ManageEngine
Powering IT ahead

Firewall Analyzer 7.2

Admin Server - User Guide

www.fwanalyzer.com

fwanalyzer-support@manageengine.com

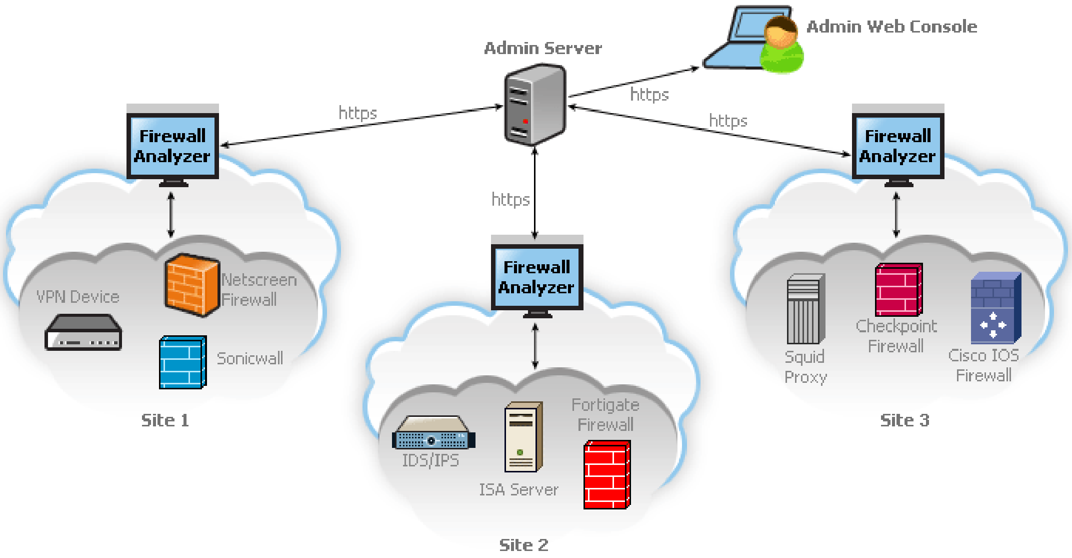
Table of Contents

Introduction - Firewall Analyzer Distributed Edition Admin Server

An enterprise spread across geography finds it difficult to manage the Firewalls in different branch office locations. To simplify this task Firewall Analyzer provides Distributed Edition. This edition employs distributed model.

What is Firewall Analyzer Distributed Edition?

Firewall Analyzer Distributed Edition is a distributed setup of Firewall Analyzers. It consists of one Admin server and N number of Collector servers. The Collector servers are installed at different geographical locations (one per LAN environment) and connected to the Admin server. This allows the network administrators to access the details of the Firewalls at different remote locations in a central place. All the reports, alerts and other Firewall information can be accessed through one single console. The administrator of large enterprises with various branch locations through out the globe stand benefited with this edition. For Managed Security Service Providers (MSSP) it is a boon. They can monitor the Collector server installed at different customer places from one point.



Firewall Analyzer Distributed Edition addresses requirements like the following:

- Aggregated Firewall log management of whole enterprise in different physical locations.
- Scalable architecture supporting 100s of Firewalls.
- Centralized monitoring using single console view.
- Secured communication using HTTPS.
- Exclusive segmented and secured view for various customers of MSSP.

This User Guide will help you install Firewall Analyzer distributed set up, and get familiar with the Firewall Analyzer Admin server user interface. If you are unable to find the information you are looking for in this document, please let us know at fwanalyzer-support@manageengine.com

About Firewall Analyzer Distributed Edition Admin Server

Firewall Analyzer Distributed Edition Admin Server provides unified display of reports, alerts and other information collected, correlated, and analyzed from enterprise-wide heterogeneous devices by the Collector Servers. The Collector Servers are registered with Admin Server. The Admin Server manages the Collector Servers.

The following are some of the key features of the Distributed Edition Admin Server release:

Feature	Description
Managing multiple collectors	Manage, Delete, Enable, Stop, Reset Collector servers
Dashboard	Provides a quick view of current traffic statistics and security activity across all devices for a selected Collector server
Advanced user management	Allows you to create different users and set appropriate access privileges for Admin server only
Multi-platform support	Runs on Windows and Linux platforms
Allows rebranding	The Distributed Edition can be customized for use of MSSP and others
Archived file viewing	Allows viewing of archived log files in the Collector Servers
Live Reports	Live reports of all the Firewalls for a selected Collector server

Release Notes - Distributed Edition

The new features in the 7.2 Enterprise release are mentioned below.

- 7.2 - Build 7020 Distributed Edition (GA)

7.2 - Build 7020 Distributed Edition

GA release of Firewall Analyzer Distributed Edition.

Installation and Setup

System Requirements - Firewall Analyzer Distributed Edition Admin Server

This section lists the minimum system requirements for installing and working with Firewall Analyzer Distributed Edition Admin Server. Please refer our website for recommended system requirements.

- Hardware Requirements
- Supported Operating Systems
- Supported Web Browsers

Hardware Requirements

The minimum hardware requirements for Firewall Analyzer Distributed Edition Admin Server to start running are listed below.

Processor: 1GHz Intel™ Pentium 4 or equivalent

Memory*: 1 GB of RAM

Disk Space*: 3 to 5 GB for the product depending on total number of devices of all the collectors.

Firewall Analyzer Distributed Edition Admin Server is optimized for 1024x768 resolution and above.

Supported Operating Systems

Firewall Analyzer Distributed Edition Admin Server has been tested to run on the following operating systems and versions:

- Windows™ NT/2000/XP/Vista, 2003 Server and 2008 Server
- Linux - RedHat 8.0/9.0, Mandrake/Mandriva, SuSE, Fedora, CentOS

Note: If Firewall Analyzer Distributed Edition Admin Server is installed in SuSE Linux, then ensure that in the **mysql-ds.xml** file, present under *<Firewall Analyzer Home>/server/default/deploy* you replace *localhost* mentioned in the following line : *<connection-url>jdbc:mysql://localhost:33336/firewall</connection-url>* with the corresponding IP Address or DNS resolvable name of the current system where Firewall Analyzer Distributed Edition Admin Server is installed.

Supported Web Browsers

Firewall Analyzer Distributed Edition Admin Server has been tested to support the following browsers and versions:

- Internet Explorer 5.5 or later
- Netscape 7.0 or later
- Mozilla 1.5 or later
- Firefox 1.0 or later

Prerequisites - Firewall Analyzer Distributed Edition Admin Server

This topic deals with the following pre-requisites for setting up Firewall Analyzer Distributed Edition Admin Server in your enterprise.

- Ports to be Freed
- Recommended System Setup
- Changing Default Ports

Ports to be Freed

Firewall Analyzer Distributed Edition Admin Server requires the following ports to be free:

Port Number	Usage
8500	This is the default web server port. You will access the Firewall Analyzer Distributed Edition Admin Server server from a web browser using this port number. You may change this port during installation.
514, 1514	These are the default listener ports on which Firewall Analyzer Distributed Edition Admin Server listens for incoming logs exported from devices.
33336	This is the port used to connect to the MySQL database in Firewall Analyzer Distributed Edition Admin Server

💡	Look up Changing Default Ports for help on changing the default ports used by Firewall Analyzer Distributed Edition Admin Server

Recommended System Setup

Apart from the System Requirements, the following setup would ensure optimal performance from Firewall Analyzer Distributed Edition Admin Server:

- Run Firewall Analyzer Distributed Edition Admin Server on a separate, dedicated PC or server. The software is resource-intensive, and a busy processor may cause problems in collecting logs.
- Use the MySQL bundled with Firewall Analyzer Distributed Edition Admin Server that runs on port 33336. You need not start another separate instance of MySQL.

Changing Default Ports

Changing the default MySQL port:

1. Edit the **mysql-ds.xml** file present in the *<Firewall Analyzer Home>/server/default/deploy* directory.

2. Change the port number in the following line to the desired port number:
   ```
   <connection-url>jdbc:mysql://localhost:33336/firewall</connection-url>
   ```
3. Save the file and restart the server.

Changing the default web server port:

1. Edit the **sample-bindings.xml** file present in the *<Firewall Analyzer Home>/server/default/conf* directory.
2. Change the port number in the following line to the desired port number:
   ```
   <binding port="8500"/>
   ```
3. Save the file and restart the server.

Installing and Uninstalling - Firewall Analyzer Distributed Edition Admin Server

Firewall Analyzer is available for Windows and Linux platforms. It is available both in 32 Bit version and 64 Bit version.

Installation Procedure for various OS and CPU versions:

- Windows 64 Bit version
- Windows 32 Bit version
- Linux 64 Bit version
- Linux 32 Bit version

For more information on supported versions and other specifications, look up System Requirements.

This topic covers the following procedures:

- Uninstalling Firewall Analyzer
  - Windows
  - Linux

Installing Firewall Analyzer

Windows 64 Bit version:

The Firewall Analyzer Windows 64 Bit version download is available as an EXE file at http://manageengine.com/products/firewall/download.html

Windows 32 Bit version:

The Firewall Analyzer Windows 32 Bit version download is available as an EXE file at http://manageengine.com/products/firewall/download.html

Rest of the installation procedure remains same for both 64 Bit and 32 Bit versions.

Double-click the downloaded EXE file, and follow the instructions as they appear on screen.

- Click **Advanced Install** button.
- Read the *License Agreement* and click **Yes** button.
- Select **Distributed Edition** and click **Next** button.
- Select **Admin Server** and click **Next** button.
- If the Admin Server is behind Proxy Server, configure the **Proxy Server Host**, **Proxy Server Port**, **Proxy User Name**, and **Proxy Password** details. Click **Next** button.
- Select **Destination Folder** using **Browse** button, for installation. Click **Next** button.
- Retain or modify the Web Port of Admin Server and select the Language of Installation from the combo box. Three languages are supported for installation and they are Chinese, English, and Japanese. By default English is selected. Click **Next** button.

- Select **Install Firewall Analyzer as service** check box (recommended), if you want to install Admin Server as a service. Click **Next** button.
- Configure new Program Folder or retain the default. Click **Next** button.
- The installation details like Installation Directory, Program Folder, and Web Port are displayed. Click **Next** button.
- Now, Distributed Edition - Admin Server installation is complete.

Once the installation is complete you will notice a tray icon, which provides you with the following options.

Option	Description
Firewall Server Status	This option provides you details like *Server Name*, *Server IpAddress* , *Server Port*, *Server Status*.
Start WebClient	This option will open up your default browser and connect you to the web login UI of Firewall Analyzer Server, provided the server has already been started.
Shutdown Server	This option will shutdown the Firewall Analyzer Server.

	The tray icon option is only available for Windows !

