

# Firewall Analyzer for DFL Firewalls Quick Start Guide



# Table of Contents

<b>03</b>	<b>Introduction</b>
<b>04</b>	<b>Installation</b>
04	Firewall Analyzer step by step installation
<b>09</b>	<b>Startup</b>
09	Syslog and SNMP setup on firewall side
12	Firewall Analyzer startup
<b>13</b>	<b>Configuration</b>
13	Add syslog server and check
15	Configure SNMP on Analyzer side
16	Configure intranet
17	Configure reporting plan
18	Configure DNS
19	View firewall status and schedules
<b>20</b>	<b>Report Browsing</b>
20	Types of reports
20	Time range of reports
20	Work hours allocation
21	Protocol category for reports
<b>23</b>	<b>Appendix</b>
23	Configure user authentication for Internet access
25	Retrieve the saved logs from database

## Introduction

The Firewall DFL series is a line of products that offers a variety of functions to satisfy customer demands. For security administrators and IT managers, network monitoring and analyzing are the keys to making networks operate more efficiently. To fulfill these needs, the DFL series provides a thorough status and logging report system; this system, however, has its constraints due to the memory size. Those limitations may cause inconvenience to security administrators or IT managers occasionally. To avoid this predicament and expand the abilities of network monitoring and analyzing, we have introduced ManageEngine® Firewall Analyzer to complement our DFL series.

ManageEngine® Firewall Analyzer is a web-based, agent-less, firewall log analysis and reporting software. The software application monitors, collects, analyzes, and archives logs from network perimeter security devices and generates reports. Two prominent features of the application are network monitoring and security reports.

ManageEngine® Firewall Analyzer consists of four parts – syslog server, log parsing engine, Web GUI, and MySQL database. The Syslog server collects logs from the firewall and passes them on to the log parsing engine for further data processing. The MySQL database sorts data, produces various reports, and archives logs. To provide users with an easy and friendly way to view reports and configure their system, Web GUI was developed to achieve this goal. ManageEngine® Firewall Analyzer joins all components together to help security administrators and IT managers manage bandwidth management, network security, monitor web site visits, audit traffic, and ensure appropriate usage of networks by employees.

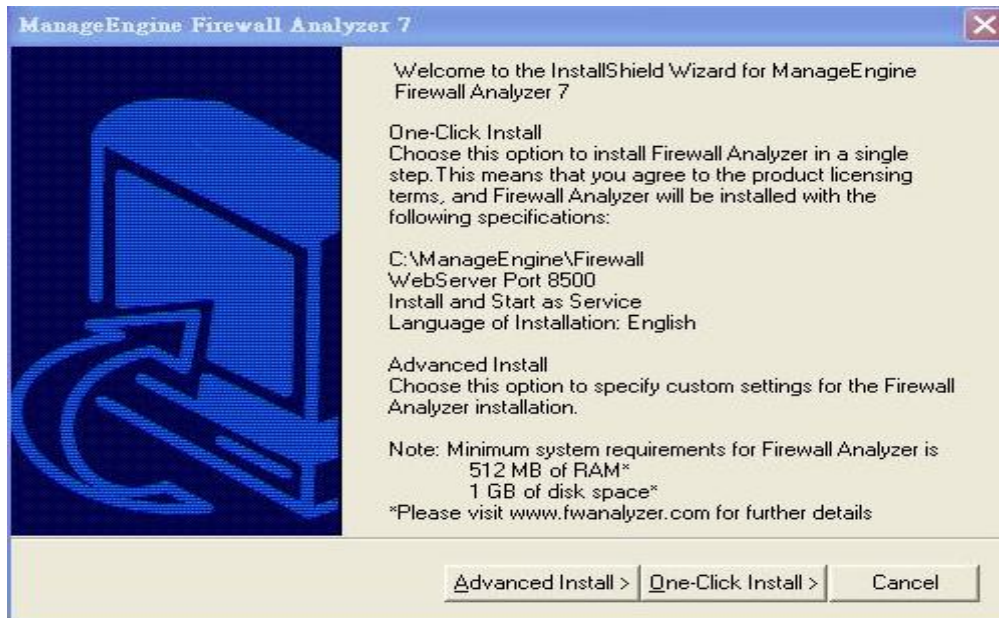
By combining a powerful DFL logging system with smart ManageEngine® Firewall Analyzer analysis, we deliver a complete network reporting and analysis solution for network administrators and IT managers.

# Installation

## Firewall Analyzer step by step installation

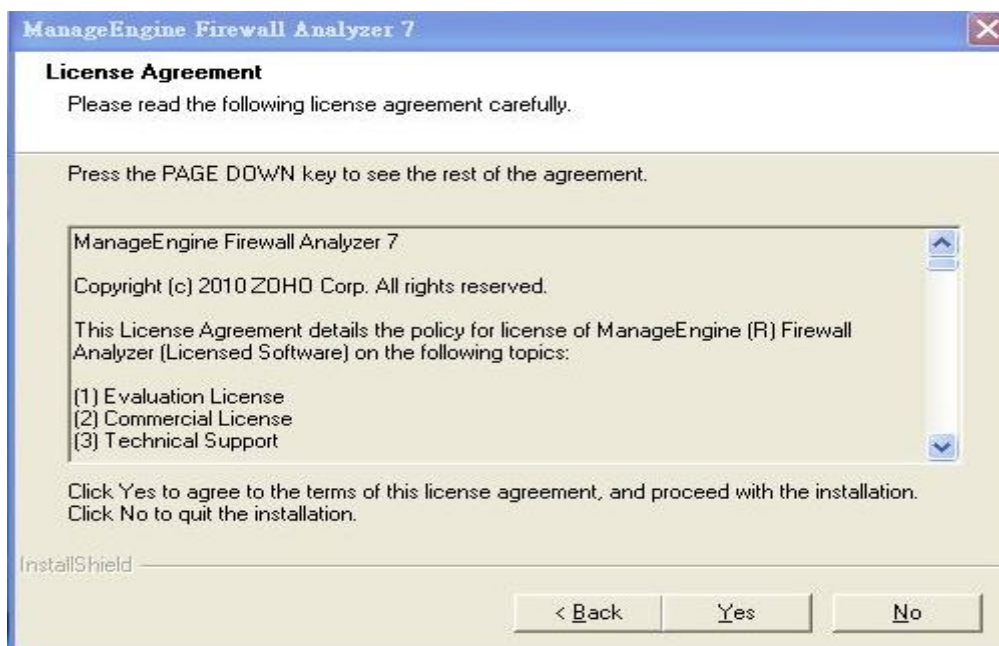
**Step 1:** Double-click ManageEngine\_FirewallAnalyzer\_7

