TrafficShield™ Application Firewall

Single-Unit (and/or Hot Backup) Installation and Configuration Manual

Version 3.0

MAN-0127-00

Service and Support Information

Product Version

This manual applies to product version 3.0 of TrafficShield™ Application Firewall.

Legal Notices

Copyright

Copyright 2002-2004, 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 iControl 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 includes 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.

Cet appareil numérique de la classe A est conforme à la norme, NMB-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

Getting Started

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 Networks TrafficShield^{TM} Application Firewall 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.

TrafficShield security application is an all-purpose web security device, packaging the most effective Web application firewall on the market with a powerful network firewall, all behind a user-friendly interface. The TrafficShield security application automatically generates security policies that are extremely accurate, ensuring that networks are constantly and completely protected.

This manual describes the single-unit deployment and the optional hot backup unit deployment.

Document Objectives

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

How This Manual Is Organized

This manual is organized differently from the TrafficShield Management Configuration tabs. This was intentional.

The GUI 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 who needs to follow a certain configuration workflow before he can begin to use the Policy Management functionality:

- 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 Installing TrafficShield Units: This chapter explains how to configure a TrafficShield unit and its hot backup.

Chapter 2 Launching TSMS: This chapter explains how to access the TrafficShield security Application and begin to navigate to the configuration screens.

Chapter 3 Configuration: The installation process is followed by a network configuration stage. In this stage, you can define a hot backup 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 4 Web Applications: This chapter explains how to create a Web application definition in TSMS and how to continue to maintain it.

Chapter 5 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 Application Firewall *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 concepts and shows how the concepts are implemented in the security policy context.

Chapter 1 Installing TrafficShield Units

This chapter explains how to install an F5 Networks TrafficShield Application Firewall.

A TrafficShield security application unit may be installed in two configurations: a single unit, and a single unit with a standby hot backup unit. Both units are identical. The hot backup unit is automatically activated when the primary unit fails.

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.

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.

Note

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

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. This address is disabled when the unit is in standby mode.

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 TrafficShield system, this would be the IP address of the Web server. After installing the TrafficShield system, 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 IPs as the number of Web applications it protects. This address is disabled when the unit is in standby mode.

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.

Server IP

This is the IP address of the real web server to which TrafficShield system forwards the requests.

Trusted IP

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

Permanent IP

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

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

Static Route

Add static routes, if needed.

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 should fail, this address will be transferred to the hot backup unit once it becomes active.)

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.

In 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 GUI.

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.

   TrafficShield system supports two types of network configuration.

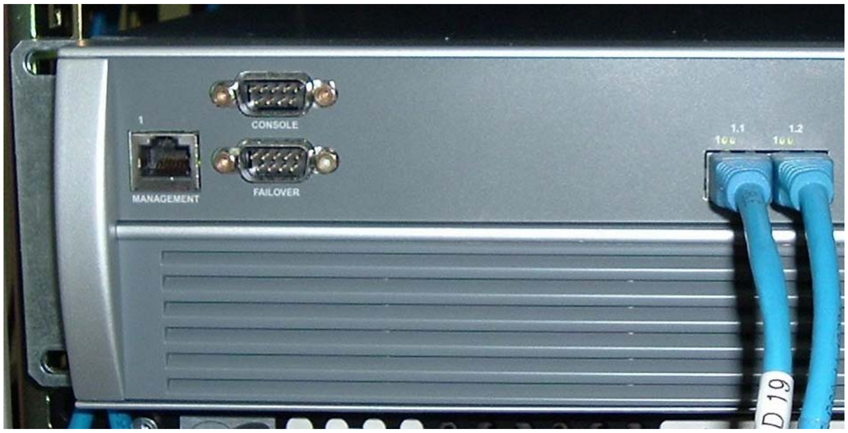
   1.1 (Eth0) – The network cable must be connected between the TrafficShield security application unit and the Web server's internal network.

   1.2 (Eth1) – This port is optional, used in cases when there is a total separation between external and internal traffic. When using this option you will need to check the relevant checkbox in the Administration -> Configuration -> System window explained later in this document.

3. Prepare a serial console terminal.

   This can be any PC with any serial console software installed on it. For example: Microsoft® 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:

   Serial device: /dev/ttyS0

   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: K@A167bC?

