

SA report series for FortiGate

Version 1.1

Installation Guide

rev. 20051125

Table of Contents

1. Introduction.....	2
2. Software Installation.....	2
3. FortiGate Configuration.....	4
Troubleshooting.....	8
1. application won't start.....	8
2. Why I can't use some functions listed in your product comparison chart.....	8
3. How can I get manuls for this software.....	8
4. How can I use your unix installer.....	9
5. Unable to connect to web report interface.....	9
6. How should I upgrade to latest release.....	9
7. I see intrusion and virus events in generated report, can I get more information.....	9
8. Why I see nothing in webfilter reports.....	10
Contact.....	11

1. Introduction

Welcome to use our reporting software developed for FortiGate integrated security device. SA report series software provide comprehensive security analysis report, with FortiGate protection, give you more secure information environment and easier management. This software come with the following features:

- ✓ **Realtime console**
Display realtime security events and receive security news from SOC in console windows, re-experience your ASIC security hardware now.
- ✓ **Report + Dashboard dual design**
Report mode generate security reports like other reporting system. New introduced dashboard mode will update all reports automatically in the background after the interval you configured, click and watch immediately without waiting.
- ✓ **Comprehensive report**
Rich report set covering traffic,IPS,antiviurs,spam,webfilter,system.
- ✓ **Cross Platform**
Based on java technology and supposed to run on any system support J2SE without problem.
- ✓ **Support multiple DBMS**
HSQL is the default database engine,MySQL or PostgreSQL can be configured to get better performance.
- ✓ **Internationalization**
Currently english,traditional chinese and simplified chinese supported.

2. Software Installation

Before you proceed, Please download and install Java 2 Platform Standard Edition 5.0. It's available at this URL:

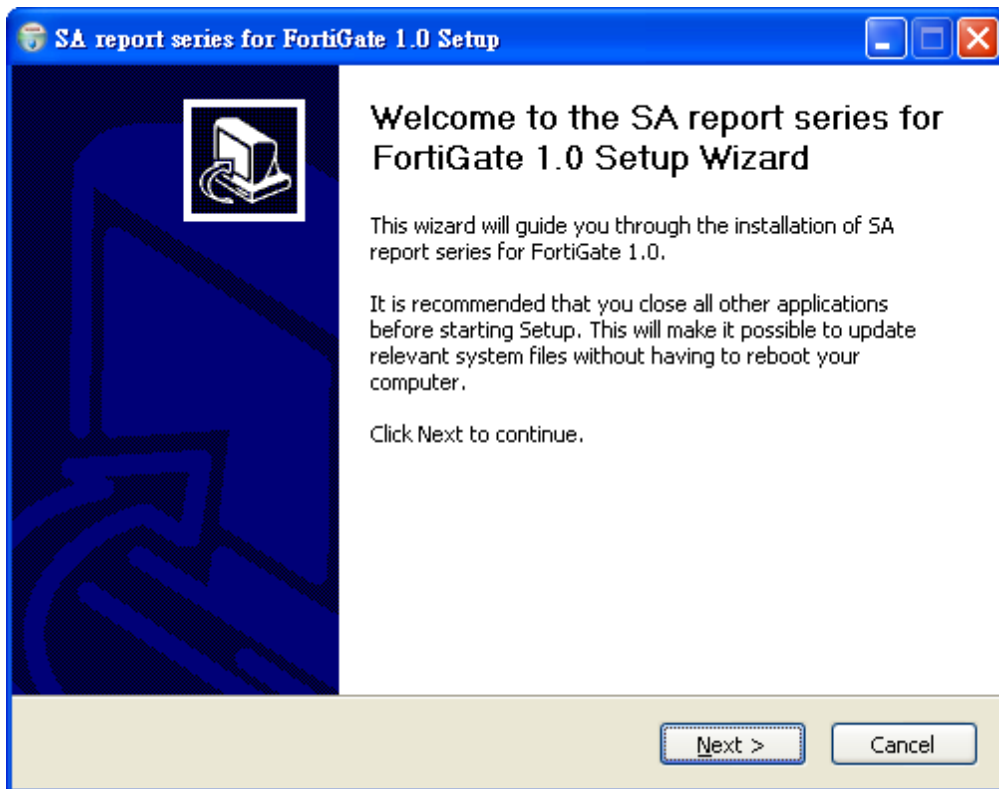
<http://java.sun.com/j2se/1.5.0/download.jsp>

Step 1

Double click on downloaded file ' SAfortigate1.1.exe ' to start installation.

