

FortiGuard Analysis and Management Service

Version 1.3.0

Revision 2

Administration Guide

FortiGuard Analysis and Management Service Administration Guide

Version 1.3.0

Revision 2

May 22, 2009

© Copyright 2009 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	5
Customer service and technical support.....	5
Training	5
Fortinet documentation	5
Scope	6
Conventions	6
Using the FAMS service	9
About FAMS and FAMS portal	9
About accounts, contracts, and quota	9
Scalable architecture	10
Language support.....	10
Time zone settings.....	10
User types.....	10
E-Discovery accounts	11
Using the FAMS portal.....	11
Signing up for a FAMS account	11
FAMS portal GUI layout.....	12
Using the Dashboard	12
Using the Real Time Monitor	12
Using the management service	12
Using the analysis service	13
Using the tools	13
Index	15

Introduction

The FortiGuard Analysis and Management Service (FAMS) is a subscription-based service that provides remote management, logging, and reporting for all FortiGate models running FortiOS 3.0 or higher.

The subscription-based service is available from the FAMS portal web site, which provides a central location for configuring logging, reporting and remote management. From the FAMS portal web site you can also view subscription contract information, such as daily quota and the expiry date of the service.

This section introduces you to FAMS and the following topics:

- [Customer service and technical support](#)
- [Fortinet documentation](#)
- [Conventions](#)

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at <https://support.fortinet.com>.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Center article [What does Fortinet Technical Support require in order to best assist the customer?](#)

Training

Fortinet Training Services provides classes that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at <http://campus.training.fortinet.com>, or email them at training@fortinet.com.

Fortinet documentation

The Fortinet Technical Documentation web site, <http://docs.fortinet.com>, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Center.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

Fortinet Knowledge Center

The Fortinet Knowledge Center provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Center at <http://kc.fortinet.com>.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

Scope

This document explains how to:

- get a FAMS service contract
- set up a FAMS account
- configure the FortiGate devices to use the FAMS service
- how to use the FAMS portal web site to manage FortiGate devices and analyze FortiGate logs

After you log on to the portal web site, you can also use the online help.

Conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at <http://ietf.org/rfc/rfc1918.txt?number-1918>.

CLI constraints

CLI constraints, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable input for a given parameter or variable value. CLI constraint conventions are described in the CLI Reference document for each product.

Notes, Tips and Cautions

Fortinet technical documentation uses the following guidance and styles for notes, tips and cautions.



Tip: Highlights useful additional information, often tailored to your workplace activity.



Note: Also presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.



Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<pre>config system dns set primary <address_ipv4> end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments : (null) opmode : nat</pre>
Emphasis	HTTP connections are <i>not</i> secure and can be intercepted by a third party.
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></pre>
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com .
Keyboard entry	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
Navigation	Go to <code>VPN > IPSEC > Auto Key (IKE)</code> .
Publication	For details, see the FortiGate Administration Guide .

Using the FAMS service

This section contains the following topics:

- [About FAMS and FAMS portal](#)
- [Using the FAMS portal](#)

About FAMS and FAMS portal

The FortiGuard Analysis and Management Service (FAMS) is a subscription-based service that provides remote device management and centralized logging and report services for all FortiGate models running FortiOS 3.0 or higher.

The FAMS service is provided to devices through the Internet, and managed through a portal web site. This portal web site provides a central location for all the features that the service provides, such as editing account information, and reviewing logs.

To sign up and log on to the FAMS portal, from a web browser, go to <https://fams.fortinet.com>.

About accounts, contracts, and quota

The FAMS service is account-based. You can create as many accounts as you want. For example, if you are managing devices for several companies or departments, you can create an account for each company/department. Then you can add all the company's devices to that company's account.

If you have multiple accounts, the FAMS portal logon page will allow you to choose which account you want to log on.

Each account has a storage quota that can be shared by all the devices that you add under the account. And the storage quota is controlled by the contracts you purchase.

You can purchase more contracts to increase the quota if necessary. After you purchase a new contract, you can enter the contract number by going to *Management > Settings > Account Information* on the FAMS portal.