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 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.

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.

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.

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]:1

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

Enter the network IP mask for the permanent IP.

Enter network interface (eth)

Specify the network interface card through which the TrafficShield system 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 enter the TrafficShield Web Administrator's Access IP/Network (remote manager host):192.168.1.40

You activate the TrafficShield Management Station GUI 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

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

Please enter the initial TrafficShield Web Administrator's username:admin

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.

Running tsconfig.pl for the Hot Standby Unit

The hot backup standby unit MUST be configured in the TSMS application before running the tsconfig.pl script.

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

Note

The primary 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 hot 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 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 hot 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.

Chapter 2 Launching TSMS

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

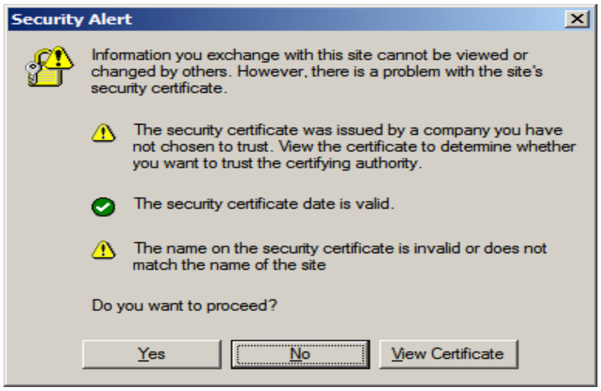
Accessing TSMS

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 TS 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.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

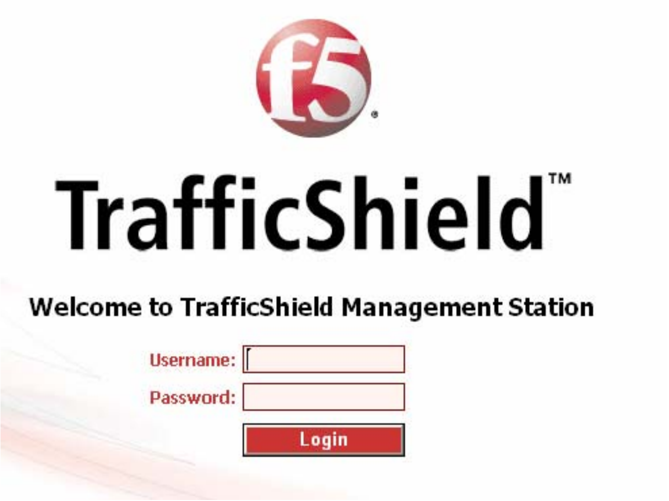
✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

2. Click yes to continue.

   The logon page opens.



Welcome to TrafficShield Management Station

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

Using the TrafficShield Wizards

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

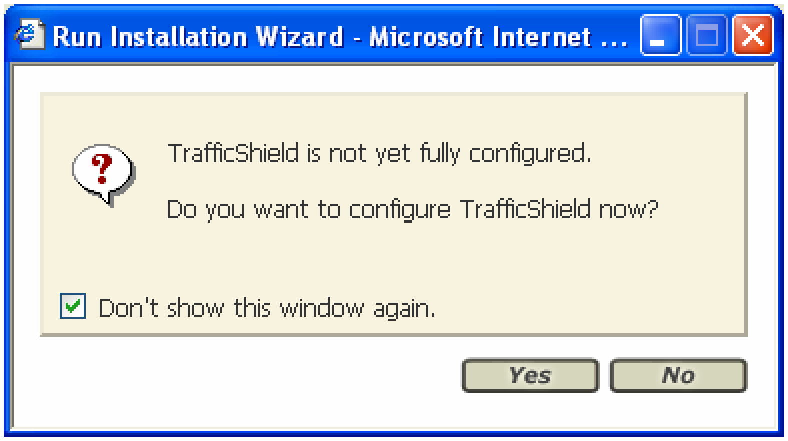
The TrafficShield Unit Configuration Wizard:

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 now (if this is not your first access, the monitoring page opens).



TrafficShield is not yet fully configured.

Do you want to configure TrafficShield now?

☑ Don't show this window again.