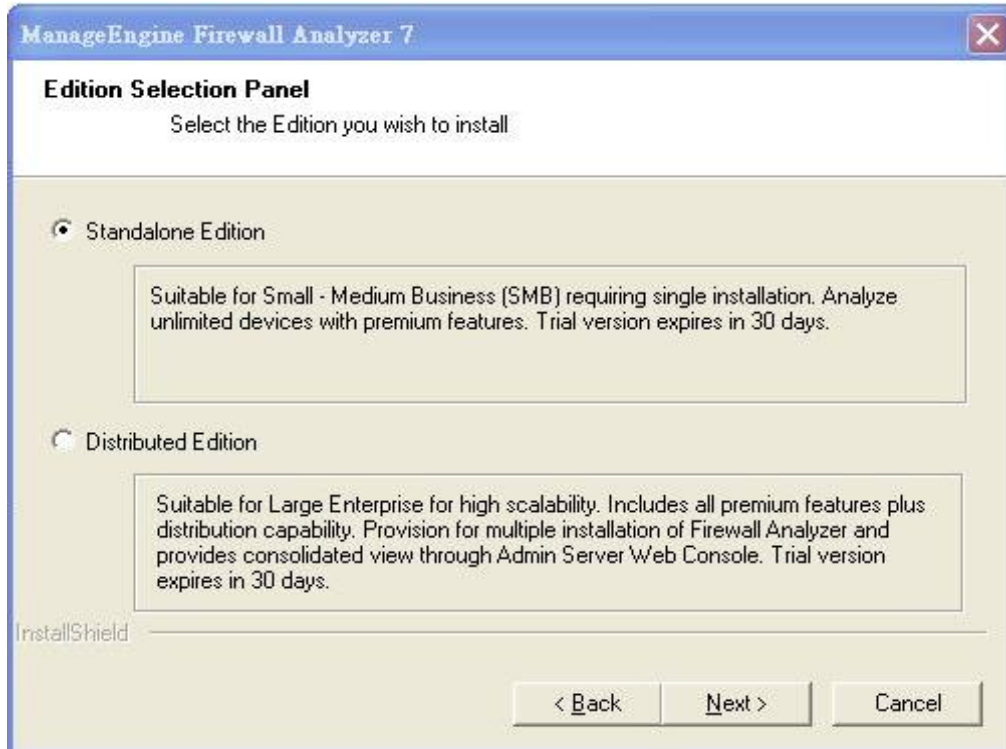
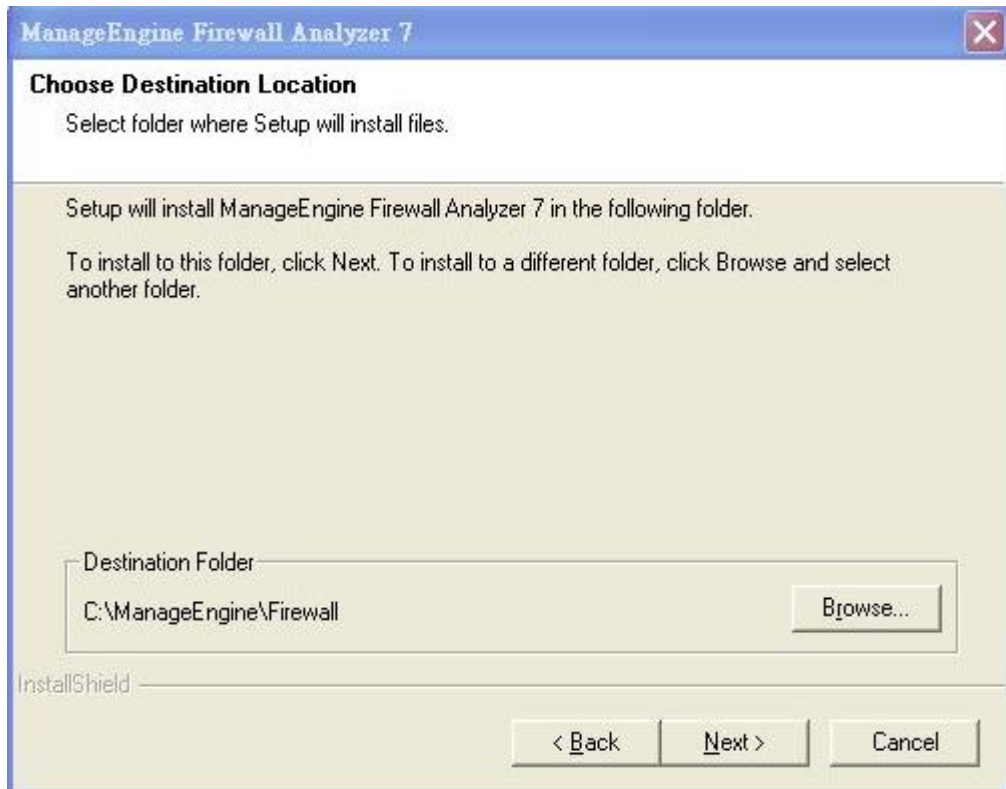
**Step 2:** Select Advanced Install



**Notice:** ManageFirewall Analyzer requires at least 512 MB of RAM and 1 GB of disk space.

**Step 3:** Click "Yes" to agree to the terms of this license agreement



**Step 4:** Select "Standalone Edition"**Step 5:** Choose Destination Location



**Step 6:** Select port and language

Please change default Web Port 8500 to unused ports e.g. 8505 to avoid port conflicts. If you don't change the web port, you may encounter initialization problems when Firewall Analyzer starts up.

**ManageEngine Firewall Analyzer 7**

**Port and Language Selection Panel**  
Select the Firewall Analyzer WebServer port and the language for installation.

Firewall Analyzer uses 8500 as the default web server port.  
If you want to use a different web server port, enter the port number here.

Web Port: 8505

Language of Installation: English

Web Protocol: http

Note :Please ensure that your web browser supports the chosen language

InstallShield: \_\_\_\_\_

< Back Next > Cancel

**Step 7:** Select "Install Firewall Analyzer as service"

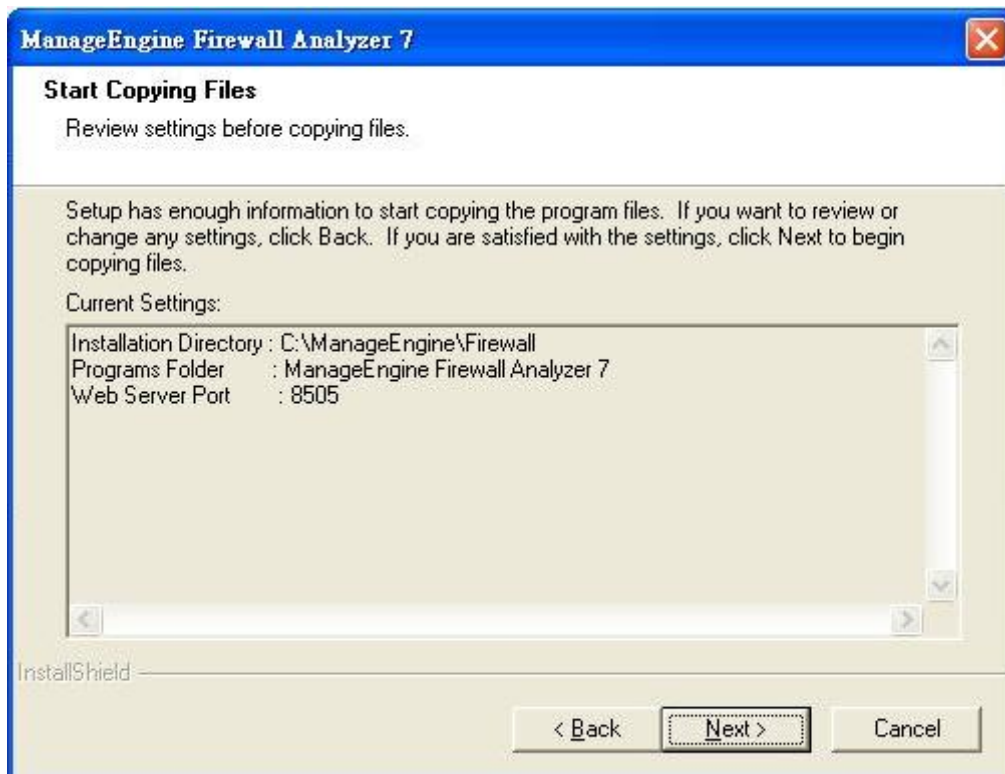
**ManageEngine Firewall Analyzer 7**

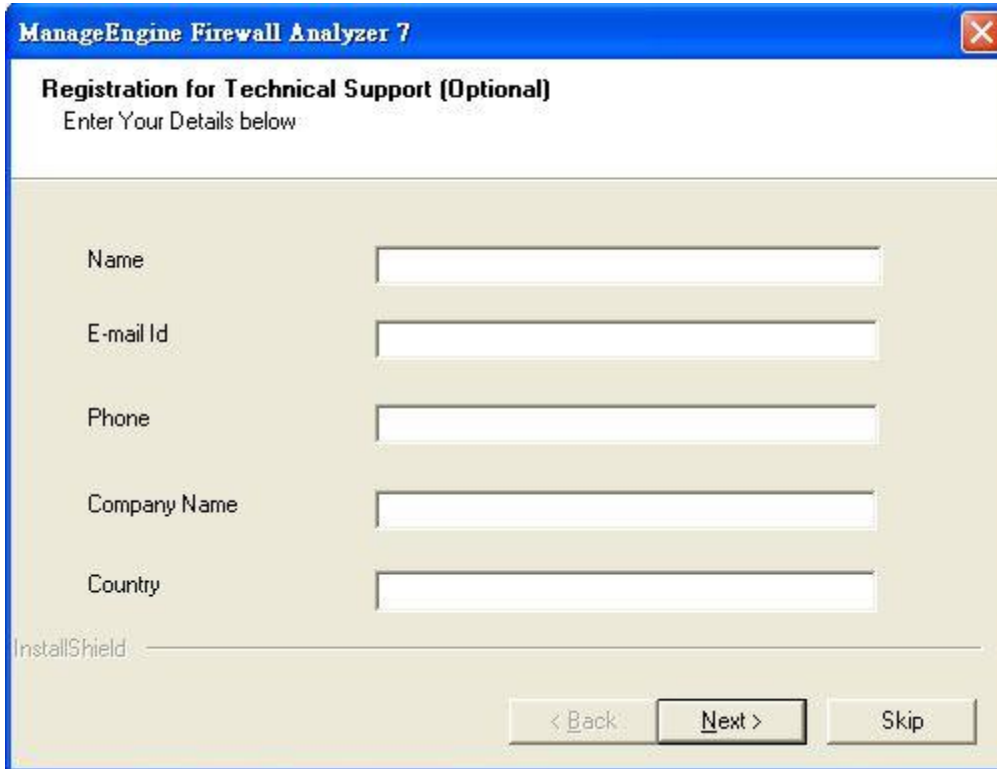
**Windows Service**  
This option will install ManageEngine Firewall Analyzer 7 as a Windows service