When you add a device, you can allocate quota to the device. When a device reaches its quota limit, old logs/reports are rolled out and removed. In addition to quota, each device has a maximum daily data transfer volume as 1/100 of its quota. Daily volume count starts when the device starts up.

To add a device to an account, go to *Management > Device* on the portal.



Note: After you add the device to an account and enter the contract number, the device will be automatically registered. You do not need to register your device by going to Fortinet's support web site. However, for other devices that are not using FAMS service, you must register them as usual for them to get update services.

Scalable architecture

The FAMS scalable architecture is capable of supporting a large number of FortiGate devices. Devices of an account are assigned to a manager server and a log server based on the load-balancing algorithm. FAMS also has backup servers to ensure uninterrupted service.

Communication between servers and devices are secure and encrypted. The server and device use account ID to identify each other. For information about creating an account ID, see [“Signing up for a FAMS account” on page 11](#).

Language support

The FAMS portal has three types of language settings.

- Logon page language at <https://fams.fortinet.com>: this page supports three languages: English, Chinese, and Japanese. Note that the language setting on this page only affect the logon page. It does not affect the portal language or the report language.
- Portal language: this is the language you can choose to display on the portal web site after you log on. You set the portal language for each user when you create the user account. To create a user account, on the portal, go to *Management > Settings*. Currently, English, Chinese and Japanese languages are supported.
- Report language: this is the language used to generate log reports. You select the report language when you sign up for an FAMS account. You can also change the report language by editing the account information after you log on to the portal. Currently, English, Chinese and Japanese languages are supported. To configure the report language settings, on the portal, go to *Management > Settings > Account Information*.

Time zone settings

Timestamps of logs and reports on the FAMS portal are based on device time zone settings, not the FAMS server time zones. Scheduled tasks such as firmware upgrade and script are also based on device time zone settings.

When you create or configure a FAMS account (see [“Signing up for a FAMS account” on page 11](#)), you also configure time zone settings. Since the FAMS server has many servers all over the world, this time zone setting is used to determine the closest FAMS server that the devices will connect to. Therefore, this time zone is not necessarily the device’s time zone. For example, if you have multiple devices in different time zones, you may want to choose a server that is close to most of the devices.

User types

A FAMS user can be one of the three types: admin, non-admin and e-Discovery.

- Admin users have read and write privileges.
- Non-admin users only have read privileges.
- E-Discovery users can only view search result of E-discovery tasks. E-Discovery users usually are third party members, for example, lawyers who need to read archived email messages. For details, see [“E-Discovery accounts” on page 11](#).

Only the admin users can create user accounts. To create a user, on the FAMS portal, go to *Management > Settings*.

E-Discovery accounts

An e-Discovery account can be created to view the search results of the devices' archived data. For example, a lawyer may use the e-Discovery account to view the archived email messages.

To use the e-Discovery feature:

- 1 Configure the FortiGate device to archive full email messages to FAMS by going to *Firewall > Protection Profile > Content Archive* on the FortiGate web-based manager.
- 2 On the FAMS portal, create an e-Discovery account on the *Management > Settings* page.
- 3 On the *Management > E-Discovery* page, create a new E-Discovery task, which define the email search criteria and schedules.
- 4 Then the e-Discovery user can log on to the portal and view the search results.

Using the FAMS portal

This section describes the functions and tips about using the FAMS portal.

This sections contains the following topics:

- [Signing up for a FAMS account](#)
- [Using the Dashboard](#)
- [Using the Real Time Monitor](#)
- [Using the management service](#)
- [Using the analysis service](#)
- [Using the tools](#)

Signing up for a FAMS account

Before you can use the FAMS portal, you must sign up for a FAMS account. For details about FAMS accounts, see [“About accounts, contracts, and quota” on page 9](#).

To sign up for an account, go to the FAMS portal web site at <https://fams.fortinet.com>.

When signing up for an account, pay attention to the following issues:

Account ID vs logon user name

The service account ID is the identifier that the FortiGate devices need to communicate with FAMS servers. The ID is not your logon user name to the portal. The logon user name is your email address.

Time zone settings

The time zone setting determines which FAMS server you want the device connect to. See [“Time zone settings” on page 10](#).

