FORTINET®

High Performance Network Security

FortiClient EMS - Administration Guide

VERSION 1.0

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

October 19, 2015

FortiClient EMS 1.0 Administration Guide

04-100-225910-20151019

TABLE OF CONTENTS

Change Log

Date	Change Description
October 19, 2015	Initial release
November 6, 2015	Updated to add info about stacked licenses
January 28, 2016	Clarified wording in the Preparing the AD Server for Deployment section
March 4, 2016	Clarified wording around licensing for FortiGate when used with FortiClient EMS.
March 18, 2016	Clarified that the FortiClient EMS installer does not let you choose an installation location.
July 11, 2016	Clarified that Windows users with No Access cannot log into FortiClient EMS.

Introduction

FortiClient Enterprise Management Server (FortiClient EMS) is a security management solution that enables scalable and centralized management of multiple endpoint devices (computers). FortiClient EMS provides an efficient and effective administration of endpoints running FortiClient. It provides visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.

FortiClient EMS is designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints. Some of the benefits of deploying FortiClient EMS include:

- Remotely deploying FortiClient software to Windows PCs
- Updating profiles for endpoint users regardless of access location, such as, administering antivirus, web filtering, VPN, and signature updates
- Administering FortiClient endpoint registrations, such as, accept, de-register, and block registrations
- Managing endpoints, such as, status, system, and signature information
- Identifying outdated versions of FortiClient software

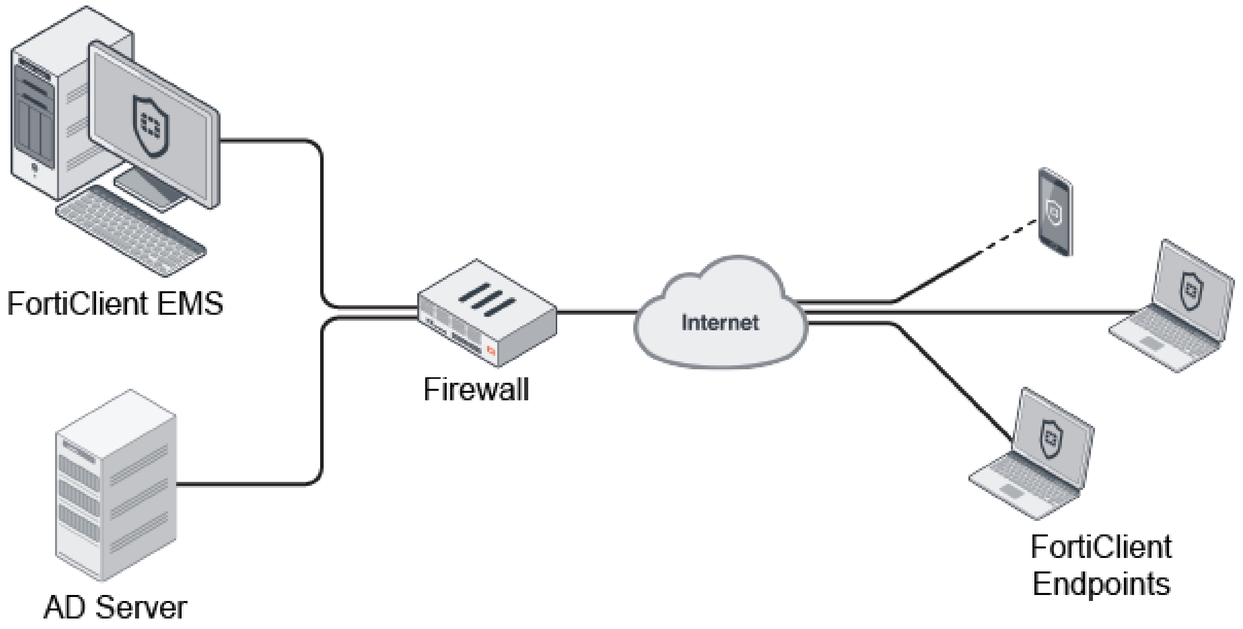
You can manage endpoint security for both Windows and Mac OS X platforms by using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view.

Components of FortiClient EMS

FortiClient EMS provides the infrastructure to install and manage FortiClient Endpoint software. FortiClient protects endpoint clients from viruses, threats, and risks. FortiClient EMS can be used to ensure that clients are compliant with the organization's security profiles.

The following table lists the components of FortiClient EMS.

Component	Description
FortiClient EMS	Manages the client computers (endpoints) that connect to your network. It includes the following software: • The console software that manages security profiles and client computers. • The server software provides secure communication to and from the client computers and the console.
Database	Stores security profiles and events. The SQL database is installed as part of the FortiClient EMS installation.
FortiClient	Enforces security and protection technologies on the client computers (endpoints). It runs on the servers, desktops, and portable computers that you wish to be secured. See the *FortiClient Administration Guide* on docs.fortinet.com for more information.



FortiClient EMS allows you to:

- Establish and enforce security profiles
- Manage the deployment, configuration, updates, and reports of antivirus protection from an integrated management console
- Protect endpoint clients against viruses, blended threats, and security risks
- Obtain a consolidated view of multiple security components across all endpoint clients in your network
- Perform integrated installation of security components and set profiles

FortiClient EMS and Fortinet Endpoint Security Management

FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network. Refer to the product documentation available for FortiClient EMS for detailed information on how to install and use FortiClient EMS.

Documentation

You can access the FortiClient EMS documentation from the following link: docs.fortinet.com

The FortiClient EMS documentation set includes the following documents:

- *FortiClient EMS 1.0 Release Notes*
  This document describes new features and enhancements in the FortiClient EMS system for the release and lists any known issues and limitations. This document also defines supported platforms and the required minimum system requirements.
- *FortiClient Enterprise Management Server 1.0 - QuickStart Guide*

This document describes how to install and begin working with the FortiClient EMS system. It provides instructions on installation, deployment, and also includes a high-level task flow for using the FortiClient EMS system.

- *FortiClient EMS 1.0 Administration Guide*

  This document describes how to set up FortiClient EMS and use it to manage FortiClient endpoints. It includes information on how to configure multiple endpoints, configure and manage profiles for the endpoints, and view and monitor the FortiClient endpoint profile status.

What's New in FortiClient EMS 1.0

The new features in FortiClient EMS 1.0 include the following:

FortiClient Endpoint Registration Server

FortiClient end users can register to the EMS. The process is similar to registering to a FortiGate. The end user provides the IP address or Fully Qualified Domain Name (FQDN) of the EMS in the Endpoint Control registration box in FortiClient. The EMS shows basic information about the registered endpoint, including:

- Computer name
- User name
- IP address
- Registration status (on-net, off-net, offline, etc.)
- Operating system
- FortiClient version
- FortiGuard engine and signature update status

Endpoint Profiles

Different FortiClient configurations can be created by using an easy to use Web-based Manager or by harnessing the flexibility provided by the FortiClient XML configuration.

A profile can be assigned to a group of registered endpoints. Profiles can be created, updated or removed. Updated profiles will be pushed to registered users automatically. Users may register at any time to retrieve the latest assigned profile. A default profile is assigned to registered endpoints that do not have a designated profile.

The Basic Configuration offers the most commonly used configuration options. A *show advanced option* button is provided within the Basic view. This exposes more options in the Basic view, allowing the administrator to modify most FortiClient options without manually editing the XML configuration.

Endpoints in Active Directory Domain Services

For organizations that use Active Directory Domain Services (AD server) to manage computers, there is an easy to use interface to import computers into the EMS. Computers that join the AD server will be listed in the EMS, preserving the AD Organizational Unit (OU) structure. The EMS presents basic information about each computer as retrieved from the AD server, including:

- Computer name
- Organizational unit (and structure)
- Operating system

A group of computers imported into the EMS may be assigned any endpoint profile. If any of the endpoints in the domain register to the EMS, additional information become available, such as:

- User name
- IP address
- Registration status

Endpoints in Workgroups

The EMS will automatically detect any computer running Microsoft Windows that is running the Computer Browser Service within the same local network. These computers are listed in the EMS, with similar details as endpoints discovered from an AD server. The name of the workgroup replaces information about the organizational unit from the AD server.

Scanning local workgroups is disabled by default. Go to the *View* > *Settings* menu item to enable it.

Remote Endpoints

Not all computers within an organization will show in the Computer Browser Service. For companies that do not already use an AD server to manage computers, users can join the EMS by registering to it directly. This also works for devices that do not support the AD server or Computer Browser Service. Remote users can register to the EMS by providing the IP address or FQDN of the EMS to FortiClient.

Custom Groups

Computer endpoints may be added into the EMS using multiple methods:

- Importing from an Active Directory (AD) server
- Discovering computers from the local network
- Registering manually from the installed FortiClient

Endpoints imported from an AD server may already have a structured organization or containers. Similarly, computers discovered from the local network may already belong to an intended workgroup. In the event that these pre-existing structures do not match present or future needs, new custom groups can be created in the EMS. Endpoints can then be moved into the custom groups as required.