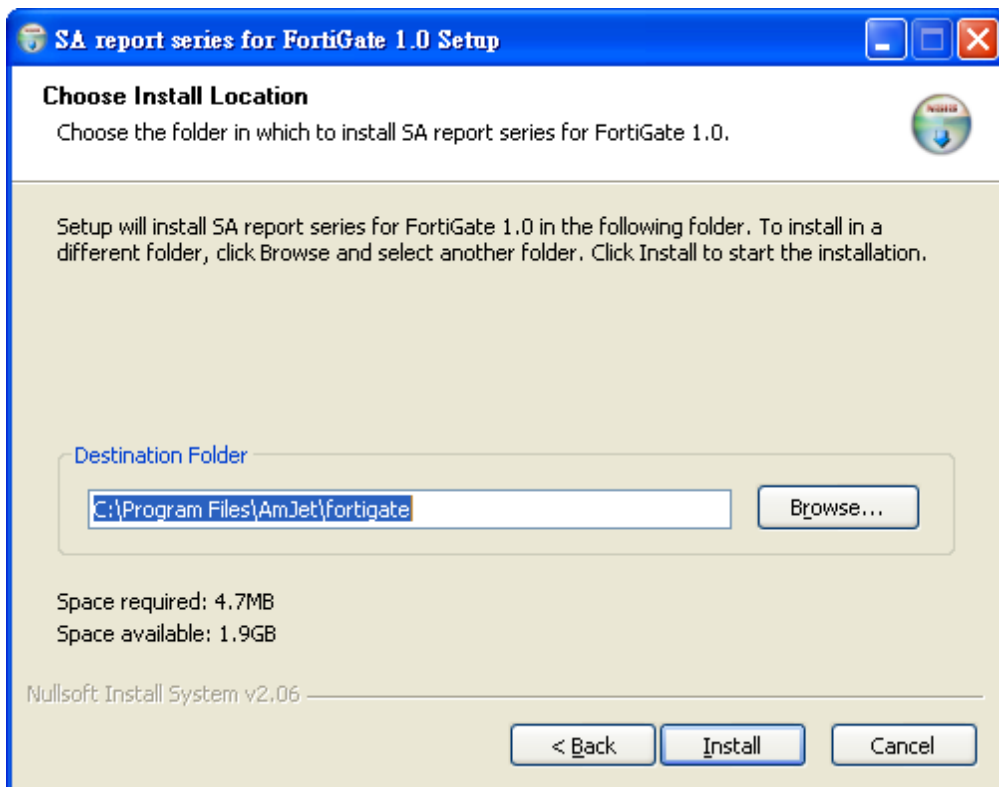
Step 2

The screen will display software information, please click on 'Next' to proceed.