Linux:

Linux 64 Bit version:

The Firewall Analyzer Linux 64 Bit version download is available as a BIN file at http://manageengine.com/products/firewall/download.html

Linux 32 Bit version:

The Firewall Analyzer Linux 32 Bit version download is available as a BIN file at http://manageengine.com/products/firewall/download.html

Rest of the installation procedure remains same for both 64 Bit and 32 Bit versions.

1. Download the BIN file, and assign **execute** permission using the command: `chmod a+x` *<file_name>*`.bin`
   where <*file_name*> is the name of the downloaded BIN file.
2. Execute the following command: `./`*<file_name>*`.bin`

	During installation if you get an error message stating that the temp folder does not have enough space, try executing this command with the -`is:tempdir` <*directory_name*> option, where <*directory_name*> is the absolute path of an existing directory. `./<file_name>.bin -is:tempdir` <*directory_name*>

3. Follow the instructions as they appear on the screen.

- Click **Advanced Install** button.
- Read the *License Agreement* and click **Yes** button.
- Select **Distributed Edition** and click **Next** button.
- Select **Admin Server** and click **Next** button.
- If the Admin Server is behind Proxy Server, configure the **Proxy Server Host**, **Proxy Server Port**, **Proxy User Name**, and **Proxy Password** details. Click **Next** button.
- Select **Destination Folder** using **Browse** button, for installation. Click **Next** button.
- Retain or modify the Web Port of Admin Server and select the Language of Installation from the combo box. Three languages are supported for installation and they are Chinese, English, and Japanese. By default English is selected. Click **Next** button.
- Select **Install Firewall Analyzer as service** check box (recommended), if you want to install Admin Server as a service. Click **Next** button.
- Configure new Program Folder or retain the default. Click **Next** button.
- The installation details like Installation Directory, Program Folder, and Web Port are displayed. Click **Next** button.
- Now, Distributed Edition - Admin Server installation is complete.

This will install Firewall Analyzer - Admin server on the respective machine.

Uninstalling Firewall Analyzer

Windows:

1. Navigate to the Program folder in which Firewall Analyzer has been installed. By default, this is **Start > Programs > ManageEngine Firewall Analyzer 6** .
2. Select the option **Uninstall Firewall Analyzer**.
3. You will be asked to confirm your choice, after which Firewall Analyzer is uninstalled.

Linux:

1. Navigate to the *<Firewall Analyzer Home>/server/_uninst* directory.
2. Execute the command `./uninstaller.bin`
3. You will be asked to confirm your choice, after which Firewall Analyzer is uninstalled.

📝	At the end of uninstallation you will be taken to the Uninstallation Feedback Form where you can provide reasons for your product uninstallation. This would help us improve this product.

Starting and Shutting Down - Firewall Analyzer Distributed Edition Admin Server

Once you have successfully installed Firewall Analyzer, start the Firewall Analyzer server by following the steps below.

This topic covers the following procedures:

- Starting Firewall Analyzer
  - Windows
  - Linux
  - Start the service
- Shutting down Firewall Analyzer
  - Windows
  - Linux
  - Stop the service
- Configure Firewall Analyzer as Linux service

Starting Firewall Analyzer

Windows:

Click on **Start > Programs > ManageEngine Firewall Analyzer 7 > Firewall Analyzer** to start the server.

Alternatively, you can navigate to the *<Firewall Analyzer Home>\bin* folder and invoke the **run.bat** file.

Windows Service:

Ensure that the Firewall Analyzer application is installed as Windows Service. When you install with single click, by default it will be installed as Windows Services. If you have carried out custom installation, and chose not to install the application as Windows Service, carry out the procedure to convert the application installation as Windows Service. After this, carryout the following procedure to start as Windows Service.

- Go to the Windows **Control Panel**, Select **Administrative Tools > Services**.
- Right-click **ManageEngine Firewall Analyzer 7** and select **Start** in the menu.
- Alternatively, select **Properties**. The **<Service> Properties** screen opens up.
- In the **General** tab of the screen, check the **Service status** is "*Stopped*" and **Start** button is in enabled state and other buttons besides are grayed.
- Click **Start** button to start the server as windows service.

Linux:

Navigate to the *<Firewall Analyzer Home>/bin* directory and execute the **run.sh** file.

As soon as this is done, a command prompt window opens showing startup information on several modules of Firewall Analyzer. Once all the modules have been successfully created, the following message is displayed:

```
Server started.
Please connect your client at http://localhost:8500
```

where `8500` is replaced by the port you have specified as the web server port during installation.

Starting the Firewall Analyzer service in Linux

/etc/init.d/firewallanalyzer start

Check the status of Firewall Analyzer service

/etc/init.d/firewallanalyzer status
ManageEngine Firewall Analyzer 7.0 is running (15935).

Shutting Down Firewall Analyzer

Follow the steps below to shut down the Firewall Analyzer server. Please note that once the server is successfully shut down, the MySQL database connection is automatically closed, and all the ports used by Firewall Analyzer are freed.

Windows:

1. Navigate to the Program folder in which Firewall Analyzer has been installed. By default, this is **Start > Programs > ManageEngine Firewall Analyzer 6** .
2. Select the option **Shut Down Firewall Analyzer**.
3. Alternatively, you can navigate to the *<Firewall Analyzer Home>\bin* folder and invoke the **shutdown.bat** file.
4. You will be asked to confirm your choice, after which the Firewall Analyzer server is shut down.

Windows Service:

Ensure that the Firewall Analyzer application is installed as Windows Service. When you install with single click, by default it will be installed as Windows Services. If you have carried out custom installation, and chose not to install the application as Windows Service, carry out the procedure to convert the application installation as Windows Service. After this, carryout the following procedure to start as Windows Service.

- Go to the Windows **Control Panel**, Select **Administrative Tools > Services**.
- Right-click **ManageEngine Firewall Analyzer 7**, and select **Stop** in the menu.
- Alternatively, select **Properties**. The **<Service> Properties** screen opens up.
- In the **General** tab of the screen, check the **Service status** is "*Started*" and **Stop** button is in enabled state and other buttons besides are grayed.
- Click **Stop** button to stop the windows service.

Linux:

1. Navigate to the *<Firewall Analyzer Home>/bin* directory.
2. Execute the **shutdown.sh** file.
3. You will be asked to confirm your choice, after which the Firewall Analyzer server is shut down.

Stopping Firewall Analyzer service in Linux

```
/etc/init.d/firewallanalyzer stop
Stopping ManageEngine Firewall Analyzer 7.0...
Stopped ManageEngine Firewall Analyzer 7.0.
```

Check the status of the service again

```
/etc/init.d/firewallanalyzer status
ManageEngine Firewall Analyzer 7.0 is not running.
```

To configure Firewall Analyzer as service in Linux, after installation

Normally, the Firewall Analyzer is installed as a service. If you have installed as an application and not as a service, you can configure it as a service any time later. The procedure to configure as service, start and stop the service is given below.

To configure Firewall Analyzer as a service after installation, execute the following command.

```
sh configureAsService.sh -i
```

Usage of Firewall Analyzer service command

```
<Firewall Analyzer Home>/bin # /etc/init.d/firewallanalyzer
Usage: /etc/init.d/firewallanalyzer { console | start | stop | restart | status | dump }
```

Accessing the Web Client - Firewall Analyzer Distributed Edition Admin Server

Firewall Analyzer is essentially a firewall, VPN, and proxy server log analysis tool that collects, stores, and reports on logs from distributed firewalls, and proxy servers on the network.

Once the server has successfully started, follow the steps below to access Firewall Analyzer.

1. Open a supported web browser window
2. Type the URL address as ***http://<hostname>:8500*** (where *<hostname>* is the name of the machine on which Firewall Analyzer is running, and *8500* is the default web server port)
3. Log in to Firewall Analyzer using the default username/password combination of **admin/admin**.

Once you log in, you can view the Firewall reports from various Collector Servers and more.

If you want to access the web client from the same machine on which Firewall Analyzer is installed, execute the **startClient.bat/.sh** file from the *<Firewall Analyzer Home>/bin* directory.

- On a Windows machine, you can also access the web client from the Start menu by clicking on **Start > Programs > ManageEngine Firewall Analyzer 6 > Firewall Analyzer Web Client**.
- On a Windows machine, you can also access the web client from the System Tray by right-clicking on **Firewall Analyzer Tray Icon > Start Web Client**.

License Information - Firewall Analyzer Distributed Edition Admin Server

After you log in to Firewall Analyzer, click the **Upgrade License** link present in the top-right corner of the screen. The License window that opens, shows you the license information for the current Firewall Analyzer installation.

The License window displays the following information:

- Type of license applied - Trial or Registered (Professional, Premium)
- Product version number
- Number of days remaining for the license to expire
- Maximum number of devices that you are allowed to manage

Upgrading your License

Before upgrading the current license, make sure you have the new license file from ZOHO Corp. saved on that system.

1. Browse for the new license file, and select it.
2. Click **Upgrade** to apply the new license file.

The new license is applied with immediate effect.

Contact fwanalyzer-support@manageengine.com or sales@manageengine.com for any license-related queries.

Getting Started

Using the Dashboard

The Dashboard is shown when the **Home** tab is clicked. It is the first page you see when you log in. You can also customize your **Dashboard Views** as per requirements.

Dashboard Views selection is available only in the **Home** tab.

Select the Firewall Analyzer Collector Server, of which you want to view the dashboard, in the **Dashboard Views** of the left navigation panel.

Once the Collector Server is selected, the Dashboard dynamically changes to display the current statistics for each device whose log files are analyzed. The Firewall Analyzer dashboard shows the:

- Traffic Overview Graphs
- Security Overview Graphs
- Traffic Statistics
- Security Statistics
- Basic Search
- Advanced Search

The **Traffic Overview** graphs shows protocol-wise distribution of traffic across each device. At one glance, you can see the total traffic generated by each protocol group across each device. You can also drill down from the bars in the graph to see specific protocol usage in the Protocol Usage Report.

The **Security Overview** graphs shows distribution of security events like attack, virus, port scans, denied events, failed log ons, etc.. generated across each device. Drill down from the bars in the graph to see the corresponding events generated.

Firewall Analyzer will recognize only those firewall log messages which contains the attribute denoting a port scan. Currently Firewall Analyzer recognizes the attribute denoting a port scan for Fortigate, NetScreen & CheckPoint firewall's alone.

The **Traffic Statistics** table, shows the Traffic Overview graph's data in more detail, with specific percentage values of incoming and outgoing traffic per protocol group across each device. The **Show** bar lets you view the the top 5(default) / 10 / 15 or All protocol groups, captured in the logs across the configured devices. You can click on the Traffic IN, Traffic OUT, and Total Traffic for each protocol group of the configured device to obtain the drill-downs of the traffic. You can view the intranet's settings of various Collector Servers.

