong Distinguished Name.
391769	Users can still register to EMS even after the license expires.
392819	<i>All Endpoints</i> only displays the endpoints in Workgroups.
393123	No email alert sent for <i>C&C Attack Communication</i> with botnet.
394345	Clients are still offnet when EMS is configured to changed from offnet to onnet.

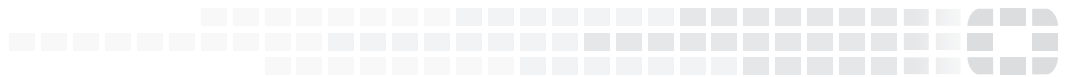
Bug ID	Description
394949	Users can not use remote access if the custom host name contains a special character.
397943	Out-of-date even if AV signature versions are the same.
399709	Hostname is different from the distinguished name.
402357	FortiClient upgrade may cause Reboot pop-up to loop.
402441	Alert emails not being sent when malware is detected.
404667	Unable to remove endpoint from quarantine after connection flap with EMS.
405421	SSL certificate date is displayed as invalid in browsers.
407262	Can not import computer from AD server.
408546	Cannot set <i>Connection Key</i> .
408804	Incorrect FCT AV quarantined message sent to EMS.
409145	Fail to import second AD domain.
410030	Failed connection attempts to <code>fgdl.fortigate.com</code> .
410482	CA Certificate is not usable after upgrading to 1.0.4.
410618	Android and iOS cannot register to EMS build 1.0.4 build 121.
410627	FortiClient uninstall through EMS is not working.
412410	EMS should disable related button when importing a domain.
413095	Log potential duplicated UID.
413275	Failed to uninstall EMS via control panel.
416635	<code>FCMServer</code> log use out of disk space.
421951	Unable to see devices in <i>Other Endpoints</i> .
423809	FQDN change did not update the notification server.
423995	Notification server is only :8013.

Known Issues

The following issues have been identified in version 1.2.0. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
384879	MsSqlCmdLnUtils is not uninstalled.
393691	EMS server should notify if port is already in use.
400439	FortiSandbox will only respond to an authorized FortiClient.
409651	il is not sent with Gmail SMTP server.
413868	Failed to remove user from old LDAP server after switching LDAP server in the <i>User Management</i> page.
416006	Upload log to FortiAnalyzer setting state did not change properly.
416020	Device status not correct after uninstall.
416998	Dual Registration to EMS(1.0.5) and FortiGate (5.6 GA) cannot unregister.
417288	Different feature icons in profiles, client details and FortiClient console.
421319	Need to have the option to disable <i>Block Malicious Websites</i> when onnet.
421706	After upgrade from 1.0.5, 1.2.0 uninstaller asks for source path.
423326	Should enable <i>All Web Download Submission</i> option when enabling the EMS Sandbox feature.
434328	sslv3 and tls1.0 cannot be disabled on EMS server.
434534	FortiGate allows more special characters in the profile name than EMS.
434974	IE 11 Too slow to show advanced settings.
434993	When uninstalling FCT, the FCT status does not update.
435899	There is no schedule prompt or reboot prompt when upgrading fct 870 to 1068 from EMS.
435991	EMS GUI updates overwrite entire the XML configuration tab.
436238	VCM signature not sent to EMS.

Bug ID	Description
436443	EMS should support computers with the same names.
436618	Option <i>Mark as Uninstall</i> should not be visible if client is online.
436629	<i>IP Address</i> switches to <i>All</i> after upgrade.
436829	Application signature categories are not up to date.
436844	No permission is required to reset deployment.
436953	Inactive timeout doesn't work properly.
437081	Duplicate records after scan.



Copyright© 2017 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.