



# TrafficShield™ Installation and Configuration Manual

version 3.1



# Service and Support Information

## Product Version

This manual applies to product version 3.1 of the TrafficShield™ Application Firewall.

## Legal Notices

### Copyright

Copyright 2002 - 2005, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable Control user licenses. F5 reserves the right to change specifications at any time without notice.

### Trademarks

F5, F5 Networks, the F5 logo, BIG-IP, 3-DNS, iControl, GLOBAL-SITE, SEE-IT, EDGE-FX, FireGuard, Internet Control Architecture, IP Application Switch, iRules, OneConnect, Packet Velocity, SYN Check, Control Your World, ZoneRunner, uRoam, FirePass, and TrafficShield are registered trademarks or trademarks of F5 Networks, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. F5 Networks' trademarks may not be used in connection with any product or service except as permitted in writing by F5.

### Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

### Export Warning

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

### FCC Compliance

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause interference, in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

### Canadian Regulatory Compliance

This class A digital apparatus complies with Canadian I CES-003.

### Standards Compliance

The product conforms to ANSI/UL 60950-1-2002 1st edition and Certified to CAN/CSA C22.2 No. 60950-1-3 first edition.

---



---

---

# Table of Contents

---

---



<b>I</b>		
<b>Introduction</b>		
	Product overview .....	1-1
	Document objectives .....	1-1
	How this manual is organized .....	1-1
	Audience and assumed knowledge .....	1-2
	Related documentation .....	1-2
<b>2</b>		
<b>Installing TrafficShield Units</b>		
	Installing TrafficShield units .....	2-1
	TrafficShield Load Balancer configuration .....	2-1
	Network terminology .....	2-2
	TrafficShield private network .....	2-2
	Private IP .....	2-2
	Service IP .....	2-2
	IP to Web server .....	2-3
	Server IP .....	2-3
	Trusted IP .....	2-3
	Permanent IP .....	2-3
	Static Route .....	2-3
	Gateway .....	2-3
	Alias IP .....	2-4
	Installation procedure .....	2-5
	Running tsconfig.pl for the Standby unit .....	2-9
<b>3</b>		
<b>Launching TSMS</b>		
	Accessing TSMS .....	3-1
	Using the TrafficShield Wizards .....	3-2
	The TrafficShield Unit Configuration Wizard: .....	3-2
	The Web Application Configuration Wizard: .....	3-3
	The Crawler Configuration Wizard .....	3-3
	Installing the Package Wizard .....	3-4
<b>4</b>		
<b>Configuration</b>		
	Configuring the TrafficShield units .....	4-1
	Units .....	4-1
	Route Table .....	4-2
	IP Aliases .....	4-3
	Licensing .....	4-6
<b>5</b>		
<b>Web Applications</b>		
	Defining a new Web Application .....	5-1
	Web Application Wizard .....	5-2
	Editing an existing Web Application .....	5-11
	Service Properties .....	5-11

## 6

### Administration

Users .....	6-1
Alerts .....	6-4
Defaults .....	6-6
Negative Regular Expressions Policy Defaults .....	6-6
Creating a Pool of Expressions .....	6-6
Assigning Expressions .....	6-7
System .....	6-9
Restart .....	6-10
Reboot .....	6-10
Shutdown .....	6-10
Upgrades .....	6-11
Adding a Software Package .....	6-11
Install Package Wizard .....	6-12
Rollback .....	6-14
Backup .....	6-15
Defining Backup Schedules .....	6-15
Testing the Destinations .....	6-17
Permanent IP Addresses .....	6-19
Downloads .....	6-21
Policy Browser .....	6-21
Support tools .....	6-22
Export Configuration .....	6-22
Record Traffic .....	6-24
F5 Support Website .....	6-24

### Glossary





I

---

---

# Introduction

---

---

- Product overview
- Document objectives
- How this manual is organized
- Audience and assumed knowledge
- Related documentation



## Product overview

Web applications are the single greatest point of contact most people have with corporations today. However, these applications let users through the traditional security perimeter around the company's IT infrastructure, allowing access to sensitive internal data. Today the Web application is the security perimeter. That is, enterprises are relying on the security of each application to keep users from accessing restricted data or systems. Browser-based applications are inherently difficult to secure and full of vulnerabilities.

F5<sup>®</sup> Networks TrafficShield<sup>™</sup> security application, is a dedicated appliance built to protect applications by preventing hackers from stealing customer and corporate data. It automatically maps each application to determine every legal user action, and then blocks actions not known to be legal according to this map.

This manual describes the single-unit deployment and the optional Standby unit deployment.

## Document objectives

This user guide describes how to configure and manage TrafficShield security applications. Configuration Administration operations are using the TrafficShield Management Station (TSMS), a Web-based tool built into the TrafficShield security application units.

## How this manual is organized

The user interface organization is based on an everyday user's perspective: the user has configured the TrafficShield security application and has now switched to an ongoing maintenance focused mode.

The manual's focus is on the first-time user performing the initial steps to install the TrafficShield security application:

- Pre-configure the Unit outside TSMS
- Launch TSMS and complete the unit configuration.
- Register the production license.
- Define all relevant Web Applications.

Only then will the user be able to create policies and be able to utilize all the other Configuration and Policy management features of this product.

This manual consists of the following chapters:

**Chapter 1 Introduction:** This chapter provides an overview of the TrafficShield security application, traces the document objectives, how the manual is organized, the targeted audience and their assumed knowledge, and a note about related documents

**Chapter 2 Installing TrafficShield security application units:** This chapter explains how to configure a TrafficShield security application and its Standby unit.

**Chapter 3 Launching TSMS:** This chapter explains how to access the TrafficShield security application and begin to navigate to the configuration screens.

**Chapter 4 Configuration:** The installation process is followed by a network configuration stage. In this stage, you can define a Standby unit, if not defined during installation, set static routes and assign aliases to the network cards. This chapter focuses on these topics as well as additional configuration parameters and Licensing.

**Chapter 5 Web Applications:** This chapter explains how to create a Web application definition in TSMS and how to continue to maintain it.

**Chapter 6 Administration:** This chapter describes administrative operations such as defining additional users, backups, downloading helpful utilities, etc.

## Audience and assumed knowledge

This document is intended for network operators and security administrators. Additional information and technical support is available on demand.

## Related documentation

The TrafficShield Security Policy User Manual explains how to set up a TrafficShield security policy and how to apply it to a Web application. The manual presents the TrafficShield security application concepts and shows how the concepts are implemented in the security policy context.



# 2

---

---

## Installing TrafficShield Units

---

---

- Installing TrafficShield units
- Network terminology
- Installation procedure



## Installing TrafficShield units

This chapter explains how to install an F5 Networks TrafficShield security application units.

A TrafficShield security application unit may be installed in two configurations: a single unit, or a single unit with a Standby unit. Both units are identical. The Standby unit is automatically activated when the active unit fails.

**◆ Note**

---

*The TrafficShield security application should always be installed behind a network firewall before deployment on a network.*

## TrafficShield Load Balancer configuration

The TrafficShield security application software can also be installed in a Load Balancer configuration, in which the Database and TSMS application will be installed on two units (Active and Standby units) and the Shield application will be installed on all other units.

## Network terminology

Before you install and configure the TrafficShield security application unit, you need to determine several IP addresses. This section describes the function of each address.

The following section demonstrates a typical TrafficShield security application deployment and the relevant IP addresses.

### TrafficShield private network

This is the network which all TrafficShield security application units use to communicate between each other for management purposes.

### Private IP

An IP address uniquely assigned to a TrafficShield security application unit. Each unit may have only one private IP address. The Private IP address will be assigned as an alias of the Eth0 network card. If the intended topology of the TrafficShield security application consists of more than one unit, then the internal communication between the units will be based on Private IP addresses.

### Service IP

The IP address at which the TrafficShield security application unit receives requests directed to the Web application. In a network not protected by the TrafficShield security application, this would be the IP address of the Web server. After installing the TrafficShield security application, you can assign the Web server's current IP address to the TrafficShield security application unit as a service IP (the Web server will get a different address).

---

**◆ Note**

*In some cases this is the IP address which is mapped to the DNS A record of the web server. Usually this is an external IP.*

Each TrafficShield security application unit may have as many Service IP addresses as the number of Web applications it protects. This address is disabled when the unit is in standby mode.

Service IP addresses may be assigned to either the Eth0 or Eth1 card, according to the Box Installation and System Configuration.



## IP to Web server

This is the IP address allocated on the TrafficShield security application unit for communicating with the Web server. This IP address is used by all Web applications. This IP address is usually an internal address. This address is disabled when the unit is in standby mode.

You can set both the IP to Web Server and the Service IP to the same address, if the Service IP addresses are attached to Eth0.

## Server IP

This is the IP address of the real Web server to which the TrafficShield security application forwards the requests.

## Trusted IP

An IP address authorized to send to the Web server extended HTTP methods such as PUT, DELETE, etc.

## Permanent IP

An IP address allocated to the TrafficShield security application unit that allows an Administrator to access the unit even when it is in standby mode.

One TrafficShield security application unit may have multiple Permanent IP addresses.

Permanent IP addresses may be assigned either to Eth0 or to Eth1 cards, depending on whether the Administrator intends to install and administer the unit internally or externally.

## Static Route

Add static routes, as required.

## Gateway

This is the default gateway for the TrafficShield security application unit.

## Alias IP

This optional IP address can be used for management purposes. This address is published only on the active unit. If the active unit fails, this address will be transferred to the Standby unit once it becomes active.

**◆ Note**

---

*The permanent IP and the Alias IP can be configured for the internal interface as well.*

## Installation procedure

This section explains how to configure a single unit and/or its standby unit after they have been physically connected to the network.

At this stage you will be asked to run a script that defines the minimal parameters needed by the TrafficShield Management Station (TSMS) to continue the installation via the user interface.

### **To install and configure a unit in the single-unit topology**

1. Connect a power cable to the TrafficShield security application unit.
2. Connect the TrafficShield security application unit to the network.

The TrafficShield security application supports two types of network configuration:

(Eth0 only) - A single network cable, plugged into the Eth0 card (port 1.1), connects the TrafficShield security application unit, Web server's internal network and service network. This option may be selected when there is no security need to physically separate the client-to-unit traffic from the unit-to-web server traffic.

Accordingly, the service IPs should be attached to Eth0 at the System Configuration step in the graphical user interface. See the Configuring the TrafficShield units section in Chapter 4.

(Eth0 and Eth1) - Two network cables, plugged into the Eth0 card (port 1.1) and Eth1 card (port 1.2) respectively. The Eth0 card connects the TrafficShield application unit to the Web server's internal network and to additional TrafficShield Application units. This option ensures a total separation between external and internal traffic. Accordingly, the service IPs should be attached to Eth1 at the System Configuration step in the user interface. See the Configuring the TrafficShield units section in Chapter 4.

3. Prepare a serial console terminal.  
This can be any PC with any serial console software installed on it.  
For example: Microsoft<sup>®</sup> Hyper terminal.

4. Attach a serial cable from the serial console terminal to the RS232 serial console port on the TrafficShield security application unit's front panel. Please see photograph below.



5. Launch your serial console software per the software manufacturer's instructions.
6. Configure your serial console software as follows:
  - baud rate (speed) of: 19200 bit per sec
  - Parity: Odd
  - Data: 8
  - stop Bit: 1
7. Log on to the TrafficShield security application unit using the following username and password:
  - User: root
  - Password: default
8. You can change the password using tools supplied by your operating system, or during the next step.
9. Type `/ts/install/tsconfig.pl` and hit Enter.