The traffic values in the table let you drill down to see traffic details for the corresponding protocol group in the Protocol Usage Report.

The **Quick Reports** link provides you 'quick' access to the top level details of traffic like Top Hosts, Top Destinations, Top Conversations, Top Protocol Groups, Top Firewall Rules, Top VPN Reports, and Top Attack Reports for the corresponding firewall.

	Quick Reports for Squid Proxies will provide only the following reports: Top Hosts, Top Destinations, and Top Conversations.

The **Security Statistics** table, shows the Security Overview graph's data in more detail, along with the distribution of the **Configured Alerts**. The Configured Alerts are classified according to the priority as High, Medium, and Low. Clicking on the alert counts against *High*, *Medium*, *Low*, or *All Alerts* will list you complete details like Alert Profile name, the generated time, the device for which the alert was raised, the alert priority, and the status of the alert.

The security statistics table provides you with the counts for **attacks**, **virus**, **failed log ons**, **security events**, and **denied events**.

Attacks: Firewall Analyzer will recognize only those firewall log messages which contains the attribute denoting an attack.

Virus: Firewall Analyzer will recognize only those firewall log messages which contains the attribute denoting a virus.

	Currently Firewall Analyzer recognizes the attribute denoting a virus for almost all firewall's except Cisco Pix, whose log messages do not contain the attribute denoting a virus.

Failed Log Ons: Firewall Analyzer will recognize only those firewall log messages which contains the attribute denoting a failed log on.

	Currently Firewall Analyzer recognizes the attribute denoting a failed log on for Fortigate, NetScreen, Cisco Pix, & Identiforce firewall's Failed Log Ons are not available for CheckPoint firewall's

Denied Events: Firewall Analyzer will recognize only those firewall log messages which contains the attribute denoting a denied request.

Security Events: The Security Events in Firewall Analyzer are based on the severity attributes *Emergency*, *Alert*, *Critical*, and *Error* only.

	Since *Security Events* are based on severity attributes, they may also include the other events like *port scans*, *attacks*, *virus*, *failed log ons*, *security events*, and *denied events*.

Clicking on the counts against each of the above events in the security statistics table will lead you to the corresponding the quick reports for those events.

Search

Doing a search in Firewall Analyzer UI is easy. Firewall Analyzer offers both Basic Search and Advanced Search in the product.

Basic Search, enables you to search for the following :

Search for	Description
Hosts	Refers to the IP Address or DNS Names which were recorded in the firewall logs *example: 192.168.0.1,web-server*
Protocol Identifiers	Refers to the list of protocols and protocol identifiers that are available in the Protocol Groups page (Settings >> Protocol Groups) *example: 6969/tcp, icmp, IPSec*
User Names	Refers to the authenticated user name required by some firewall's *example: john, kate*
Attack	Refers to the attack name. *examples: UDP Snort, Ip spoof*
Virus	Refers to the Virus name. *examples: JS/Exception, W32/Mitglieder*

Advanced Search, offers numerous options for making your searches more precise and getting more useful results from the Aggregated Logs Database. It also allows you to search from the Raw Firewall Logs.

In Advance Search, you can search the logs for the selected devices, from the aggregated logs database or raw firewall logs, and define matching criteria.

Selected Devices

In this section, you can choose the devices for which you want the logs to be searched. If no device is selected or you want to change the list of selected devices, select the devices.

1. Click **Change Selection** link.
2. **Select Devices from the list** window pops-up. In that window, All Devices with selection check box and individual devices with selection check boxes options are available.
3. Select the devices by selecting the check boxes as per your requirement. Click **OK** to select the devices and close the window or click **Cancel** to cancel the operation and close the window.

The selected devices are displayed in this section.

Search From

In this section, you can select one from the two options:

1. Aggregated Logs Database
2. Raw Firewall Logs

1. **Aggregated Logs Database**

   Select this option if you want to search from the aggregated logs database.

2. **Raw Firewall Logs**

   Select this option if you want to search from the raw firewall logs. Selecting this option will enable the following options:

   a. **Raw VPN Logs**
   b. **Raw Virus/Attack Logs**
   c. **Raw Device Management Logs**
   d. **Raw Denied Logs**

   Select the above logs options as per your requirement.

Define Criteria

This section, enables you to search the database for attributes using more than one following criteria's:

Criteria	Description
Protocol	Refers to the list of protocols and protocol identifiers that are available in the Protocol Groups page (Settings >> Protocol Groups) *example: 8554/tcp, rtsp, IPSec*
Source	Refers to the source host name or IP address from which requests originated
Destination	Refers to the destination host name or IP address to which requests were sent
User	Refers to the authenticated user name required by some firewall's *example: john, kate*
Virus	Refers to the Virus name. *examples: JS/Exception, W32/Mitglieder*
Attack	Refers to the attack name. *examples: UDP Snort, Ip spoof*
URL	Refers to the URL, which you want to search
Rule	Refers to the Firewall Rule, which you want to search
Device	Refers to the device from which logs are collected
Message	Refers to the log message texts stored in the DB

- If the search string exists then the search result will be intelligently displayed based on the report category in which it occurred.
- By default, the search is carried out for the time period selected in the Global Calendar present in the left pane of the UI.
- You can also search within the search results.

Advanced Search of Imported Firewall Logs

You can carry out Advanced Search on the imported Firewall logs.

Using the Sub Tab

The sub tab provides links to frequently accessed monitoring information in Firewall Analyzer.

The following report can be viewed by clicking the corresponding links in the sub tab:

Link	Action
Interface/Zone Reports	View live traffic reports for the past one day for each firewall of the selected Collector Server, on a 5-minute average

The following tasks can be done by clicking the corresponding links in the sub tab:

Link	Action
Collector Settings	Add a Collector server to receive details from different devices
Alert Profile	View alert profile which trigger alerts and send notifications
Search & Advanced Search	Offers numerous options for making your searches more precise and getting more useful results. Reports can be scheduled from the search results.

Using The Left Navigation Pane

The left navigation pane provides quick links to different tasks and reports in Firewall Analyzer Distributed Edition - Admin server. The components present in the left navigation pane depend on the tab that is currently selected.

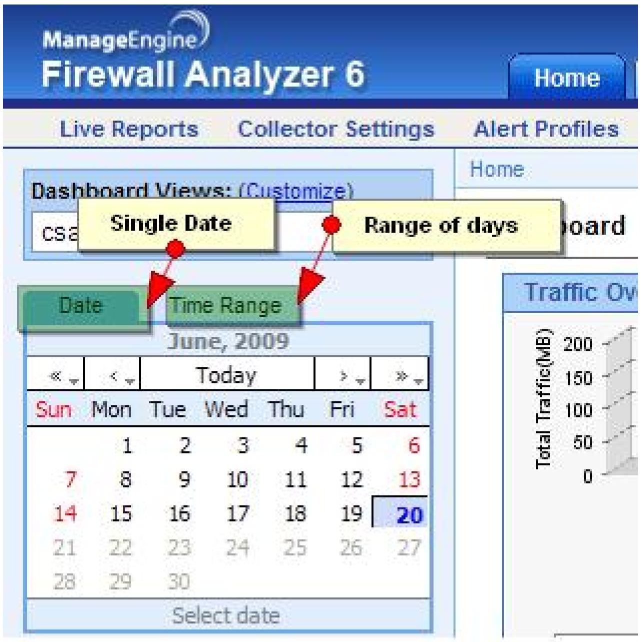
The following is a list of all components found in the left navigation pane:

Component	Description
Dashboard Views	List all the custom dashboard views created by the user. 'All Devices' view is the default dashboard view.
Global Calendar	Allows you to select the time period for all reports from one place. By default, the current day's data from 00:00 Hrs to the current time is shown.
Firewalls	Includes links to generate reports for each firewall from which logs have been collected. Click on the icon against each firewall to view reports for that firewall alone in a new window. Click on the icon against each firewall to obtain Quick Reports of the top level details of traffic like Top Hosts, Top Destinations, Top Conversations, etc for the corresponding firewall.
Squid Proxy Reports	Includes links to generate reports for each squid proxy server from which logs have been collected. Click on the icon against each squid proxy server to view reports for that squid proxy server alone in a new window. Click on the icon against each squid proxy server to obtain Quick Reports of the top level details of traffic like Top Hosts, Top Destinations, and Top Conversations for the corresponding Squid Proxy.
My Report Profiles	Includes links to view custom reports created in corresponding Collector server.
Bookmarks	Allows you to set a bookmark for the current page, and manage existing bookmarks

Most of the tasks in the left navigation pane can be done from the main tabs also, by clicking the corresponding links. The left navigation pane provides a quicker way to perform the same tasks.

Using Calendar

You can use the calendar to select a single date or range of days to view various details of the reports, alerts, and logs of the Firewalls. There are two tabs provided on top left corner of the calendar to select a single day or range of days. Refer the screen shot given below:



Dashboard View Customization

In the **Dashboard Views** section, you can see **Customize** link besides "*Dashboard Views:*" title to customize the dashboard view and a combo box listing all the available Dashboard Views with **Default** view.

To customize the dashboard view, click **Customize** link. **Dashboard View Customization** page appears. It lists all the dashboard views available to the user.

The dashboard view customization page lets users to:

- Create multiple dashboard views based on the groups assigned to the user. Each view can be configured to show a list of assigned groups. The created dashboard views are listed in the Dashboard Views combo box in the left navigation pane top of the Home tab.
- Edit any of the listed views created by user, except the **Collector Server** dashboard views.
- Set any one of the views as default dashboard view.
- Delete any of the listed views created by user, except the **Collector Server** dashboard views and the default dashboard view, if any of the created dashboard view is set as a default dashboard view.

To create a new group view

Click **Create Group View** link. The **Create Group View** screen pops-up.
In that screen,

- Enter a name for the view in the **View Name** text box.
- Select the required Collector Server from the **Collector Servers** combo box as per your requirement, which lists all the Collector Servers registered with this Admin server.
- Select the devices from the **Available Groups** list, and move it to the **Dashboard View Groups** list.
- Select the **Set this view as Default View** check box option to make this view as the default dashboard view upon user login.
- Click **Update** to create the device view and **Close** to close the screen.

Now you can see the new view created is listed in the **Dashboard View Customization** page.

To edit a device view

To edit a view, click the ✎ icon of the view to be edited. The **Edit Group View** screen pops-up. The procedure is same as that of create device view.

To set a device view as default view

Select any one of the listed views to be **Set as default**. The default dashboard view is indicated by the 🏠 icon and all other views by the 🏠 icon.

Click the ⌂ icon of the view, which you want to set as default view. Now the ⌂ icon changes to 🏠 icon and in the previous default view, the 🏠 icon changes to ⌂ icon.

