FortiClient EMS - Best Practices

Version 6.2

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: techdoc@fortinet.com

April 18, 2019
FortiClient EMS 6.2 Best Practices
04-620-552946-20190418

TABLE OF CONTENTS

Overview

This guide is a collection of best practices guidelines for using FortiClient EMS. Use these best practices to help you get the most out of your FortiClient EMS products, maximize performance, and avoid potential problems.

Installing and licensing EMS

Before installing EMS, it is recommended to review the server, hardware, software, and port requirements in the *FortiClient EMS Administration Guide*. Also, follow the guidelines below:

- Ensure that EMS is installed on a dedicated server.
- Check that port 443 is not in use.
- Ensure access to EMS is available. Open any firewall ports as needed.
- By default, FortiClient EMS is installed with SQL Server Express. If you have an existing instance of SQL Server (Express, Enterprise, or Standard) installed on the EMS server, you can customize the SQL Server instance by installing EMS using the CLI. Note that when managing more than 5000 endpoints, it is recommended to use FortiClient EMS with SQL Server Enterprise or Standard. See the *FortiClient EMS Administration Guide* for details.

It is recommended to provide remote users direct access to the EMS server. In this case, you must configure EMS FQDN-accessible from the inside and outside. You must also open the following ports to allow client access:

- 8013: receive profile updates
- 10443: allow downloading software updates

SQL database management

The following lists best practices when using SQL Server with FortiClient EMS:

- By default, FortiClient EMS is installed with SQL Server Express. However, SQL Server Express has a 10 GB limit. If managing more than 5000 users, it is recommended to use EMS with a licensed version of SQL Server, such as Enterprise or Standard, which support redundancy, backup, and more database entries and storage.
- Perform SQL database backups regularly.
- Practice data redundancy to ensure an instance of the database is available at all times.
- Restore the database and clean up old entries on a regular basis.

EMS server configuration

Server settings

The following lists tasks that require direct access to the EMS console. Other tasks can be done via remote HTTPS access.

- Decide whether to assign an FQDN or static IP address to the FortiClient EMS server. Do not assign a dynamic IP address to the EMS server.
- Enable remote HTTPS access for administrators.
- Set the hostname and FortiClient download URL. Ensure endpoints can access the download URL by navigating to it from a browser on one of the endpoints.

Logs settings

Configure log level and the number of days to keep logs. These settings affect database size. If managing a large number of endpoints, it is also recommended to reduce the number of days EMS stores logs and alerts.

FortiGuard settings

Enable FortiManager. You can use FortiManager or Micro-FortiGuard Server for FortiClient to download signature updates from FortiGuard. When managing more than 5000 endpoints, it is recommended to use Micro-FortiGuard Server for FortiClient or FortiManager for local updates and category lookup.

For details, see the *Micro-FortiGuard Server for FortiClient Administration Guide* or the *FortiManager Administration Guide*.

Endpoints settings

- Keep alive interval: The keep alive interval is the interval between endpoint connections to the EMS server to check for profile updates. If managing a large number of endpoints, a large number of endpoints frequently connecting to the EMS server can affect server and network performance. In this case, it is recommended to increase the keep alive interval.
- License timeout interval: This setting is useful for EMS administrators who need to manage reusing licenses. The minimum license timeout interval is one day. You should modify this setting based on the number of licenses and of managed endpoints.

Administrator

- Change the password for the default administrator after logging in. Use a strong password that combines uppercase and lowercase letters, numbers, and symbols. There is no password recovery mechanism for the default admin user. It is recommended therefore to keep the admin password safe. It is also recommended to create additional user accounts in case the administrator password is lost.
- Add a remote administrator.
- Add local Windows users.
- Super administrator permissions allow the administrator to access and modify all settings on the EMS server. These permissions should be restricted to as small a group as possible to ensure security for both the server and endpoints.
- You cannot configure an administrator to have access to only certain groups or OUs within a domain. You can only configure an administrator to have full access to a domain or no access at all.

Alerts settings

You can configure an email server and EMS to email alerts to you. It is recommended to receive alerts about non-compliant and unregistered endpoints.

- EMS Alerts: enable receiving information in case of issues with the EMS server
- Endpoint Alerts: enable receiving information about security events on endpoints
- SMTP server: configure to receive email alerts

Endpoint provisioning

FortiClient EMS provides scalable and centralized management of multiple endpoints. One of the following endpoint management structures is recommended depending on the use case.