## Running tsconfig.pl for the Primary (Active) unit

The `/ts/install/tsconfig.pl` script will prompt you to enter the following parameters.

---

### ◆ Note

*All IPs and values displayed below are examples only. Some IP addresses entered during the installation process may have multiple instances. In such cases, the installation program allows you to enter one address. You can later add other instances, using TSMS.*

---

### ◆ Tip

*It is important to prepare all the required information before beginning the configuration.*

**Enter current system password:**

Enter the system password of the unit. This password has been delivered to you by the TrafficShield security application supplier. You must change it (in the next step) in order to ensure maximum security.

**Enter new password:**

Enter a new password for the unit. This replaces the root password with your own private and secure password.

**Re-enter new password:**

Re-enter the new password

**TrafficShield topology**

The system prompts you to choose a topology.

Type 1 for single unit topology, or 2 for External Load Balancer Topology (option 2 not supported in current version).

**Which type of unit would you like to configure?**

- (1) Single Unit system
- (2) External Load Balancer topology  
>1

Enter 1 to access the single unit configuration tool.

**Which type of unit would you like to configure?**

- (1) Single Unit system
- (2) Standby for Single Unit  
>1

Enter 1 to access the single unit configuration tool.

**The current system time is (12:37:52 06/01/2004). Do you want to change the system time? (y/n) [n]: y**

Enter Y if the date and time shown are not correct.

**Please enter the current date (mm/dd/yyyy):10/15/2003**

This and the next question appear if you entered Y in the previous question. Enter the current date in the format shown in the question.

**Please enter the current time (hh:mm:ss):13:38:50**

Enter the current time.

**The new system time will be (13:38:50 10/15/2003). Is this correct? (y/n) [y]:**

Confirm the new date and time by typing y.

Or type N to restart the date-time entry cycle.

**Please enter the TrafficShield private network [192.168.223.0]:**

Specify the unit's private network address (first 3 octets of the unit's IP address, followed by zero).

**Please complete TrafficShield private IP [192.168.223.X].**

Complete the unit's private IP address by entering the last octet.

**Would you like to set Permanent IP? (y/n) [n]: y**

Enter y if you want to define a permanent IP address for the unit.

**Enter Permanent IP: 192.168.1.237**

Enter the permanent IP address.

**Enter permanent IP Mask [255.255.255.0]:**

Enter the network IP mask for the permanent IP.

**Enter network interface (eth) [0, 1]**

Specify the network interface card through which the TrafficShield security application user will access the TrafficShield security application unit. Enter 0 or 1 for 1.1 (eth0) or 1.2 (eth1), respectively.

◆ **Tip**

---

*If you are only using one network connection, it must be connected to the 1.1 network port and you must type 0 here.*

**Would you like to set a static route for the permanent IP? (y/n) [y]:**

Enter y if you want to define a static route.

**Enter Destination Network:**

If you answered Y to the previous question, specify the network address of the internal network from where the permanent IP can be accessed.

**Enter Netmask [255.255.255.0]:**

Enter the network mask of the internal network's address.

**Enter Gateway:**

Enter the gateway address.

**Please enter the TrafficShield web administrator's access IP/Network (remote manager host):**

You activate the TrafficShield Management Station user interface through a Web browser from any PC on the network to which the unit is connected. Specify the IP address of the PC from which you will access TSMS in order to define policies. You can define the network as well.

**Please enter the Access IP/Network netmask [255.255.255.0]:**

Specify the network address and network mask for the Web administrator's access IP address.

**Please enter the initial TrafficShield Web administrator's username:**

Enter the user name to specify when accessing the TrafficShield Management Station using its Web interface.

**Please enter the initial TrafficShield Web administrator's password:**

Enter the password to specify when accessing the TrafficShield Management Station using its Web interface.

**Please confirm password:**

Re-enter the password.

**Please confirm the following settings:**

Examine the settings displayed. Enter **y** to confirm them or **N** to restart the configuration cycle.

**Would you like to apply these settings (y/n) [y]**

Enter **y** to apply the settings to the single unit.

To complete the single unit installation, please launch TSMS.  
See Chapter 3, Launching TSMS.

## Running tsconfig.pl for the Standby unit

The Standby unit **MUST** be configured in the TSMS application before running the tsconfig.pl script.

After configuring the Standby unit in TSMS, you must restart the single unit machine (the active machine).

Run the /ts/install/tsconfig.pl script on the standby unit.

**◆ Note**

*The Primary (Active) unit must be configured before you configure the standby unit.*

When you are asked to select the unit type from a list, select (2) Standby for single unit.

The procedure involves a shorter series of questions, as follows:

**Please enter the TrafficShield private network [192.168.223.0]:**

Specify the standby unit's private network address (first 3 octets of the unit's IP address, followed by zero).

**Please complete TrafficShield private IP [192.168.223.X]:1**

Complete the Standby unit's private IP address by entering the last octet of the unit's IP address in the private network.

**Would you like to set permanent IP? (y/n) [n]: y**

If you want to set a permanent IP address for the standby unit as well, enter **y**.

**Enter permanent IP: 192.168.1.237**

Enter the permanent IP address of the standby unit.

**Enter permanent IP mask**

Enter the network mask for the permanent IP of the standby unit.

**Enter network interface (eth)**

Specify the network interface card through which the TrafficShield security application user will access the TrafficShield security application unit. Enter 0 or 1 for 1.1 (eth0) or 1.2 (eth1), respectively.

◆ **Tip**

---

*If you are only using one network connection it must be connected to the 1.1 network port and you must type 0 here.*

**Would you like to set a static route for the permanent IP? (y/n) [y]:**

Enter **y** if you want to define a static route.

**Enter destination network:**

If you answered **y** to the previous question, specify the network address of the internal network from where the permanent IP can be accessed.

**Enter netmask:**

Enter the network mask of the internal network's address.

**Enter gateway:**

Enter the gateway address.

**Please confirm the following settings:**

Examine the settings displayed. Enter **y** to confirm them or **n** to restart the Standby unit configuration cycle.

**Would you like to apply these settings (y/n) [y]**

Enter **y** to apply the settings to the standby unit.

The next step consists of configuring the TrafficShield security application unit and creating and configuring the Web applications.





# 3

---

---

## Launching TSMS

---

---

- Accessing TSMS
- Using the TrafficShield Wizards



## Accessing TSMS

This chapter explains how to access the TrafficShield security application and begin to navigate to the configuration screens.

You access the TrafficShield security application through the TrafficShield Management Station, the TSMS.

### To access TSMS

1. On a PC from which the TrafficShield security application unit can be reached, use your Web browser to connect to the TrafficShield management portal. Point the browser to the TrafficShield security application Private or Permanent IP specified during the initial configuration script. Use custom SSL port 1043:  
<https://ip.add.re.ss:1043>  
 A security alert message may appear.



2. Click Yes to continue. The logon page opens.



3. Enter the TrafficShield Web Administrator's user name and password that you defined earlier, and click the Login button.

## Using the TrafficShield wizards

The next step consists of configuring the F5 Networks TrafficShield security application and creating and configuring the Web applications. TrafficShield Management Station (TSMS) offers a wizard that you can use to enter the configuration parameters

There are various TrafficShield wizards available. As each TrafficShield wizard works a little differently, please carefully read the following overview of the different workflows.

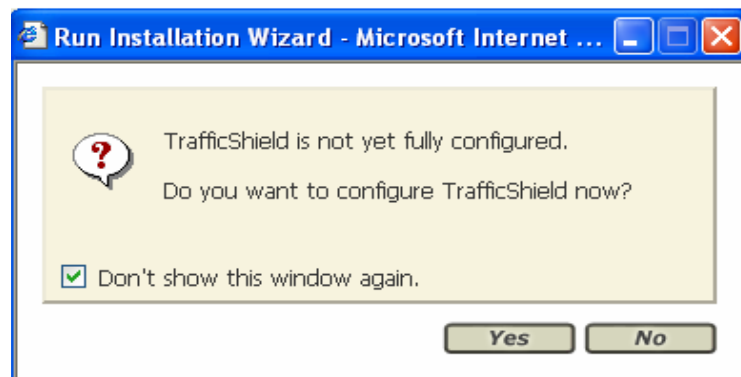
### The TrafficShield Unit Configuration Wizard:

**Purpose:**

The Wizard allows you to further configure the unit with additional information.


**Access:**

**First-time** access: When you access TSMS for the first time or after re-installing the unit software, the wizard starts automatically and asks you whether you want to configure TrafficShield security application unit now (if this is not your first access, the monitoring page opens).



Click Yes to start the wizard or if you do not want to run the wizard now, click No to stop it.

**Regular** access: The next time you access TSMS, the Monitoring tool is selected by default. To access the wizard at any time, select Administration > Configuration > System and click the

“Run TrafficShield installation wizard”  icon. See figure below.



**General:**

The actual wizard windows displayed are almost identical to the manually accessible windows of the TrafficShield security application unit configuration tool. See Chapter 4, for explanations on the screens and fields.

## The Web Application Configuration Wizard:

**Purpose:**

Allows you to create and edit records for the Web applications protected by TrafficShield security application.

**Access:**

In the Administration > Configuration > Web Applications tab, click the **Add** button.

**General:**

The Web Application Configuration Wizard contains a subset of all the fields displayed when working in edit mode. Therefore, the wizard is explained separately from the edit mode screens in this document.

## The Crawler Configuration Wizard

**Purpose:**

Guides you through the basic configuration of the Crawler settings that control the TrafficShield security application actions.

**Access:**

If you use the Web Application Wizard, at the end you are asked if you would like to run the Crawler Wizard. If you choose this option, the Wizard is opened automatically

Or

In the Policy Management > Policy Properties > Build Tools Section click the  icon.

**General:**

More details on how and when to use the Crawler Wizard can be found in the Policy management user manual, in the chapter on creating a policy.

## Installing the Package Wizard

**Purpose:**

Allows the user to upgrade the provided TrafficShield security application software packages.

**Access:**

In the Administration > Maintenance > Upgrades tab choose the unit and then click Show Packages to display the list of the currently installed packages on the unit.

Click the Install Package button to activate the new Package installation process.

**General:**

This wizard guides the user through the installation process. For more details, see Chapter 6, *Administration*, in this manual.



# 4

---

---

## Configuration

---

---

- Configuring the TrafficShield units
- Licensing





## Configuring the TrafficShield units

The installation process is followed by a TrafficShield security application unit configuration stage. You must completely define at least one unit to be able to navigate to other areas in the application.

### To access single-unit configuration parameters:

1. If you are not already connected to the TSMS application, access TSMS through a Web browser, from a PC connected to the network where the unit resides.
2. Click the Administration button.
3. On the navigation panel, under Configuration, click the System tab.

**System Topology: Single Unit** Update TrafficShield

**TSMS and SHIELD**

Attach Service IPs to Eth1

**Units** Add Edit Remove

Select	Unit Id	Private IP	IP to Web-Server	Management	Core
<input type="checkbox"/>	00:00:00:00:00:00	192.168.117.1	192.168.52.117	TSMS	✓

**Route Table** Add Edit Remove

Select	Network	Netmask	Gateway
<input type="checkbox"/>	192.168.4.0	255.255.255.0	192.168.52.254

**IP Aliases** Add Edit Remove

Select	IP Alias	Mask	Interface
No entries found			

4. Select the Attach service IPs to ETH1 option if you want to channel the service traffic to the second network (eth1) card as well.
5. Enter the information described in the subsequent sections of this chapter. After entering the information, click the Update TrafficShield button to save the information to the TrafficShield tables. You may be required to restart the TrafficShield unit.