An organizational structure can be represented in the EMS using nested custom groups. The EMS administrator can apply FortiClient profiles to groups at various levels. Nested groups with unassigned profiles inherit profiles from their immediate parent group.

Dashboard Summary

Managed endpoints' activities are summarized in the EMS dashboard page on the landing page after signing into the EMS GUI. Pie charts are used to show the number of managed clients, online/offline status of clients, and on-net/off-net status of clients. A bar chart shows a summary of warnings, inactivity, and protection status for managed endpoints.

The sections in each of the charts are live links. Any section of the pie or bar charts may be clicked to find all matching records reflected in the summary.

Antivirus Scan Results

The EMS will show the current antivirus (AV) scanning in the GUI. Statuses are provided for each managed client that is online.

FortiClient runs scheduled AV scans by default. The EMS administrator may include AV scanning schedules in endpoint profiles. The administrator may also request a one-time AV scan from the EMS GUI. For each of these scanning requests, the EMS displays the current status.

Alert Messages

The EMS generates various notifications for the administrator. These are available in the EMS GUI by selecting the *Alert Icon* (a bell). Examples of events that generate alerts include:

- New version of FortiClient is available
- FortiClient deployment failed
- Unable to check for signature updates
- Error encountered while downloading AD server entries or while checking for local computers

A red label is associated with the *Alert* icon when new notifications are available or received. It is cleared once the alert has been viewed.

Trial License

FortiClient EMS provides a trial period of 60 days from the time of installation (with 20,000 seats). These licenses will allow EMS administrators to evaluate the product's full feature set with a sufficiently large number of endpoints as desired. Once the trial license expires, the default free license will revert to 10 seats.

A valid product license may be applied any time during or after the trial period. The number of licenses required is based on the number of clients that are deployed or registered by the EMS: one license is required for each client that is deployed or managed.

FortiClient Deployment

The EMS can be used to deploy and install FortiClient on computers running Microsoft Windows. The computers must have joined an AD server that has been added into the EMS. The deployed FortiClient installer may be repackaged to install only some of FortiClient's features. FortiClient can automatically register to the EMS once installation is completed. The AD server requires some simple group policy changes to prepare it for FortiClient deployment.

Endpoints managed by FortiGate Devices

The EMS can deploy FortiClient to endpoints that are, and will continue to be, managed by a FortiGate. FortiClient profiles can be loaded from a FortiGate to the EMS, and then distributed to new endpoints that are registered to the FortiGate.

The FortiGate, in this case, may be configured to enforce Network Access Control (NAC). FortiClient needs to register to the FortiGate to satisfy NAC requirements. FortiClient will continue to send notifications to the EMS. The administrator can monitor FortiClient registration status from the EMS.

Management Capacity

The EMS is intended for use by enterprises. It has the capacity to manage a large number of endpoints. The following are suggested EMS host system hardware configurations, depending on the number of endpoints being managed.

Suggested minimum EMS system hardware

Max number of managed endpoints	Number of Virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
10,000	2	4	default
20,000	4	8	default
30,000	4	8	120 seconds default
40,000	4	8	120 seconds default
50,000	4	8	120 seconds default

For the purpose of this table, an Intel i5 processor with two cores and two threads per core will be considered to have 4 virtual CPUs.An Intel i3 processor with two cores and one thread per core has two virtual CPUs.

Each registered FortiClient sends a short keep alive message to the EMS at a regular interval. The keep alive message carries various update information from the client to the EMS. If a modification or change is made on the EMS, it sends it to the clients in the keep alive reply.

The default keep alive interval in FortiClient EMS is 60 seconds by default. To change the keep alive interval, go to the *View* > *Settings* menu item, and change the *Keep Alive Interval* option on the *Server Settings* tab.

When FortiClient is registered to FortiOS (FortiGate) instead of FortiClient EMS, the default keep alive interval in FortiOS 5.2 is 120 seconds.

Overview

This section provides an overview of how to:

- Install and configure FortiClient EMS.
- Discover endpoint devices and deploy FortiClient
- Monitor and update endpoint devices

Installing and configuring FortiClient EMS

Before installing FortiClient EMS, it is recommended that you read the *FortiClient EMS Release Notes* and the *FortiClient Enterprise Management Server - QuickStart Guide* available on docs.fortinet.com to become familiar with relevant software components and other important information about the product.

Following is an overview of how to install and configure FortiClient EMS.

1. Prepare for the FortiClient EMS installation. See Installation Preparation on page 17.
2. Install FortiClient EMS. See Installing FortiClient EMS on page 22.
3. Log into FortiClient EMS. See Logging into FortiClient EMS on page 23.
4. License FortiClient EMS. See Licensing and registering FortiClient EMS on page 24.
5. Configure FortiClient EMS settings. See Configuration on page 26.
6. Configure user accounts and permissions. See User Management on page 30.

Deploying FortiClient to endpoints

Following is an overview of how to discover endpoint devices and deploy FortiClient on the endpoint devices from FortiClient EMS.

1. Discover endpoint devices. See Discovering endpoints on page 34.
2. Add FortiClient installers to FortiClient EMS, and specify what FortiClient features to install. See Adding installers on page 39.
3. Configure profiles to select the FortiClient installer and specify settings for the features that it will install. See Configuring profiles on page 43.
4. Prepare domains and workgroups for deployment. See Preparing the AD Server for Deployment on page 49.
5. Assign profiles to domains and workgroups to deploy FortiClient on endpoints. See Assigning profiles to endpoints on page 44.

Managing and updating endpoint devices

Following is an overview of how to monitor endpoint devices.

1. Monitor endpoint status. See Viewing endpoint status on page 52.
2. Monitor FortiClient EMS status. See Viewing the Dashboard on page 52.
3. Update profiles to update FortiClient on endpoint devices. See Editing profiles on page 44.

Installation Preparation

Before you install FortiClient EMS in your network, you should consider the following concepts and requirements to help you prepare for the installation:

- Licensing options for FortiClient EMS. See Licenses on page 17.
- Installation requirements and dependencies. See Requirements and dependencies on page 19.
- Server readiness checklist. See Server readiness checklist for installation on page 21.

Licenses

This section describes the licensing options available for FortiClient EMS. It provides information about the number of supported FortiClient endpoints for each type of license to help you determine which license best suits your needs.

Description of licenses for FortiClient EMS

FortiClient EMS supports the following types of licenses:

- Free trial license
- Purchased license

Free trial license

When you install FortiClient EMS, the free trial license is enabled by default. The free trial license supports 20,000 FortiClient endpoints for 60 days from the time of installation. FortiClient EMS consumes one license count for each managed FortiClient device.

No license key is required for the free trial license. When the trial period expires, FortiClient EMS automatically reverts to a free default license that supports a maximum of 10 FortiClient endpoints. The free default license does not require a license key.

Fifteen days before the trial license expires, FortiClient EMS starts generating alerts. An alert is displayed when you log into FortiClient EMS, and you can view the alerts in the alert log. See Alerts and Log Messages on page 53.

You can upgrade to a purchased license at any time to continue supporting all of the managed FortiClient endpoints.

Purchased license

Each purchased license allows management of one FortiClient endpoint. You must purchase a minimum quantity of 100 FortiClient EMS licenses.

You can stack FortiClient EMS licenses for a term of up to 5 years.

The purchased license requires a license key and a yearly subscription.

For example, if you purchased 100 licenses for FortiClient EMS, you must install a license key on FortiClient EMS, and then you can register 100 FortiClient endpoints for one year. If you want to register more FortiClient endpoints, you must purchase another license. A yearly subscription is required for each license unit.

You can use a licensed FortiClient EMS to deploy, provision, and manage FortiClient endpoints. However, if you have a FortiGate in your network, you can buy an *Add-On FortiGate Endpoint* license to enforce Endpoint Compliance on the firewall while endpoints are being managed by FortiClient EMS. Using FortiGate with FortiClient EMS is optional.

Summary of licenses

The following table summarizes the license model for FortiClient EMS.

FortiClient EMS licenses	When used	Supported number of endpoints	Subscription	License key
Free trial license	Used by default after installing FortiClient EMS	20,000 FortiClient endpoints for a maximum of 60 days. When the trial period expires, FortiClient EMS automatically reverts to a free default license.	Not required	No
Free default license	Used only after the free trial license expires	10 FortiClient endpoints. FortiClient EMS defaults to this license after the time period expires for the free trial license.	Not required	No
Purchased license	Used when you purchase and install the license key	One unit of license supports 100 FortiClient endpoints. You can purchase any number of license units	Requires yearly subscription	Yes

Licenses for component applications

Common services or applications do not require a license. See the *FortiClient Enterprise Management Server - QuickStart Guide* for more information about the common components.

During the installation of common services required for FortiClient EMS, you are not asked for license information.

Help with licensing

For licensing issues with FortiClient EMS, contact the licensing team at Fortinet Technical Assistance Center (TAC):

- Phone: +1-866-648-4638
- Technical support: support.fortinet.com/

Requirements and dependencies

You can install and use FortiClient EMS as a standalone product on an active directory server or a standalone Windows machine. Requirements for installation and operation vary in relation to the presence of other software on the server and according to how you use FortiClient EMS.

