FortiClient EMS - Release Notes

Version 6.0.1

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 COOKBOOK
https://cookbook.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: techdocs@fortinet.com

July 24, 2018
FortiClient EMS 6.0.1 Release Notes
04-601-498632-20180724

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-07-23	Initial release.
2018-07-24	Updated What's New on page 8.

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 introduced in FortiOS 5.0 and enhanced in FortiOS 5.2. Like FortiOS, EMS supports all FortiClient platforms: Microsoft Windows, Mac OS X, Linux, 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 can use a FortiGate or EMS to manage their installations.

This document provides the following information for FortiClient EMS 6.0.1 build 0077:

For information about FortiClient EMS, see the *FortiClient EMS 6.0.1 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 Mac OS X
- FortiClient for Linux
- FortiClient for Android OS
- FortiClient for iOS

The FortiClient version should be 5.4.0 or newer.

FortiClient is supported on multiple Microsoft Windows, Mac OS X, 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 EMS6.0.1 GUI:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Internet Explorer is no longer 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

Deploying FortiClient upgrade to Windows 7

FortiClient EMS disables TLS 1.0, 1.1 for all incoming SSL connections. On Microsoft Windows 7 (and likely Windows Server 2008 R2) devices, the WinHTTP library FortiClient uses for file downloads does not use TLS 1.0/1.1 by default. When deploying FortiClient from EMS 6.0.1 to Windows 7 endpoints that already have FortiClient 6.0.1 or older installed, the deployment may fail.

This issue only exists when deploying from EMS 6.0.1 to Windows 7 endpoints with FortiClient installed. It does not exist when:

- Deploying to Windows 8.1 or 10
- Deploying from EMS 6.0.0 or older
- The endpoint does not have FortiClient installed

There are various ways to address this issue.

Enabling TLS 1.2 on Windows 7 using registry settings

Follow the discussions in Update to enable TLS 1.1 and TLS 1.2 as a default secure protocols in WinHTTP in Windows to add a registry setting.

1. Install the Windows Update Hot Fix:
   Update to enable TLS 1.1 and 1.2 as default secure protocols in WinHTTP (KB3140245)

   

   If regular Windows Update is enabled by default, this KB is already installed.

2. Create a DWORD registry entry: DefaultSecureProtocols in the path:
   - On systems running x86 architecture:
     HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
   - On systems running x64 architecture
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp

   Set the value to 0x00000A00 to enable both TLS 1.1 and 1.2.

Enabling TLS 1.0 and 1.1 in EMS

EMS 6.0.1 provides an option in *System Settings* to enable support for TLS 1.0 and 1.1 for file downloads. The EMS administrator may use this option when deploying FortiClient upgrades to Windows 7 endpoints. Once deployment is complete, you can disable the option.

What's New

The core features of FortiClient EMS 6.0.1 include the following:

Enhanced FortiClient integration with FortiSandbox scanning

EMS retrieves the list of file types from FortiSandbox. The EMS administrator may create endpoint profiles with predefined or custom lists of file types, and assign the same to endpoint groups.

Through EMS, FortiClient is able to receive a list of valid file types to monitor locally. New files introduced into the local file system with matching file types are sent to the FortiSandbox.

This feature requires FortiClient (Windows) 6.0.1 and FortiSandbox 3.0.0

EMS REST API - Web Filter profile update

The EMS administrator may import endpoint profiles from FortiManager. The existing feature to import endpoint profiles from FortiGate has been improved.

License expiry grace period

When the license expires, the number of supported FortiClient instances remains unchanged for a few days. This allows the EMS administrator some time to download a renewal license from FortiCare and upload it to EMS.

During this grace period, the EMS GUI displays the license status as *Expired*, along with a link to upload a renewal license. The GUI shows the number of seats available as 10.

After the grace period is over, the number of supported FortiClient instances goes back to 10 and the license status changes to *Trial*, unless (and until) the renewal license is uploaded.

FortiClient local update server

Micro-FortiGuard Server for FortiClient is a local update server for FortiClient endpoints. FortiClient can receive software and signature updates locally from Micro-FortiGuard Server for FortiClient instead of reaching out to FortiGuard Distribution Server, helping save WAN bandwidth. It is recommended that organizations with more than 5000 FortiClient endpoints use Micro-FortiGuard Server for FortiClient to receive local updates.

For details, see the *Micro-FortiGuard Server for FortiClient Administrator Guide* that is available on the Fortinet Document Library under FortiClient EMS.

Upgrading

Upgrading from previous EMS versions

FortiClient EMS 6.0.1 supports upgrading from the following EMS versions:

- 6.0.0
- 1.2.4 and later

Downgrading to previous versions

Downgrading FortiClient EMS6.0.1 to previous EMS versions is not supported.

Resolved Issues

The following issues have been fixed in version 6.0.1.

Endpoints (AD domains, workgroups)

Bug ID	Description
497116	One of OUs from the same domain goes to unmanaged status automatically.

Endpoint profiles

Bug ID	Description
492613	The length of [dbo].[group_container].[dn] should be increased to 1024 chars (or higher).
445380	Add option to show block message from FortiClient bubble popup for HTTPS site.
480822	EMS option to control (enable/disable) sending of vulnerability statistics in FortiClient.
489959	AD daemon always at 25%.

FortiClient deployment

Bug ID	Description
495908	EMS not assigning installer to most endpoints.
496947	Signing software packages with EMS fails.

Other

Bug ID	Description
468898	Disabled TLS 1.0 support to be compliant with PCI-DSS 3.2
474317	Setting option names in EMS GUI are not clear.
491635	*First Detected* in *Software Inventory* should be local time.
492216	Editing LDAP user permissions is not working.
495534	FCEMS_UpdateDaemon consuming 100% CPU.

Known Issues

The following issues have been identified in version 6.0.1. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Endpoint profiles

Bug ID	Description
483826	FortiClient sending IPsec SA delete when xauth is not completed in two minutes.
487488	Provide a message when profile cannot be opened due to missed signatures.
496118	Port 8443 used by EMS for Chromebooks, and should not be assigned to regular EMS.
497672	Add GUI option for allowing websites when a rating error occurs.
500009	EMS failed to push Sandbox synced high risk extensions list to FortiClient.
500061	Sandbox extension list should not be all.

FortiClient deployment

Bug ID	Description
496895	When using EMS to upgrade FortiClient from 5.6 to 6.0.0, installer waits until someone logs in to start.

Notifications and email

Bug ID	Description
468475	Email alerts stopped working.
489562	Mail server rejecting EMS email alerts.

Other

Bug ID	Description
414539	EMS should get renewal licenses information from FDS.
482404	Clearing logs via GUI is incomplete.
502049	Summary LDAP query returned an error (code referral).