Multiple account logon

If you create multiple accounts with the same email address (i.e., logon user name), when you log on to the portal, you will be prompted to choose which account you want to log on. You can only log to one account at a time.

FortiGate configuration instructions

After you successfully sign up, you will receive a confirmation email. Follow the instructions in the email to configure your FortiGate devices before you can use the FAMS service.

FAMS portal GUI layout

The FAMS portal has

Using the Dashboard

The Dashboard is the default page you see after you log on to the portal.

The Dashboard is highly customizable. An account can have as many as 10 pages. Within each page, you can add widgets and define page layout.

By default, a Service page and a Report-1 page are created automatically on the Dashboard.

Using the Real Time Monitor

The FAMS server uses a management tunnel to send SNMP messages to the FortiGate devices to get device status. Only management tunnel enabled devices can have RTM widgets defined on the FAMS portal dashboard.

To enable the FortiGuard management service on a FortiGate device

- 1 On the FortiGate web-based manager, go to *System > Admin > Central Management*.
- 2 Enable the FortiGuard service, enter the FAMS account ID, and configure other settings.

Using the management service

The FAMS management service includes:

- Upgrading device firmware on the *Management > Device* page.
- Managing device configuration revisions on the *Management > Device* page.
- Deploying scripts to devices. Scripts allow you to deploy identical configuration items to many devices. For example, if all of your devices use identical administrator access profiles, you can create the access profile once as a script, and then deploy the script to all devices which should use those same settings.
- Adding contracts on the *Management > Settings* page. For details about contracts, see [“About accounts, contracts, and quota” on page 9](#).
- Managing account users on the *Management > Settings* page. For details about users, see [“User types” on page 10](#).

Using the analysis service

The FAMS server, similar to a FortiAnalyzer unit or a Syslog server, can store all the FortiGate log files, such as content logs and traffic logs.

On the Analysis page of the FAMS portal, you can view, search and browse through log files of each registered device. You can also view and generate reports.

Reports are automatically provided for each device and can be generated from the *Analysis > Report* page. Generated reports are provided as PDF files. Reports display the gathered log data in bar and pie graphs within the PDF file.

Reports help you to:

- view network usage and patterns to make informed decisions
- discover and address vulnerabilities across dispersed device installations
- minimize the effort required to identify attack patterns when customizing policies to prevent attacks
- monitor Internet surfing patterns for compliance with your company policy
- identify your web site visitors for potential customers.

Using the tools

The FAMS service provides you with the convenience of two tools:

- **Topology tool** -- similar to the Topology tab found on most FortiGate devices, allows you to create and save a diagram of your specific network. Multiple network diagrams can also be created and saved on the service's servers, which can then be retrieved whenever needed.
- **FortiConverter tool** -- allows you to convert Cisco, Juniper and CheckPoint firewall configuration files into FortiGate configuration format, so that you can deploy the configurations to the FortiGate devices.

Index

A

- account
 - creating, 11
 - FAMS, 9
- account ID, 11
- admin, 10
- analysis service, 13
- architecture
 - scalable, 10

C

- comments, documentation, 6
- contract
 - FAMS, 9
- customer service, 5

D

- dashboard
 - using, 12
- documentation
 - commenting on, 6
 - Fortinet, 5

E

- e-Discover
 - using, 11
- e-Discovery, 10

F

- FAMS
 - about, 9
- FortiConverter, 13
- FortiGate documentation
 - commenting on, 6
- FortiGuard Analysis and Management Service, 5, 9
- Fortinet customer service, 5
- Fortinet documentation, 5
- Fortinet Knowledge Center, 6

I

- ID
 - account, 11
- introduction
 - Fortinet documentation, 5

L

- language
 - portal, 10
 - report, 10
 - supported, 10

M

- management service, 12

N

- non-admin, 10

P

- portal
 - about, 9

Q

- quota, 9

R

- real time monitor, 12
- RTM, 12

S

- scalability, 10
- service
 - analysis, 13
 - management, 12

T

- technical support, 5
- time zone, 10
- tools, 13
- topology tool, 13
- type
 - user, 10

U

- user type, 10

W

- widget, 12

Z

- zone
 - time, 10

FORTINET®

www.fortinet.com

FORTINET®

www.fortinet.com