To delete a device view

To delete a view, click the ✕ icon of the view to be deleted.

Default View: The default dashboard view is the one which appears in the **Home** tab, upon user login. User can create and set any view as default view. Default view will appear automatically only when the user closes the client and re-logs in. User can view any of the listed dashboard views and traversing between the tabs will not change the view.

Reports

Live Reports

The **Live Reports** provide a live visual representation of the traffic load across network links. Graphs are similar to that of MRTG, with the aim of providing a simple way to see exactly how much inbound and outbound traffic was generated for each device.

- Interface/Zone Reports For all devices
- Live Reports of Each Firewall Device
- Live Reports of Each Squid Device

Live Reports For all devices (Interface/Zone Reports link in the sub tab)

Click the **Interface/Zone Reports** link in the sub tab to see the Interface wise live reports for all devices, for the last 24 hours, over a 5-minute average.

Interface/Zone Live Reports Dashboard (Last 24 Hours) screen opens up. In that screen you will find **Device - Interface details** table. It will list all the devices and their interfaces. Click the **Show All** link or **+ tree** icon to the left of the device in the list. **Hide All** link or **- tree** icon will display the list of devices and the numbers of interface the device has. The expanded table lists the **Device Name**, **Interface Name**, **Bandwidth IN**, and **Bandwidth OUT**. Bandwidth IN and Bandwidth Out will display the bandwidth usage of the interface in percentage and the average speed in Kbps.

Click on the **Live Reports** link below the device in the list to view the live reports for that device alone.

Click on the individual interfaces (shown as **portN**) of the device in the list to view the only the live reports of the interface of the device.

Live Reports of Each Firewall Device

On the top right side of the Report screen, there will be two combo boxes. They are:

- Refresh
- Export as

Refresh

The **Refresh** combo box lets to enable or disable refreshing of the Live reports and lets you to choose the refreshing interval of the Live reports. There will be three field values for filtering. They are:

- Never Refresh
- Refresh Every 1 Min
- Refresh Every 5 Min
- Refresh Every 10 Min

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Click the **Live Reports** link present inside the list of reports for a device, to see the live reports for that device alone, over all the time periods described above.

The graphs for each device shows the minimum, maximum, and average amount of incoming and outgoing traffic through that device, over several time periods. Traffic is broken down into the last day, last week, last month, and last year, with an average granularity of 5 minutes, 30 minutes, 2 hours, and 1 day respectively.

The incoming and outgoing bandwidth can be viewed in Kbps.

Drill down from each of the graphs in the live report to see the following details:

Graph	Description
Inbound/Outbound Traffic Conversations	The inbound/outbound conversations for all hosts across this device. This data is available only for the last day's traffic over a 5-minute average granularity.
Top Hosts	The top hosts contributing to inbound/outbound traffic across this device. Drill down from this graph to see the corresponding conversations for each host, during the selected time period.
Top Protocol Groups	The top protocol groups used in inbound/outbound traffic across this device. Drill down from this graph to see the corresponding conversations using each protocol group, during the selected time period.
Top Users	The top users contributing to inbound/outbound traffic across this device. Drill down from this graph to see the corresponding conversations for each user, during the selected time period.

Live Reports will not be available for devices whose logs do not contain the "duration" field.
For example: *WatchGuard, SonicWall, Astaro, IP Filter Linux Firewall, etc...*

Live Reports of Each Squid Proxy Device

On the top right side of the Report screen, there will be two combo boxes. They are:

- Refresh
- Export as

Refresh

The **Refresh** combo box lets to enable or disable refreshing of the Live reports and lets you to choose the refreshing interval of the Live reports. There will be three field values for filtering. They are:

- Never Refresh
- Refresh Every 1 Min
- Refresh Every 5 Min
- Refresh Every 10 Min

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Click the **Live Reports** link present inside the list of reports for a device, to see the live reports for that device alone, over specific time periods.

The graphs for each device shows the minimum, maximum, and average amount of outgoing traffic through that device, over several time periods. Traffic is broken down into the last day, last week, last month, and last year, with an average granularity of 5 minutes, 30 minutes, 2 hours, and 1 day respectively.

The outgoing bandwidth can be viewed in Kbps.

	Live Reports will not be available for devices whose logs do not contain the "duration" field.

Viewing Report Profiles

Custom reports in Firewall Analyzer are grouped into report profiles, and listed under the **My Report Profiles** category. A report profile can contain a combination of pre-defined and custom reports. The **My Report Profiles** section is present in the **Reports** tab and the left navigation pane.

Viewing Firewall Reports

Firewall Analyzer offers a rich set of pre-defined reports that help in analyzing bandwidth usage and understanding network behavior.

The following reports are generated based on Firewall logs:

- Traffic Reports
- Protocol Usage Reports
- Web Usage Reports
- Mail Usage Reports
- FTP Usage Reports
- Telnet Usage Reports
- Streaming & Chat Reports
- Event Summary Reports
- VPN Reports
- Firewall Rules Reports
- Inbound & Outbound Traffic
- Intranet Reports
- Internet Reports
- Security Reports
- Virus Reports
- Attack Reports
- Spam Reports
- Protocol Trend Reports
- Traffic Trend Reports
- Event Trend Reports
- Admin Reports
- VPN Trend Report

All the above reports can be accessed from the **Left Navigation Pane**. You need to select the specific Colletor Server to view the reports of the Firewalls monitored by the Collector Server. **Select the Collector:** combo box lists all the Collector servers registered with this Admin server. Select the Collector server as per your requirement. All the reports include links to several sections of the report which can be seen when the ⊞ icon, or the report bar itself is clicked. Click on each section to go to the corresponding section of the report directly, or click the **View Report** link to view the entire report with all the sections.

On a broad level, reports in Firewall Analyzer are classified into the following types:

Report	Description
My Report Profiles	View custom report profiles to report on specific parameters
Firewall Reports	View traffic reports, protocol usage, event summary, etc. for each firewall
Squid Proxy Reports	View top talkers, site details, and squid usage summary for each squid proxy server

Squid Proxy Server Reports

Squid is a widely used proxy cache for Linux and UNIX platforms. Squid is usually used together with a firewall to secure internal networks from the outside using a proxy cache.

The **Squid Proxy Reports** section in Firewall Analyzer includes reports that are based on squid proxy cache logs. This section can be accessed from the left navigation pane or the **Reports** tab.

The following reports are generated based on squid proxy cache logs:

- Top Talkers Report
- Site Details Report
- Squid Usage Summary

Apart from these reports, **Live Reports** are available for squid proxy servers also. The Live Report for each squid proxy server shows the traffic load across the server, over different time periods.

Alerts

Viewing Alerts

Select the **Alerts** tab to see the list of alerts triggered.

You need to select the specific Colletor Server to view the alerts of the Firewalls monitored by the Collector Server. **Select the Collector:** combo box lists all the Collector servers registered with this Admin server.

By default, the Alerts tab lists all the alerts triggered so far. The list shows the timestamp of the alert, the host which triggered it, the alert priority, and the status of the alert. Clicking on each alert profile would provide the details of the alert like why, when, & for which device the alert was triggered.

Viewing Alerts for an Alert Profile

The Alerts box on the left navigation pane lists all the alert profiles created so far. Click on each alert profile to view the corresponding list of alerts triggered.

The ✉ icon against an alert profile indicates that an email notification has been setup.
The 📜 icon against an alert profile indicates that a **Run Program** action has been setup.
The 📱 icon against an alert profile indicates that an SMS notification has been setup.
The **Alerts** tab lets you view alerts for various alert profiles set up.

System Settings

The **Settings** tab lets you configure several system settings for the server running Firewall Analyzer, as well as other settings.

The following is the the list of configuration options available under the System Settings section:

Setting	Description
Alert Profiles	Click this link to view the alert profiles set up so far
Archived Files	Click this link to configure archiving intervals, or load an archived file into the database
Rebranding FWA Web Client	To customize Firewall Analyzer Web Client to suit the needs of Managed Security Service Providers (MSSPs) or large enterprises

The following is the the list of configuration options available under the Administration Settings section:

Setting	Description
Intranet Settings	Click this link to view the intranet configuration of the selected Collector Server to identify internal and external traffic
Collector Settings	Click this link to configure the details of the Collector Servers registered with this Admin Server
User Management	Click this link to add, edit, or delete users in Firewall Analyzer
Server Diagnostics	Click this link to view system-related information for Firewall Analyzer
Mail Server Settings	Click this link to configure the mail server to send the alert notification and reports by Email
Collector Availability Alert	Click this link to configure to trigger alerts if there was no logs from Colletor server for a specifc period of time
SMS Settings	Click this link to configure the alert notification by SMS messages
External Authentication Settings	Click this link to configure Active Directory and RADIUS server authentication

Alert Profile Details

The **Alert Profiles** link lets you view all the alert profiles of a selected Collector server, set up so far.

Select the Collector: combo box lists all the Collector servers registered with this Admin server. Select the Collector server as per your requirement.

💡	The Alert Profiles of various Collector servers are displayed. The profile are view only. You cannot edit/change/modify the profile configuration.

The Alert Profiles table lists the following details of all the existing alert profiles:

Columns	Description
Edit	Option to edit the alert profile **disabled** for Admin server.
Profile Name	Name of the alert profile
Criticality	Criticality of the alert triggered by the profile
Action	Action on the profile to be carried out **disabled** for Admin server.
# Alerts	Number of times alert has been triggered for this profile
Alert Type	Email, SMS, Run Program are the alert types will be displayed depending on the configuration.
Mail-Id	Email address associated with the Email alert type of the alert profile

Click an alert profile to see the corresponding list of alerts triggered.

Alert Type

The ✉ icon indicates that an email notification has been set up for this alert profile. The corresponding email address is also displayed next to this icon.

Archiving Log Files

The **Archived Files** page lists the files that have been archived for devices Collector Server wise, along with options to load the file to view the report and search. Firewall Analyzer Collector Server archives the logs received from each device (which it monitors), and zips them in regular intervals.

Select the Collector: combo box lists all the Collector servers registered with this Admin server. Select the Collector server as per your requirement.

The **Archived Files** page lists the zipped files for each device, along with the archived time, file size, and archiving status.

The list contains the following columns:

- Device
- FileName
- StartTime
- ArchivedTime
- FileSize
- Status
- Action

Loading Archived Files

To load an archived file for search, click the **Load to Search** link against the device for which you need to see archived data. Once the file is fully loaded, you can search for data in the archives, and view specific information.

Viewing Data from Archived Files

Once the archive is fully loaded, click the **Report** link to search for specific data in the archive. In the **Raw Log Search** popup window that opens, enter the criteria for the data, such as the firewall, user name, protocol, etc. Choose traffic logs or security logs, the time interval for which you want to see the data that meets all or any of the criteria. Click **Search** to view the records that match the criteria that you have specified.