## Units

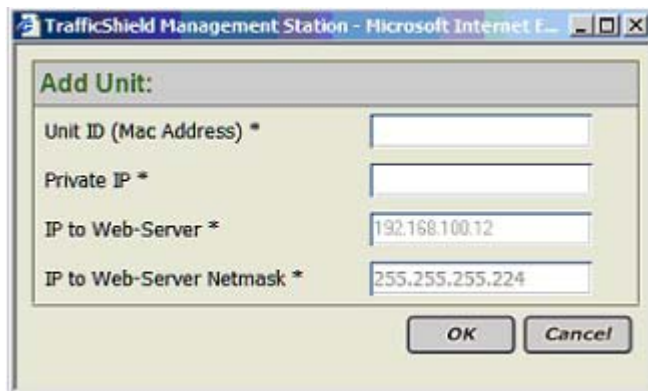
Use the Units section:

- To add the IP to Web Server address, the network mask, and the gateway for the TrafficShield security application unit, if you didn't define it via the TrafficShield security application unit Configuration Wizard.

- To add the MAC Address and the Private IP for the Standby unit defined during the installation process.

### To add the Standby unit

1. In the Units section, click the Add button.  
The Add Unit dialog box opens.



2. Enter the unit's ID (MAC address) and its private IP address.  
Both the main (active) and Standby units use the same IP address
3. Click OK.

## Route Table

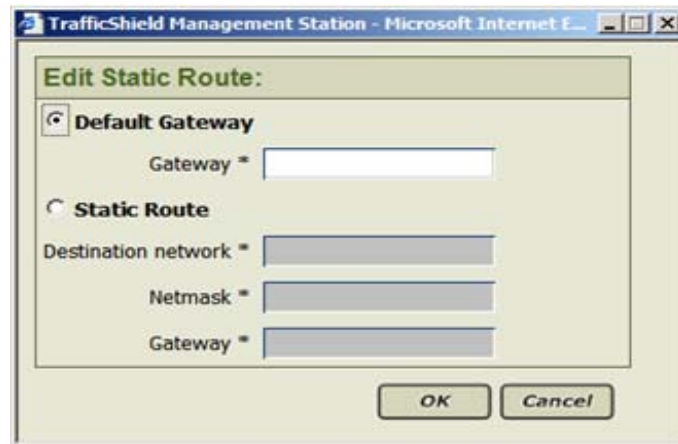
If a gateway different from the default gateway exists in your network, use the Static Route feature to specify the gateway details. TrafficShield security application looks first for the static route and uses the default gateway if it does not find one.

The procedure described below allows you to add more routes.

### To enter or modify static routes:

1. In the Route Table section, click the Add button or select the unit by checking the check box located to the left of the relevant unit and click the Edit button.

The Add or Edit Static Route dialog box opens.



2. Select the Default Gateway or Status Route.
3. You can handle incoming requests either via the default gateway or via a static route of your choice.
  - a) If you chose to accept requests via the default gateway, in the Gateway field, enter its IP address.
  - b) If you chose to accept requests via another route, enter the following information:
    - Destination Network:** Specify the destination network address which the gateway is used for.
    - Gateway:** Specify the gateway's IP address.
    - Mask:** Specify the network mask.
4. Click OK.

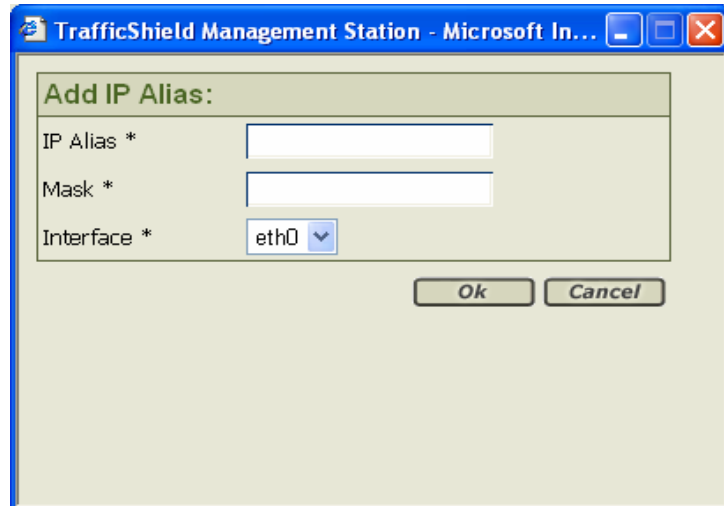
The static route definition appears on the main page.
5. Repeat the above procedure for all the static routes you intend to use.
6. When you are done, click the Update TrafficShield button.

## IP Aliases

The IP aliases section is designed to assign additional IP addresses to one or both of the network cards, for management purposes. For example: a user desiring to access the TSMS user interface using an alias or directly by SSH.

### To assign IP addresses to the network card:

1. In the IP Aliases section, click the Add button.  
The Add IP Alias dialog box opens.



2. Enter the following information:

**IP Alias:** Specify the IP address.

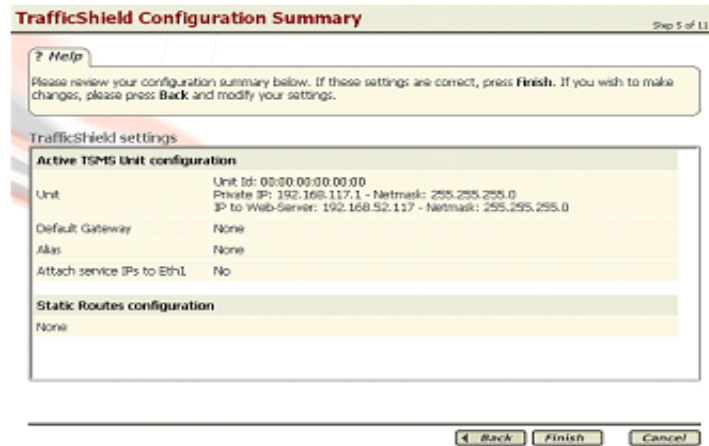
**Mask:** Specify the network mask.

**Interface:** Select the network card to which you want to assign this address.

3. Click OK.  
The IP alias definition appears on the main page.
4. Repeat the above procedure for all the aliases you intend to use.
5. When you are done, click the Update TrafficShield button.

If you configured your unit using the Configuration Wizard, the Configure Standby machine screen will appear.

6. Select the Configure Standby Machine option (radio button).  
The Summary screen appears.



7. Click Finish.  
The Return to TSMS screen appears.
8. You can return to TSMS, or if you choose the Configure Web Application button, the New Web Application Wizard will start automatically.

## Licensing

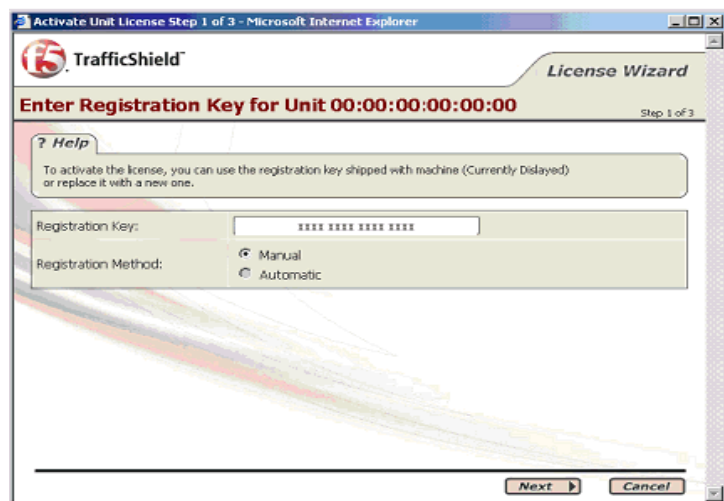
The TrafficShield security application is delivered to you with a license that you should activate before you allow users to access the application for browsing. External users can visit and browse through the Web application only after the license has been activated.

You need to activate the license also after changing the TrafficShield security application, for example, after upgrading it.

When you acquire a TrafficShield security application for the first time, the TrafficShield security application units are delivered to you with a registration key recorded in them, and you do not need to obtain one. In any other case where the license should be updated, you need to obtain the registration key before you perform the procedure explained below.

### To activate the license:

1. Select the Administration button at the top of the TSMS window.
2. In the Maintenance menu, select Licensing.  
A list of the installed TrafficShield security application units appears. You need to license each unit separately.
3. Click the Activate License button of the unit you want.  
This starts the licensing wizard and opens the Enter Registration Key window.



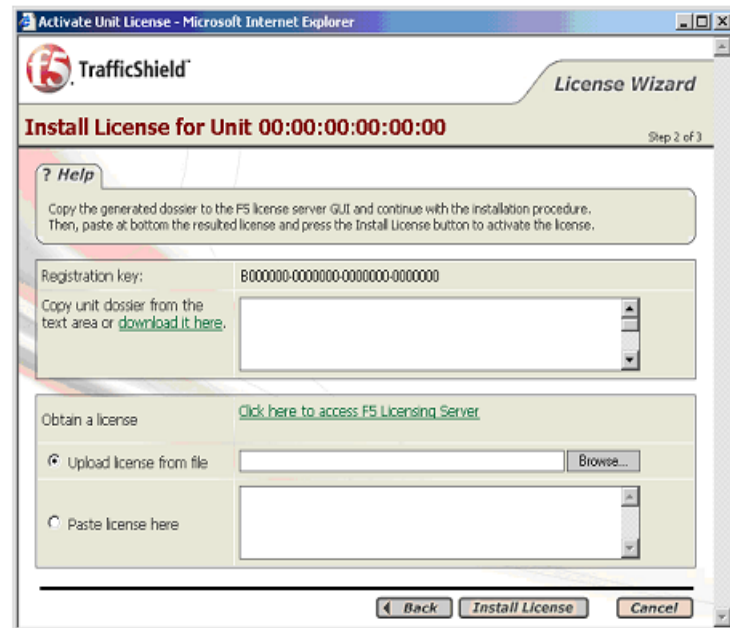
The Registration Key field displays the key currently stored in the selected TrafficShield security application unit.

You have two options: Automatic or Manual.

4. If you select Automatic, you will be asked to supply your registration key and after clicking next, the system will download the license automatically from the F5 server.

5. If you select Manual, do one of the following:
  - If this is your first licensing, click the Next button.
  - If you are performing the licensing operation as a result of system changes that require a new registration key, enter the key in this field, and click Next.

The Install License for Unit window appears.



This window displays a dossier that you need to save on your computer. You will use it in subsequent steps.

**Note:** The dossier is an encryption of a string containing a set of physical hardware elements of the machine.

6. Decide how you want to save the dossier information. You have two choices:
  - To save the dossier information in a file in order to load in the F5 License Activation Screen:
    - a) Click the “download it here” link.  
A “save as” box opens.
    - b) Select a folder and enter a filename indicating where to save the dossier. This returns you to the Install License for Unit window.
  - To copy the dossier information directly to the F5 license activation screen:
    - a) Copy the dossier information.

7. Click the link “Click here to access F5 Licensing Server”. This opens a new browser window and connects you to the F5 licensing server.