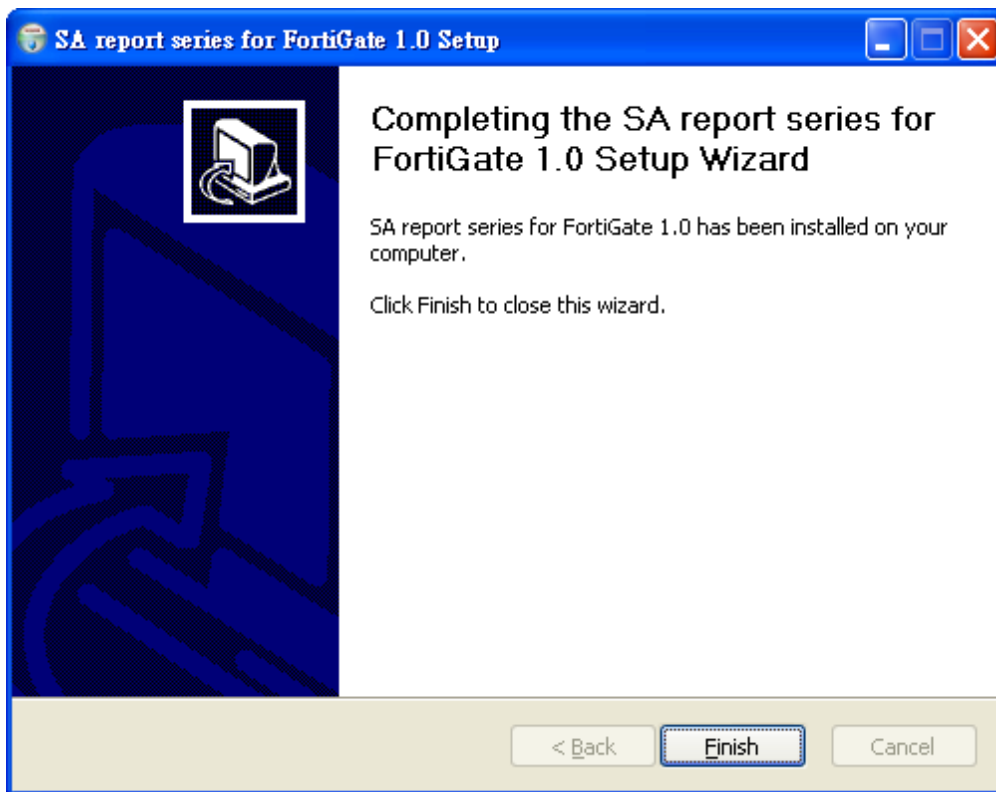
Step 3

Please select destination directory and click on 'Install' to start installation.



Step 4

The installation completed when you see the following screen.



3. FortiGate Configuration

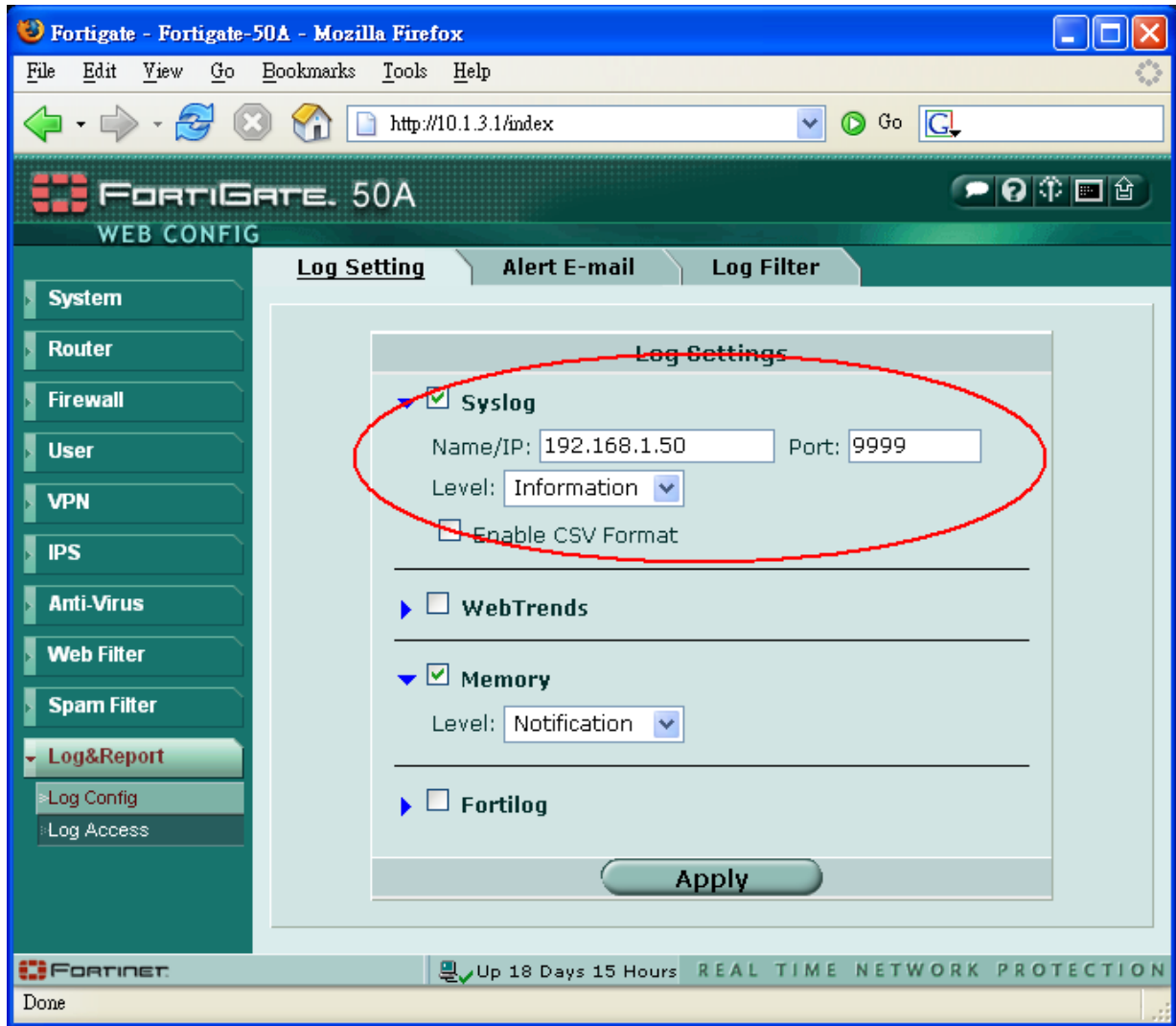
We suggest using udp port above 1024 to receive FortiGate syslog message, especially on unix platform. The default port to receive syslog message is 9999, here is the brief instruction to configure your FortiGate.