The Search Result screen displays **Device Name**, **Defined Criteria**, **Searched From** (*Traffic Logs* or *Security Logs*) details on the top left side. You have the **Edit Search Criteria** link on the top right side.

In the **Search Result Between <Selected Time Interval>**, you can view the **Formatted Logs** or **Raw Logs** by selecting the respective tabs.

You can configure the columns of the Search Result table. You can also select **View per page** to select the number of log entries to be displayed in a single page.

Rebranding Firewall Analyzer Web Client

To customize the Firewall Analyzer Web Client follow the steps given below:

1. In the Firewall Analyzer web client, select the **Settings** tab.
2. In **Settings** screen, select the **System Settings > Rebranding FWA Web Client** link. Rebranding **Firewall Analyzer Web Client** page appears.

The **Rebranding FWA Web Client** link lets you to customize all the logos, images, and links used in the Firewall Analyzer Web Client to suit the needs of the MSSPs (Managed Security Service Providers).

The rebranding screen contains two sections. At the top you have the **Customize Images** section. In this section, you can customize logos and images. At the bottom you have the **Customize Strings/Links** section. In this section, you can customize strings and links.

Customize Images

Replace the default images with your company/enterprise images

Client Logos & Images	Where it is used	Image Size & Thumbnail	New Image
Company Logo	Login Page	129*39 pixels	
Product Logo	Login Page	289*59 pixels	
Top Band Image	Client Header	232*47 pixels	
Server Status Image	Tray Icon [Windows]	400*60 pixels	

Customize Strings/Links

Replace the default strings/links with your company/enterprise strings/links

Client Strings & Links	Where it is used	Existing String/Link	New String/Link
Company Name	Login Page	Zoho Corp.	
Brand Name	Login Page	ManageEngine	
Company Website	Login Page	www.manageengine.com	
Product Website	Login Page	www.fwanalyzer.com	
Support E-Mail	Login Page	fwanalyzer-support@manageengine.com	
Sales E-Mail	About Popup	sales@manageengine.com	

Click **Update** to update the customized images/logos and strings/texts. Click **Cancel** to cancel the customizing the web client operation.

📝	- You can customize Zoho Corp/ManageEngine images/links as per your requirement. - Customization takes effect only for the changed images/links, else default images/links are retained. - Size of new image should be of same size as the default image. - Images with the following file extensions are only permitted: **.jpg**, **.gif**, and **.png**

Admin Settings

Viewing Intranet Settings

The Intranet Settings page will list the configured Intranet details of all the devices of the corresponding Collector Server. These devices have been configured to send their logs to the specific Firewall Analyzer Collector Server for analysis.

Click the **Intranet Settings** link to view the defined intranet.

Option to specify the Intranet Settings, like networks or a range of IP addresses to identify machines behind a firewall, is available in the Collector Server. By adding the machines or IP addresses that are located within your network (LAN), you can identify and distinguish between traffic that is generated within your network, and traffic that is coming from, or destined outside your network.

Adding Different Users

Click the **User Management** link to create and manage the different users who are allowed to access the Firewall Analyzer Distributed Edition - Admin server.

The different types of users and their respective privileges are described in the table below:

User	Description
Administrator	This user can do all operations meant for Distributed Edition - Admin server including adding additional users and more
Operator	This user can do all Administrator operations **except** configuring the user
Guest	This user can only view device details, and basically has only read-only privileges. The Alerts & Support tabs are not available for guest users

By default, an Administrator user with username as **admin** and password as **admin**, and a Guest user with username **guest** and password **guest** are already created.

If you have logged in as an Administrator user, the **User Management** page lists all the users created so far.

You can view the users based on user type. Select the user type from the **Select User Type** combo box. The three user types listed are: *Administrator*, *Operator*, and *Guest*.

You can view the users alphabet wise. **All** option and the alphabets are listed above the user list. Select **All** option or the alphabet under which the user login name will be available.

Viewing Login Details

If you have logged in as an Administrator user, click the User Audit **View** link against a user to view the corresponding user audits. The **User Audit** page shows the remote host IP address from which the user logged on, the timestamp of the login, and the duration of the session.

The description the user details available in the user list table are explained below:

User Detail	Description
User Name	The user's login name
No. of HostGroups	The number of host group(s) to which the user will be having access
Access Level	The access level privilege of the user
Domain Name	The domain in the network to which the user belongs to
User Audit	The corresponding user audits information

Delete

Select all users check box if you want to delete all the users and individual user(s) check boxes to delete the selected users. There is a check box against each user below the all user check box. Click **Delete** button to delete all the or selected user(s) from the list of users accessing Firewall Analyzer.

Assign Role

Select the users for whom the host group(s) need to be assigned/re-assigned. Select the access level of the user from the **Access Level** combo box. The three access levels listed are: *Guest*, *Operator*, and *Administrator*. Click **OK** to save the new changes. Click **Cancel** to cancel assigning the role operation.

Assign Group(s)

Select the users for whom the host group(s) need to be assigned/re-assigned. Select the host group to which the user will be having access. All the available host groups are listed in the **Available HostGroup(s)** list. Select the host groups and click right arrow. The selected host groups are displayed in the **Selected HostGroup(s)** list. If you want to remove any host group from the **Selected HostGroup(s)** list, select the host groups and click left arrow. The removed host groups will be listed back in the **Available HostGroup(s)** list.

Adding a New User

- Click the **Add New User** link to add another user to access Firewall Analyzer.
- Enter the new user's login name in the **User Name** text box. The user name should be unique. If you want the user name as password, select the **Use Login Name as Password** check box.
- Enter the user's password in the **Password** text box. The password should be of 5 to 20 characters long.
- Re-enter the user's password in the **Verify Password** text box.
- Select the access level of the user from the **Access Level** combo box. The three access levels listed are: *Guest*, *Operator*, and *Administrator*.
- Enter default e-mail address the user in the **Email Address** text box.
- Select the host group to which the user will be having access. All the available host groups are listed in the **Available HostGroup(s)** list. Select the host groups and click right arrow. The selected host groups are displayed in the **Selected HostGroup(s)** list. If you want to remove any host group from the **Selected HostGroup(s)** list, select the host groups and click left arrow. The removed host groups will be listed back in the **Available HostGroup(s)** list.
- Click **Add User** to add this user to the list of users accessing Firewall Analyzer. Click **Cancel** to cancel the adding user operation.

Editing User Details

If you have logged in as an Administrator user, the **User Management** page lists all the users created so far.

- Click the **Edit** link to edit the user details. You can change the access level, password, and optionally, the default e-mail address for this user.

- You can edit the host groups associated with the user. Select the host group to which the user will be having access. All the available host groups are listed in the **Available HostGroup(s)** list. Select the host groups and click right arrow. The selected host groups are displayed in the **Selected HostGroup(s)** list. If you want to remove any host group from the **Selected HostGroup(s)** list, select the host groups and click left arrow. The removed host groups will be listed back in the **Available HostGroup(s)** list.
- Once you are done, click **OK** to save the new changes. Click **Cancel** to cancel editing the user operation.

OR

If you have logged in as an Operator or Guest user, click on the **Account Settings** link to change your password and default e-mail address.

Once you are done, click **OK** to save the new changes. Click **Cancel** to cancel editing the user operation.

Firewall Analyzer User Privileges

Types of User Privileges in Firewall Analyzer

- **Administrator** - Can view details of all Firewalls/Collectors.
- **Operator** - Can view details of the Firewalls/Collectors assigned to him and cannot perform User Management.
- **Guest** - Has read-only privileges for the Firewalls assigned to him.

Comparison of Feature Access to the Users

Sl No	Feature Name	Administrator	Operator	Guest
1	User Management Create/Modify/Delete users	Yes	No	No
2	Dashboard View Customization	For all Firewalls	Only for Firewalls assigned to him.	Only for Firewalls assigned to him
3	Advanced Search	Yes	Yes	The user can perform advanced search except Save as Report Profile.
4	Bookmark	The user can view only his bookmarks.	The user can view only his bookmarks.	The user can view only his bookmarks.
5	User Assistance • Tell a Friend • Upgrade License • Help • Feedback • About	Yes	Yes	No

Changing Account Settings

Click the **Account Settings** link under the **Settings** tab to change the default password and e-mail address set for this account. You cannot change the account's user name or access level.

Once you have made the required changes, click **Save User Details** to save the changes. Click **Cancel** to return to the default **Settings** tab.

	This option is visible only for users with **Guest** or **Operator** access level

Collector Settings

Click the **Collector Settings** link under the **Settings** tab. The **Manage Collectors** page opens up. The tabular list contains individual and select all Collector servers check boxes.

Delete Collectors

Select required Collector server(s) or select all Collector servers to delete. Click the ✗**Delete Collector(s)** link on top left side of the page. The selected Collector server(s) will be deleted.

Collector Details	Description
Collector Name	Display Name/Host Name of the Collector server. ✎**Edit Collector Details** icon. Use the icon to update the admin username and password whenever any changes are made in the Collector.
Collector Status	Status of the Collector server, whether **Up** UP or **Down** Down
Last Collection Time	The time of last log collection by the respective server.
Data Collection Status	If the log collection is on the ✓ status icon appears and if the log collection is not happening then the ✗ status icon appears with appropriate error message.
No of Devices	Number of Firewalls being monitored by the corresponding Collector server.
Flow rate (messages/sec)	Number of log messages received per second by the Collector
Time Zone	The time zone in which the Collector Server is located.
Action	Use the **Enable** option to change Data Collection status. **Stop / Up** - Stops the data collection/Starts the data collection **Reset** - Resets the data collection and starts collecting data from scratch

Edit Collector Details

Click the ✎**Edit Collector Details** icon. The **Edit Collector Details** window pops up. Change the *User Name*, *Password*, *Web Protocol*, *Web Port* and *Display Name* of the Collector Host as per requirement. The Collector Host Name will be displayed and it is non-editable.

⚠	• User with administrative privilege should alone be configured, else data collection from corresponding collector server will fail. • You can not use Active Directory or RADIUS Server Authenticated Admin user credentials for Data Collection in Admin Server

Once you have made the required changes, click **Save** to save the changes. Click **Cancel** to cancel the user detail changes.

Viewing Server Diagnostics

Click the **Server Diagnostics** link to see server-specific device information. This information will be useful while troubleshooting the server or reporting a problem.