**Activate License (BIG-IP 9.x, FirePass 5.x and TrafficShield)**

Use this page to submit a BIG-IP V9.x, FirePass V5.0 or TrafficShield dossier for license activation. If you are attempting to activate a license for BIG-IP V4.x or iSMAN, please click [here](#).

To activate your product you will need your product dossier.

Enter your dossier

or

Select your dossier file

Use this License Activation Page to activate licenses for BIG-IP version 9.0 or greater or FirePass version 5.0 or greater. If you are not activating a license for the versions mentioned above, please go to [license.f5.com](http://license.f5.com) for more options.

8. Save your information in the way consistent with your previous choice:
  - If you created a file, use the browser button to load the file.
  - If you copied it, then paste the dossier information in the dossier window.
9. Choose Next to continue. The dossier information is processed and the following F5 Networks licensing screen is displayed:

```
Download license
Platform ID : TrafficShield
Appliance SN : bip000000a
#
# Outbound License Dossier Validation
#
Dossier :
oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
dddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
#
# Outbound License Authorization Signature
#
Authorization :
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
#
# -----
# Copyright 1996-2004, F5 Networks, Inc.
# All rights reserved.
# -----
```



10. Copy the full form to the clipboard, or click the download button to download a copy of the license file.
11. Return to the TrafficShield security application's Activate unit license window.

**TrafficShield™ License Wizard**  
**Install License for Unit 00:00:00:00:00** Step 2 of 3

**? Help**  
 Copy the generated dossier to the FS license server GUI and continue with the installation procedure. Then, paste at bottom the resulted license and press the Install License button to activate the license.

Registration key: 000000-000000-000000-000000  
 Copy unit dossier from the text area or [download it here](#).

Obtain a license [Click here to access FS Licensing Server](#)

Upload license from file

Paste license here

12. You must now enter the license information received from F5.
  - If you saved the information in a file, choose the “Upload license from file” radio button, click the Browse button and select the license file created by the F5 licensing server.
  - If you copied the file to the Clipboard, select the “Paste license here” radio button and paste the contents of the license file.
13. Click the *Install License* button.  
 The Activate License for Unit window appears.



14. Click the Back button to return to previous step.
15. Click Finish to close the window.

### **How to view License Information**

You can view the details of a specific license by clicking on the Active link in the Units list.

Click on the “Click here to view full license” link to display full details of the license.



# 5

---

---

## Web Applications

---

---

- Defining a new Web Application
- Editing an existing Web Application



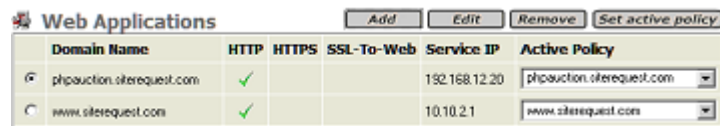
## Defining a new Web Application

This chapter explains how to create a new Web application definition in the F5® Networks TrafficShield™ Management Station (TSMS), how to configure it, maintain it and remove existing Web Applications definitions.

TrafficShield™ security application will only allow traffic routed through it to known Web applications. In other words, each Web application sitting behind the TrafficShield security application in the network must be defined individually.

### To define a new Web application:

1. At the top of the TSMS page, select **Administration > Configuration > Web Applications**.  
Web Application is selected by default.
2. If this is not the first time you are defining a Web application, a list of existing Web application definitions will be displayed.



Domain Name	HTTP	HTTPS	SSL-To-Web	Service IP	Active Policy
phpauction.siterequest.com	✓			192.168.12.20	phpauction.siterequest.com
www.siterequest.com	✓			10.10.2.1	www.siterequest.com

3. Click the **Add** button to open the Web Application Wizard
4. Enter the relevant information. See **Step 1: Web Application Name**, on page 5-2.  
The Wizard will ask you at the end if you would like to run the Crawler Wizard or to return to the TSMS.

### ◆ Note

*Manually creating a web application creates a default policy for the web application. Click the Set Active Policy button located in the Administration > Configuration > Web Application Window.*

## Web Application Wizard

All the information entered into the Wizard's fields of the various screens are for demonstration purposes only.

### Step I: Web Application Name

The screenshot shows a wizard window titled "Web Application Wizard" with the TrafficShield logo. The current step is "Web Application Name" (Step 1 of 3). A help box contains the following text: "Enter the **Fully Qualified Domain Name** of the Web application as defined in your organization (e.g., yourcompany.com). The Web application record you create now will appear in the Administration - Web Applications tab when the wizard concludes its operation. If you TrafficShield installation protects multiple applications, you can define additional one by running the wizard again or through the Administration - Web Applications option." Below the help box is a section labeled "FQDN" with a text input field containing the label "Fully Qualified Domain Name: \*". At the bottom right, there are "Next" and "Cancel" buttons.

#### **FQDN Fully Qualified Domain Name**

Enter the fully qualified domain name of the Web application as defined in your organization (e.g., www.siterequest.com).

- Click **Next** to continue.

## Step 2: Service IP

**TrafficShield™** Web Application Wizard

**Service IP** Step 2 of 9

**? Help**

TrafficShield intercepts incoming requests by taking over the IP address of the Web server. Specify the current IP address and network mask of your Web server. Normally, this is the IP address which is mapped to the DNS 'A' record of the Web server.

**Service IP**

Service IP: \*

Service IP Netmask: \*

### Service IP, Service IP Netmask

Specify the Web Application IP address and the corresponding network mask.

Click **Back** to go back to the previous step.

-Or-

Click **Next** to continue.

## Step 3: HTTP Settings

**TrafficShield** Web Application Wizard

### HTTP Settings

 Step 3 of 9

? **Help**

To allow access to the Web application using HTTP, check the **Use HTTP** box and fill in the other details.

**Use HTTP**

**Server properties**

Web Server IP: *	<input type="text"/>
Web Server Port: *	<input type="text" value="80"/>
Max Sessions: *	<input type="text" value="1000"/>
Verification Object: *	<input type="text"/>

◀ Back Next ▶ Cancel

### Use HTTP

To allow HTTP access to the Web application, select the Use HTTP option and enter the appropriate information. You need to configure at least one protocol: HTTP or HTTPS (next step).

### Server IP, Server Port

Specify the Web server's IP address and port. The address is used for communications with the TrafficShield unit.

Specify the maximum number of simultaneous sessions TrafficShield security application can open in its interactions with the Web server.

### Max. Sessions

The number of sessions that can be opened, and therefore the number of visitors that can be served simultaneously, depends on the capacity of the Web server.

### Number of Visitors

The number of visitors that can be served simultaneously refers to the actual number of established connections, while in reality there is a greater number of connections in the process being established or closed. The maximum session should reflect the total of all three session statuses.



◆ **Tip**

*If you are not familiar with your server configuration, please consult your system administrator about the maximum number of simultaneous clients, connection time-out definitions, etc.*

**Verification Object**

This is an optional field that enables the user to verify that the TrafficShield security application is responding correctly to a pre-defined test object.

Click **Back**, to go back to the previous step.

-Or-

Click **Next** to continue.

## Step 4: HTTPS Settings

**TrafficShield™** Web Application Wizard

**HTTPS Settings** Step 4 of 9

? **Help**

To allow access to the Web application using HTTPS, check the **Use HTTPS** box and fill in the other details.

**Use HTTPS**

**Server properties**

Web Server IP: \* 192.168.4.100 Max Sessions: \* 1000

Web Server Port: \* 443  Keep SSL connection to web-server

💡 Verification Object:

**SSL Files**

Type: PEM **Upload**

Key: \* N/A  Browse...

Cert: \* N/A  Browse...

**Use SSL Password**

Password:

Confirm Password:

**Back** **Next** **Cancel**

**Use HTTPS**

To allow HTTPS access to the Web application, select this box. All the fields in the section become enabled.

◆ **Note**

*You need to configure at least one protocol: HTTP (see previous step) or HTTPS.*

**Server IP, Server Port**

Specify the Web server's internal IP address and port. The address is used for internal communications with TrafficShield security application.

**Max. Sessions**

Specify the maximum number of simultaneous sessions TrafficShield security application can open in its interactions with the Web server. The number of sessions that can be opened, and therefore the number of visitors that can be served simultaneously, depends on the capacity of the Web server.

◆ **Note**

*“The number of visitors that can be served simultaneously” refers to the actual number of established connections, while in reality there is a greater number of connections in the process being established or being closed. The maximum session should reflect the total of all three session statuses.*

◆ **Tip**

*If you are not familiar with your server configuration, please consult your system administrator about the maximum number of simultaneous clients, connection time-out definitions, etc.*

**Keep SSL connection to web-server**

Selecting this box will cause TrafficShield security application to maintain the SSL connections to the Web server. If you choose not to enable this option, TrafficShield security application will decrypt the SSL traffic and will use HTTP to send the requests to the Web server.

◆ **Note**

*Requests will flow to the server quicker without encryption.*

**Verification Object**

This is an optional field that enables the user to verify that the TrafficShield security application is responding correctly to a pre-defined test object.

**Key and Certificate Files**

Click the Browse button and select the files that hold the SSL key and certificate. Then, click the Upload button. The files should be in PEM format.

**Use SSL Password checkbox**

If the SSL key file is password-protected, check the Use SSL Password check box.

**Password**

Specify the password for key file.

**Confirm Password**

Type the password again for confirmation.

Click **Back**, to go back to the previous step.

-Or-

Click **Next** to continue.

**Step 5: Aliases**

**TrafficShield™** Web Application Wizard

**Aliases** Step 5 of 9

**? Help**

If the Web application uses several Web application names (or several DNS CNAME records), all of them pointing to the Web application you are defining now (as specified in Fully Qualified Domain Name earlier), in **Domain Name** enter the alias.

**Aliases**

No.	Domain Name
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>

**◆ Note**

*You must add the Service IP Address if you want to access the site via the IP address instead of the host name.*

Enter a new alias if the Web application uses several Web application names (or several DNS CNAME records), all of them pointing to the Web application you are defining now (as specified in the Fully Qualified Domain Name earlier).

You need to define in advance all of the aliases that might appear in requests addressed to this Web application. TrafficShield security application will block requests containing undefined destinations.

◆ **Tip**

*If you wish to allow access to the Web application by specifying its actual IP address, define the IP address as an alias by entering it in the Domain Name box.*

Click **Back**, to back go to the previous step, or **Next** to continue.

## Step 6: Create Policy

The screenshot shows the TrafficShield Web Application Wizard at Step 6 of 9, titled "Create Policy". The interface includes a "TrafficShield" logo and the wizard title. A help box contains the following text: "A Web application must have a policy as soon as you exit this wizard. In this page you establish a preliminary policy by letting the wizard create a **Default Policy** or by importing a previously exported policy." Below the help box, there are two radio button options: "Create default policy." (which is selected) and "Import existing policy: N/A" (with a "Browse..." button and an "Upload" button). At the bottom of the wizard, there are three buttons: "Back", "Next", and "Cancel".

A web application must have a policy as soon as you exit this wizard. In this page you will establish a preliminary policy by letting the wizard create a Default Policy or by importing a previously exported policy.

Click **Back**, to go to the previous step, or **Next** to continue.

## Step 7: Web Application configuration summary

The screenshot shows the 'Web Application Wizard' interface for TrafficShield. The title bar includes the TrafficShield logo and the text 'Web Application Wizard'. Below the title bar, the main heading is 'Web Application configuration summary' with 'Step 7 of 9' on the right. A yellow box with a question mark icon and the text '? Help' contains the message: 'This page summarizes the information you have entered so far.' Below this is a section titled 'Web settings' which contains a table of configuration details. At the bottom of the window are three buttons: 'Back', 'Finish', and 'Cancel'.