Install Firewall Analyzer as service

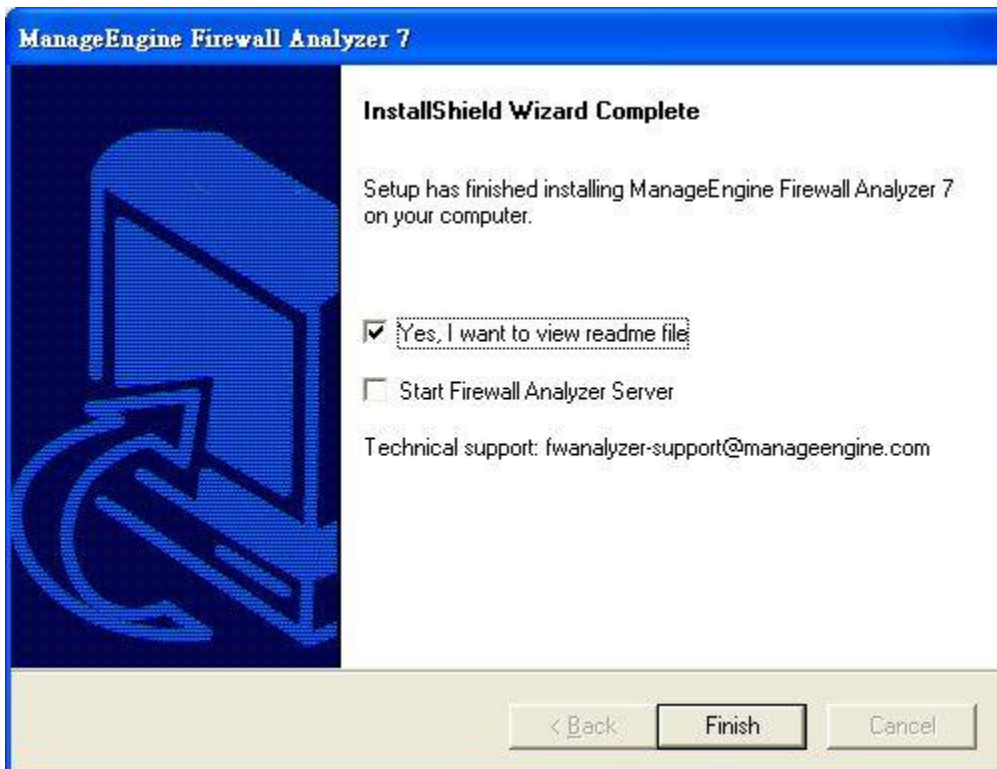
InstallShield: \_\_\_\_\_

< Back Next > Cancel

**Step 8:** Name the Program Folder**Step 9:** Click Next to start copying files

**Step 10:** Skip Registration process

The screenshot shows a dialog box titled "ManageEngine Firewall Analyzer 7" with a close button in the top right corner. The main heading is "Registration for Technical Support (Optional)" followed by the instruction "Enter Your Details below". There are five text input fields labeled "Name", "E-mail Id", "Phone", "Company Name", and "Country". Below these fields is a label "InstallShield:" followed by a horizontal line. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Skip".

**Step 11:** Finish Firewall Analyzer installation

The screenshot shows a dialog box titled "ManageEngine Firewall Analyzer 7" with a close button in the top right corner. The main heading is "InstallShield Wizard Complete". Below this, the text reads "Setup has finished installing ManageEngine Firewall Analyzer 7 on your computer." There are two checkboxes: the first is checked and labeled "Yes, I want to view readme file"; the second is unchecked and labeled "Start Firewall Analyzer Server". Below the checkboxes, the text "Technical support: fwanalyzer-support@manageengine.com" is displayed. At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".



# Startup

## Syslog and SNMP setup on firewall side

Before Firewall Analyzer can collect logs from the firewall, the firewall has to set up Syslog and SNMP parameters first. You can add a syslog receiver or SNMP event receiver by navigating to **System -> Log and Event Receivers -> Add** as shown in Figure 1.

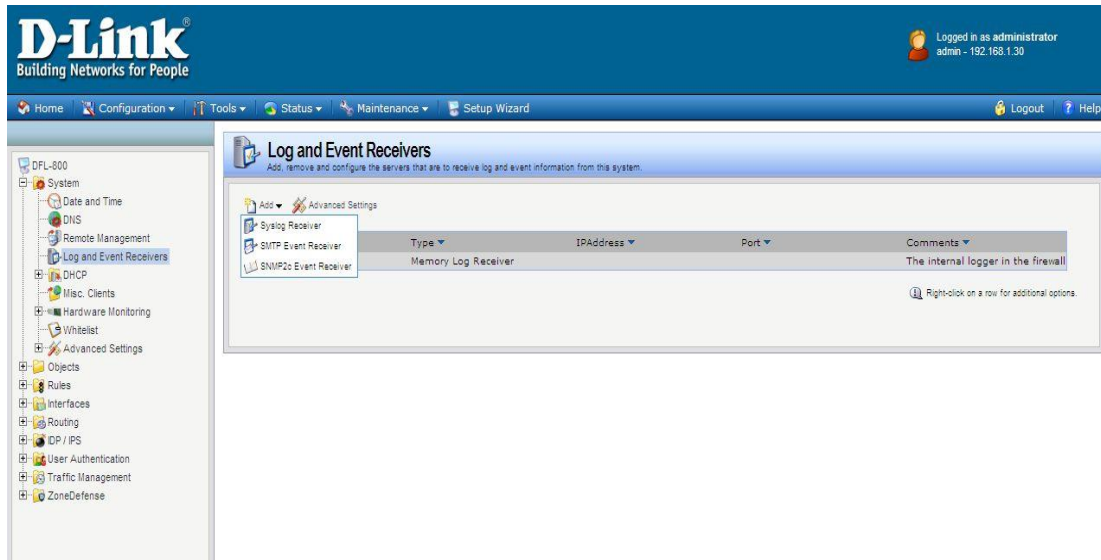


Figure 1: Log and Event Receivers

After you choose syslog receiver, more options are shown on the screen as shown in Figure 2.