Server hardware and system requirements

Component	Description
Operating System	One of the following: • Microsoft Windows Server 2012 and 2012 R2 • Microsoft Windows Server 2008 R2 • Windows Installer MSI installer version 3.0 or later
System Hardware	• 2.0 GHz 64-bit processor, dual core (or two virtual CPUs) • 2 GB RAM • 5 GB free hard disk space • Gigabit (10/100/1000baseT) Ethernet adapter See also Management Capacity on page 13.
Network	• Internet access
Endpoint Client	• FortiClient v5.2.4 or later

Required services and ports

You must ensure that required ports and services are enabled for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with clients and servers running associated applications.

Communication	Service	Protocol	Port
FortiClient endpoint registration	File transfers	TCP	8013 (default)
Computer browser service	Enabled		
Samba (SMB) service • During FortiClient deployment, endpoints may connect to the FortiClient EMS server using the SMB service.	Enabled		445

Communication	Service	Protocol	Port
Distributed Computing Environment / Remote Procedure Calls (DCE- RPC) • The FortiClient EMS server connects to the endpoints using RPC for FortiClient deployment.	Enabled		135
Active Directory server connection	When used as a default connection		389
Windows	HTTP	TCP	80
Internet Information Services (IIS)	HTTPS	TCP	443, 10443
SQL server			

⚠ Ensure that the Computer Browser Service is running. On Windows Server 2012 R2, the service is disabled by default. If this service is not active, FortiClient EMS cannot detect computers on the same network, even if they are available.

Server readiness checklist for installation

Use the following checklist to prepare your server for installation, after you verify that the server meets the requirements described in Requirements and dependencies on page 19”.

Checklist	Readiness Factor
	Temporarily disable security applications. You must temporarily disable any antivirus software on the target server before you install FortiClient EMS. Installation might be slow or disrupted while these programs are active. Note that a server might be vulnerable to attack when you uninstall or disable security applications.
	Carefully consider the date and time settings that you apply to your server.
	Confirm that required services and ports are enabled and available for use by FortiClient EMS.
	Ensure that no conflict exists with Port 80 and 443 for Apache service to function properly.

Installation

Before you install and license FortiClient EMS on a server, ensure that you have:

- Reviewed Licenses on page 17
- Met the requirements listed in the Requirements and dependencies on page 19
- Completed the Server readiness checklist for installation on page 21
- Logged into the server as administrator. The administrator user account is equivalent to a Windows administrator account and provides access to all common services, FortiClient EMS, and other application tasks. You can use this account to initially log in to the server and to create other user accounts for normal day-to-day use of the applications.

It is recommended that you install FortiClient EMS on a dedicated server in a controlled environment. Installing other software applications can interfere with the normal operation of FortiClient EMS.

Installing FortiClient EMS

Installing and licensing FortiClient EMS requires the following steps:

1. Be aware of software dependencies.
2. Obtain or locate the FortiClient EMS installation program.
3. Run the FortiClient EMS installation program.

Software dependencies

The EMS requires Microsoft SQL Server 2014 Express to be installed on the server. The EMS installer will automatically install it if it is not already installed. Microsoft SQL Server Express has its own software dependencies. Some of these must be downloaded during the EMS installation. For this reason, access to the internet is required during installation.

The setup progress bar may appear to freeze for about 15 minutes while installing Microsoft SQL Server 2014 Express. The full EMS installation can take about 20 minutes to complete.

Obtaining the FortiClient EMS installation program

FortiClient EMS is available for download from the following locations:

- Fortinet Support website (support.fortinet.com)
- Sales representative

Running the FortiClient EMS installation program

To install FortiClient EMS:

1. Double-click the downloaded installation file for FortiClient EMS. The installation wizard starts.

If you are not logged into the server as an administrator, right-click the installation file and select *Run as administrator*.

2. Follow the installation wizard instructions.

   In the License terms and agreement window: Select *I agree to the license terms and conditions* if you agree with the license terms and conditions. If you do not agree, the installation process stops.

3. Click *Install*.

   The applications that will be installed are displayed. The FortiClient EMS installation package includes the following applications: *FortiClient EMS, Microsoft SQL Server 2012 Express Edition, Apache HTTP server*. The installation setup process begins.

4. Continue following the installation wizard instructions.

   After the program has installed, the *Setup Successful* window is displayed.

5. Click *Close*.

   A desktop icon is created, which opens the FortiClient EMS application home page.

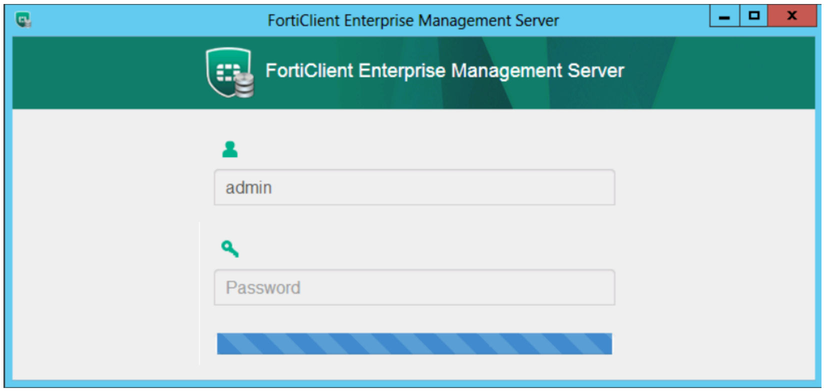
6. Re-enable any antivirus applications that you temporarily disabled.

Logging into FortiClient EMS

FortiClient EMS runs as a service on Windows computers.

To open FortiClient EMS:

1. Double-click the FortiClient EMS icon, or select *Start* > *All Programs* >FortiClient EMS to start the application.
2. Log in by using the default admin account. Enter `admin` for user name, and leave the password field empty. Click *Sign in*. The FortiClient EMS application opens.


FortiClient Enterprise Management Server
FortiClient Enterprise Management Server
Password

admin

The client automatically closes if it is idle for 120 minutes.

3. Add a password to the administrator account by going to *View -> User Management*. See also Configuring user management on page 31.
4. To exit the application, click *Admin* > *Logout* on the toolbar.

Accessing FortiClient EMS remotely

FortiClient EMS can be accessed using a web browser in lieu of the GUI.

- To access the EMS from the EMS server, visit `https://localhost`.
- To access the server remotely, use the server's hostname: `https://<server_name>`.

Ensure that you can ping <server_name> remotely. This can be achieved by adding it into a DNS entry, or by adding it to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

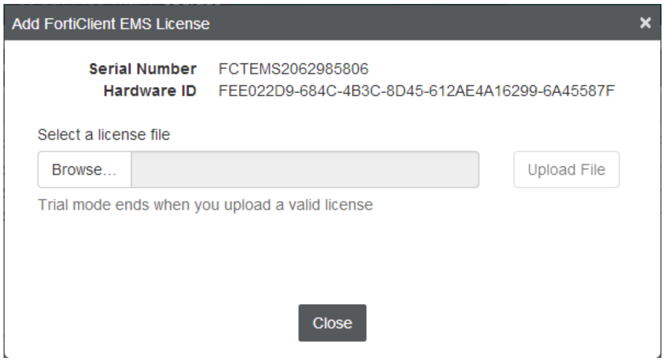
Licensing and registering FortiClient EMS

When you install FortiClient EMS, the free trial license is enabled by default. If you plan to use the trial mode, you can skip this procedure. A license is not required when you are using FortiClient EMS in trial mode.

If you have purchased a license, you must obtain and install the license key. A Fortinet Support login is required, and you must also register your copy of the FortiClient EMS software on FortiCare.com. When registering, you must provide the Product Authorization Key (PAK) that you obtain from FortiCare.

To license and register FortiClient EMS:

1. Obtain a login to the Fortinet Support site (support.fortinet.com/Home.aspx). If you already have a login, skip this step.
2. In FortiClient EMS, obtain the product serial number by selecting *View* > *Upgrade Licenses*.



Add FortiClient EMS License

Serial Number FCTEMS2062985806
Hardware ID FEE022D9-684C-4B3C-8D45-612AE4A16299-6A45587F

Select a license file

Trial mode ends when you upload a valid license

3. Register the product serial number on the Fortinet support site (support.fortinet.com/Home.aspx). *FortiCare* generates the license key file, which includes the expiry date, serial number, and information about the number of clients.
4. Download the license key file from www.forticare.com.

If you are not a registered user, download the license file from Fortinet Support downloads (www.fortinet.com/en-us/support/downloads).

5. Install the license key in FortiClient EMS:
   a. Select *View* > *Upgrade Licenses*.
   b. Click *Browse*, and locate the license key file.
   c. Select *Upload File*.

Upgrading the FortiClient EMS license

To upgrade the FortiClient EMS license:

1. Go to *View* > *Upgrade License*. The Add FortiClient EMS License pane is displayed.
2. Click *Browse*, locate the license key file, and click *Upload File*.