Web Application Name	
FQDN	www.php.com

Service IP	
Service IP	IP: 192.168.51.52 - Netmask: 255.255.255.0

HTTP Settings	
Use HTTP	Yes
Server IP	192.168.4.100
Server port	80
Max sessions	1000
Verification Object	None

Upon completion of the wizard configuration, the Web Application configuration summary window is displayed.

Review this information and proceed in either way:

- Click **Back** to go back to the previous step.
- Click **Cancel** to exit without saving.
- Click **Finish** button to save and exit the Wizard.

If you clicked Finish, the following window appears.



This screen offers 2 options:

**Return to TSMS** - Returns to the TSMS window.

**Configure Crawler** - Automatically opens the Crawler configuration Wizard.

-Or-

Click **Close** to exit the wizard.

◆ **Tip**

---

*Once you have completed this step and returned to TSMS, activate your default policy by clicking the Set active Policy button located in the Administration > Configuration > Web Application Window.*

# Editing an existing Web Application

## Service Properties

The Service Properties section is designed to specify the Web application's domain name and IP address.

Service Properties	
Fully Qualified Domain Name: *	<input type="text" value="www.php.com"/>
Service IP: *	<input type="text" value="192.168.51.52"/>
Service IP Netmask: *	<input type="text" value="255.255.255.0"/>
Log All Requests:	<input type="checkbox"/>

Enter the following information:

### Fully Qualified Domain Name

Enter the fully qualified domain name of the Web application as defined in your organization (e.g., www.siterequest.com).

### Service IP, Service IP Netmask

Specify the Web Application IP address and the corresponding network mask.

### ◆ Note

*The Web Application IP address is the TSMS unit's service IP.*


### Log All Requests

If you check this button, all incoming requests, including the valid ones, are posted to the Forensics - Illegal requests section (Policy Management tab).

The valid requests are used to fill in the blanks when investigating gaps between illegal requests. Both types of requests can be filtered out in Forensics. The valid requests are marked with a green checkmark and the invalid requests are marked with a red X.

## HTTP Settings

Use this section if the Web application can be accessed using HTTP.

HTTP Settings			
<input checked="" type="checkbox"/> Use HTTP			
Web Server IP: *	<input type="text" value="192.168.4.100"/>	Web Server Port: *	<input type="text" value="80"/>
Max Sessions: *	<input type="text" value="1000"/>	 Verification Object:	<input type="text"/>

Enter the following information:

### Use HTTP

To allow HTTP access to the Web application, check this box and enter the information described below. You need to configure at least one protocol: HTTP or HTTPS (next step).

### Server IP, Server Port

Specify the Web server's IP address and port. The address is used for communications with the TrafficShield security application.

### Max. Sessions

Specify the maximum number of simultaneous sessions TrafficShield security application can open in its interactions with the Web server. The number of sessions that can be opened, and therefore the number of visitors that can be served simultaneously depends on the capacity of the Web server.

### ◆ Note

*“The number of visitors that can be served simultaneously” mentioned above, refers to the actual number of established connections, while in reality there is a greater number of connections in the process being established or being closed. The maximum session should reflect the total of all three session statuses.*

### ◆ Tip

*If you are not familiar with your server configuration, you need to consult with your system administrator about the maximum number of simultaneous clients, connection time-out definitions, etc.*

### Verification Object

This is an optional field that enables the user to verify that the TrafficShield security application is responding correctly to a pre-defined test object.




## HTTPS Settings

Use this section if the Web application can be accessed using HTTPS.

### HTTPS Settings

Use HTTPS

#### Server Parameters

Web Server IP: *	<input type="text" value="192.168.4.100"/>	<input checked="" type="checkbox"/> Keep SSL Connection to Web-Server
Max Sessions: *	<input type="text" value="1000"/>	Web Server Port: * <input type="text" value="442"/>
 Verification Object:	<input type="text"/>	

### Use HTTPS

To allow HTTPS access to the Web application, select this box and the section becomes enabled.

#### ◆ Note

*You need to configure at least one protocol: HTTP (previous step) or HTTPS.*

### Server IP, Server Port

Specify the Web server's internal IP address and port. The address is used for internal communications with TrafficShield security application.

### Max. Sessions

Specify the maximum number of simultaneous sessions TrafficShield security application can open in its interactions with the Web server. The number of sessions that can be opened, and therefore the number of visitors that can be served simultaneously, depends on the capacity of the Web server.

#### ◆ Note

*“The number of visitors that can be served simultaneously” mentioned above, refers to the actual number of established connections, while in reality there is a greater number of connections in the process being established or being closed. The maximum session should reflect the total of all three session statuses.*

#### ◆ Tip

*If you are not familiar with your server configuration, you need to consult with your system administrator about the maximum number of simultaneous clients, connection time-out definitions, etc.*

### Keep SSL connection to web-server

Checking this box will cause TrafficShield security application to maintain SSL connections to the Web server. If you choose not to enable this option, TrafficShield security application will decrypt the SSL traffic and will use HTTP requests to access the Web server.

**◆ Note**

*Requests will flow to the server more quickly without encryption.*

### Server Certificate

Server Certificate	
Key File: * N/A	<input type="text"/> <input type="button" value="Browse..."/>
Certificate File: * N/A	<input type="text"/> <input type="button" value="Browse..."/>
<input checked="" type="checkbox"/> Use SSL Password	
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>

Enter the following information:

#### Key and Certificate Files

Click the **Browse** button and select the files that hold the SSL key and certificate. Then, click the **Upload** button. The files should be in XSO9 format.

#### Use SSL Password checkbox

If the SSL key file is password-protected, check the Use SSL Password check box.

#### Password

Specify the password for key file.


#### Confirm Password

Type password again for confirmation.

## Client Certificate

If application end-users are required to present a certificate when accessing the Web application, you will need to complete this information in the Client Certificate Window.

**Client Certificate**

 Verify Client Certificate

CA Certificate File: \* N/A

Revocation File: N/A

Chain Verification Depth:

Verify Fail if no Peer Certificate.

Verify Only Once.

Enter the following information:

### Verify Client Certificate

Select the **Verify Client Certificate** check box to instruct TrafficShield security application to request Client certificate information.

### CA Certificate File

Browse to select the CA (Certificate Authority) certificate to verify client certificates and then click the Upload button.

### Revocation File

Browse to select the appropriate client's certificate revocation file, if applicable, and then click the Upload button. You can remove the revocation file by clicking the Remove button.

### Chain Verification Depth

The chain verification depth is used to define the level of CA verification required to verify the authenticity of the CA File.

### Verify Fail if no Peer Certificate

Check this check box to terminate the SSL handshake if no client certificate was provided.

### Verify Only Once

Check this check box to verify the client certificate only during the initial handshake. If this box is not checked, client certificate verification is performed for each request.

### ◆ Note

*We highly recommended that you check the "Verify Fail if no Peer Certificate" check box to ensure SSL handshake termination if no client certificate was provided; the client may use SSLv2 or SSLv3 versions.*

## Additional Aliases

This step is designed to define aliases for the current application.

Click the Add button to open a new row, and enter the following information.

Check the check box and click the Remove button to remove the Alias from TrafficShield security application.

---

**◆ Note**

*You must add the Service IP Address if you wish to be able to access the site via the IP address instead of the host name.*

Enter a new alias if the Web application uses several Web application names (or several DNS CNAME records), all of them pointing to the Web application you are defining now (as specified in Fully Qualified Domain Name earlier).

You need to define in advance all of the aliases that might appear in requests addressed to this Web application. TrafficShield security application will block requests containing undefined destinations.

---

**◆ Tip**

*If you wish to allow access to the Web application by specifying its actual IP address, define the IP address as an alias by entering it in the Domain Name box.*

## Trusted IPs for Extended Methods

Use this section to specify source IP addresses that are allowed to send requests containing extended HTTP methods, such as PUT or DELETE.

No.	Administrator IP
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>

---



# 6

---

---

## Administration

---

---

- Users
- Alerts
- Defaults
- System
- Upgrades
- Backup
- Permanent IP Addresses
- Downloads
- Support tools



# Users

This chapter describes administrative operations such as defining additional users, backups, downloading helpful utilities, upgrade of the software version, etc. All of the subjects discussed here can be found under the Administration Tab.

During the installation stage you were asked to define the TSMS Administrator as the initial super user. It is possible to add additional users who are authorized to access the TrafficShield security application and back up TrafficShield data.

## To add users

1. Select the **Administration** button.
2. In the **Configuration** menu, select the **Users** tab.  
The Users page appears.



3. Click **Add**.  
The Add User page opens.

The screenshot shows the 'Add User' page. At the top right, it says 'Current User: root Version: 3.1.1.24'. There are 'Add' and 'Cancel' buttons. The form fields are:

- Username: \*
- Password: \*
- Confirm Password: \*
- Group: \* (dropdown menu showing 'Administrator')
- Web Application: \* (dropdown menu showing 'All Web Applications')
- Access IP: \* (with a 'Remove' button)
- Access Network: \* (with 'Add' button)
- Active User:
- Full Name:
- Email:
- Phone:

On the right side, there are radio buttons for 'Access IP' (selected) and 'Access Network'. Below 'Access IP' are fields for 'IP:'. Below 'Access Network' are fields for 'Network:' and 'Netmask:'.

4. In the **Username** field, enter the name that the user should specify when accessing TSMS.
5. In the **Password** field, enter the password that the user should specify when accessing TSMS.

6. In the **Confirm Password** field, enter the password again.
7. In the **Group** field, select the group to which this user belongs.  
The group determines the operations that this user will be allowed to perform in the TrafficShield security application.

The following table describes the attributes of each group.

User Type	Authorization
Administrator	The Administrator has access to all Web applications defined in TSMS and can perform all operations in TSMS.
Web Application	AdministratorAccess only to the Web Application. This user can only create additional users for his allowed Web Application. The assignment is made in the Web Application field.
Policy Editor	Access to the Policy Management tool only within the context of the assigned application. Currently this user can access any policy of any web application. The user cannot view the Administration and Monitoring tabs.
Monitoring	Access to the Monitoring tool only. Users in this group can only view data.

8. In the Web Application field, select the Web application that this user will be authorized to access.  
Each user may access one application. To allow a user to access more than one Web application, define a separate user record for each.  
This field is not accessible if the user group is Administrator, as administrators have access to all applications.
9. In the **Access IP** field, specify the IP addresses of the computers from which this user is entitled to access TSMS. You can specify a single IP address or a network address.
10. Clear the **Active User** box to withdraw this user's access permissions without deleting the user record.  
Select the check box again to re-enable the user.
11. In the **Full Name**, **E-mail** and **Phone** fields, enter the full name, e-mail address and the telephone number of this user.
12. To complete the process of adding a user, do one of the following:
  - a) To allow access from individual IP addresses, select the Access IP radio button.



- b) To allow access from any IP address in a network, select the Access Network radio button.
13. Enter the IP address or the network address.
14. Click the **Add** button.  
The address moves to the box on the left.  
*Note: You can remove an address by selecting it in the left box and clicking the Remove button.*
15. Repeat the procedure for all relevant addresses.
16. Click the **Add** button. This closes the Add User page. The user record appears in the main page.
17. Click the **Update TrafficShield** button.

# Alerts

The alerts feature allows you to collect events and to send them to SNMP, Syslog. The TrafficShield security application Alerts mechanism can collect events of different types.