Step 1

Logon to FortiGate web interface as administrator.

Step 2

From left menu, click **Log & Report** >>> **Log Config**. Select syslog and supply necessary information as the picture demonstrated below.

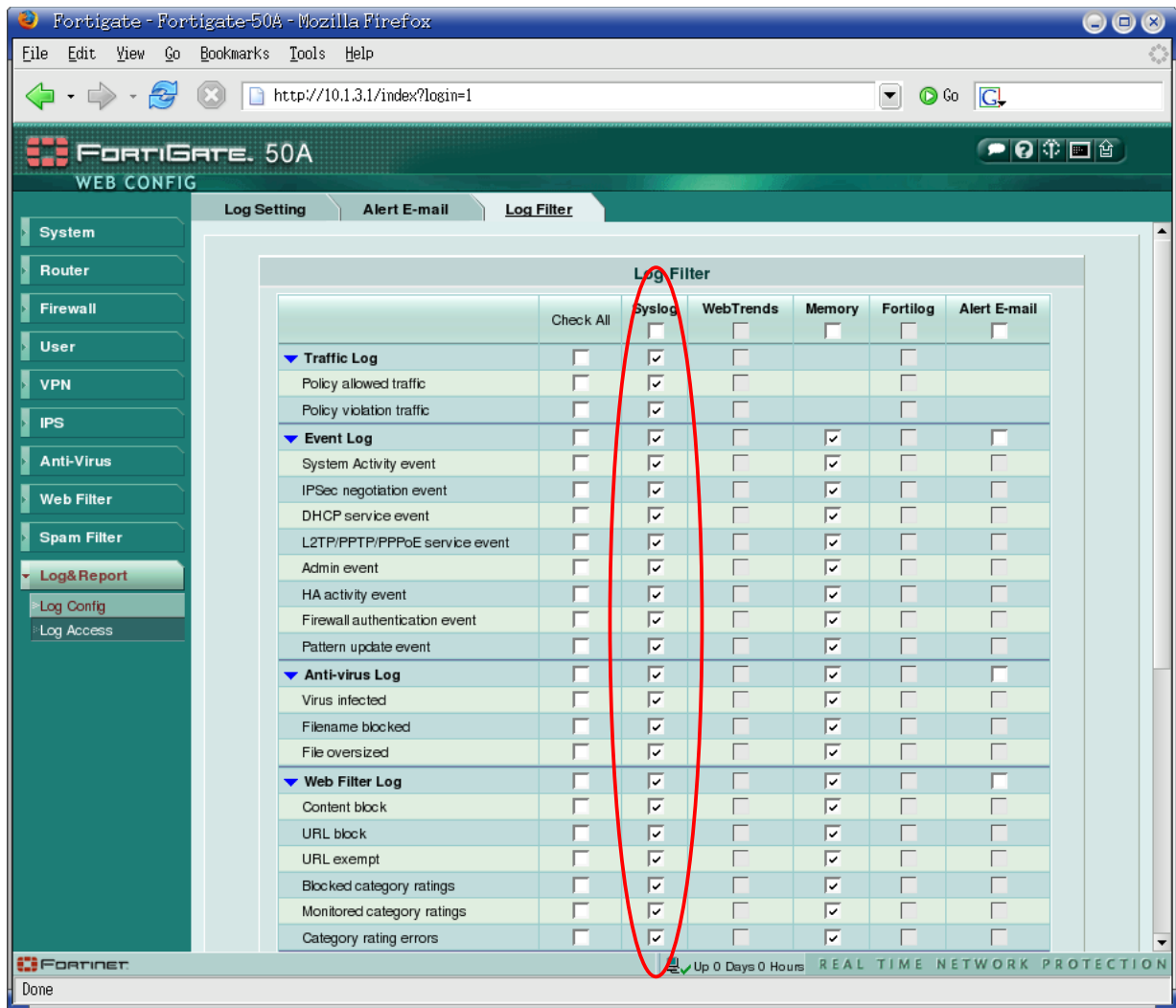


Note 1. Please select **Information** in Level pulldown to receive most complete events.