Uninstalling FortiClient EMS

Use the *Programs and Features* pane of the Control Panel in Microsoft Windows to uninstall FortiClient EMS.

FortiClient EMS installs the following dependencies. If they are not being used by other applications on the same computer, they can be uninstalled manually after the EMS has been removed.

- Microsoft ODBC Driver 11 for SQL Server
- Microsoft SQL Server 2008 Setup Support Files
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2014 (64-bit)
- Microsoft SQL Server 2014 Setup (English)
- Microsoft SQL Server 2014 Transact-SQL ScriptDom
- Microsoft Visual C++ 2010 x64 Redistributable – 10.0
- Microsoft Visual C++ 2010 x86 Redistributable – 10.0
- Microsoft Visual C++ 2013 x86 Redistributable – 12.0
- Microsoft VSS Writer for SQL Server 2014
- SQL Server Browser for SQL Server 2014

To uninstall FortiClient EMS:

1. Select *Start* > *Control Panel* > *Programs* > *Uninstall a program*.
2. Select *FortiClient Enterprise Management Server*, and click *Uninstall*.
3. Follow the uninstallation wizard prompts.

Configuration

This section describes how to configure FortiClient EMS server settings and log settings. It also describes how to import CA certificates as well as back up and restore the database.

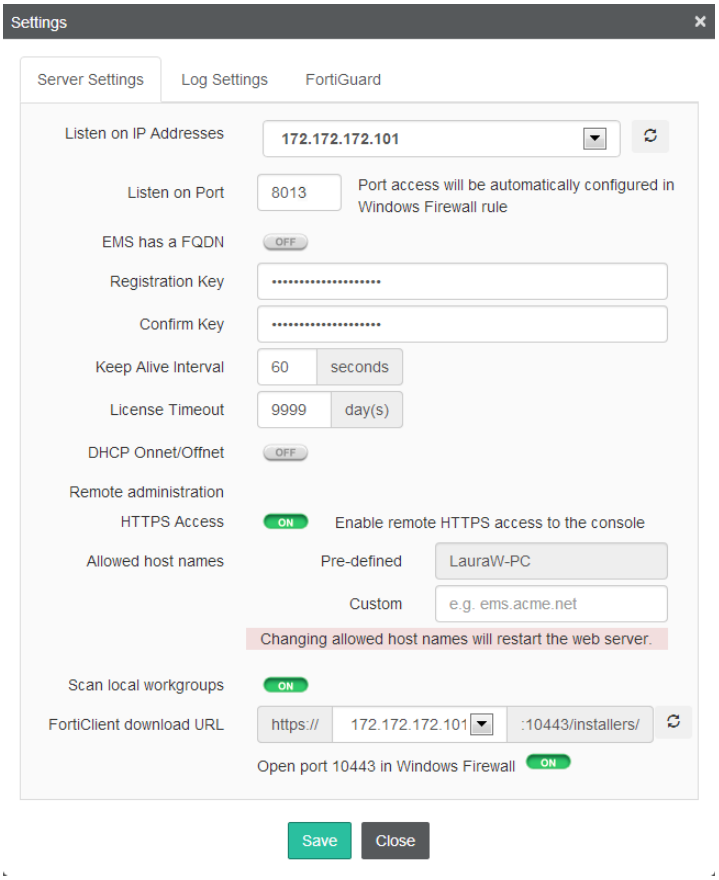
Configuring FortiClient EMS

Configuring server settings

FortiClient EMS installs with a default IP address and port configured. You can change the IP address and port, and configure other server settings for FortiClient EMS.

To configure server settings:

1. Go to *View* > *Settings*.
2. Click the *Server Settings* tab, and configure the options. For a description of the options, see Server Settings tab on page 28.
3. Click *Save*.



Listen on IP Addresses: 172.172.172.101

Listen on Port: 8013 — Port access will be automatically configured in Windows Firewall rule

EMS has a FQDN: OFF

Registration Key: ••••••••••••••••••••

Confirm Key: ••••••••••••••••••••

Keep Alive Interval: 60 seconds

License Timeout: 9999 day(s)

DHCP Onnet/Offnet: OFF

Remote administration

HTTPS Access: ON — Enable remote HTTPS access to the console

Allowed host names: Pre-defined LauraW-PC; Custom e.g. ems.acme.net

Changing allowed host names will restart the web server.

Scan local workgroups: ON

FortiClient download URL: https:// 172.172.172.101 :10443/installers/

Open port 10443 in Windows Firewall: ON

Configuring log settings

You can specify what level of log messages to capture in the logs for FortiClient EMS. You can also specify when to automatically delete logs and alerts.

To configure log settings:

1. Go to *View* > *Settings*.
2. Click the *Log Settings* tab, and configure the options. For a description of the options, see Log Settings tab on page 29.
3. Click *Save*.

Importing certificates

You can import CA certificates into FortiClient EMS.

To import certificates:

1. Go to *View* > *CA Certificate Management*.
2. Click *Import*.
3. Browse to the CA certificate, and click *Upload*. The CA certificate is uploaded.
4. Click *Close*.

Backing up and restoring the database

You can back up and restore the FortiClient EMS database.

To back up the database:

1. Go to *View* > *Database Management*. The Database Operations pane is displayed.
2. Click *Backup Database*.

   When the database backup is complete, Windows Explorer is displayed with the database backup file selected.

To restore the database:

1. Go to *View* > *Database Management*. The Database Operations pane is displayed.
2. Click *Browse*, and select the database backup file.
3. Click *Restore Database*.

   When the database is restored, a message is displayed. The message instructs you to wait for the restored database to be reloaded.

4. Wait for the restored database to be reloaded.

Configuration references

This section contains descriptions of the fields used to configure FortiClient EMS.

Server Settings tab

Following is a description of the fields on the *View* > *Settings* > *Server Settings* tab.

Option	Description
Listen on IP Addresses	Displays the default IP address for the FortiClient EMS server. You can change the IP address by typing a new IP address. FortiClient will register to the FortiClient EMS on the specified IP address.
Listen on Port	Displays the default port for the FortiClient EMS server. You can change the port by typing a new port number. FortiClient will register by using the specified port number.
EMS has a FQDN	Turn on to specify a fully qualified domain name (FQDN) for the FortiClient EMS server.
EMS FQDN	Displayed when *EMS has a FQDN* is turned on. Type the FQDN for the FortiClient EMS server. FortiClient can register by using either the specified IP address in the *Listen on IP Addresses* option or the specified FQDN.
Registration Key	Add the registration key for FortiClient EMS. FortiClient must provide this key during registration. There is no registration key by default.
Confirm Key	Add the registration key for FortiClient EMS again to confirm the key.
Keep Alive Interval	Each registered FortiClient sends a short keep-alive message to FortiClient EMS at the specified interval.
License Timeout	A license seat is consumed by each registered FortiClient. If a FortiClient unregisters from FortiClient EMS, the license seat is retained in anticipation that the FortiClient will re-register. The registration record is deleted if the FortiClient does not re-register within the given timeout.
DHCP Onnet/Offnet	Enable to monitor endpoints that are within the company network (on-net). Endpoints that register to FortiClient EMS from outside of the company network are considered off-net.
Remote administration	Specify settings for remote administration access to FortiClient EMS.
HTTPS Access	Turn remote HTTPS access to FortiClient EMS console on and off. When enabled, administrators can use a browser and HTTPS to log into the FortiClient EMS console. When disabled, administrators can only log into FortiClient EMS console on the server.
Allowed host names	Available when *HTTPS Access* is turned on. Displays the pre-defined host name of the server on which FortiClient EMS is installed. You can change the host name. When you change the host name, the web server restarts.

Option	Description
Scan local workgroups	Turn on to enable FortiClient EMS to automatically scan workgroups on the network to discover endpoint devices in the workgroups.
FortiClient download URL	FortiClient installers created on FortiClient EMS will be made available for download at the URL.
Open port 10443 in Windows Firewall	Turn on to open port 10443, and turn off to close port 10443. Port 10443 is used to download FortiClient.

Log Settings tab

Following is a description of the fields on the *View* > *Settings* > *Log Settings* tab.

Option	Description
Log level	Select the level of messages to include in FortiClient EMS logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiClient EMS logs.
Auto Remove Logs	Type the number of days that you want to store logs. For example, if you type 30, logs will be stored for 30 days. Any logs older than 30 days are automatically deleted.
Remove All Logs	Click to immediately delete all FortiClient EMS logs.
Auto Remove Alerts	Type the number of days that you want to keep alerts. For example, if you type 30, alerts will be kept for 30 days. Any alerts older than 30 days are automatically deleted.
Remove All Alerts	Click to immediately delete all FortiClient EMS alerts.

FortiGuard tab

FortiClient EMS regularly connects to FortiGuard to determine the current versions of FortiClient software and signatures that are available. The information is compared to the update information provided by each registered FortiClient endpoint. A summary of outdated registered endpoints is available on the FortiClient EMS dashboard.

Following is a description of the fields on the *View* > *Settings* > *FortiGuard* tab.