## To collect alerts

1. Select the Administration button.
2. In the Configuration menu, select Alerts.  
The Alerts page opens.
3. Examine the sections to see the types of alerts that your version of the TrafficShield security application collects. The procedure is identical in all cases; only the destination server parameters are different.



4. Click the Add button in a section.  
The "Add SNMP" box opens.



- 
5. Select the types of events to capture by checking one or more of the options described below.

<b>Option</b>	<b>Collects</b>
Security	Events identified as attacks.
User	Operations performed by TSMS users. For example, logging in to TSMS is a user event.
TrafficShield System	Events related to operations at system level. For example, rebooting units is a system event.
TrafficShield Syslog	Events registered at the OS system log.

6. Enter the server IP address relating to the server that will receive the events.
7. If necessary, repeat the operation to create alert collection records that combine different types of alerts and/or send alerts to different servers.
8. Click the “Update TrafficShield” button.

## Defaults

### Negative Regular Expressions Policy Defaults

TrafficShield security application policies use expressions to check the existence or absence of certain text strings in incoming requests as a way of identifying attacks. For example, you can use a regular expression to detect a suspicious string in a URI included in a request.

The expressions are “negative” in that requests that do meet the expression's requirements are blocked.

The use of negative regular expressions involves the following stages:

1. Create a pool of regular expressions.
2. Apply the regular expression to the request component it is designed to check (e.g., URI, header).
3. Use the regular expression in the policy.

The regular expressions become active only after you assign them to policies. The sections that follow explain how to build the pool of expressions and how to associate them with request elements they are designed to check. For details on how to actually use the regular expressions in a policy, see the Security Policy User Manual.

### Creating a Pool of Expressions

When you create an expression it goes to a pool of expressions. Subsequently, you can select expressions from the pool and assign them to various application elements.

#### To create a regular expression

1. Click the **Administration** button.
2. On the navigation panel, under Configuration, select the Defaults tab.

The regular expressions page opens, listing any expressions you may have defined previously.

RegExp Pool			
<input type="checkbox"/>	Used	RegExp Name	Description
No entries found			

Negative RegExp Policy Defaults		
<input type="checkbox"/>	RegExp Name	Apply to
No entries found		

- In RegExp Pool, click the **Add** button.  
The Add RegExp page opens.

- In RegExp Name, enter a name that will help you identify the regular expressions when creating policies.
- In RegExp, type the expression by following the standard Regular Expression syntax.
- In Description, optionally type a few words that describe the expression.
- Click the Save button.  
The regular expression definition appears on the main page.
- Repeat the above procedure for all the expressions you intend to use.

## Assigning Expressions

Regular expressions residing in the pool can be used to check various strings such as URIs, or the contents of the request headers. The next step is to determine what each of the expressions included in the pool is for.

### To assign an expression to an application element

- Click the **Administration** button.
- On the navigation panel, under Configuration, select **Defaults**.
- In Negative RegExp Policy Defaults, click the **Add** button.  
The Add Negative RegExp page opens.

- In RegExp Name select the name of the regular expression you want to assign to an application element.  
The drop-down list displays the regular expressions currently included in the pool.

5. In Apply To, select where to apply the expression.

The options are:

<b>Option</b>	<b>Applies the regular expression to</b>
URI	The URI segment of the request.
Server response data	The response returned from the Web server.
Header value	The request's HTTP header.
Key-value pairs	The parameters and values included in the request. A parameter and its value follow the URI, separated by "?". Example: ...?name=Steve.

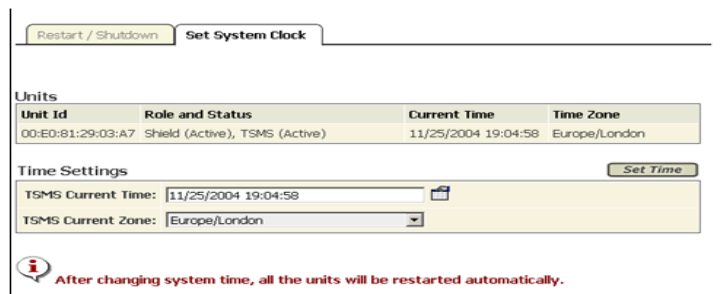
6. In Except RegExp, you can enter another regular expression that defines an exception to the rule set by the selected expression.
7. Click the **Save** button.  
The regular expression definition appears on the main page.
8. Repeat the above procedure for all the expressions you intend to use.

## System

You can shut down or reboot a TrafficShield unit, or restart the TSMS from within the TSMS user interface. Major modifications in the configuration require you to restart the units. For example, when you modify the system configuration (system page), a verification object in a Web application page, or the system time in one of the units.

### To set the system time

1. Click **Administration > Maintenance > System**.  
In the screen that appears, click the **Set System Clock** tab and set the system time.



Unit Id	Role and Status	Current Time	Time Zone
00-E0:81:29-03:A7	Shield (Active), TSMS (Active)	11/25/2004 19:04:58	Europe/London

Time Settings

TSMS Current Time:

TSMS Current Zone:

**After changing system time, all the units will be restarted automatically.**

2. Set the Time zone, Time and date, and when finished, click the Set Time button. The unit restarts and you will be sent to the Login page.

### To restart, reboot, or shut down TrafficShield system

1. In the Administration tool, select the System tab under Maintenance.  
The existing TrafficShield security application unit records are listed.



<input type="checkbox"/> Unit Id	Role and Status	Private IP
<input type="checkbox"/> 00.00.00.00.00.00	Shield (Active), TSMS (Active)	192.168.124.1

2. Select the unit by checking its selection box in the leftmost column.
3. Click the appropriate button > Restart, Reboot, or Shutdown.

## Restart

Restart affects only the TrafficShield Management Station [TSMS].

**◆ Note**

---

*Restart affects only the TrafficShield security application components and not the Operating System.*

The following actions require Restart:

- Changing verification object in HTTP/HTTPS
- Changing any parameter in client certificate
- Changing any internal parameter
- Changing any parameter in system page

## Reboot

Reboot halts the system and resets the hardware. You must wait several minutes before connecting to your unit.

**◆ Note**

---

*If you have a Standby unit installed, it will become the Active unit and the other re-booted unit will become the Standby unit.*

## Shutdown

Shutdown powers the unit down. To turn the power back on, you will need to manually turn on the power button.



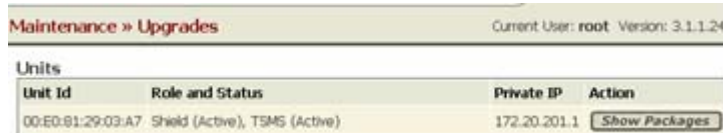
## Upgrades

This section describes the upgrade package wizard workflow. By following this wizard, the user can install a new package. At the end of the installation, dependant on the package contents, you may be required to restart or reboot the TrafficShield unit.

### Adding a Software Package

#### To add a Software Package

1. Select the Administration tab at the top of the TSMS window.
2. In the Maintenance menu, select Upgrades. A list of the installed TrafficShield security application units appears. If you have one Active unit and a Standby unit, you must upgrade each unit separately.

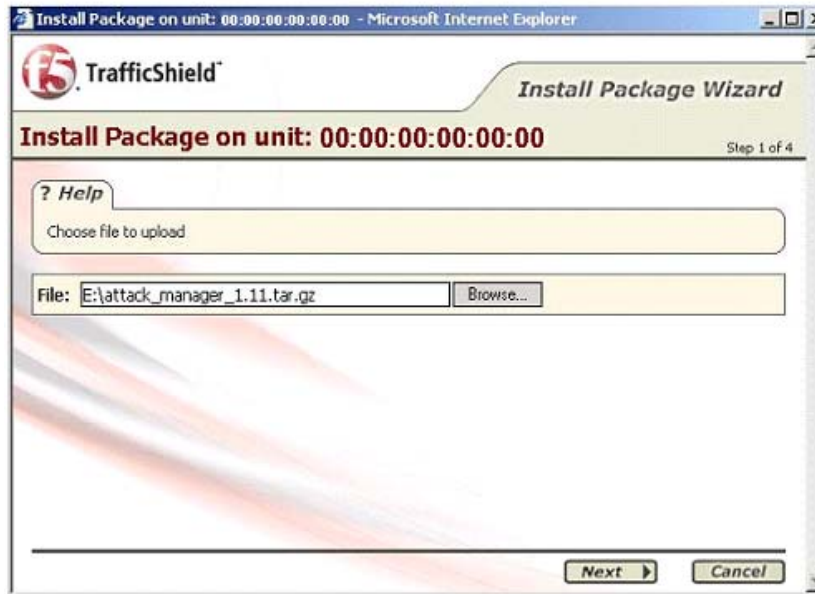


3. Choose the relevant unit to upgrade and click the **Show Packages** button. The Currently Installed packages window will be displayed. If this is the first upgrade you perform on the system, no row will be displayed.



4. Click the **Install Package** button to open the Install Package Wizard.

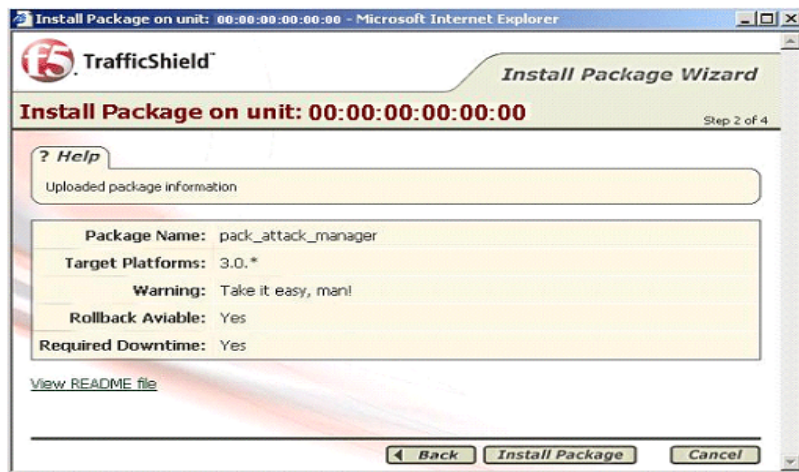
## Install Package Wizard



### Step 1: Upload the package file

1. Use the browser to locate the package file you wish to upgrade.
2. Click the **Next** button.

### Step 2: Package Information uploaded and displayed



**Fill in the fields as indicated:**

#### Package Name

Logical name of the package is not necessarily identical to the file name.

### Target Platforms

This is the TrafficShield security application minimum version number required to install this package.

### Warning

Sometimes the user needs to be aware of a certain risk or problem that the installation of this package may cause under specific circumstances (for example: the user must reboot the unit, reactivate the policy etc.).

We highly recommended that you read the notes and explanations provided in the README file that can be accessed by clicking the View README file link.