Note 2. CSV log not supported, please don't select **Enable CSV Format** checkbox.

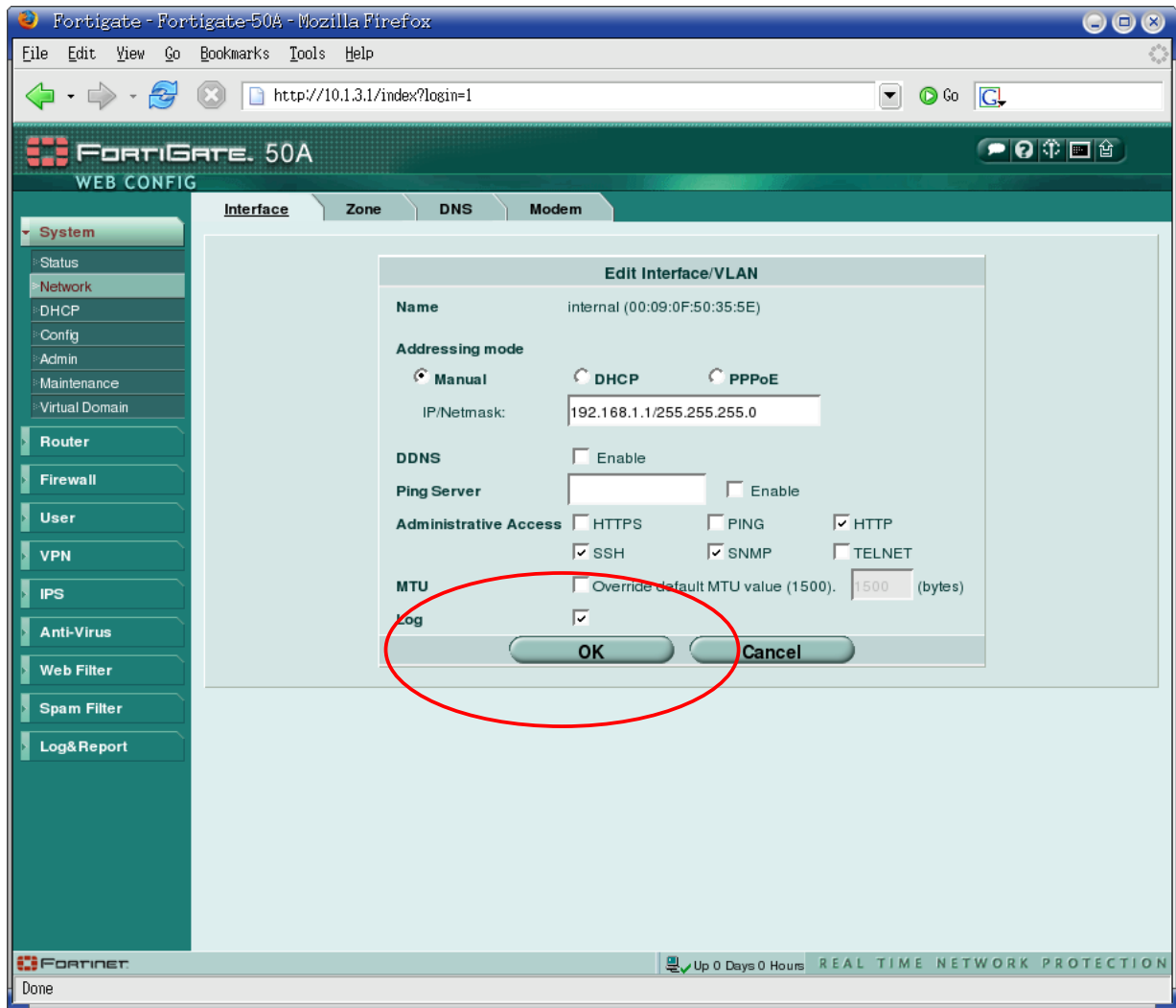
Step 3

From left menu, click **Log & Report >>> Log Filters**. Choose syslog items you want to receive as the picture demonstrated below.