The various information boxes on this page are described in the table below:

Box	Description
License Information	This box shows details about the license that is currently applied.
System Information	This box shows device information for the Firewall Analyzer server
Installation Information	This box shows details about the Firewall Analyzer installation on the server machine
JVM Memory Information	This box shows statistics on the amount of memory used by the JVM

Configuring Collector Server Availability Alerts

In Firewall Analyzer Admin Server, alert can be triggered, if the Firewall Analyzer Admin Server is unable to fetch data from the specific Firewall Analyzer Collector Server. The alert triggering is configurable. Collctor non-availability alert configuration notifies the user through e-mail, when the Firewall Analyzer Admin Server is not able to fetch data from the Firewall Analyzer Collector Server(s).

Follow the procedure given below to configure the triggering of alert:

- Select the **Settings** tab in the Web Client. On the right side of the screen, you will see **Admin Settings** section below the **System Settings** section. In the **Admin Settings** section, there will be **Collector Availability Alert** link.
- Click the **Collector Availability Alert** link. The **Collector Availability Alert** page opens. In the screen, there will be a link +**Add Alert** on the left side top to add an alert. Below the link, the configured alerts are listed in a table. The details of the table columns are:

Columns	Description
Device Names	The names of the Firewall Analyzer Collector Servers, for which this alert will be triggered, if the servers fails to allow the Admin Server to fetch the data.
Alert Mail Address	Failure to fetch the data from the above mentioned Firewall Analyzer Collector Server will trigger an alert to send e-mail to the configured users e-mail IDs.
Phone Number	The mobile phone number to which the SMS alert notification will be sent.
Location	The location of the Firewall Analyzer Collector Server
Owner	The user to whom the alerts triggered will be automatically assigned
Time Interval (minutes)	The time duration within which the data should be available to the Firewall Analyzer Admin Server. Failure to fetch the data within this time duration will trigger this alert.
Action	This indicates whether the configured alert is enabled or disabled.

- To configure an alert, click the +**Add Alert** link. The **Create Availability Alert** page opens.
  - Select the firewall devices for which this alert needs to be triggered using the **Change Selection** link. A pop-up window **Select Devices from the list** opens to select the devices. In this the first option will be **All Devices**, and below the **All Devices** option the devices are listed. Select the **All Devices** option or devices as per requirement. The selected devices are displayed under the **Selected Devices**.
  - In the **"If the logs are not received from the above selected firewall(s) for at least (15 minutes/30 minutes/60 minutes/2 hours/6 hours/12 hours/1 day)"** part, select the time duration from the combo box. The time interval options available are: 15 minutes, 30 minutes, 60 minutes, 2 hours, 6 hours, 12 hours, and 1 day.
  - Configure the following in the **Send Alert as** section:
    - Select the **Mail** check box.

  - Enter the e-mail address in the **Mail To** text box, to which the alert has to be sent. Enter multiple e-mail addresses separated by a comma(,).
  - Optionally, you can modify the e-mail subject in the **Subject** text box as per your requirement.

If the Mail Server is not configured the following note appears and there is a link provided to configure the Mail Server. Configure the Mail Server in order to get the mail alerts.

Note: Mail Server is not configured. Click here to configure the Mail Server.

  - Select the **SMS** check box.
  - Enter the mobile phone number in the **SMS To** text box, to which the alert has to be sent. Enter multiple phone numbers separated by a comma(,).

If the SMS Settings is not configured the following note appears and there is a link provided to configure the SMS Settings. Configure the SMS Settings in order to get the SMS alerts.

Note: Mail Server is not configured. Click here to configure the Mail Server.

  - Select the **Run Script (SNMP)** check box.
  - Select the script to be run in the **Location** field. Click the **Choose File** button to browse the location of the script file. Besides the button, the selected file name will be displayed. If no file is chosen, **No file chosen** is displayed.

- After choosing all the required values, click **Add Alert** to save and activate the new alert. Click **Cancel** to cancel the alert configuration.

Setting up the Mail Server

You need to configure the mail server on Firewall Analyzer Admin Server in order to receive email alert notifications.

Click the **Mail Server Settings** link to edit the mail server settings. Enter the following details:

Field	Description
Outgoing Server Name	Enter the name of the SMTP server on your network which is used for outgoing emails.
Port	Enter the port used by the SMTP server. Usually this is 25.
Authenticate for every Login	If your SMTP server requires you to authenticate yourself before sending an email, check this option. Otherwise leave it unchecked. * The below two fields are active only when this checkbox is checked.
User Name*	Enter the user name used to authenticate email sending from this machine.
Password*	Enter the corresponding password for the typed user name.
Sender MailId	Enter the Sender or From Address which needs to be mentioned in the outgoing emails.By default, *firewallreport@localdomain.com* will be mentioned as the sender mailid. The **Test Server** button is for testing the mail server configurations. You can give your email-id in the "Enter Recipient Mail Id" field, which comes-up when you click Test Server. If the mail server configurations have been given correctly you will receive a Test Mail.

After all the details have been filled in, click **Save Changes** to save the mail server settings.

💡	If the mail server is not configured, you will see an error message when you are setting up an email alert notification to be emailed automatically. Click the **Configure Mail Server now** link inside the error message to configure the above settings from the opened popup window.

SMS Settings

The SMS setting is similar to Mail Server setting. You need to configure the SMS settings in order to SMS alert notifications in your cellular phone.

⚠	This option is visible only for users with **Admin** access level

Click the **SMS Settings** link under the **Settings** tab to configure the port in which the SMS equipment is connected and mobile phone number to test the functioning of port.

On clicking the link, SMS Settings screen open up on the right hand side.
In that you will see **GSM Communication Port Name** text box and **Test Port** button.

- Enter the communication port name (For example: **COM1**) in the text box.
- Click the **Test Port** button.
- On clicking the button, a window pops-up to enter phone number to test port.
- Enter mobile phone number with '+' sign and country code (For example: +19259249500).
- Click **OK** button. If the port & SMS equipment is functioning properly, you will get a test message on the phone. Click **Cancel** button to abort the testing.

Once you have entered the required port number and tested it, click **Save Changes** to save the changes. Click **Cancel** to return to the default **Settings** tab.

💡	The phone number entered in the pop-up screen is meant only for testing the SMS port. Phone numbers to which the Alerts are to be SMS notified need to be configured in individual Alert profiles.

Supported Modems for SMS Notifications

Following is a list of the modems supported in OpManager for SMS Notifications.

S No	Modem Version	Baud Rate	Manufacturer
1	Itegno 3000	115200	Wavecom
2	Itegno WM1080A	115200	Wavecom
3	Wavecom M1306B		Wavecom
4	MultiTech MultiModem MTCBA-G-F1		
5	Wavecom Fastrack M1206B	115200	Wavecom

Mobiles Supported

S No	Mobile Model	Baud Rate	Manufacturer
1	Motorola E398	9600	Motorola
2	Nokia 6210		Nokia
3	Nokia 6310		Nokia
4	Nokia 6230i		Nokia
5	Nokia 8250		Nokia
6	Nokia 6610	115200	Nokia
7	Nokia 7210	115200	Nokia
8	Sony Ericsson T610	19200	Sony Ericsson
9	Sony Ericsson W800i	115200	Sony Ericsson
10	samsung sgh-c100	9600	Samsung
11	Sharp GX30	115200	Sharp
12	Sony Ericsson k700	115200	Sony Ericsson
13	Motorola RAZR V3	115200	Motorola
14	Nokia 7610	115200	Nokia
15	Nokia 3310/3315	19200	Nokia
16	Siemens M35	19200	Siemens
17	Siemens M50	19200	Siemens
18	Siemens C45	19200	Siemens

Can’t find the modem or the mobile you have in this list?

No worries! check whether the device, you have, meets the following configuration.

- Modem/ Mobile must have GSM functionality with a provision to insert the SIM card.
- Should support 7bit (GSM default alphabet), 8bit and Unicode (UCS2) encoding.
- Firewall Analyzer uses AT commands to send SMS, so the device should respond to AT commands. [If required, test using HyperTerminal]

If all the above criteria match, Firewall Analyzer will support your modem/ mobile phone.

External Authentication Settings

Firewall Analyzer provides two more external authentication apart from the local authentication. They are **Active Directory** authentication and **Remote Authentication Dial-in User Service (RADIUS)** authentication. If you import users from Active Directory or if you add a RADIUS server details, you will find the **Options >>** link besides the **Login** button in the Firewall Analyzer Client UI Login screen. If you click the **Options >>** link, **Log on to** field will appear below the **Password** field. The Log on to field will list the following options:

- **Local Authentication** - If the user details are available in local Firewall Analyzer server user database
- **Radius Authentication** - If the user details are available in RADIUS server and dummy user entry should be avilable in local Firewall Analyzer server user database
- **Domain Name(s)** - If the details of the user of a domain is imported from Active Directory into the local Firewall Analyzer server user database

Enter the **User Name** and **Password**. Select one of the three options in **Log on to** (**Local Authentication** or **Radius Authentication** or **Domain Name**). Click **Login** button to log in to Firewall Analyzer Client UI.

Active Directory Configuration Settings

Users in the AD (Active Directory) can be imported into Firewall Analyzer server. You have to select the required OUs (Organizational Units) under the Listed domains. You can re scan the network to find domains. Login to individual servers of the domain to get the OUs listed and select the OUs as per your requirement. Use the server credentials (User Name & Password) to login to the server. For the first time, all the users will be imported into Firewall Analyzer. On subsequent or periodic imports, only the new user added to the AD will be imported.

> The imported users will be added in the Firewall Analyzer server with the following constraints:
>
> **Access Level** as *Operator* and will have access to all the Firewall devices.

Procedure to configure AD settings

Click the **External Authentication Settings** link under the **Settings** tab to configure the AD user details import, periodic import, and to enable user authentication usage. On clicking the **Active Directory** tab, the **Active Directory Configurations** page opens up. In that page, you will find the following sections:

- Import users from Active Directory
- Schedule
- Authentication

Import users from Active Directory

In this section, you will find **Import Users** button. Click the button and **Import users from Active Directory** screen pops-up.
In that screen, you will find the following items:

- **Domain Name** combo box & **Rescan Network** link

  Domain Name combo box will list all the available domains in the network. Besides the combo box, you will find the **Rescan Network** link. Clicking the link will re scan the network to find out all the available domains. Select the domain from the combo box as per requirement.

- **Server Name**

  If you want to list the OUs of a particular server, enter the server name in the text box.

- **User Name**
- **Password**

  If you want to access a server and get list of (Organizational Units) OUs, enter the user name and password of the server in the text boxes.

- **Login & List OUs** button

  After entering the server name to be accessed and the credentials for server access, click this button to get the list of (Organizational Units) OUs.

- **Cancel** button

  If you want to cancel the access to server and get list of OUs operation canceled, click this button.

Schedule

In this section, you will find a check box to schedule the import of users periodically from AD and a Save button.

every __ days" check box. Enter the periodicity of user import in days.