### Rollback Available

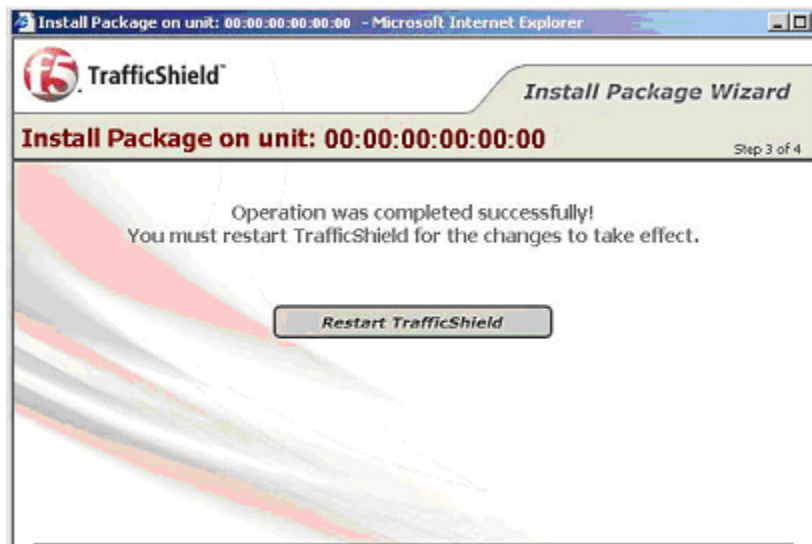
This field indicates whether it would be possible to roll back to previous status after installation, should problems occur.

### Required Downtime

Sometimes the new package may take effect only after the TrafficShield unit has been reactivated. The user needs to know that the TrafficShield security application will not be protecting the user's application during the installation time.

- Click the **Back** button, to go to the previous step or choose Install Package to continue.

### Step 3: Package successfully installed



- This screen indicates the successful completion of the package installation to TrafficShield security application. In the example above, the specific package requires the user to restart the unit. Should this not be required, the Restart TrafficShield button will not be displayed.
- Click the **Finish** button, to close the Wizard without restarting the unit.

## Rebooting

In this case, it is the user responsibility to reboot the unit later, in order to activate the changes created by the package installation.

## Rollback

After installing a new software package, problems may occur due to unforeseen circumstances. In some cases it is possible to roll back after installing a new software package. If you have already installed five sequential packages and you roll back the fifth package, you will roll back to the fourth package.

### To roll back from an installation

1. Select the **Administration** tab at the top of the TSMS window.
2. In the **Maintenance** menu, select **Upgrades**. A list of the installed TrafficShield units appears. If you have an Active unit and a Standby unit, you will need to roll back each unit separately.
3. Choose the relevant Unit to roll back and click the Show Packages button. The Currently Installed packages window will be displayed.
4. Click the **Rollback** button next to the relevant package to roll back. A message will be displayed only if the rollback was unsuccessful.

Currently installed packages				
Unit Id 00:00:00:00:00:00				
Package	Version	Updated at	Description	Action
pack_attack_manager	1.11	2004-09-23 11:33:58	This package replace attack_manager.pl with new one.	Rollback

A unit reboot may be required in order to activate the rollback changes.

### ◆ Note

*Please note that if you have installed several packages, and you wish to roll back to a specific package, please roll back in an orderly sequence without skipping any of them (5, 4, 3, etc.).*

## Backup

You can set a schedule for automatically backing up the TrafficShield security application configuration parameters and the security policies. The configuration parameters and the security policies can be backed up separately or in a single operation. You can also define different backup schedules for the same material and thus create backup “generations” and even create different schedules that direct the data to different backup computers.

The backup procedure utilizes the SSH protocol. The TrafficShield security application initiates an SCP procedure to the backup server, using the backup user name and password that must reside on the backup machine.

The backup file is compressed using the targz compression software.

The backup file size is dependent on the TrafficShield configuration, however, it can reach up to around 100MB.

A built in test backup feature enables you to check the accuracy of your settings. See below for details.

## Defining Backup Schedules

To secure yourself against hardware failures or unintended modifications to the system, in which case you might want to rollback to the system previous stage, we recommend that you regularly schedule backups.

### To schedule backups

1. Click the **Administration** button.
2. In the **Maintenance** menu, select the **Backup** tab.  
The Backup page opens.

Backup Targets							Test Backup	Add	Edit	Remove
<input type="checkbox"/>	Active	Target IP	Path	Schedule Rule	Backup Type	Last Backup				
<input type="checkbox"/>	Yes	192.168.101.99	c:\bup	* 22 * * *	Full backup	N/A				

3. Click the **Add** button. The Add Backup Target page opens.

The screenshot shows a web form titled "Add Backup Target" with "Add" and "Cancel" buttons in the top right. The form contains the following fields and options:

- Active:** A checked checkbox.
- Target IP: \*** A text input field. A red note below it reads: "Note: Target machine must support SSH."
- Path: \*** A text input field.
- Username: \*** A text input field.
- Password: \*** A text input field.
- Confirm Password: \*** A text input field.
- Schedule Rule: \*** A row of five dropdown menus labeled "Minute", "Hour", "Day of Month", "Month", and "Day of Week".
- Backup Type: \*** A radio button selected for "Full Backup". Below it, under "Backup Only:", there are two checkboxes: "TrafficShield Configuration" and "Policies", both of which are unchecked.

4. Enter the information described below.

**Active**

If you want this schedule to work, make sure that this box is checked.

At first, you may want to create schedules with this box cleared in order to prevent the system from running backups before you are ready to do so. You can activate a schedule at any time by checking this box.

**Target IP**

Specify the IP address of the computer where the backed up data will be stored.

Note that the backup procedure uses Secure Shell (SSH). The target computer should be configured to use this protocol.

**Path**

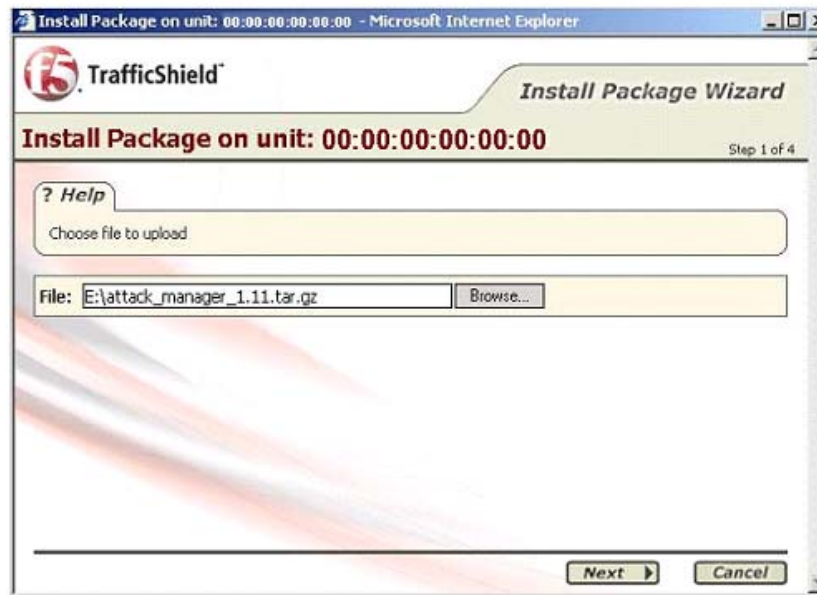
Specify the path to the folder where you want to store the data on the backup computer's disk.

**Username, Password**

Specify the user name and the password that are needed to access the backup computer.

**Confirm Password**

Type the password again.



Specify the schedule using the UNIX cron syntax.

*Note: The Format is in this order: minute hour day month weekday. The command is: Minute: Minutes after the hour (0-59), Hour: 24 hour format (0-23), Day: Day of the month (1-31), Month: Month of the year (1-12), Weekday: Day of the week (0-6; the 0 refers to Sunday). For more information, please refer to relevant web sites.*

### **Backup Type**

Select what to back up.

If you select the Backup Only radio button, TrafficShield security application allows you to mark the type of information to back up via this definition.

5. Click the **Add** button.  
The backup definition appears on the main page.
6. Repeat the above procedure for all the backup schedules you want to define.  
Defining different schedules for the same material creates “generations”. A “generation” helps you restore data as it was at the time the generation was created.
7. Click the Update TrafficShield button.

## Testing the Destinations

This procedure is designed to check that the data supplied in the backup definition is correct. The test checks the correctness of the destination IP address, the user name and password, and the path, as entered in the backup definition.

### **To test a destination**

1. In the Backup Targets page, select the backup entry to test.
2. To select an entry, mark its check box on the leftmost column. You can test one backup entry at a time.
3. Click the **Test Backup** button.  
If all data is correct, a confirmation message appears.

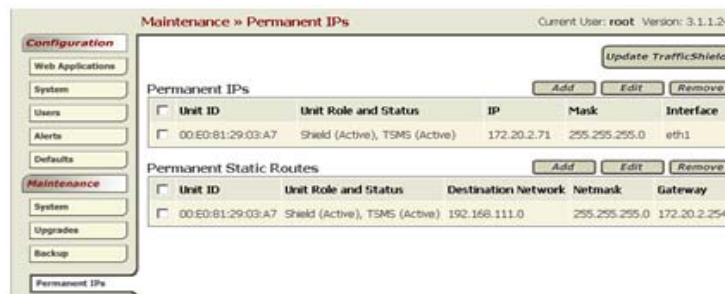


## Permanent IP Addresses

Each TrafficShield security application unit may have one or more permanent IP addresses that remain usable even when TrafficShield processes are down. This is not mandatory. If you need permanent addresses, define them as explained below. You can either add/edit a Permanent IP, or add/edit a Permanent Static Route.

### To set a permanent IP address

1. Click the **Administration** button at the top of the TSMS window.
2. In the **Maintenance** menu, select **Permanent IPs**.



3. Click the Add button above the Permanent IPs window to add a new Permanent IP.

4. Enter the following information:

#### Unit ID

Select the unit to which you want to assign a permanent IP address.

#### IP, Mask

Enter the unit's permanent IP address and its network mask.

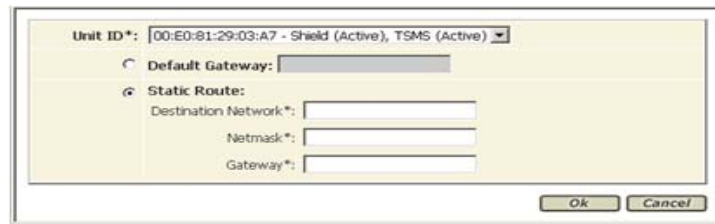
#### Interface

Each unit has two network cards. Select the card to which you want to assign a permanent IP address.

5. Click **OK**.  
The permanent IP address definition appears on the main page.
6. Repeat the above procedure for all the permanent IP addresses you need to define.
7. Click the **Update TrafficShield** button to update the unit.

### To set a permanent Static Route

1. Click the **Administration** button at the top of the TSMS window.
2. In the **Maintenance** menu, select **Permanent IPs**.
3. Click the Add button above the Permanent Static Route window to add a new Permanent Static Route.



4. If the PC resides in an external network, enter the following:

#### **Unit ID**

Select the unit to which you want to assign a permanent IP address.

#### **Default Gateway**

The default IP address of the gateway

#### **Static Route Network**

ItemDescription

#### **Static Route Mask**

The netmask of the destination network address.

#### **Static Route Gateway**

The IP address of the gateway

5. Click **OK**.  
The permanent Static Route definition appears on the main page.
6. Repeat the above procedure for all the permanent Static Route addresses you need to define.
7. Click the **Update TrafficShield** button to update the unit.

## Downloads

TrafficShield supports four types of Policy Browser downloads. Two for the Windows platform and two for the Linux platform.

Select the appropriate Policy Browser that corresponds to your system configuration.