  - 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 module is selected by default. To access the wizard at any time, select Administration -> Configuration-> System and click on the "Run TrafficShield installation wizard" icon.

General*:*

- The actual wizard windows displayed are almost identical to the manually accessible windows of the TrafficShield security application unit configuration tool. Therefore, please refer to Chapter 3 Configuration, the TrafficShield unit configuration section 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

  Or

  - In the Administration->Configuration->Web Applications tab click the icon in the Web Applications tab.

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 Create Policy chapter.

The Install Package Wizard:

Purpose*:*

- Allows you to upgrade the TrafficShield security application security current software packages.

Access*:*

- In the Administration->Maintenance->Upgrades tab choose the relevant unit and then package that you wish to upgrade. Click the Show Packages button, which displays the currently installed packages list. Click the *Install Package* button to activate the Wizard.

General*:*

- This wizard guides the user through the installation process. More details can be found in Chapter 5 Administration in this document.

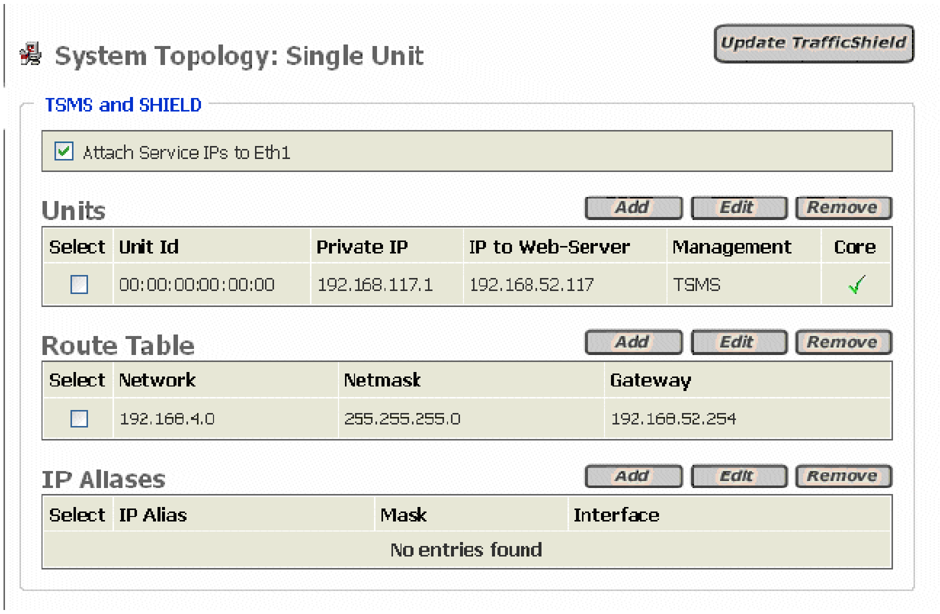
Chapter 3 Configuration

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

TSMS and SHIELD

☑ Attach Service IPs to Eth1

Units

Select	Unit Id	Private IP	IP to Web-Server	Management	Core
□	00:00:00:00:00:00	192.168.117.1	192.168.52.117	TSMS	✓

Route Table

Select	Network	Netmask	Gateway
□	192.168.4.0	255.255.255.0	192.168.52.254

IP Aliases

Select	IP Alias	Mask	Interface
No entries found			

4. Check the Attach service IPs to ETH1 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.

Units

Use the Units section:

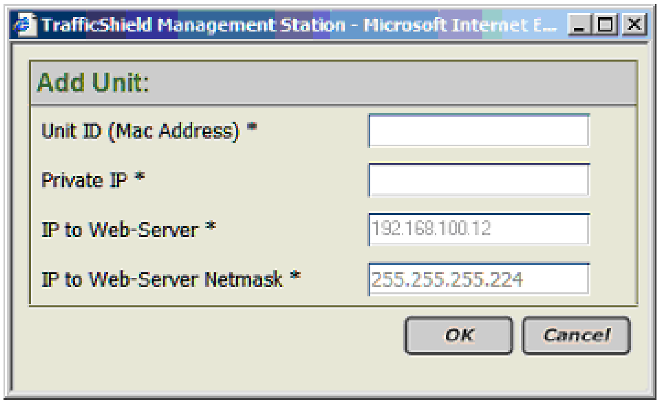
- To add the IP to Web Server address, the network mask, and the gateway for the TrafficShield security application unit, if you didn’t define it via the TrafficShield security application unit Configuration Wizard.