Option	Description
Use FortiManager for client software/signature update	Turn on to use FortiManager for updating FortiClient software or signatures. You must specify the IP address or host name for FortiManager as well as the port number.
Use proxy for updates	Turn on to specify a proxy for updates to FortiClient software.

To configure FortiManager for use by FortiClient on each endpoint, see System Settings tab on page 47.

User Management

This section describes the default user accounts and permissions for FortiClient EMS. It also describes how to change the administrator password and how to configure Windows users.

Default user accounts and permissions

FortiClient EMS authenticates your user name and password at log in and establishes your role within the application. This role defines your access to and task permissions for FortiClient EMS.

If you are not authorized for certain tasks or devices, the related menu items, items in content pages, and buttons are hidden or disabled. In addition, a message informs you that you do not have permission to view the selected information or perform the selected operation.

The default administrator user has full access and permissions. It has access to all configured LDAP servers and has authority to configure other user privileges. The administrator has complete access to all FortiClient EMS permissions, including modification, profile assignment, approval, discovery, and deployment.

By default, the default administrator account can give Windows user accounts access to FortiClient EMS. When you give a Windows user access to FortiClient EMS, you can choose between the following profiles:

- No Access
- Administrator

When you choose *No Access*, the Windows user cannot log into FortiClient EMS.

When you choose *Administrator*, the Windows user can log into FortiClient EMS and view content as well as perform tasks. You can also configure the level of access and permissions for the Windows user.

Following is a description of the default settings for *No Access* and *Administrator* for Windows users:

Permissions	No Access	Administrator
View Endpoints	No	Yes
View Groups	No	Yes
View Profiles	No	Yes
Add Endpoints	No	Yes
Search for Endpoints	No	Yes
Create Work groups	No	Yes
Delete Work groups	No	Yes
Assign Profiles	No	Yes

Permissions	No Access	Administrator
Delete Profiles	No	Yes

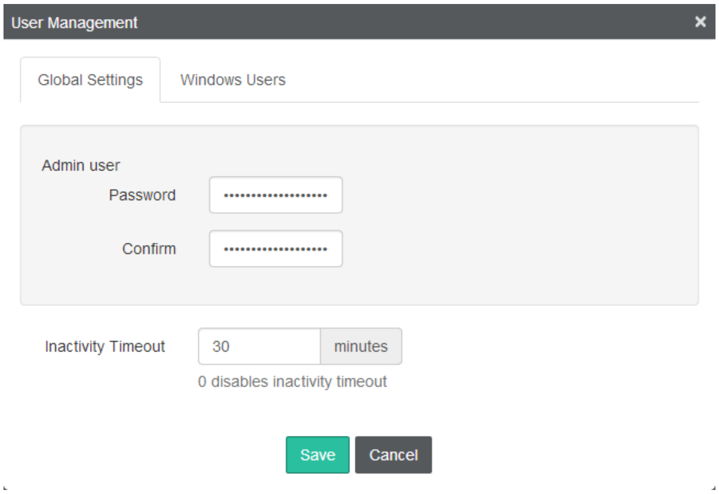
Configuring user management

Changing the administrator password

By default, the password is blank for the administrator account. You should add a password to increase security.

To change the administrator password:

1. Go to *View* > *User Management*.
2. On the *Global Settings* tab, change the password.
3. Click *Save*.



Admin user

Password ••••••••••••••••••

Confirm ••••••••••••••••••

Inactivity Timeout 30 minutes

0 disables inactivity timeout

Configuring Windows user accounts

You can configure Windows users to have no access to FortiClient EMS, or you can configure Windows users to have administrator access to FortiClient EMS.

The list of Windows users is derived from the server on which FortiClient EMS is installed. If you want to add more Windows users, you must add them to the server.

To configure windows users:

1. Go to *View* > *User Management*.
2. On the *Windows Users* tab, select a Windows user from the *User* list.
3. Perform one of the following actions:
    a. To give the selected user no access to FortiClient EMS, click *No Access*. For a description of the permissions, see Default user accounts and permissions on page 30.

   b. To give the selected user administrator access to FortiClient EMS, click *Administrator*, and then configure the options. For a description of the options, see Windows Users tab on page 32.

4. Click *Save*.

User Management references

This section contains descriptions of the fields used to configure user management.

Global Settings tab

Following is a description of the fields on the *View* > *User Management* > *Global Settings* tab.

Option	Description
Admin user	Change the password for the admin user account
Password	Change the password for the admin user account. By default the password is blank. You can specify a password by typing in the password.
Confirm	Confirm a new password by typing the password in again.
Inactivity Timeout	Specify how long to keep inactive users logged into FortiClient EMS. When the time expires, the user is automatically logged out of FortiClient EMS. Type 0 to keep inactive users logged into FortiClient EMS indefinitely.

Windows Users tab

Following is a description of the fields on the *View* > *User Management* > *Windows Users* tab.

Option	Description
User	Select the Windows user for whom you want to configure administrator access and permissions for FortiClient EMS.
No Access	Click to give the selected Windows user no access to FortiClient EMS.
Administrator	Click to give the selected Windows user administrator access to FortiClient EMS, and then use the settings to configure access and permissions.
LDAP Access	Available only when *Administrator* is selected.
Permissions	Available only when *Administrator* is selected. Use the settings to configure permissions to FortiClient EMS for the selected Windows user.
Use Windows Password	Selected to allow the Windows user to use a Windows password to log into FortiClient EMS.

Option	Description
Create / Delete / Rename LDAP Records	Select to allow the Windows user to create, delete, and rename LDAP records. Clear to disable this permission.
Create / Delete Filters	Select to allow the Windows user to create and delete filters. Clear to disable this permission.
Endpoints	Use the following options to configure permissions for the selected Windows user.
Block / Unblock / Deregister / Quarantine / Unquarantine Endpoints	Select to allow the Windows user to block, unblock, deregister, quarantine, and unquarantine endpoints. Clear to disable this permission.
Run commands on Endpoints	Select to allow the Windows user to run commands on endpoints. Clear to disable this permission.
Can access Software Manager	Select to allow the Windows user to access the *View* > *Software Management* options. Clear to disable this permission.
Can access Certificate Management Policies	Select to allow the Windows user to access the *View* > *CA certificate Management* options. Clear to disable this permission.
Assign / Unassign Policy / Custom Groups Management	Select to allow the Windows user to assign to endpoints and unassign profiles from endpoints as well as manage custom groups. Clear to disable this permission.
Create / Delete / Edit / Rename Policy	Select to allow the Windows user to create, delete, edit, and rename profiles. Clear to disable this permission.
Edit Advanced Policy	Select to allow the Windows user to use the advanced settings when editing a profile. Clear to disable this permission.

Endpoints

Endpoints can be discovered automatically or manually with Active Directory Domain Service or Windows workgroups. You can import and synchronize information about user and computer accounts from an Active Directory server with LDAP or STARTTLS service. You cannot add, delete, or move groups within an imported group. After importing, workgroups are listed under *Other groups* in the Endpoints pane of the interface.

Discovering endpoints

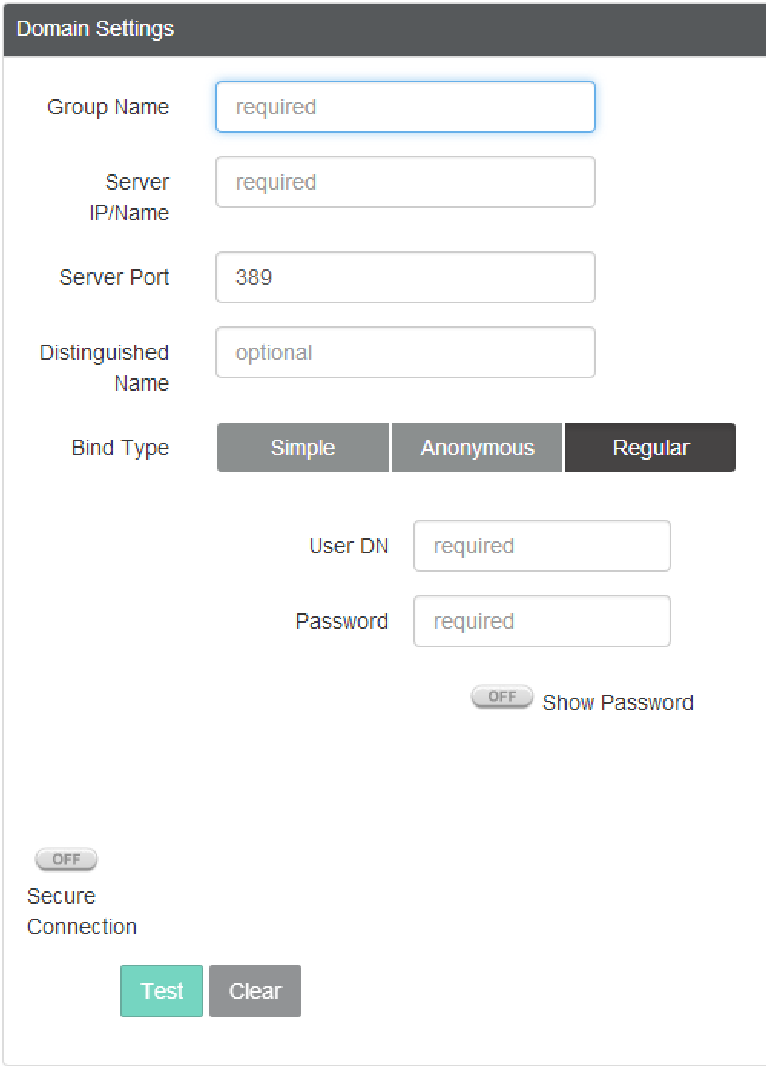
You can discover endpoints by adding an Active Directory (AD) domain service or by enabling FortiClient EMS to automatically discover endpoints in Windows workgroups. You can also register a FortiClient endpoint to FortiClient EMS from the endpoint.