Click **Save** button to save the changes.

Authentication

In this section, you will find the status (**Status: Disabled**) of the AD authentication to be used for users imported from AD and Enable button.

Click **Enable** button to use AD authentication for the users imported from AD. On clicking the button the status will change to **Enabled** (**Status: Enabled**) and the **Enable** button will change to **Disable**.

RADIUS Server Configuration Settings

You can also leverage the RADIUS authentication for user access bypassing the local authentication provided by Firewall Analyzer.

In the RADIUS server authentication the users credentials are sent to the RADIUS server. The server checks for the user credentials and sends the authentication successful message to Firewall Analyzer server.

	Note: If the user has only RADIUS server authentication, create the user in Firewall Analyzer with dummy password. On user logging in with RADIUS server authentication, the dummy password in the local server is ignored and the user credentials are sent to RADIUS server for authentication. Refer the procedure given in the Adding Users document to add a new user with dummy passowrd.

You can make Firewall Analyzer work with RADIUS server in your environment. This section explains the configurations involved in integrating RADIUS server with Firewall Analyzer.

Procedure to configure RADIUS server settings

To configure RADIUS server in Firewall Analyzer, provide the following basic details about RADIUS server and credentials to establish connection:

Click the **External Authentication Settings** link under the **Settings** tab to configure the RADIUS server configuration. On clicking the **Radius Server** tab, the configuration fields are displayed. In that page, you will find the following fields:

RADIUS Server Settings	Description
Radius Server IP	The IP Address of the machine in which the RADIUS server is running. Enter the host name or IP address of the host where RADIUS server is running
Radius Server Authentication Port	The port used by the RADIUS server for authenticating users. Enter the port used for RADIUS server authentication. By default, RADIUS has been assigned the UDP port 1812 for RADIUS Authentication.
Radius Server Protocol	The protocol used by the RADIUS server for authenticating users. Select the protocol that is used to authenticate users. Choose from four protocols: • **PAP** - Password Authentication Protocol • **CHAP** - Challenge-Handshake Authentication Protocol • **MSCHAP** - Microsoft Challenge-Handshake Authentication Protocol • **MSCHAP2** - Version 2 of Microsoft Challenge-Handshake Authentication Protocol

RADIUS Server Settings	Description
Radius Server Secret	The secret string used for connecting RADIUS client (Firewall Analyzer) with the server. Enter the RADIUS secret used by the server for authentication
Authentication Retries	The number of retries the RADIUS server to permit for authenticating users. Select the number of times you wish to retry authentication in the event of an authentication failure

Tips and Tricks

Frequently Asked Questions - Firewall Analyzer Distributed Edition

For the latest list of Frequently Asked Questions on Firewall Analyzer - Distributed Edition, visit the FAQ on the website or the public user forums.

General

1. **Who should go for Firewall Analyzer - distributed setup (Distributed Edition)?**

   We recommend distributed setup (Distributed Edition):

   - If your's is a **large enterprise**, which have hundreds of security devices (like Firewalls, IPS, IDS), VPN devices and proxy devices to manage across different geographical locations.
   - If you are a **Managed Security Service Provide** (MSSP), having a large customer base spread across geographical locations.

2. **How many Collector Servers can a single Admin Server manage?**

   One Admin Server is designed to manage 50 Collector Servers. However, we have carried out simulated testing in our laboratory, which effortlessly managed 20 Collector Servers.

3. **During installation of Admin Server, I am prompted for Proxy Server details? When should I configure it?**

   You need to configure the proxy server details during **Admin Server** installation, if the **Admin Server** needs to pass through **Proxy Server** to contact **Collector Servers**.

4. **Can I convert the existing "*Standalone*" Firewall Analyzer installation to a "*Distributed Setup*"?**

   Yes, you can. Ensure that the existing installation of **Firewall Analyzer build is 6000**. To convert, you need download the Firewall Analyzer 7.0 exe/bin and install as **Admin Server** and then you need to convert the existing installation of Firewall Analyzer 7.0 to **Collector Server**. Refer the procedure in the below help link:

   Procedure to convert existing Standalone Edition Firewall Analyzer installation to Distributed Edition Collector Server

5. **I have deleted the Collector Server from Admin Server. How do I re-add?**

   Once you have deleted the **Collector Server**, to re-add follow the procedure given below:

   - Reinitialize the Collector Server.

- Re-register the Collector Server with Admin Server by executing the *<Firewall Analyzer Home>\troubleshooting* **\registerWithAdminServer.bat/sh** file.
- Restart the Collector Server.

6. **Where the collected logs are stored, whether in Collector Server database or in both Collector Server and Admin Server databases?**

All the logs collected by the Collector Server are stored in the Collector Server database only. For archiving, there is a provision to forward the logs to the Admin Server, but not for storing in the Admin Server database.

Secured Communication Mode (HTTPS)

1. **What is the mode of communication between Admin Server and Collector Server?**

By default, the mode of communication is through **HTTP**. There is also an option to convert it to secured mode of communication **HTTPS**. Refer the procedure in the below help link, to setup secure communication mode between Admin and Collector Server.

2. **I have changed the Collector Server communication mode to HTTPS, after installation. How to update this info in Admin server?**

Click on **Settings tab > Collector Settings link** in *Admin Server UI* and click on the **Edit** icon of specific Collector and select the appropriate protocol and configure the web server port details.

Licensing

1. **What are the "Licensing Terms" for Firewall Analyzer Distributed Edition?**

Firewall Analyzer Distributed Edition license will be applied in Admin Server. The number of devices for which the license is purchased, is utilized among the registered Collector Servers. You can keep adding the devices in various Collector Servers till the total number of licenses purchased get exhausted. View the number of devices managed by each Collector Server in the Collector Settings page.

If the number of devices being collectively managed by all the registered Collector Servers, exceed the number of License purchased, a warning message appears in the Admin Server. In that scenario, you have various options.

- Purchase license to manage the additional devices.
- Otherwise, check the number of devices being managed by each Collector Server in the Collector Settings page in the Admin Server.
  - Go to the individual Collector Server License Management page and manually manage the licenses. Unmanage the lesser required devices and make the managed devices count equal to the number of licenses.
  - You can also remove a registered Collector Server in the Admin Server to make the managed devices count equal to the number of licenses.

2. **In Collector Server there no is option to apply the license? How the license get applied in the Collector Server?**

   Yes, there is no option to apply the license in **Collector Server**. The license applied in **Admin Server** will be automatically propagated to all **Collector Servers**.

3. **"*License Restricted*" alert is showing in Admin Server, even though I have unmanaged additional devices in Collector Server. Why?**

   The managed/unmanaged status of devices in Collector Server are synchronized with Admin Server during the data collection cycle, which happens at an interval of 5 minutes.

Troubleshooting Tips - Firewall Analyzer Distributed Edition

For the latest Troubleshooting Tips on Firewall Analyzer, visit the Troubleshooting Tips on the website or the public user forums.

Trouble Shooting - General

1. **When I login, why "*No Data Available*" is shown?**

   Check for the following reasons:

   - Click on the current date in the **Calendar**. If data is displayed, then there could be some time difference between **Admin** and **Collector Server**.
   - If both **Admin** and **Collector Server**s are in different time zones, then you need to choose the appropriate time using **Calendar**.

2. **Data collection is not happening?**

   The possible reasons could be:

   The **Admin Server** unable to contact **Collector Server** or the **Collector Server** status is **down**.

   a. If the **Admin Server** is unable to contact **Collector Server**,
      i. The **Collector Server** added may not be of **Distributed Server** type.
      ii. The **username** and **password** configured for respective **Collector Server** may not have **Administrative** privilege.

   b. If the **Collector Server** status is **down**, check for the following conditions:
      i. Is the **Collector Server** running? Is the **Port** and **Protocol** information configured **correct**?
      ii. Is the **Admin Server** needs to pass through **Proxy Server**? If so, is the same has been configured?
      iii. Are the **Ports** required are opened/allowed in **Firewall(s)**?

3. **When Alert count is clicked, "Security Statistics" page is shown with "No Data Available" message?**

   The possible reasons are listed below:

   - Time difference between **Admin** and **Collector Server**.
   - All report page are fetched from Collector Server directly, but the generated alerts are fetched from **Admin Server**. The generated alerts from all **Collector Servers** are synchronized periodically (at 5 minutes interval). This could be the case where the generated alerts are yet to be synchronized.

- If you have converted a standalone Firewall Analyzer installation to **Collector Server**, previously generated alerts will not be synchronized. Only new alerts will be synchronized.

Trouble Shooting - Collector Server Synchronization

1. **After installing *Collector Server*, unable to start it. It says "*Distributed Edition: Problem encountered while registering with Admin Server.*"?**

   This happens when **Collector Server** fails to establish contact with **Admin Server**.
   The conditions under which communication could fail are listed below:

   a. **Admin Server** is not running in configured machine at given port.
   b. **Collector Server** needs to pass through **Proxy Server** and it has not been configured. In case configured, check if values are valid.
   c. Appropriate ports (**8500** - default web server port), (**8763** - default HTTPS port) are not opened in Firewall(s).
   d. **Build** mismatch between **Admin** and **Collector Servers**.

2. **Installed both *Admin* and *Collector Servers*, but when I login into *Admin Server*, I see *Collector Settings* page only. Why?**

   - This could be because the data collection for all the **Collector Servers** added in the **Admin Server** are yet to happen. By default, the data collection for a **Collector Server** is scheduled every 5 minutes.
   - No device/resource exists in **Collector Server**.

3. **In Admin Server, the status of the Collector Server is shown as "*Down*", even though I am able to view reports for devices in it?**

   The status update of the **Collector Server** is performed at the end of every data collection cycle which is scheduled for every 5 minutes.

Other Tools and Utilities

Configuring Secure Communication (SSL) between Admin and Collector Servers

The SSL protocol provides several features that enable secure transmission of Web traffic. These features include data encryption, server authentication, and message integrity.

You can enable secure communication from web clients to the Firewall Analyzer server using SSL.

> The steps provided describe how to enable SSL functionality and generate certificates only. Depending on your network configuration and security needs, you may need to consult outside documentation. For advanced configuration concerns, please refer to the SSL resources at http://www.apache.org and http://www.modssl.org

- **Generating a valid certificate**
- **Disabling HTTP**
- **Enabling HTPPS (SSL)**
- **Verifying SSL Setup**
- **Configuring HTTPS Configuration Parameters for 64 bit/128 bit encryption**
- **Using the existing SSL certificate**
- **How to install SSL certificate for Firewall Analyzer**

Generating a valid certificate

Stop the server, if it is running.