Before deploying to the production server, test deployment with a test endpoint group and test profiles. If the test deployment is successful, then attempt deployment on the production server.

Use case	Endpoint management structure
Active Directory (AD) is set up and same structure is desired for endpoint management.	AD integration: • Put endpoints in OUs • Keep OU structure • Group changes made in EMS do not sync back to AD (one-way sync only) • Endpoints in security groups are not imported into EMS
Large deployment that needs custom grouping or does not have AD setup	Automated group assignment. See the *FortiClient EMS Administration Guide* for details.
Small deployment	Custom groups: • Manually create groups in EMS, then move endpoints into groups • By default, endpoints are placed in the *Other Endpoints* group

Endpoint provisioning consists of the following steps. For details on each step, see the *FortiClient EMS Administration Guide*.

1. Create a profile and gateway IP list. It is recommended to create a profile for each deployment package. It is recommended to put the addresses for all FortiGate units in one gateway IP list. Ensure the FortiGate is located as physically close as possible to the endpoints being monitored.
2. Create a deployment package. Select the desired FortiClient features to deploy to endpoint. See FortiClient feature recommendations on page 11 for details.
3. Assign the deployment package to a profile.
4. Create an endpoint policy. Assign the profile and gateway IP list to the policy. Assign the policy to the desired endpoint group.

FortiClient endpoints lock configuration changes in the FortiClient console. The end user cannot change the configuration.

For an initial deployment, you can deploy FortiClient using the Microsoft AD server, or send the FortiClient download link from EMS to users. After the initial deployment, you can push future updates from EMS.

For an initial deployment of FortiClient (macOS), deploy FortiClient (macOS) manually.

Create a profile for the *Other Endpoints* group, and assign the profile to the group. This allows you to assign preferred settings to any FortiClient endpoints assigned to the *Other Endpoints* group.

FortiClient feature recommendations

When creating deployment packages in FortiClient EMS to deploy FortiClient to endpoints, it is recommended to include different sets of FortiClient features to install depending on the endpoint. Do not install components that are not required. For example, if you have no users who need to access the network remotely, do not install the Remote Access feature.

Endpoint description	Recommended features
No third-party AntiVirus product installed	• Security Fabric Agent (Vulnerability Scan) • Advanced Persistent Threat (APT) Components (FortiSandbox) • AntiVirus, Anti-Exploit • Web Filtering
Only VPN needed (endpoint already has a third-party AntiVirus product installed)	• Security Fabric Agent (Vulnerability Scan) • Secure Access Architecture Components (SSL and IPsec VPN)

The following lists the recommended options to enable for each feature:

Feature	Recommended options
AntiVirus	• *Block Access to Malicious Websites* • *Block Known Communication Channels Used by Attackers*: This feature uses Application Firewall. If Application Firewall is not enabled, it will still be active if *Block Known Communication Channels Used by Attackers* is enabled. • *Automatically Submit Suspicious Files to FortiGuard for Analysis*: Unless restricted by the organizational security policy, it is recommended to enable this option. It allows faster detection of malicious files. • *Exclusions*: Follow the OS and other software vendors' recommendations to configure AV scan exclusions. It is important to configure recommended exclusions on servers. • If FortiClient is deployed on a Windows Server with Web Filter and Application Firewall components, *Block Access to Malicious Websites* and *Block Known Communication Channels Used by Attackers* should be disabled. *Scan Email* should also be disabled for Windows Servers.
Web Filter	• Block *Security Risk* site category • *Client Web Filtering When On-Net.*: This option should be enabled. See the *FortiClient EMS Administration Guide* for details. • *Log All URLs* and *Log User Initiated Traffic*: These will be logged to FortiAnalyzer only and not to EMS. • *Exclusion List*. See the *FortiClient EMS Administration Guide*.
VPN	The following options are available when configuring a VPN tunnel: • *Allow Non-Administrators to Use Machine Certificates*: You must configure the `<run_fcauth_system>` element. See the *FortiClient XML Reference* for details. • *Save Password*