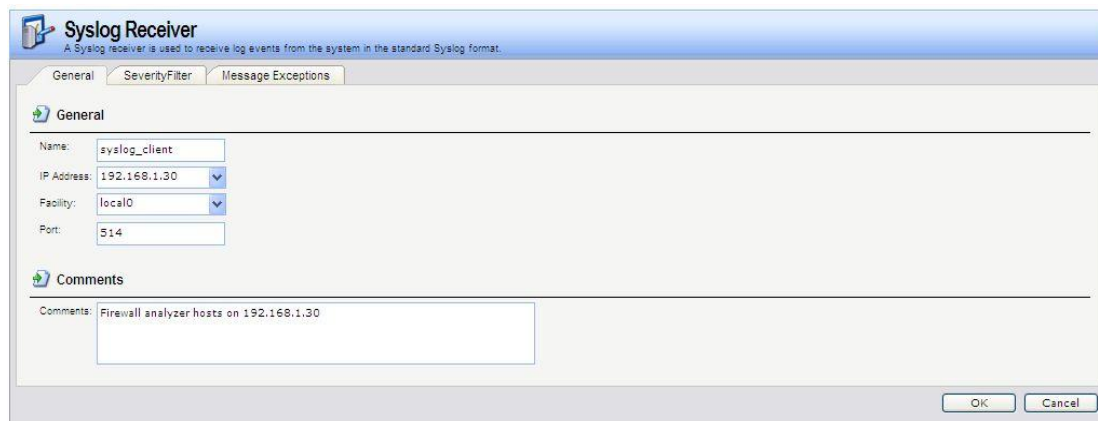


Figure 2: Syslog Receiver Configuration, General tab

### In General tab (Figure 2):

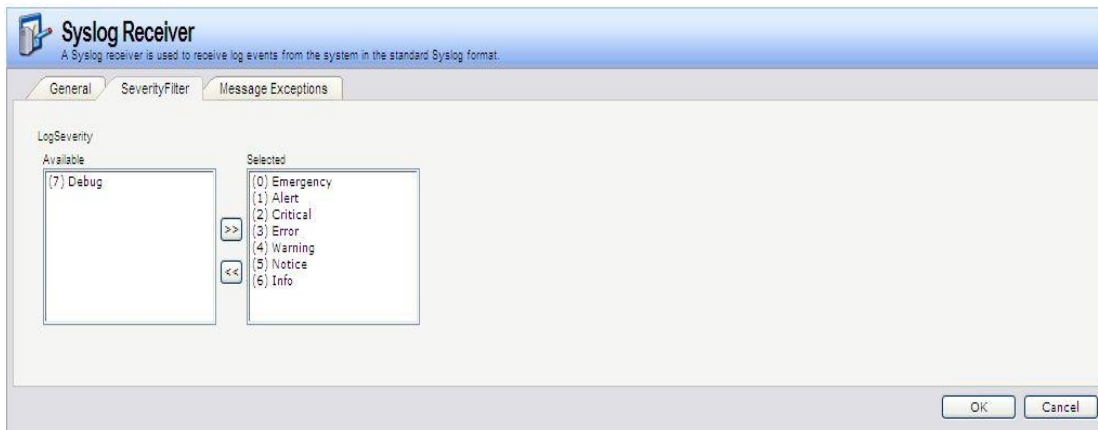
**Name:** syslog\_client

**IP Address:** 192.168.1.30 ——— In this example, firewall analyzer hosts on 192.168.1.30

**Facility:** local0 (default)

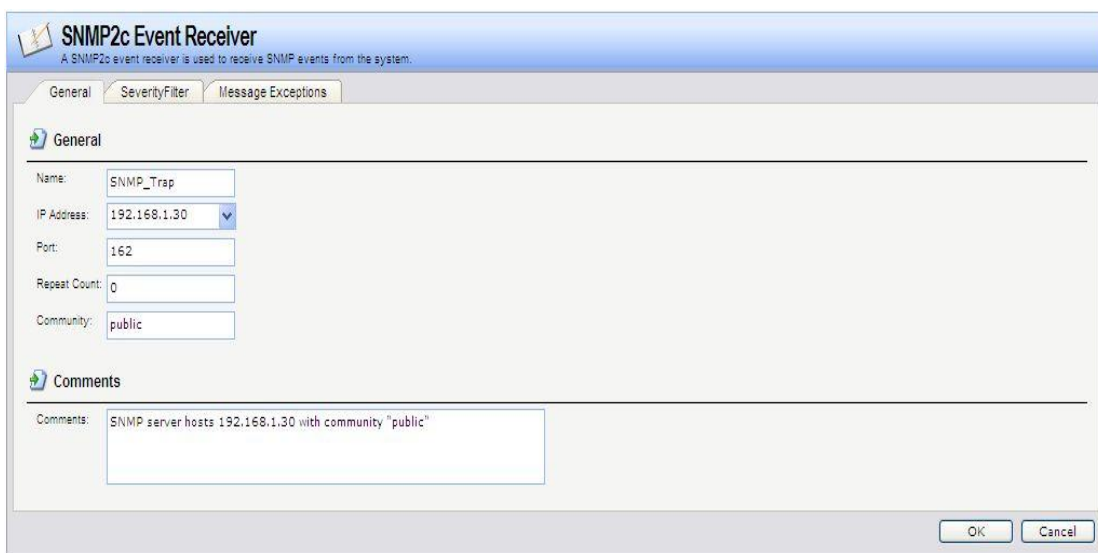
**Prot:** 514 (default)

The severity of each event is predefined by NetDefendOS. For each event, the order of severity from high to low is **Emergency -> Alert -> Critical -> Error -> Warning -> Notice -> Info -> Debug**. You can select the events which you want to send to the syslog receiver in SeverityFilter tab as shown in Figure 3.



**Figure 3:** Syslog Receiver Configuration, SeverityFilter tab

Click OK to finish the syslog receiver setting and navigate to **System -> Log and Event Receivers -> Add** again to add a SNMP2c Event receiver as shown in Figure 4.



**Figure 4:** SNMP2c Event Receiver configuration, General tab

**In General tab (Figure 4):**

**Name:** SNMP\_Trap

**IP Address:** 192.168.1.30 ——— In this example, firewall analyzer hosts on 192.168.1.30

**Port:** 162

**Repeat Count:** 0

**Community:** public

Like what we did during syslog receiver configuration, you can choose what events you want to send to SNMP2c Even receiver as shown in Figure 5.



Figure 5: SNMP2c Event Receiver configuration, Severity Filter tab

You can list all the receivers as shown in Figure 6.

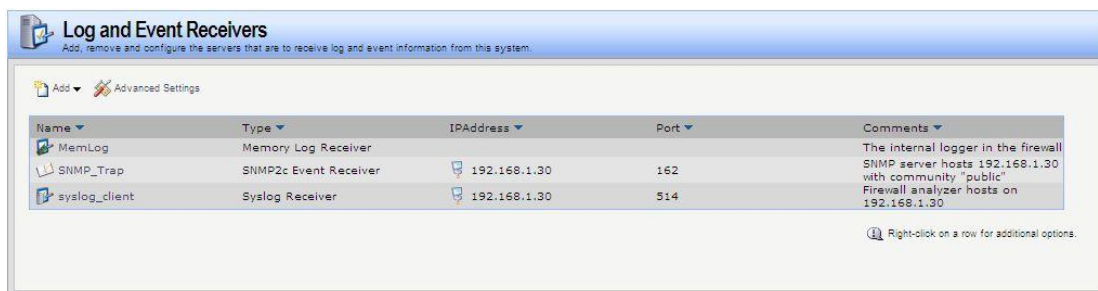


Figure 6: Log and Event Receivers, listing all receivers

A situation where too many log packets the firewall can send out per second may cause damage is if a log receiver to which the firewall sends is not active. The server will send back an *ICMP Unreachable* message, which may cause the firewall to send another log message, which in turn will result in another *ICMP Unreachable* message, and so on. By limiting the number of log messages the firewall sends every second, the administrator can avoid encountering such an undesirable situation where bandwidth is consumed unnecessarily; this value, however, should never be set too low, as this may result in important events not being logged.

To modify this value, please navigate to **System -> Log and Event Receivers -> Advanced Settings** as shown below in Figure 7.



Figure 7: Log and Event Receivers, Advanced Settings

## Firewall analyzer startup

There are two ways to start up Firewall Analyzer. Just click the shortcut icon on the desktop or navigate to **Start -> Programs -> ManageEngine Firewall Analyzer 7 -> Firewall Analyzer** to start up Firewall Analyzer. It may take a few minutes to initialize Firewall Analyzer, and then a web page will pop out to ask you to log into Firewall Analyzer as shown below in Figure 8. The default username and password for the first login is admin/admin.



**Figure 8:** Firewall Analyzer login page

If Firewall Analyzer fails to start up, the reason may result from port conflicts as described in Step 6 of installation. To solve this problem, you must release all the ports that are required by Firewall Analyzer but are being occupied by other network applications.

# Configuration

## Add syslog server and check

You will see the following message on the homepage as shown in Figure 9 after successfully logging in to Firewall Analyzer if you don't follow the instructions described in the **Startup-Syslog and SNMP setup on firewall side** chapter, or change the default syslog port 514 to another port (D-View also utilizes port 514 as the default syslog listening port and therefore you should change the Firewall Analyzer syslog default port to another port to avoid port conflicts).