Step 4

You can decide to log events or not while defining firewall policy. If you also want to log events happened on FortiGate network interface, please click on Log checkbox in interface tab.



Troubleshooting

1. application won't start

- I. Is your license still valid?
Please double click on 'user.cer' file under installation directory and check if already expired. You can contact our customer support to get a valid demo license.
- II. Wrong preference setting?
Please delete 'preference.xml' file under installation directory and start application again. Invalid preference setting might be the problem.

2. Why I can't use some functions listed in your product comparison chart

There are 2 possible reasons:

- I. Report delivery through email need JavaMail software, PostgreSQL and MySQL integration need JDBC software. Those softwares are not bundled in our package due to license issue. Our application will disable related function and preference setting if necessary files not installed. Please refer to Appendix in User's Guide, download and install above software. After restart application, related function and preference setting will be enabled automatically.
- II. Since this software first released, we received a lot of suggestions and feedbacks from our partners or customers. We will improve existing functions or add new functions to new release according to those precious opinions. To find out latest release, please visit the following url.

<http://isolution.dyndns.biz/cht/security/software.html>

1.1 build 050811 means current version number is 1.1 and newest update released at Aug 11, 2005. If you press 'About' button in toolbar, you will see a similar version string. If the version you are running is earlier than latest release, some new functions might be added after the time you download. Please follow FAQ 4 to upgrade to latest version.

3. How can I get manuals for this software

We provide pdf format manuals.

- I. English and Traditional Chinese manuals are available under **manuals** directory of your installation path
- II. It is also available for download in our software product URL listed below:
English: <http://isolution.dyndns.biz/en/security/software.html>
Traditional Chinese: <http://isolution.dyndns.biz/cht/security/software.html>

4. How can I use your unix installer

Simply use command '<JDK or JRE path>/bin/java -jar fortigate_installer1.1.jar' to start installation process. There are 2 notice here:

- I. Unix installer do not create application shortcuts
- II. Please check ram256.sh or ram512.sh if JRE definition matches you Java installation

5. Unable to connect to web report interface

- I. Check your license type
Web report interface only available if you have enterprise license installed.
- II. Make sure your preference saved
If you didn't specify web access password in preference, web access will not be allowed.

6. How should I upgrade to latest release

- I. Backup event database
If you are using HSQL database engine, please backup all files under directory <install path>/db before upgrade. You can skip this step if you do not need old data.
- II. Backup your preference
Please backup <install path>/preference.xml before upgrade if you want to keep your current preference setting.
- III. Uninstall current version
Please follow uninstall procedure according to your operating system.
- IV. Install new version
Please follow the procedures described in our installation guide.
- V. Restore event database
Please copy all files you backup in step 1 to <install path>/db and overwrite existing files.
- VI. Restore your preference
Please copy preference.xml file you just backup in step 2 to <install path> and overwrite existing file.

7. I see intrusion and virus events in generated report, can I get more information

released after 1.1 b050912

For IDP events, right click on data row in **attack signature analysis** report. A browser will popup and redirect you to fortinet's knowledge center for more detailed information. For virus events, also right click on data row in **virus attack analysis** report and get a browser to display fortinet's virus database.

released before 1.1 b050912

For IDP events, you can click on ID column in **attack signature analysis** report. A browser will popup and redirect you to fortinet's knowledge base for more detailed information. For virus events, you can click on virus column in **virus attack analysis** report and get a browser to display fortinet's virus database.

8. Why I see nothing in webfilter reports

- I. You must have webfilter rules, fortigate will send matched events to syslog facility. So, no violated event will be sent if no defined rule.
 - II. If you subscribe and enable FortiGuard – Web Filtering service, fortigate will try to identify visited URL and notify syslog facility. So no surfing event will be sent while FortiGuard – Web Filtering service disabled.
- ** firmware 2.80 build 184 will send surfing events while FortiGuard – Web Filtering service disabled. You will see some warning about rating server. Later firmware seems depend on FortiGuard.

Contact

AmJet Digital Co, Ltd.

Phone: 886 2 89214377

Web: <http://isolution.dyndns.biz>

Support email: support@isolution.dyndns.biz

Skype: amjetd

MSN: support@isolution.dyndns.biz