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

To add the hot backup unit:

1. In the Units section, click the Add button.

   The Add Unit dialog box opens.



TrafficShield Management Station - Microsoft Internet E...

Add Unit:

Unit ID (Mac Address) *	
Private IP *	
IP to Web-Server *	192.168.100.12
IP to Web-Server Netmask *	255.255.255.224

2. Enter the unit's ID (MAC address) and its private IP.

   Both the main and hot backup units use the same IP to Web address.

3. Click OK.

Route Table

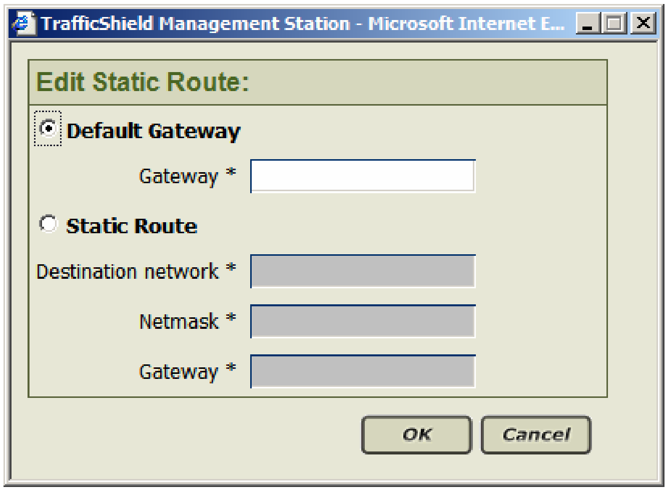
If a gateway different from the default gateway exists in your network, use the Static Route feature to specify the gateway details. TrafficShield security application looks first for the static route and uses the default gateway if it does not find one.

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 checkbox located to the left of the relevant unit and click the Edit button.

   The Add or Edit Static Route dialog box opens.



Edit Static Route:

● **Default Gateway**

Gateway *

○ **Static Route**

Destination network *

Netmask *

Gateway *

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.

   - If you chose to accept requests via the default gateway, in the Gateway field, enter its IP address.

   - 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.

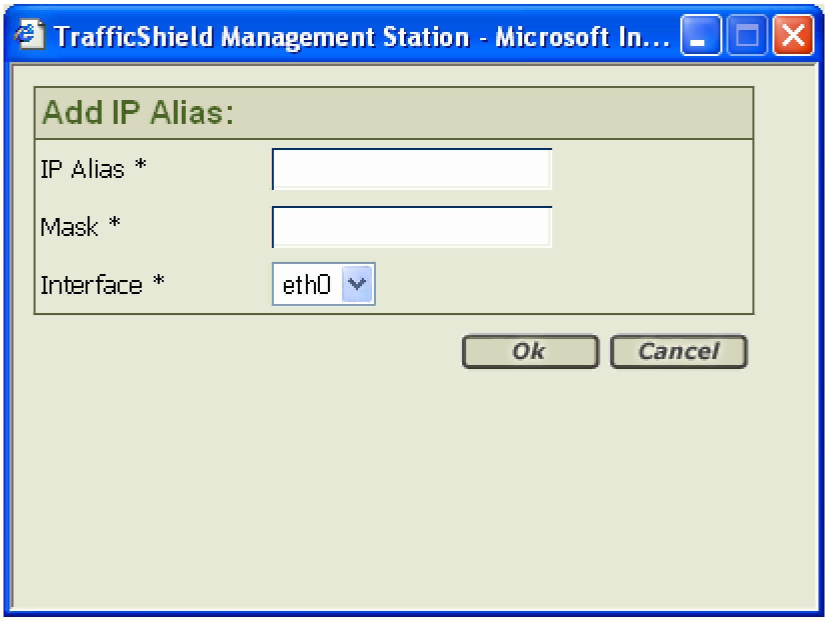
IP Aliases

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 GUI 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.