Adding an Active Directory Domain service

You can add endpoints by identifying the endpoint devices that are part of an Active Directory (AD) domain service.

To search for endpoints using Active Directory Domain Service:

1. Click *Endpoints* > *Add a New Domain*. The *Domain Settings* page opens.



Domain Settings

Group Name: required

Server IP/Name: required

Server Port: 389

Distinguished Name: optional

Bind Type: Simple | Anonymous | [✓ Regular]

User DN: required

Password: required

OFF Show Password

OFF Secure Connection

2. On the *Domain Settings* page, set the options. For a description of the options, see Domain Settings pane on page 37.
3. Click *Test* to test the domain settings connection.
4. If the test is successful, select *Save* to save the new domain. If not, correct the information as required then test the settings again.

Enabling automatic discovery of endpoints with Windows workgroups

You can enable automatic discovery of endpoint devices in the local Windows workgroups.

To enable automatic discovery of workgroups:

1. Go to *View* > *Settings*.
2. Turn on *Scan local workgroups*. For a description of the options, see Server Settings tab on page 28.

3. Click *Save*.
4. View the discovered endpoints in the *Endpoints* > *Workgroups* list.

Registering manually from FortiClient

You can manually register FortiClient endpoints to FortiClient EMS by specifying the IP address for FortiClient EMS in FortiClient.

FortiClient 5.2.4 or later must be installed on the endpoint device to use the antivirus scan feature of FortiClient EMS.

To register an endpoint to FortiClient EMS

1. Ensure that FortiClient 5.2.4 or later is installed on the endpoint (device).
2. In FortiClient, select *Register to FortiGate*.
3. Enter the IP address configured for the FortiClient EMS. See Configuring FortiClient EMS on page 26.
4. Select *Go* to register FortiClient.

For more information about endpoint management, refer to the *FortiClient Administration Guide* available on the docs.fortinet.com site.

The registration port may be appended to the registration IP address on FortiClient and separated by a colon. When the port is not provided, FortiClient attempts to register to the IP address given by using the default port. The default registration port in FortiClient 5.2 is 8010 and in FortiClient 5.4 is 8013. FortiClient EMS listens for registration on port 8013 by default.

Viewing discovered endpoints

After FortiClient EMS has discovered endpoints, you can view details about the endpoints.

To view endpoints:

1. Go to *Endpoints* to view all discovered endpoints.
2. Select an endpoint to view its details.
3. Got to *Endpoints* > *Workgroups* > *All Groups* to view all endpoints in all groups.
4. Select an endpoint to view its details.

Managing endpoints

You can manage endpoints from the *Endpoints* pane. Some options are available as buttons, and some options are available in the right-click menu. Right-click an endpoint to display the menu.

Option	Description
Refresh	Refresh the list of domains or workgroups.

Option	Description
Show empty containers	Click to display a list of domains without endpoints.
Add a New Domain	Click to add a new Active Directory (AD) server to FortiClient EMS.
Assign profile	Select and apply a profile to the selected workgroup.
Unassign profile	Select to unassign a profile from a selected workgroup.
Exclude from management	Select to exclude the selected workgroup from management by FortiClient EMS. You can also exclude individual endpoints within the workgroup from management by FortiClient EMS.
Enable management	Select to enable FortiClient EMS to manage the selected workgroup. You can also enable management by FortiClient EMS for individual endpoints within the workgroup.
Create group	Select to create a group or subgroup. You can then move devices into the group or subgroup.
Rename group	Select to rename the selected group or subgroup.
Delete group	Select to delete the selected group or subgroup.
Move devices	Select to move the devices from the selected group to another group.
Full AV scan	Select to start a full antivirus scan on the selected workgroup.
Quick AV scan	Select to start a quick antivirus scan on the selected workgroup.

Endpoint references

This section contains descriptions of the fields used to discover endpoints.

Domain Settings pane

Following is a description of the fields on the *Endpoints > Domains > Add a domain* pane.

Option	Description
Group Name	Enter a name for the group. The name will be displayed in the FortiClient EMS Endpoint view
Server IP/ Name	Type the IP address or name.
Server Port	Type the port number.

Option	Description
Distinguished Name	Type the distinguished name (optional).
Bind Type	Select the bind type. Simple, Anonymous, Regular . When you select *Regular*, enter the User DN and password.
User DN	Available when *Bind Type* is set to *Regular*. Type the user DN.
Password	Available when *Bind Type* is set to *Regular*. Type the user password.
Show Password	Available when *Bind Type* is set to *Regular*. Turn on and off to show or hide the password.
Secure Connection	Turn on to enable a secure connection protocol.
Protocol	Available when *Secure Connection* is *On*. Select the LDAPS or STARTTLS secure connection protocol.
Certificate	Available when *Secure Connection* is *On*. Select a certificate (optional).
Test	Tests the domain settings connection. If the test is successful, select *Save* to save the new domain. If not, correct the information as required, and then test the settings again.
Clear	Reset the content of the *Domain Settings* page.

Installers

FortiGuard Distribution Network

FortiClient EMS automatically connects to FortiGuard Distribution Network (FDN) to provide access to FortiClient installers that you can use with FortiClient EMS profiles. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS.

Adding installers

Creating endpoint registration IP lists

You can identify the IP address of the FortiClient EMS or FortiGate that will manage endpoints after FortiClient is installed. The FortiClient installed on the endpoint uses the IP address to automatically register with the management server.

To create endpoint registration IP lists:

1. Go to *View* > *Endpoint Registration IP List*. The *Endpoint Registration IP Lists* pane is displayed.
2. Click *Add*, and configure the options. For a description of the options, see Endpoint Registration IP List on page 41.
3. Click *Save*.

Adding FortiClient installers to FortiClient EMS

When a connection to FortiGuard Distribution Network (FDN) is available, FortiClient installers are available in FortiClient EMS for you to select in FortiClient EMS. You must select and add the FortiClient installers that you want to use to FortiClient EMS, so you can use the installers with profiles.

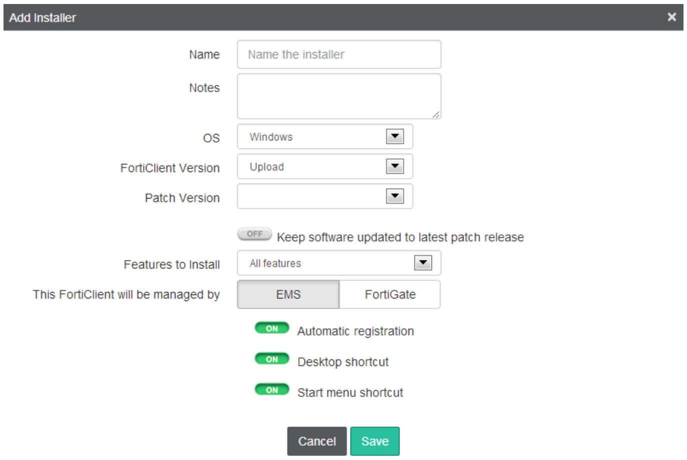
When you add the installer to FortiClient EMS, you can specify what FortiClient features to include in the installer for the endpoint. You can include a feature in the installer, and then disable the feature in the profile. Because the feature is included in the installer, you can update the profile later to enable the feature on the endpoint.

You can also specify whether FortiClient EMS or FortiGate will manage the endpoint after FortiClient is installed.

You cannot edit a FortiClient installer after you add it to FortiClient EMS. You can delete the installer, and add it again.

To add FortiClient installers to FortiClient EMS:

1. Go to *View* > *Software Manager*. The *FortiClient Software Manager* pane is displayed.
2. Click *Add*. The Add Installer pane is displayed.