Feature	Recommended options
	• *Auto Connect* • *Enable Local LAN* • *Dead Peer Detection*: It is recommended to disable this option when on a poor connection, as this option can cause dropped connections. • *Enable Implied SPDO* • *Auto Keep Alive* • *On Connect/On Disconnect Scripts*
Vulnerability Scan	• Configure *Scheduled Scan* • Enable *Automatic Patching* for vulnerabilities that are rated *High* and above • Some programs, such as Adobe software and Java, cannot be patched automatically. For these programs, manual patch is required. See the *FortiClient Administration Guide* for details.
System Settings	• *UI* > *Require Password to Disconnect from EMS*: A password lock can be used to allow end users to disconnect FortiClient from EMS using a configured password. Instead of disabling the option for users to disconnect, it is recommended to leave it enabled and configure the password lock. This allows administrators to disconnect FortiClient using the configured password when needed and is useful for troubleshooting scenarios. • *Log* > *Level*: It is not recommended to set the log level to Debug, except for troubleshooting purposes. • *Update* > *Use FortiManager for Client Signature Update*: FortiClient downloads updates directly from FortiGuard servers. Ensure all endpoints can access the update servers. If a FortiManager or Micro-FortiGuard Server for FortiClient is present, it can be used to receive signature updates. • *Endpoint Control* > *Disable Unregister*: When enabled, FortiClient cannot disconnect from EMS. It is recommended to use *Require Password to Disconnect from EMS* instead. • *Endpoint Control* > *On-Net Subnets* and *Endpoint Control* > *Gateway MAC Addresses*: See the *FortiClient Administration Guide* for how FortiClient determines on-net/off-net status. The MAC address list is optional and can only be used with on-net subnet configuration.

Since only Vulnerability Scan and AntiVirus are supported on Windows Server machines, it is recommended to create separate installers for them where only AntiVirus is enabled. Windows Servers do not support Web Filter or Application Firewall, so these features must be disabled on the installer.

When creating a deployment package, if *Keep updated to the latest patch* is enabled, the deployment package is automatically updated when a new FortiClient version is available on FDS servers, then deployed to endpoints. To control software updates manually, disable this option. It is recommended to disable this feature on installers used to deploy FortiClient to servers to prevent uncontrolled service disruption during a FortiClient upgrade.

If a FortiGate is present, connect Fabric Agent to FortiGate for deep visibility. List the FortiGate IP address in the gateway IP list so the endpoint can connect to the authorized FortiGate.

EMS maintenance

The following lists best practices for EMS maintenance:

- Ensure to regularly upgrade FortiClient EMS whenever a new version is upgrade. For details on each release, check the *FortiClient EMS Release Notes*.
- Back up the EMS database weekly by going to *Administration* > *Back up Database*.
- Review alerts regularly.
- For details on migrating EMS to a new server, see Use Case: Migrating EMS to a New Server.

To ensure server security, follow these best practices for server hardening:

- User account best practices:
  - Configure user accounts with strong, complex passwords. Change passwords regularly. Do not reuse passwords.
  - Lock accounts after a number of login failures. Login failures may be illegitimate attempts to gain access to your system.
  - Do not permit users to configure accounts with empty passwords.
  - Limit user accounts to access only what they need. Increased access should only be granted on an as-needed basis.
- Firewall best practices:
  - Configure the system firewall. Proper setup of a firewall can prevent many attacks.
  - Consider using a hardware firewall.
- Avoid using insecure protocols that send your information or passwords in plain text format.
- Minimize unnecessary software on your servers.
- Keep your operating system up-to-date. Ensure to install any security patches.
- Minimize open network ports to only what is needed for your specific circumstance.
- Maintain proper database backups.
- Ensure physical server security.

Troubleshooting

Seeing file path for a vulnerable application

You can see the file path for a vulnerable application in FortiClient.

1. In FortiClient on the endpoint, go to *Vulnerability Scan*, then click the number of total vulnerabilities.
2. Expand the desired vulnerability. FortiClient displays the file path for the vulnerable application.

Gathering debug logs

1. Create an endpoint profile intended for troubleshooting.
2. Set the log level to *Debug*.
3. Create a new endpoint group, then move the desired endpoint to the group.
4. Assign the new profile to an endpoint policy, then assign the endpoint policy to the group. This turns on debugging for the endpoint.
5. Repeat the desired action on the endpoint.
6. Run the Diagnostic Tool in FortiClient and send the output to Fortinet support.
7. Set the log level in the profile back to *Info*.

If experiencing slow performance or abnormally high CPU usage with FortiClient, it is recommended to enable then disable Application Firewall, then AntiVirus. This may solve the issue without need for further troubleshooting.

Change log

Date	Change Description
2019-04-18	Initial release.

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.