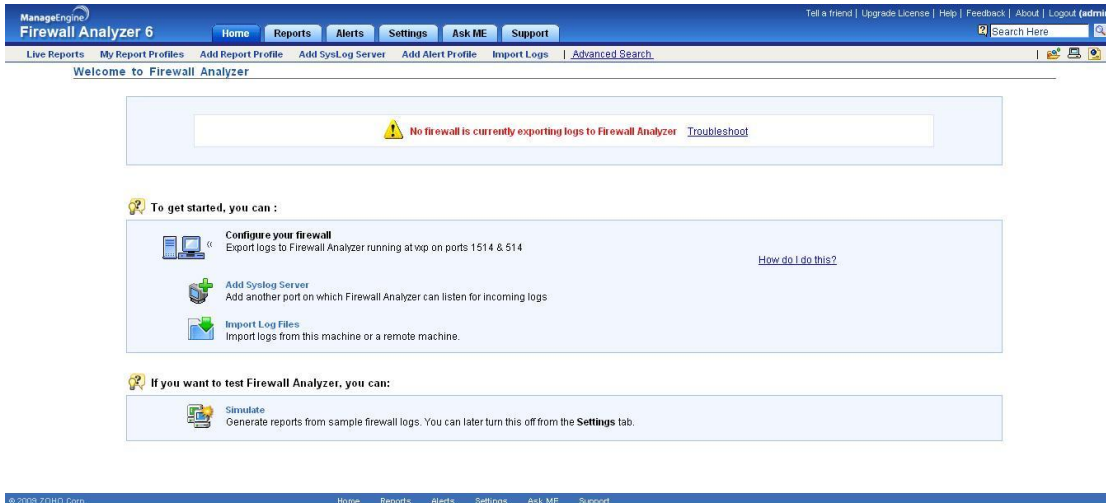


Figure 9: Firewall Analyzer first startup page

To receive logs from firewall and activate Firewall Analyzer, please follow the instructions described in the **Startup-Syslog and SNMP setup on firewall side** chapter or click "Add SysLog Server" in the sub-bar or in the middle of Figure 9 to set up the correct syslog server listening port as shown in Figure 10.

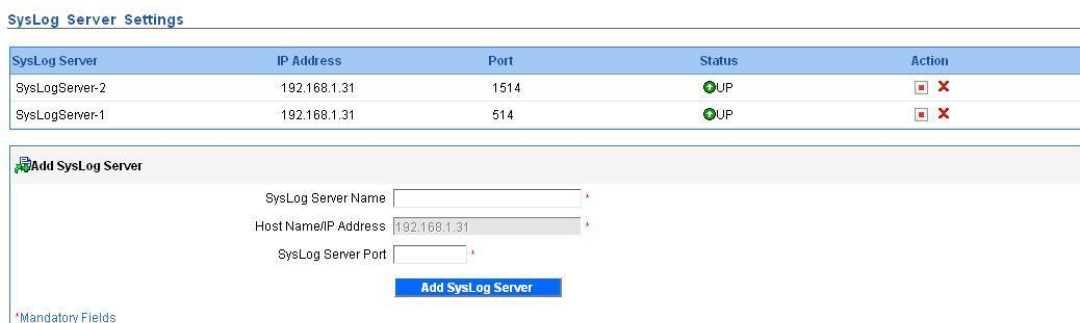


Figure 10: Syslog Server Settings

After you input the right syslog settings, Firewall Analyzer starts to synchronize with and receive logs from servers as shown in Figure 11. Firewall Analyzer will begin to generate the first reports after receiving 5,000 logs from the firewall. This means that you will see "No Data available" in all the charts of all reports until Firewall Analyzer receives the 5,000<sup>th</sup> log. When the first reports appear depends on the generating rate of logs (Please refer to Figure 7: Log and Event Receivers, Advanced Settings).



## Welcome to Firewall Analyzer

**No firewall is currently exporting logs to Firewall Analyzer** [Troubleshoot](#)

**To get started, you can :**

- Configure your firewall**  
Export logs to Firewall Analyzer running at [Firewall Analyzer](#) [Firewall](#)  
*Started receiving data. Reports will be generated in few seconds ...*
- Add Syslog Server**  
Add another port on which Firewall Analyzer
- Import Log Files**  
Import logs from this machine or a remote machine.

[How do I do this?](#)

**If you want to test Firewall Analyzer, you can:**

- Simulate**  
Generate reports from sample firewall logs. You can later turn this off from the **Settings** tab.

Figure 11: Started receiving logs from firewall

If Firewall Analyzer successfully synchronizes with the firewall, you will find the IP address of the firewall in the home page as shown in Figure 12.

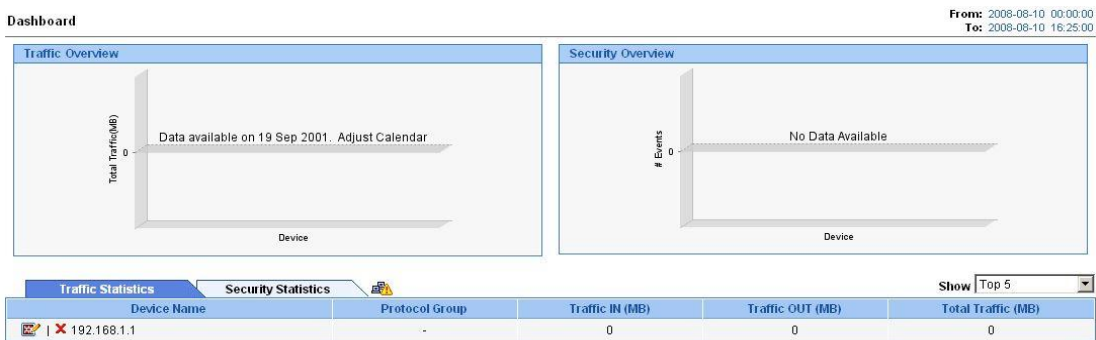



Figure 12: A synchronized firewall is shown on the home page

You can click the  icon to set the Display Name, Downlink Speed, and Uplink Speed of the firewall as shown in Figure 13.

ManageEngine Firewall Analyzer - Microsoft Internet ...

**Edit Firewall Property**

Firewall Name	192.168.1.1
Firewall IP	192.168.1.1
Display Name	DFL-860
Vendor Type	Clavister Firewall
Down link Speed (in Kbps)	1024.0
Up Link Speed (in Kbps)	1024.0

\* Link speed is used to calculate the percentage utilization in Live Reports.

**Update** **Close**

Figure 13: Firewall settings

## Configure SNMP on FireWall Analyzer side

The live reports and traffic of each interface, e.g. WAN, LAN, are gathered through SNMP traps sent by the firewall. Before Firewall Analyzer can collect live data, you must set up the SNMP parameters described in the **Startup-Syslog and SNMP setup on firewall side** chapter and also configure FireWall Analyzer as follows:

1. Click Interface/Zone Reports at the sub-bar
2. Click "Set Global SNMP Parameters"

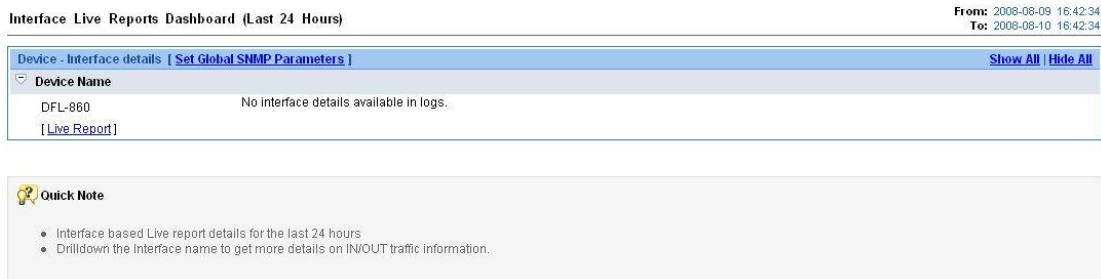


Figure 14: Interface Live Reports Dashboard

1. Input the "SNMP Community" and "SNMP port" values as shown in Figure 15.

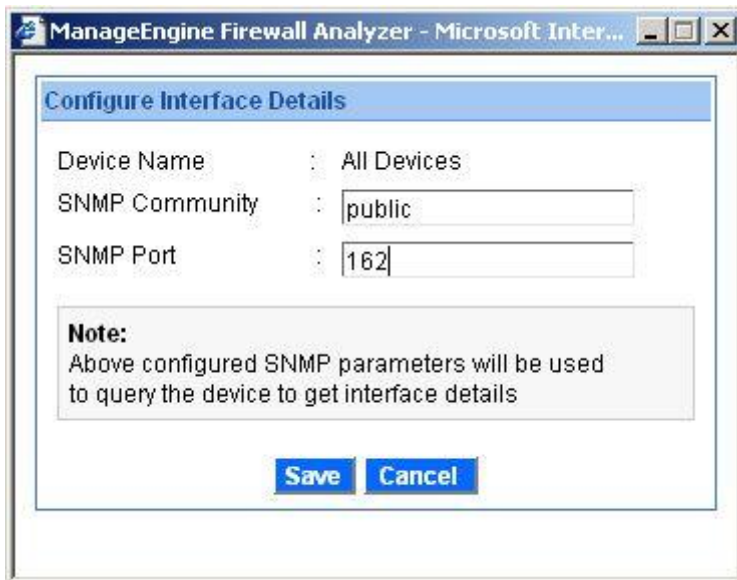


Figure 15: Configure Interface Details

**Note:** Live reports may not work due to SNMP OIDs inconsistency. We are working on it.

## Configure intranet

For network analysis purposes, traffic engineers may want to differentiate internal traffic from external traffic. We can achieve this by using Intranet Settings. Please navigate to **Settings -> Admin Settings -> Intranet Settings** as shown in Figure 16.