Add Installer

Name: Name the installer

Notes:

OS: Windows

FortiClient Version: Upload

Patch Version:

OFF Keep software updated to latest patch release

Features to Install: All features

This FortiClient will be managed by: EMS FortiGate

ON Automatic registration

ON Desktop shortcut

ON Start menu shortcut

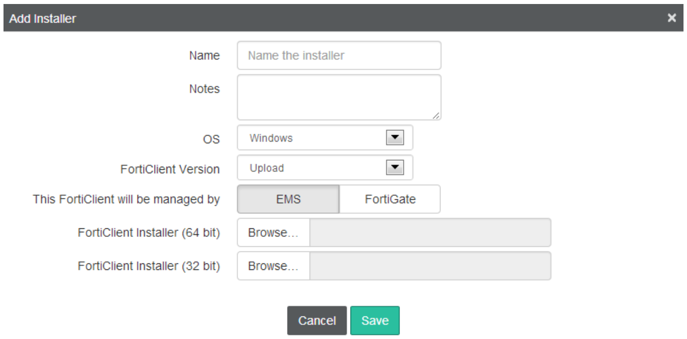
3. Select a FortiClient installer, and configure the options. For a description of the options, see Add Installer reference on page 41.
4. Click *Save*. The installer is added to FortiClient EMS and displayed on the *FortiClient Software Manager* pane.

Adding custom FortiClient installers to FortiClient EMS

You can create a custom FortiClient installer and add it to FortiClient EMS. Alternately, if a connection to FDN is not available, you might need to manually download a FortiClient installer and add it to FortiClient EMS. For more information, see FortiGuard Distribution Network on page 39.

To add custom FortiClient installers to FortiClient EMS:

1. Download a FortiClient installer.
2. Go to *View > Software Manager*. The *FortiClient Software Manager* pane is displayed.
3. Click *Add*. The Add Installer pane is displayed.
4. In the *FortiClient Version* list, select *Upload*. For a description of the options, see Add Installer reference on page 41.



Add Installer

Name: Name the installer

Notes:

OS: Windows

FortiClient Version: Upload

This FortiClient will be managed by: EMS FortiGate

FortiClient Installer (64 bit): Browse...

FortiClient Installer (32 bit): Browse...

5. Click the *Browse* button, and select the custom installer.
6. Click *Save*. The installer is added to FortiClient EMS and displayed on the *FortiClient Software Manager* pane.

Installer references

This section contains descriptions of the fields used to configure installer packages.

Endpoint Registration IP List

Following is a description of the fields on the Endpoint Registration IP List page.

Option	Description
Name	Type a descriptive name for the list of endpoint registration IP addresses.
Notes	(Optional) Type notes about the list.
IP Addresses	Type the IP address and port for FortiGate devices by using the following format: IP:port
Registration Key	Turn on to enter the registration key for FortiGate devices that FortiClient endpoints can use for registration.
EMS IP/FQDN	Displays the IP address and port for FortiClient EMS. You configure this IP address on the *View* > *Settings* page.

Add Installer reference

Following is a description of the fields on the Add Installer page.

Option	Description
Name	Type a descriptive name for the installer.
Notes	(Optional) Type notes about the installer.
OS	Select *Mac OS X* or *Windows* to identify the operating system for which the installer file is created.
FortiClient Version	Select the installer for the FortiClient version that you want to deploy to endpoints.
Patch Version	Select the patch version for the FortiClient installer if applicable.
Features to install	Available when *OS* is set to *Windows*. Select what features you want to include in the FortiClient installer. Only selected features are included in the installer. Excluded features are excluded from the installer. You can configure selected features when you configure the FortiClient EMS profile.

Option	Description
This FortiClient will be managed by	Available when *OS* is set to *Windows*. Select *EMS* or *FortiGate* to identify whether FortiClient EMS or FortiGate will manage the endpoints after FortiClient is installed. You must also select the IP address for the FortiClient EMS or FortiGate that will manage the endpoint. The FortiClient endpoint uses the IP address to automatically register with the management server. For example, if FortiClient EMS will manage the FortiClient endpoint, select the IP address for FortiClient EMS. If FortiGate will manage the FortiClient endpoint, select the IP address for the FortiGate.
Automatic registration	Available when *OS* is set to *Windows*. Turn on for FortiClient endpoints to automatically register with the management server, which is either FortiClient EMS or FortiGate. Turn off to disable automatic registration with management server.
Desktop shortcut	Available when *OS* is set to *Windows*. Turn on for a FortiClient desktop shortcut to be created when FortiClient is installed on endpoints. Turn off to disable this feature.
Start menu shortcut.	Available when *OS* is set to *Windows*. Turn on for a FortiClient start menu shortcut to be created when FortiClient is installed on endpoints. Turn off to disable this feature.
FortiClient Installer	Available when *OS* is set to *Mac OS X*. Select the FortiClient installer that you created for Mac OS X.
FortiClient Installer (64 bit)	Select the 64-bit FortiClient installer that you created.
FortiClient Installer (32 bit)	Select the 32-bit FortiClient installer that you created.

Profiles

XML configuration

You can configure FortiClient profile settings in FortiClient EMS by using a custom XML configuration file. The custom file includes all settings required by the endpoint at the time of deployment. When the endpoint registers to FortiClient EMS, ensure that the complete XML configuration file is used. For more information about how to configure a profile with XML, see the *FortiClient XML Reference* on docs.fortinet.com

Configuring profiles

Importing FortiGate profiles

You can import profiles from FortiGate to FortiClient EMS and use the profiles with FortiClient EMS.

To import profiles:

1. Click *Endpoint Profiles* > *Import profile from FortiGate*. The *Import Profile from FortiGate* wizard opens.
2. Complete the options, and click *Next* until you complete the wizard.

Adding new profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any groups that you create. The default profile is designed to provide effective levels of protection. If you want to use specific features, such as application firewall, you must create new profiles or change the default profile.

Consider the following when creating profiles:

- Use default settings within a profile.
- Consider the role of the computer when changing default profile or creating new profiles.
- Create a separate group and profile for computers that require long-term special configuration.
- Use FortiClient EMS for all central profile settings, and set options for within the group instead of for the computer itself when possible.

To add new profiles:

1. Click *Endpoint Profiles* > *Add a new profile*. The *New Profile* pane opens.
2. On the *Install Options* tab, select a FortiClient installer from the *FortiClient Deployment* list.

   The selected installer controls what tabs are displayed for the profile, based on the features that the installer includes. For example, if the installer includes only the VPN feature, only the *VPN* tab is displayed for you to configure. The *System Settings* tab is always displayed.

   You can disable a feature that is included in the installer, and then enable the feature in the profile at a later date. For example, if the installer includes the Web Filter and VPN features, you can disable the Web Filter feature and keep the VPN feature enabled. When FortiClient is installed on the endpoint, the Web Feature is installed, but disabled.

3. Configure the settings on the tabs. For a description of the options on the tabs, see Profile references on page 45.
4. Click *Save* to save the profile.

Pushing profile changes to endpoints

Assigning profiles to endpoints

After creating the profile, you can assign the profile to domains or workgroups. When you assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

To assign profiles:

1. Go to *Endpoints*, and
2. Right-click a domain or group, and select *Assign Profile*, and then the profile. The profile is assigned.
3. Hover the mouse over the name of the domain or group to view the name of the assigned profile.

Editing profiles

When you edit a profile that is assigned to endpoints, the changes are automatically pushed to the endpoints when you save the profile.

To update profiles:

1. Go to *Endpoint Profiles* > *EMS Profiles*, and select a profile. The profile settings are displayed in the content pane.
2. Edit the settings. For a description of the options on the tabs, see Profile references on page 45.
3. Click Save. The changes are installed on the endpoints associated with the profile.

Managing profiles

You can manage profiles from the *Endpoint Profiles* pane by clicking the icons.

Option	Description
Refresh	Refresh the list of profiles.
Import	Click to import a profile from FortiGate.
Add a New Profile	Click to create a new profile.
Revert to default	Click to revert the default profile to its default settings.

Option	Description
Edit	Select a profile to display its settings in the content pane for editing.
Clone	Click to clone the profile.
Delete	Click to delete the profile.

Profile references

This section contains descriptions of the fields used to configure profiles.

Endpoint Profile pane

Configuration	Description
Profile Name	Type a name for the profile.
Basic	Select to configure the profile by using the GUI.
Advanced	Select to configure the profile by using XML.

Install Options tab

Configuration	Description
Install Options	Specify the type of FortiClient deployment by selecting an installer package. You can install or uninstall FortiClient on endpoints.

AntiVirus Protection tab

Configuration	Description
AntiVirus Protection	Enable antivirus protection. Configure the following options: • Real-time Protection: Enable real-time protection. • Scheduled Scan: Enable scheduled scans, and then enter the following: • Schedule Type: Daily, Weekly, or Monthly. • Scan On: If Weekly is selected, select the day of the week to perform the scan. If Monthly is selected, select the day of the month to perform the scan. • Start: Select the start time for the scheduled scan. • Scan Type: Quick system scan, Full system scan, or Custom scan. If Custom scan is selected, enter the full path of the folder that will be scanned in the Folder field. • Exclusions: Enable exclusions from the scan. Enter fully qualified excluded folder paths or files in the provided text box to exclude these folders and add files from antivirus scanning.
Show advanced options	Turn on to display and configure basic and advanced options. Turn off to display and configure only basic options.