Follow the instructions given below for SSL Installation:

If you have a keystore file for using HTTPS, place the file under *<Firewall Analyzer Home>\server\default\conf* directory and rename it as "**chap8.keystore**"

Disabling HTTP

When you have enabled SSL, HTTP will continue to be enabled on the web server port (default 8080). To disable HTTP follow the steps below:

1. Edit the **server.xml** file present in *<Firewall Analyzer Home>*/server/default/deploy/jbossweb-tomcat50.sar directory.
2. Comment out the HTTP connection parameters, by placing the <!-- tag before, and the --> tag after the following lines:

```
<Connector port="8080" address="${jboss.bind.address}"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
```

```
enableLookups="false" redirectPort="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"/>
```

Enabling HTPPS (SSL)

- In the same file, enable the HTTPS connection parameters, by removing the <!-- tag before, and the --> tag after the following lines:

```
<!--
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS" />
-->
```

> While creating keystore file, you can enter the password as per your requirement. But ensure that the same password is configured, in the **server.xml** file. Example password is configured as '**rmi+ssl**'.

Verifying SSL Setup

1. Restart the Firewall Analyzer server.
2. Verify that the following message appears in the command window after the Firewall Analyzer application is started:

```
   Server started.
   Please connect your client at https://localhost:8500
```

3. Connect to the server from a web browser by typing https://<*hostname*>:8500 where <*hostname*> is the machine where the server is running

Configuring HTTPS Configuration Parameters for 64 bit/128 bit encryption

If you want to configure the HTTPS connection parameters for 64 bit/128 bit encryption, add the following parameter at the end of the SSL/TLS Connector tag:

SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS"
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

Using the existing SSL certificate

- You can export the Wild card certificate to a **.pfx** file and then follow the instructions given below to configure the same in Firewall Analyzer.
- Stop ManageEngine Firewall Analyzer service
- Copy the **.pfx** file to the location *<Firewall Analyzer Home>\server\default\conf*
- Go to the location *<Firewall Analyzer Home>\server\default\deploy\jbossweb-tomcat50.sar* and open the file **server.xml** in word pad, and locate the entries in the file as below:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS"
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

- Replace the file name *chap8.keystore* with the pfx file name (**<pfx file name>.pfx**) and also enter the **keystoreType="pkcs12"** after the file name and also replace the **keystorePass** value '*rmi+ssl*' with the password for the **.pfx** file.

- The entries should be as given below:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/<pfx file name>.pfx"
keystoreType="pkcs12"
keystorePass="<password for the .pfx file>" sslProtocol = "TLS"
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

- Restart Firewall Analyzer service.

How to install SSL certificate for Firewall Analyzer

Follow the instructions given below for SSL Installation:

Step 1: Create a new Keystore

1. You will be using the keytool command to create and manage your new Keystore file. When you are ready to create your keystore go to the directory where you plan to manage your Keystore and certificates (*<Firewall Analyzer Home>\jre\bin\*). Enter the following command:

   keytool -genkey -alias <our_alias_name> or [Domain Name] -keyalg RSA -keystore chap8.keystore

(For example: keytool -genkey -alias tomcat -keyalg RSA -keystore chap8.keystore)

2. You will be prompted to choose a password for your keystore. You will then be prompted to enter your Organization information. When it asks for first and last name, DO NOT mention your first and last name, but rather it is your Fully Qualified Domain Name for the site you are securing say, helpdesk.yourdomain.com. If you are ordering a Wildcard Certificate this must begin with the * character say, *.yourdomain.com)
3. After you have completed the required information confirm that the information is correct by entering 'y' or 'yes' when prompted. Next, you will be asked for your password to confirm. Make sure to remember the password you choose. Your keystore file named **chap8.keystore** is now created in your current working directory.

Step 2: Generate a CSR from your new keystore

1. Next, you will use keytool to create the Certificate Signing Request (CSR) from your Keystore. Enter the following command

   keytool -certreq -alias <your_alias_name> or [Domain Name] -file csr.txt -keystore chap8.keystore

   (For example: keytool -certreq -alias tomcat -file csr.txt -keystore chap8.keystore)

2. Type the keystore password that you chose earlier and hit Enter.
3. Your CSR file named **csr.txt** is now created in your current directory. Open the CSR with a text editor, and copy and paste the text (including the BEGIN and END tags) into the CA web order form. Be careful to save the keystore file (chap8.keystore) as your certificates will be installed to it later.

Step 3: How to install your SSL Certificate

1. Download your Certificate files from the email from CA to the directory where your keystore (chap8.keystore) was saved during the CSR creation process. The certificate must be installed to this exact keystore. If you try to install it to a different keystore it will not work. The certificates you downloaded must be installed to your keystore in the correct order for your certificate to be trusted. If the certificates are not installed in the correct order, then the certificate will not authenticate properly.
2. Install the Root Certificate file:
   - Each time you install a certificate to your keystore you will be prompted for the keystore password, which you chose when generating your CSR.
   - Type the following command to install the Root certificate file:

     keytool -import -trustcacerts -alias root -file TrustedRoot.crt -keystore chap8.keystore

     NOTE: Choose 'Yes' if you get prompted with a message that says "Certificate already exists in system-wide CA keystore under alias <entrustsslca> Do you still want to add it to your own keystore? [no]:" You will get a confirmation stating that the "Certificate was added to keystore".

3. Install the intermediate certificates if any. (Follow the instructions provided by the CA)

4. Install the Primary Certificate file:
   - o Type the following command to install the Primary certificate file:

     ```
     keytool -import -trustcacerts -alias tomcat -file
     <your_domain_name>.crt -keystore chap8.keystore
     ```

     This time you should get a slightly different confirmation stating that the "Certificate reply was installed in keystore" If it asks if you want to trust the certificate. Choose y or yes. Your Certificates are now installed to your keystore file (keystore.key) and you just need to configure your server to use the keystore file.

Converting existing Standalone Edition Firewall Analyzer installation to Distributed Edition Collector Server

To convert existing Standalone Edition Firewall Analyzer installation to Distributed Edition Collector Server follow the procedure given below:

- Shutdown the Firewall Analyzer Service. Ensure that ports 33336 (default MySQL) and 8500 (default 8500) are free.
- Take a backup of **mysql** data folder.
- Open a **Command Prompt/Console** and navigate to *<Firewall Analyzer Home>/troubleshooting* directory.
- Execute the **ConvertToCollector.bat/sh** file.

  It will prompt you to take backup of **mysql** data folder and to continue running the script.

```
   Please take backup of mysql data folder before running this script.
   Do you really want to continue this script? [y/n]: y
```

- It will prompt you to shut down the server or service, if it is running.

```
   Firewall Analyzer Server is running. Server should not run while
   running this tool. Please shutdown the server before running this tool.
```

- Enter the details of the Admin Server.

```
   Enter Web Port of this server [8500] :8500
   Enter Web Server Protocol of this server [http] :http
   Enter Admin Server Name/IPAddress :firewall-test
   Enter Admin Server Web Port [8500] :8500
   Enter Admin Server Web Protocol [http] :http
```

- Enter the details of the Proxy Server, if required.

```
   Use Proxy to reach Admin server [n/y] :y
   Enter Proxy Server Name :proxy-server
   Enter Proxy Server Port :80
   Enter Proxy UserName :root
   Enter Proxy Password :public
```

- If this server registers successfully with the intended Admin Server, the following message is displayed.

```
Successfully registered with the AdminServer
Database not started. Starting .........
Table updated
....
....
....
....
Server noted as Converted Collector
TablesToSync.xml delete status ::::::: true
stopping DB Server .......
```

Open the Admin Server UI and check the Collector Settings and ensure that the converted server is listed.

- If this server cannot register with the intended Admin Server, it will prompt you to check the Admin Server availability.

```
Unable to connect with the Admin Server on given port and protocol.
Kindly ensure the following
1. Admin Server is accessible on given port and protocol.
2. Is Admin Server behind Proxy-Server ? If so, has those details been
configured ?
Exit due to error during register
```

Contacting Technical Support

The **Support** tab gives you a wide range of options to contact the Technical Support team in case you run into any problems.

Link	Description
Request Technical Support	Click this link to submit a form from the Firewall Analyzer web site, with a detailed description of the problem that you encountered
Troubleshooting Tips	Click this link to see the common problems typically encountered by users, and ways to solve them
Contact Support	Call the toll-free number +1 888 720 9500 to talk to the Firewall Analyzer Technical Support team directly
Create Support Information File [SIF]	Click this link to create a ZIP file containing all the server logs that the Technical Support team will need, to analyze your problem. You can then send this ZIP file to fwanalyzer-support@manageengine.com or upload the ZIP file to our ftp server by clicking on Upload to **FTP Server**, in the pop-up window provide your E-Mail id and browse for the zipped SIF file and then press Upload.
Need a Feature	Click this link to submit a feature request from the Firewall Analyzer web site
User Forums	Click this link to go to the Firewall Analyzer user forum. Here you can discuss with other Firewall Analyzer users and understand how Firewall Analyzer is being used across different environments
Feedback	At any time, you can click the **Feedback** link in the top pane, to send any issues or comments to the Firewall Analyzer Technical Support team.

The Support tab also displays the latest discussions in the Firewall Analyzer User Forum.

Procedure to resolve Firewall Analyzer issue with Firewall Analyzer support

Best in the industry technical support and other informal means to get Firewall Analyzer issues resolved.
Adopt the following ways progressively.

Knowledge Base & Community

- Go through the FAQ
- Look out in the trouble shooting tips
- Browse through the Firewall Analyzer forum

Best in the industry technical support

- Send email to fwanalyzer-support@manageengine.com
- Call toll free telephone number (**+1-888-720-9500**)
- Ask for a meeting (**Zoho Meeting**) – web conference

Procedure to create a Support Information File (SIF) and send the SIF to Firewall Analyzer support

We would recommend the user to create a **Support Information File** (**SIF**) and send the SIF to fwanalyzer-support@manageengine.com The SIF will help us to analyze the issue you have come across and propose a solution.

The instructions for creating the SIF is as follows:

- Login to the Web-client and click the **Support** tab.
- Click the **Create Support Information File** link show in that page.
- Wait for 30-40 Sec and again click the **Support** tab.
- Now you will find new links **Download** and **Upload to FTPServer**.
- You can either download the SIF by clicking on the **Download** link and then send the downloaded SIF to fwanalyzer-support@manageengine.com or click the **Upload to FTPServer** and provide the details asked and upload the file.

Procedure to create SIF and send the file to ManageEngine, if the Firewall Analyzer server or web client is not working

If you are unable to create a SIF from the web client UI, you can zip the files under '*log*' folder, which is located in *<Firewall Analyzer Home>\server\default\log* (default path) and send the zip file by upload it in the following ftp link: http://bonitas.zohocorp.com/upload/index.jsp?to=fwanalyzer-support@manageengine.com