The screenshot shows the Firewall Analyzer 6 web interface. The top navigation bar includes 'Home', 'Reports', 'Alerts', 'Settings', 'Ask ME', and 'Support'. The left sidebar has a 'Settings' menu with sub-items like 'SysLog Server Settings', 'Checkpoint Firewall Settings', 'Alert Profiles', 'Imported Log Files', 'Device Details', 'Archived Files', 'Schedule Listing', 'Working Hour', 'Customize Report', 'Configure DNS', 'Device Rule', 'Rebranding FWA WebClient', 'Protocol Groups', 'Intranet Settings', 'User Management', and 'Mail Server Settings'. The 'Intranet Settings' option is highlighted. The main content area is divided into 'System Settings' and 'Admin Settings'. 'System Settings' includes options for SysLog Server, Checkpoint Firewall, Alert Profiles, Configure DNS, Imported Log Files, Device Details, Archived Files, and Device Rule. 'Admin Settings' includes Protocol Groups, Intranet Settings, User Management, Mail Server Settings, Firewall Availability Alert, Server Diagnostics, Database Console, License Management, and SMS Settings.

Figure 16: Settings

In Intranet Settings, click **Action -> Change** as shown in Figure 17.

**Intranet Settings**

[Configure all devices](#)

Device Name	Intranet Settings	Action
DFL-860	No Intranets configured.	Change

Figure 17: Intranet Settings

Please select your firewall and IP Network, enter the Network and Net Mask and then click Save Settings. In the example shown in Figure 18, the firewall DFL-860 (192.168.1.1) and syslog receiver (192.168.1.30) are located in the internal subnet 192.168.1.0/24. If your firewall has more internal subnets, you must click "More" to add them.

**Intranet Settings**

No Intra-Network is configured.

**Specify Network, IP Range, or IP Address**

DFL-860

IP Network

Network: 192.168.1.0      Net Mask: 255.255.255.0

[More](#) [Fewer](#)

[Save Settings](#) [Cancel](#)

**Help**

- IMPORTANT : Try to give minimum ranges/networks as much as possible.**  
For Example : if you have three private IP Network (say 10.8.0.0, 10.9.0.0, and 10.10.0.0, each with NetMask: 255.255.0.0, then instead of adding them separately, we would recommend you to give the entire private IP network : 10.0.0.0 with NetMask 255.0.0.0, as this would improve the performance. The same is recommended for IP Range too, where you can mention Start IP: 10.0.0.0 End IP: 10.255.255.255. This is applicable to Class B & Class C networks too

Figure 18: Intranet Settings Details

## Configure reporting plan

Firewall Analyzer can automatically generate a summary report for any time period that you designate, e.g. one day, one week or one month. You can activate this service by following the steps below.

**Step 1:** Click Add Report Profile in the sub-function bar as shown in Figure 19.



Figure 19: Sub-function bar

**Step 2:** Give the report a profile name, select your desired firewall, and then click Next as shown in Figure 20.

Figure 20: Create report profile – select devices and filters

**Step 3:** Choose a report type, the file type the summary report will be saved as, schedule when the summary report will be generated, and then click Save as shown in Figure 21.

**Create Report Profile** [View Report Profiles](#)

1 Select Devices and Filters      2 Select Report Type and Schedule

### 2. Select Report Type and Schedule

**Select Report Type**

**Available Reports**

- Select All Reports
- Inbound & Outbound Traffic
- Intranet Reports
- Firewall Live Reports
- Firewall Rules Reports
- Proxy Usage (Proxy only)
- Security Reports

[Add](#)

**Save generated report as :**

Customize images for PDF Reports

---

**Schedule & Email Options**

Send report as:  PDF  CSV

Hourly     
 Daily     
 Weekly     
 Monthly     
 Only once

Generate report daily at the below specified time

Generate report on: 09 Hrs 00 Min

Generate report for: Last 24 Hours

Run on Week Days

Email the report

[Preview](#) [Save](#) [Cancel](#)

Figure 21: Create report profile – select report type and schedule

**Step 4:** Click My Report Profiles at the sub-function bar to check reports status as shown in Figure 22 and Figure 23.



Figure 22: Sub-function bar

**All Reports**  Show All

[My Report Profiles](#) | [Add Report Profile](#) | [Export Report Profiles](#) | [Import Report Profiles](#)

Report Profile Name	Created on	Last Generated Reports	Action	Scheduler Assigned
<a href="#">report profile 1</a>	2008-08-13 11:20:48	-	<span style="color: red;">✘</span> <a href="#">Create One More</a>	

[Reports Across Devices](#)

[Firewall Reports](#)

Figure 23: My Report Profiles

## Configure DNS

By default, all source and destination computers are shown in IP address format. You can change this setting to manual or automatic translation if you prefer. By navigating to **Settings -> System Settings -> Configure DNS**, you can choose the options you want as shown in Figure 24 and Figure 25.

Figure 24: Settings




**Resolve DNS Configuration**

Do Reverse lookup automatically. I want to see DNS name everywhere instead of IPAddress.

Don't do Reverse lookup automatically. Let me get an option to do that in my reports.

No lookup at all. I want to see IPAddresses everywhere.

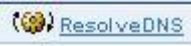
Maximum number of IP,DNS mappings in memory

 [Want to configure DNS entries manually? Click Here](#)

**Quick Note**

- Option 1  
Firewall Analyzer will do reverse lookup automatically for all IPAddresses and that will be used in all reports. If you see any IPAddresses, you can try clicking the 'ResolveDNS' link OnDemand and confirm with 'nslookup' from FWA machine.
- Option 2  
Firewall Analyzer won't do automatic reverse lookup. It will do reverse lookup for the ip's shown in the report page when you click the 'ResolveDNS' link.
- Option 3  
Firewall Analyzer will show only IPAddresses in all the reports. "Resolve DNS" link in report pages will not be shown.




**Figure 25:** Resolve DNS configuration

If you would like to manually resolve DNS, click the  icon at the top right side of any report.

## View firewall status and schedules

If you want to review all firewall and schedule executed status details, you can navigate to **Settings -> System Settings -> Device Details** as shown in Figure 26.

**Device Details****Supported Logs Received**

Device Name	Device Type	Last Update Time	Syslog Port	Status	Action	Manage Status
DFL-860	Firewall	Aug 10, 2008 18:33:49	Not Applicable	Not Applicable	 	

**Unsupported Logs Received**

Device Name	Syslog server	Syslog Port	Record Format	Notification	Action
No Data Available					

**Schedules Executed**

Report Profile	Schedule	Last Executed	Status
No Data Available			

**Figure 26:** Device Details

## Report Browsing

### Types of reports

There are many predefined reports and all of them can be categorized into real-time and non real-time reports. Only Live Reports belongs to real-time reports and others are non real-time reports. Real-time reports are gathered through SNMP traps, while non real-time reports are received from syslog clients. Whether real-time or non real-time reports, you have to correctly configure them before browsing them.

### Time range of reports

When browsing non real-time reports, e.g. traffic reports or protocol usage reports, you can change the time scale of all charts by selecting the day or time range you prefer as shown in Figure 27.

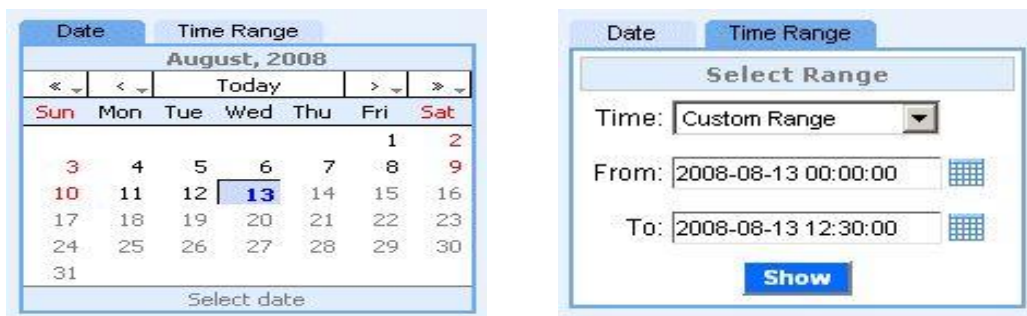


Figure 27: Date and Time Range

### Work hours allocation

In trend reports like traffic or protocol trend reports, there are charts for working and non-working hours. You can configure working hour details by navigating to **Settings -> System Settings -> Working Hour** as shown in Figure 28.