Web Filter tab

Configuration	Description
Web Filter	Enable web filtering. • Client Web Filtering when On-Net • Enable FortiGuard URL categorization: Block, Warn, Allow, or Monitor specific categories of web sites. See the FortiGuard web site for descriptions of the available categories and subcategories. • Rate IP addresses: Select to rate IP addresses. • Exclusion List: Enter specific URLs to block or allow. Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used.
Show advanced options	Turn on to display and configure basic and advanced options. Turn off to display and configure only basic options.

Application Firewall tab

Configuration	Description
Application FireWall	Enable application control. Refer to the *FortiClient Administration Guide* available on the docs.fortinet.com site for more information.

VPN tab

Configuration	Description
VPN	Enable VPN use. Refer to the *FortiClient Administration Guide* available on the docs.fortinet.com site for more information.
Show advanced options	Turn on to display and configure basic and advanced options. Turn off to display and configure only basic options.

System Settings tab

Configuration	Description
Show advanced options	Turn on to display and configure basic and advanced options. Turn off to display and configure only basic options.
UI options	Specify how the FortiClient user interface will appear when installed on endpoints.
Dashboard Banner	Turn on to display the dashboard banner in FortiClient. Turn off to hide the dashboard banner.
Password Lock Configuration	Turn on the password lock for FortiClient. Type a password in the *Password* field. Select *Show Password* to show the password in plain text.
Log Settings	Specify the log settings for FortiClient.
Client-based Logging when On-Net	Turn on client-based logging when FortiGate is being used as a DHCP server. For more information about using the on-net feature, see the *FortiClient Administration Guide*.
Upload Logs to FortiAnalyzer/FortiManager	Turn on to upload FortiClient logs to the FortiAnalyzer or FortiManager device at the specified address or hostname. Select the log upload time.
Update Settings	Specify whether to use FortiManager to update FortiClient on endpoints
Use FortiManager for client software/signature update	Turn on to enable FortiClient EMS to obtain antivirus signatures and software updates from the FortiManager device at the specified IP address or hostname. If required, enable *Failover to FDN when FortiManager is not available*.
Endpoint Control Settings	Specify settings for the endpoints
Silent Registration	Turn on to enable silent registration of endpoints, which means that endpoints are registered without user interaction. Turn off to require user interaction to register endpoints.
Log off when user logs out of Windows	Turn on to log off FortiClient when the endpoint user logs out of Windows. Turn off to remain logged in.

Configuration	Description
Disable Unregister	Turn on to forbid users from unregistering FortiClient from FortiClient EMS. Turn off to allow users to unregister FortiClient from FortiClient EMS.
Onnet Subnets	Turn on to enable onnet subnets.
Registration IP List	Turn on to select the IP address for the server that will manage the endpoint. You can select an IP address for FortiClient EMS or for FortiGate. When enabled, endpoints can automatically register with the management server after installation.
Other Options	
Install CA Certificate on Client	Turn on to select and install a CA certificate on the FortiClient endpoint.
FortiClient Single sign-On mobility agent	Turn on to enable the single sign-on mobility agent. Enter the IP address or hostname, port, and pre-shared key. Select *Show Password* to show the password.
iOS	
Distribute Configuration Profile (.mobileconfig file)	Turn on to select and distribute a configuration profile to FortiClient endpoints.

Deployment and updates

You can use FortiClient EMS to deploy FortiClient on the endpoint devices that are part of an Active Directory (AD) server. Deploying FortiClient from FortiClient EMS requires the following steps:

- Preparing the AD server for deployment
- Deploying FortiClient on endpoint devices

After FortiClient is deployed on endpoints, and endpoints are registered with FortiClient EMS, you can update endpoints by editing the profiles associated with endpoints. Profile changes are automatically pushed to the endpoints.

Preparing the AD Server for Deployment

Before you can successfully deploy a FortiClient installation, ensure that you install and prepare the AD server as follows:

1. Configure a group policy on the AD server.
2. Configure the required Windows services on the AD server.
3. Create deployment rules for Windows firewall
4. Configure Windows firewall domain profile settings

Configuring a Group Policy on the AD Server

To configure a group policy on the AD server:

1. On the AD server, open *Group Policy Management*.
2. Right-click the *Default Domain Policy* setting. The Group Policy Management Editor opens.

   A new policy will be applied to the entire AD domain. Alternatively, you can create a new Group Policy Object, and link it to one or more organizational units (OU) in the AD server that contains the endpoint computers on which FortiClient will be deployed.

Configuring Required Windows Services

To configure required Windows services:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *System Services*.
2. In the right panel, select the following:
   a. Task Scheduler: Automatic
   b. Windows Installer: Manual
   c. Remote Registry: Automatic

Creating Deployment Rules for Windows Firewall

To create deployment rules for Windows firewall:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Windows Firewall with Advanced Security* > *Inbound Rules*.
2. Right-click *Inbound Rules* and select *New Rule*.
3. Select *Predefined* from the drop-down list and select *File and Printer Sharing*.
4. Click *Next*.
5. Ensure that the *File and Printer Sharing (SMB-In)* box is select and click *Next*.
6. Select *Allow the connection* and click *Finish*.
7. Repeat steps 1 to 2.
8. Select *Predefined* from the drop-down list and select *Remote Scheduled Tasks Management* and click *Next*.
9. Ensure that the *Remote Scheduled Tasks Management (RPC)* box is checked and click *Next*.
10. Select *Allow the connection* and click *Finish*.

Configuring Windows Firewall Domain Profile settings

To configure Windows firewall domain profile settings:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Administrative Templates* > *Network* > *Network Connections* > *Windows Firewall* > *Domain Profile*.
2. Select *Allow inbound file and printer sharing* exception:
   - a. Right-click and select *Edit*.
   - b. Enable the radio button.
   - c. Provide the IP address of the EMS server in the text box.
   - d. Allow unsolicited incoming messages from these IP addresses.
   - e. Click OK.
3. Select *Allow inbound file and remote administration* exception:
   - a. Repeat steps listed in step 2 above to create an exception.

To deploy the group policy manually, execute `gpupdate /force` on the AD server to update the group profile on all endpoint clients.

Execute `gpresult.exe /H gpresult.html` on any AD client to view the group policy deployed on the endpoints.

Deploying FortiClient on endpoint devices

Before you can successfully deploy a FortiClient installation from FortiClient EMS by using an AD server, you must have prepared the AD server. See Preparing the AD Server for Deployment on page 49.

To deploy FortiClient on endpoint devices:

1. Add the AD server to FortiClient EMS by adding a domain. See Adding an Active Directory Domain service on page 34.
2. Add a FortiClient installer package to FortiClient EMS. See Adding installers on page 39.
3. Add a profile, select the FortiClient installer package, and configure FortiClient features in the profile. See Configuring profiles on page 43.
4. Assign the profile to a branch of the AD domain to push the FortiClient installation process on the endpoint devices. See Assigning profiles to endpoints on page 44.
5. Verify the deployment by monitoring FortiClient registrations to the FortiClient EMS.

Updating FortiClient endpoints

You can update FortiClient on endpoints by editing the profile associated with the endpoint. When you save the profile, the changes are automatically pushed to the FortiClient endpoints.

Endpoint status

Viewing endpoint status

You can monitor endpoint status within FortiClient EMS. Use the right content pane to review the following endpoint information:

- Endpoint status
- System information
- FortiClient registration information
- Signature information
- Outdated versions of FortiClient on the endpoint computers

To view endpoint status:

1. Go to *Endpoints*. A list of all endpoints and information about each endpoint is displayed.
2. Select an endpoint to view more details.

Viewing the Dashboard

On the dashboard, pie charts display the number of managed endpoints, online/offline status of clients, and on-net/off-net status of clients. A table shows a summary of warnings, inactivity, and protection status for managed endpoints. The sections in each of the charts are links. You can click any section of the pie charts or any row in the table to display more details.

To view the dashboard:

1. Click the *Dashboard* on the left pane. A summary of the status of the endpoints is displayed.
2. Click any of the pie charts or any row in the table to view more details about the summarized endpoints.
3. Click any of the displayed endpoints to view more details about the endpoint.

Alerts and Log Messages

You can view alerts and log messages generated by FortiClient EMS.

Viewing alerts

You can view the alerts generated by FortiClient EMS. Examples of events that generate an alert include:

- New version of FortiClient is available
- FortiClient deployment failed
- Failure to check for signature updates
- Error encountered when downloading AD server entries
- Error encountered when scanning for local computers

A red label is associated with the *Alert* icon when new notifications are available or received. It is cleared when you view the alert.

To view alerts:

1. Click the *Alert* icon (a bell) in the toolbar. The EMS Alert Logs pane is displayed.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filter* to remove the filters.

Viewing log messages

You can view the log messages generated by FortiClient EMS.

To view log messages:

1. Go to *View* > *View Logs*. The Logs pane is displayed.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filter* to remove the filters.

Viewing raw logs

You can view the logs generated by FortiClient EMS.

To view raw logs:

1. Click the *Bell* icon in the toolbar. The EMS Alert Logs pane is displayed.
2. Click *Raw Logs*. Microsoft Windows Explorer opens with the log file selected.

High Performance Network Security