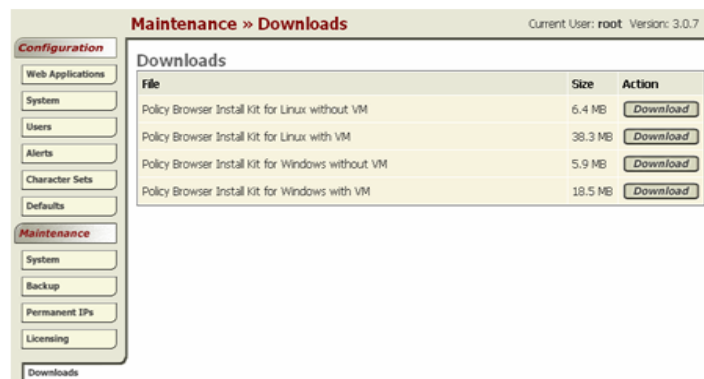
## Policy Browser

The Policy Browser is an add-on tool that enables you to record your navigation activities on your Website into an output file.

This output file will be loaded later on onto the policy and can be used to build up the policy,

### To download the Policy Browser software

1. In the **Administration** tool, select the **Downloads** tab under **Maintenance**.



2. Select the relevant Policy Browser Installation Kit from the Downloads list.
3. Click the **Download Action** button and download to a selected folder.
4. Run the downloaded executable file to install the Policy Browser on your machine.
5. At the end of the installation, run the policy browser.

#### ◆ Note

*The recorded scan is saved in mybrowser.csv. Load this file from browser recordings.*

## Support tools

The TrafficShield security application offers you the following support tools:

- Export Configuration
- Record Traffic
- F5 Support Website

## Export Configuration

This feature is intended to reproduce a TrafficShield security application unit's existing configuration for troubleshooting customer problems.

◆ **Note**

---

*Import capability option is currently limited to support and help teams.*

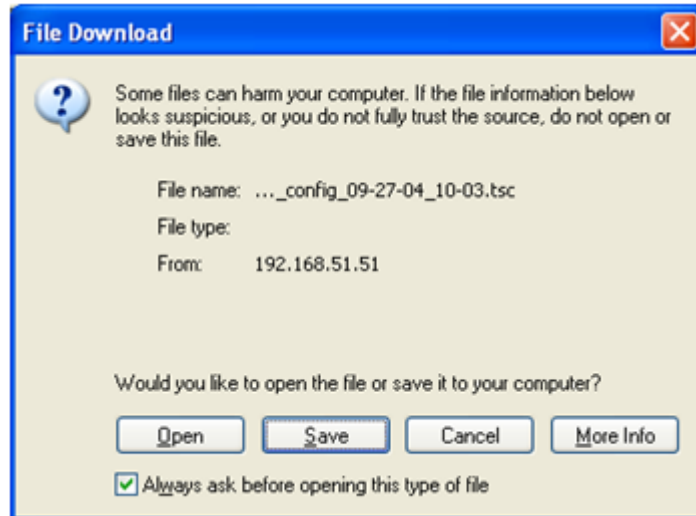
### To export your configuration to a disk

1. In the **Administration** tool, select **Maintenance**, and click the Export Configuration tab under the **Support Tools**.

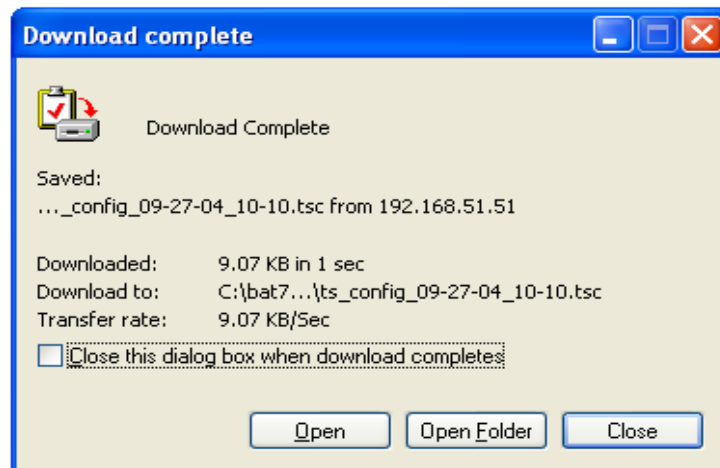


2. Choose the relevant configuration type that you wish to export.

- Click the **Export** button.  
The file Download screen opens.



- Click **Save** to open the browser, and select the target folder where you wish to save the exported file.  
The file is saved to the disk and the Download complete window appears.



- Click **Close** to return to the TrafficShield security application.  
The file was saved with a default name: ts\_config\_mm-dd-yy\_hh-mm.tsc that the user can change before saving.

## Record Traffic

This tool is used to record the traffic between the clients and the TrafficShield security application, as received on the service interfaces, through either http (**80**) or https (**443**) ports. This output is used for internal support purposes only, and is exported as part of the system configuration or copied directly.

### To record the Traffic

1. In the **Administration** tool, select **Maintenance** under the **Support Tools**.
2. Click the Record Traffic tab, and then click **Start**.  
You are required to confirm the action, and upon confirmation, the recording operation starts.



3. To end the recording, click **Stop**.

### ◆ Note

*We recommend that you not leave the tool running for long periods of time while TrafficShield system is under stress, otherwise the output file may reach its maximum size limit and the oldest part of the recording might be lost.*

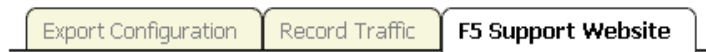
## F5 Support Website

This tool provides information about the F5 Support site, and a link to the Ask F5 Technical Support Center, where you can find additional information, solutions, and documentation for the product.

### To access the F5 Support Website

1. In the **Administration** tool, select **Maintenance** under the **Support Tools**.

2. Click the F5 Support Website tab to display the relevant web site details.



### Support

For technical support, visit F5 support web-site: <http://askf5.com>







---

---

# Glossary

---

---



**ARP**

Address Request Protocol: (a networking protocol). A method for finding a host's IP address from its Ethernet address. The sender broadcasts an ARP packet containing the IP address of another host and waits for it (or some other host) to send back its Ethernet address. Each host maintains a cache of address translations to reduce delay and loading. ARP allows the IP address to be independent of the Ethernet address, but it only works if all hosts support it.

ARP is defined in RFC 826.

The alternative for hosts that do not do ARP is constant mapping.

**Check Object**

Indicates whether TrafficShield security application should check the Object requested in the HTTP/HTTPS request against the list of its known objects before it forwards the request to the server. In case it doesn't find the requested object in the list, it generates a violation that, based on the blocking policy, can cause the request to be blocked

**Cookie**

A packet of information sent by an HTTP server to a World-Wide Web browser and then sent back by the browser each time it accesses that server. Cookies can contain any arbitrary information the server chooses and are used to maintain state between otherwise stateless HTTP transactions. Typically this is used to authenticate or identify a registered user of a Web application without requiring them to sign in again every time they access that Web application. Other uses are maintaining a "shopping basket" of goods you have selected to purchase during a session at a Web application, Web application personalization (presenting different pages to different users), and tracking a particular user's access to a Web application.

**DELETE**

An HTTP request type that requests to delete a resource on the web server.

**Domain Name**

A series of alphanumeric strings separated by periods, such as www.siterequest.com, that is an address of a computer network connection, and that identifies the owner of the address.

**Dynamic Parameter**

A dynamic parameter is a parameter in a request where the set of legal values this parameter can have is changing dynamically, and usually depends of the user session. For example, in a banking application the account number is a dynamic parameter, since each user has its own set of legal account numbers that this parameter can have. This set of legal account numbers is dynamically generated by the server and embedded in the web page sent to user. TrafficShield security application extracts this list of legal values from the web page that is sent to the user, and uses them to verify that the value sent in the request for the dynamic parameter is legal.

**Dynamic Value**

See dynamic parameter

**Entry Point**

A web page that could be the first requested page in the Web application: an end-user could get to the Entry Point by typing a URL in the browser window, opening a favorites menu, be linked from a different Web application or e-mail client. The end user could also get to the Entry Point by clicking a back button of the browser.

**Flow**

The defined access path for a browser to get from one object to another specific object.

**GET**

A type of HTTP request that does not have a content body

**Learning**

A process of making a policy more accurate by verifying how the policy complies with the traffic requests, and if there are discrepancies between the policy and the traffic requests, then translating these discrepancies into a suggestion for modifying the policy. The learning phase also enables the system administrator to verify that the policy is not generating any false positives before turning on the blocking feature. The learning process can be used to fine-tune any policy component such as requests length, parameters, and values. In case new objects are added in the Web application, TrafficShield security application can learn those objects and their flows using the learning engine.

**Length-Cookie**

The length of the cookie.

**Length-Post Data**

The length of the Data that comes with a POST request.

**Length-Query String**

The length of the Query string.

**Length-Request**

See Request Length.

**Length-URI**

The length of the URI in characters.

**Meta character**

A character or a sequence of characters that has a special meaning (<SCRIPT >, \, SELECT, INSERT, ;, `, <).

**Method**

The HTTP/HTTPS request method, e.g. GET, POST, HEAD, PUT, and DELETE.

**Non Existent Object**

The flow did not match the defined flows.

**Object**

A file or a script that generates web pages on the web server that can be requested by a user,

**Object is Allowed to modify domain Cookie**

In case an Object (i.e., a web page) includes a JavaScript/java applet/flash as part of the client-side and can change a domain cookie value, the object should be defined as "Object is allowed to modify Cookie."

**Path Traversal**

An HTTP Attack that uses patterns like ../ to get access to files not intended to viewed above the WWW root, or in order to cross directories on the server.

**Policy**

A set of rules that enables TrafficShield security application to understand if a request is valid.

**POST**

A type of HTTP request, in which a query is put into a content body and possibly compressed or encoded.

**PUT**

An HTTP request type that requests a content change on the web server.

**Query String**

Part of an HTTP request that specifies a list of parameters and values into a CGI script. For instance:

`http://www.siterequest.com/index.cgi?param1=value1&param2=value2`

Anything that comes after the question mark in the example above is a query string.

**Referrer**

A web page that requests other objects An HTML page could request picture files and other html objects to be downloaded, but pictures cannot cause other objects to be downloaded. For example, HTML, asp, php pages are usually Referrers, while gif and jpeg images are not.

**Regular Expression**

Used by UNIX utilities such as grep, sed and awk, and by editors such as vi and Emacs. A regular expression (regexp) is a sequence of characters which provides the user with a powerful, flexible and efficient test processing tool. For more details on how to write regular expressions please refer to the many books written on this subject; for example: Mastering Regular Expressions, by Jeffrey E.F. Friedl, Published by O'Reilly & Associates, Inc.

**Request Length**

The total Length of the HTTP request (in characters) which includes the request line, all headers, cookies, and post data.

**Server IP**

The IP address of the Web Server that TrafficShield security application is protecting (usually this is an internal IP address).

**Service IP**

The external IP address on which TrafficShield security application is listening for http requests. (Usually this is the IP address that the DNS A record of the Web Server is mapped to.)

**Shield Unit**

The on-line enforcing mechanism responsible for TCP session termination, requests parsing, and analyzing.

**Static Parameter**

A parameter in the request where its values are chosen from a known set of values: Name of a Country, Yes/No, etc.

**Static Value**

See static parameter.

**Target Frame**

The frame to which the object is loaded.

**Undefined Flow**

The flow did not match the defined flows.

**Undefined Object**

The object did not match any objects on the list of allowed objects.

**URI**

Part of the URL that specifies the name of the object requested: in <http://www.siterequest.com/index.html>, [index.html](http://www.siterequest.com/index.html) is the URI.