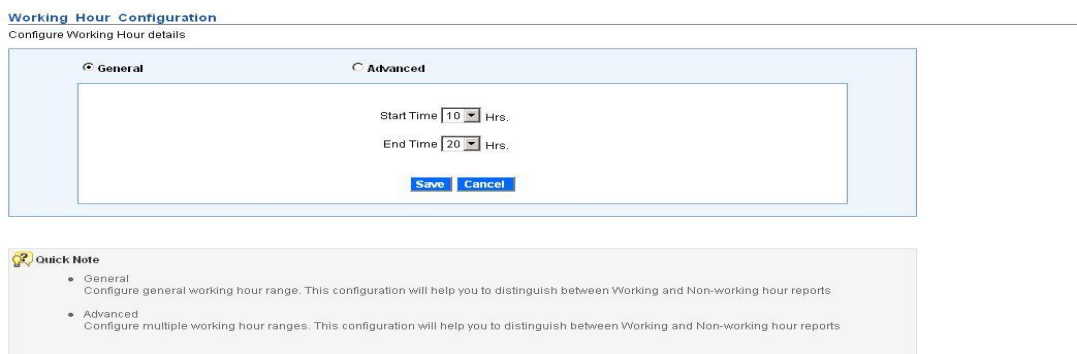
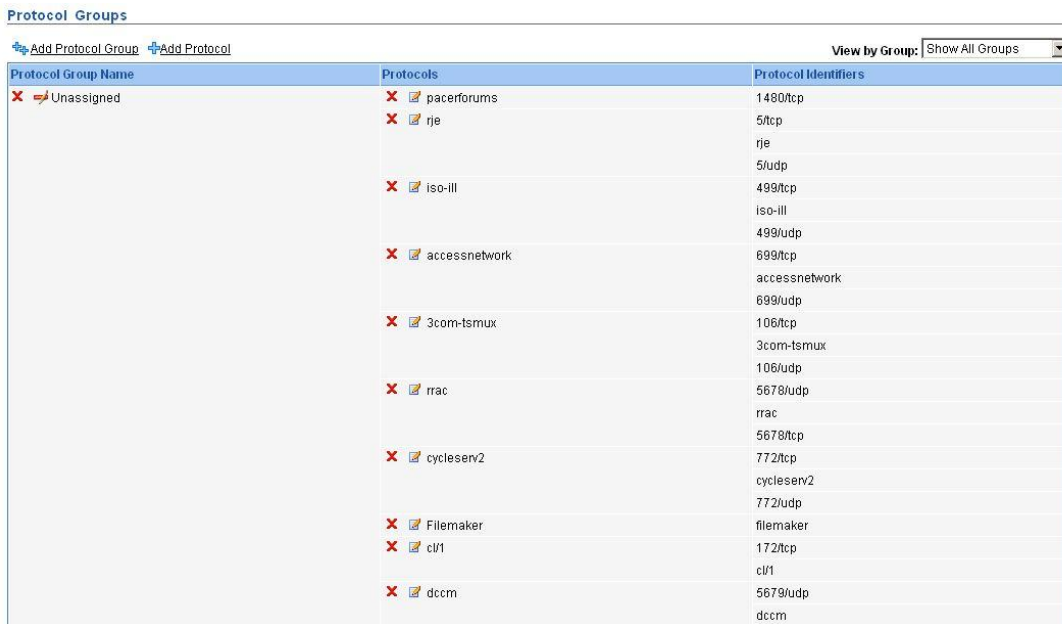


Figure 28: Working Hour Configuration

## Protocol category for reports

Firewall Analyzer distinguishes various protocols by TCP/UDP port numbers or tag names in logs. There are many predefined protocols in Firewall Analyzer. You can check all of them by navigating to **Settings** -> **Admin Settings** -> **Protocol Groups** as shown in Figure 29.



Protocol Group Name	Protocols	Protocol Identifiers
Unassigned	pacerforums	1480/tcp
	rje	5/tcp
		rje
		5/udp
	iso-iii	499/tcp
		iso-iii
		499/udp
	accessnetwork	699/tcp
		accessnetwork
		699/udp
	3com-tsmux	106/tcp
		3com-tsmux
		106/udp
	rrac	5678/udp
	rrac	
	5678/tcp	
cycleserv2	772/tcp	
	cycleserv2	
	772/udp	
Filemaker	filemaker	
clf1	172/tcp	
	clf1	
dccm	5679/udp	
	dccm	

Figure 29: Protocol Groups

You can add a new protocol by following these steps.

**Step1:** Click Add Protocol to open the Add New Protocol pop-out box.

**Step2:** Enter the group name and choose the proper protocol group as shown in Figure 30.

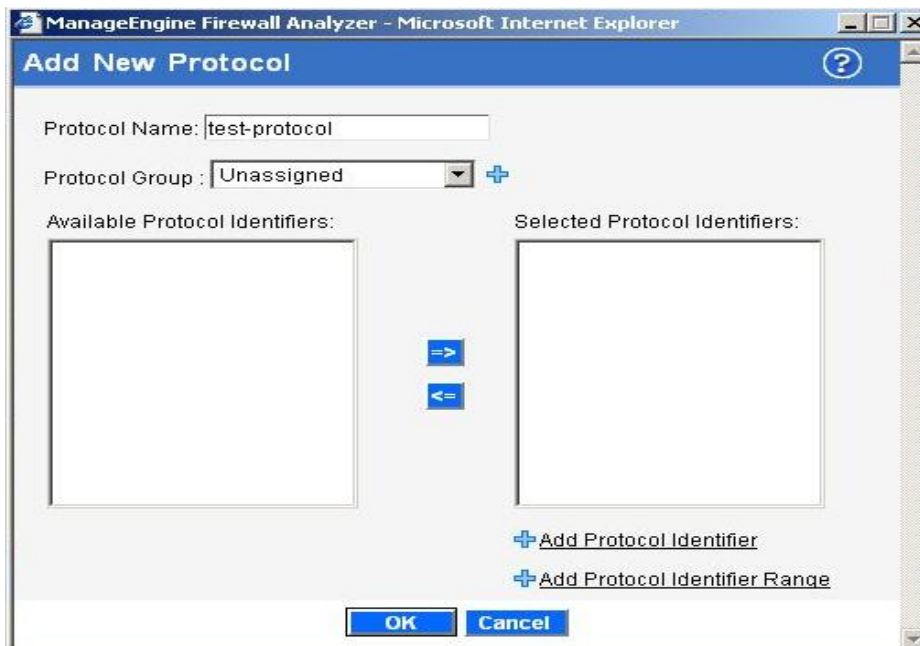


Figure 30: Add New Protocol

**Step3:** Click Add Protocol Identifier and input the identifier in the pop-out box. The identifier 1863/TCP means TCP port 1863 and 1863/UDP is for UDP port 1863 as shown in Figure 31. You can also input tag names directly.

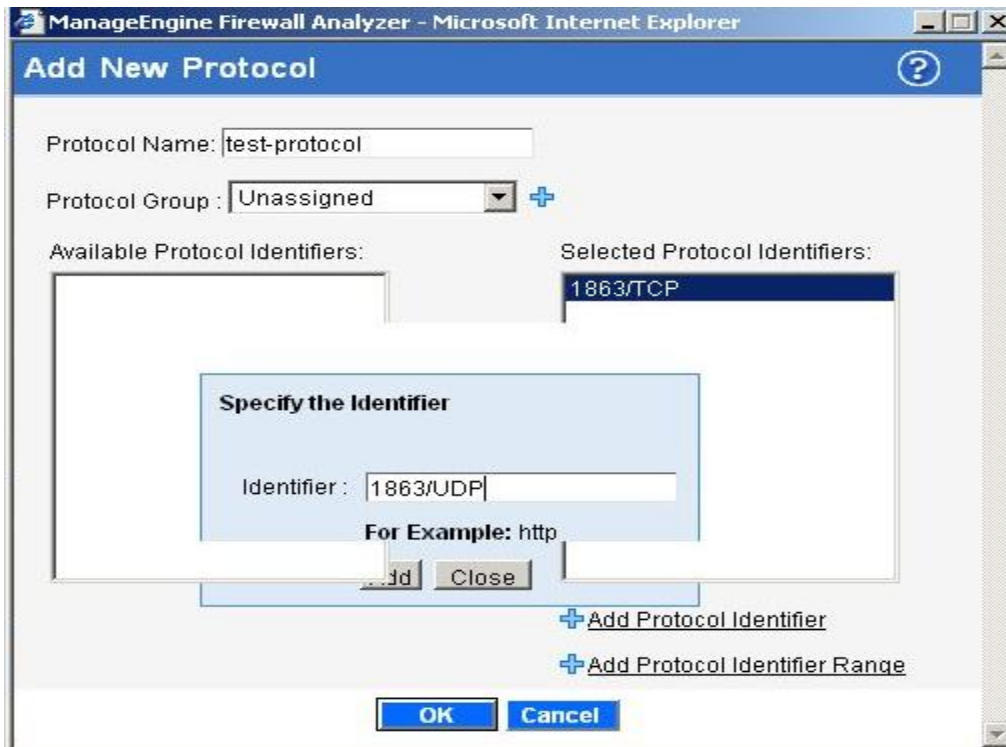



Figure 31: Specify Protocol Identifier

**Step 4:** Review all selected protocol identifiers as shown in Figure 32. If you want to remove a protocol identifier, just click on it and then click the  icon to move it to the left side – Available Protocol Identifiers.

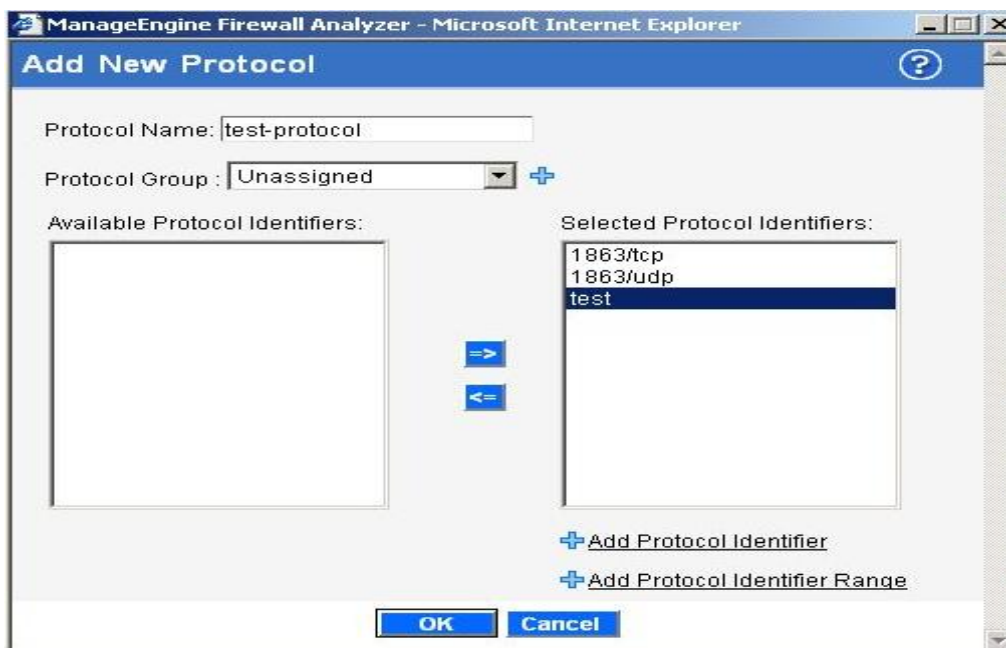


Figure 32: Add New Protocol



## Appendix

### Configure user authentication for Internet access

Here we only summarize the key steps of authentication configuration. Please refer to *Configure User Authentication for Internet Access* for more details.

#### 1. Create a new network object for authenticated users –

Refer to STEP 1 in *Configure User Authentication for Internet Access*

Navigate to **Object->Address Book->Interface Address** and add a new IP4 address.

Remember to add authenticated user names or groups in *User Authentication tab*.

The screenshot shows the 'lan-auth' configuration window with the 'User Authentication' tab selected. The 'General' section contains a text area for 'Comma-separated list of user names and groups' with the value 'webuser'. Below this is a checkbox for 'No defined credentials' which is unchecked. An information icon indicates that checking this box specifies that the network object requires user authentication but has no credentials defined.

#### 2. Change the port of Web console for latter Web access

Refer to STEP 3 in *Configure User Authentication for Internet Access*

Navigate to **System->Remote Management->Advanced Setting** and change

WebUI HTTP port to any unused port beyond 1024, e.g. 1080

WebUI HTTPS port to any unused port beyond 1024, e.g. 10444

The screenshot shows the 'Remote Management Settings' configuration window with the 'General' tab selected. The 'General' section contains several settings:

SSH Before Rules:	<input checked="" type="checkbox"/>	Enable SSH traffic to the security gateway regardless of configured IP Rules.
WebUI Before Rules:	<input checked="" type="checkbox"/>	Enable HTTP(S) traffic to the security gateway regardless of configured IP Rules.
WebUI Idle timeout:	<input type="text" value="900"/>	Number of seconds of inactivity until the HTTP(S) session is closed.
Local Console Timeout:	<input type="text" value="900"/>	Number of seconds of inactivity until the local console user is automatically logged out.
Validation Timeout:	<input type="text" value="30"/>	Specifies the amount of seconds to wait for the administrator to log in before reverting to the previous configuration.
WebUI HTTP port:	<input type="text" value="1080"/>	Specifies the HTTP port for the web user interface.
WebUI HTTPS port:	<input type="text" value="10444"/>	Specifies the HTTP(S) port for the web user interface.
HTTPS Certificate:	<input type="text" value="AdminCert"/>	Specifies which certificate to use for HTTPS traffic. Only RSA certificates are supported.

### 3. Add authenticated users in Local User Database

Refer to STEP 4 in *Configure User Authentication for Internet Access*

Navigate to **User Authentication -> Local User Database** and create the user authentication database for user name and password. Remember groups of a new user should be the same as the group marked in the *User Authentication* of the network object in Step 1.

**userA**  
User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, IPsec XAuth, Web Authentication, etc

General SSH Public Key

**General**

Name:

Password:

Confirm Password:

Groups:

**i** Comma separated list of groups  
Users that are members of the 'administrators' group are allowed to change the firewall configuration.  
Users that are members of the 'auditors' group are only allowed to view the firewall configuration.

### 4. Set User Authentication Rules

Refer to STEP 5 in *Configure User Authentication for Internet Access*

For reporting accuracy, it is recommended that you select "allow one login per username, disallow the rest" in the Restrictions tab when you create the user authentication rule.

**lan\_http\_auth**  
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how

General Log Settings Authentication Options Accounting Agent Options Restrictions

**General**

Name:

Authentication agent:

Authentication Source:

Interface:

Originator IP:  **i** For XAuth and PPP, this is the tunnel originator IP.

Terminator IP:

## 5. Set IP Rules

Refer to STEP 6 in *Configure User Authentication for Internet Access*

There are three HTTP services IP rules relative to the authentication process – one defines the internal connections to the firewall and the others regulate the connections to the external network (rules 4, 5 and 6, grouped within the blue border in the image below). Two additional rules are set to allow only authenticated traffic to pass through the firewall (rules 3 and 7, grouped within the red border in the image below). lan-auth is the Interface address of authenticated users set in step 1. The SAT action of IP rules, allow\_httpauth, transfers unauthenticated HTTP traffic to the firewall for further authentication process.

#	Name	Action	Source interface	Source network	Destination interface
1	allow_dns	NAT	lan	lannet	wan1
2	allow_ftp_passthrough	NAT	lan	lan-auth	wan1
3	allow_standard	NAT	lan	lan-auth	wan1
4	allow_httpauth	Allow	lan	lannet	core
5	allow_httpauth	SAT	lan	lannet	wan1
6	allow_httpauth	Allow	lan	lannet	wan1
7	reject_all	Reject	lan	lannet	wan1

Remember the order of IP rules is very important to the authentication process.

## 6. Save and activate the configuration

Keep in mind that next time you want to connect to the web console page, add ":" and the port number to the address, for example, <http://192.168.1.1:1080> or <https://192.168.1.1:10443>.

### Retrieve the saved logs from database

Firewall Analyzer archives all original logs received from syslog server to save disk space and also works like a logs database for further reference. If an IT staff wants to retrieve saved logs for in-depth analysis, they can navigate to **Settings -> System Settings -> Archived Files** to obtain them.



D-Link, D-Link logo, D-Link sub brand logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries. All other trademarks are trademarks of their respective manufacturers and owners.