Add IP Alias:

IP Alias *	
Mask *	
Interface *	eth0

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.

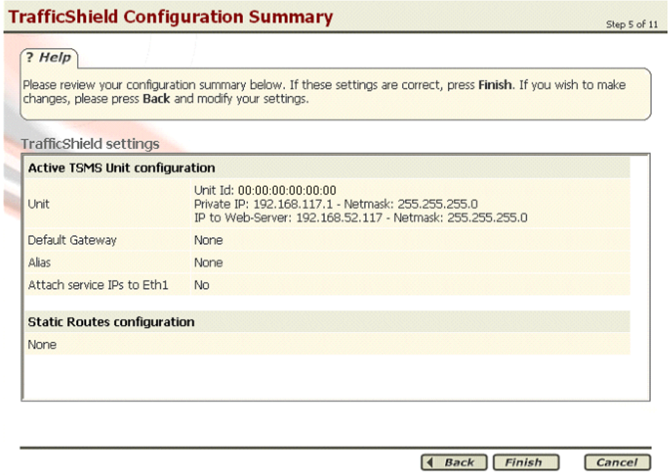
3. Click OK.

   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, you will receive the following Summary screen:



TrafficShield Configuration Summary

Step 5 of 11

Please review your configuration summary below. If these settings are correct, press **Finish**. If you wish to make changes, please press **Back** and modify your settings.

TrafficShield settings

Active TSMS Unit configuration	
Unit	Unit Id: 00:00:00:00:00:00 Private IP: 192.168.117.1 - Netmask: 255.255.255.0 IP to Web-Server: 192.168.52.117 - Netmask: 255.255.255.0
Default Gateway	None
Alias	None
Attach service IPs to Eth1	No

Static Routes configuration
None

6. You can return to TSMS, or if you choose the *Configure Web Application* button, the New Web Application Wizard will automatically begin.

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 system 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:

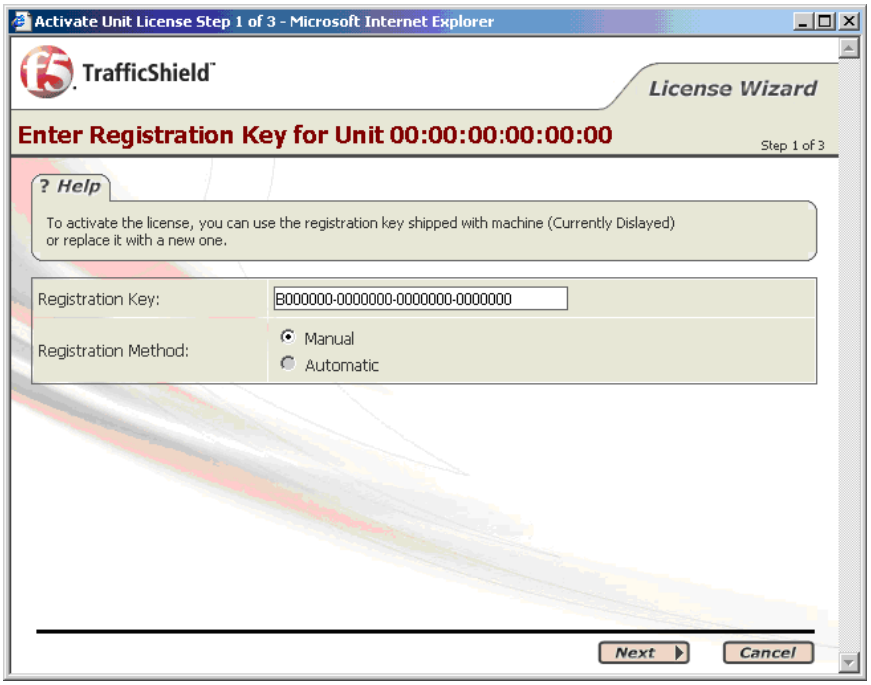
1. Select the Administration button at the top of the TSMS window.

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.


Activate Unit License Step 1 of 3 - Microsoft Internet Explorer
TrafficShield™
License Wizard

Enter Registration Key for Unit 00:00:00:00:00:00

To activate the license, you can use the registration key shipped with machine (Currently Dislayed) or replace it with a new one.

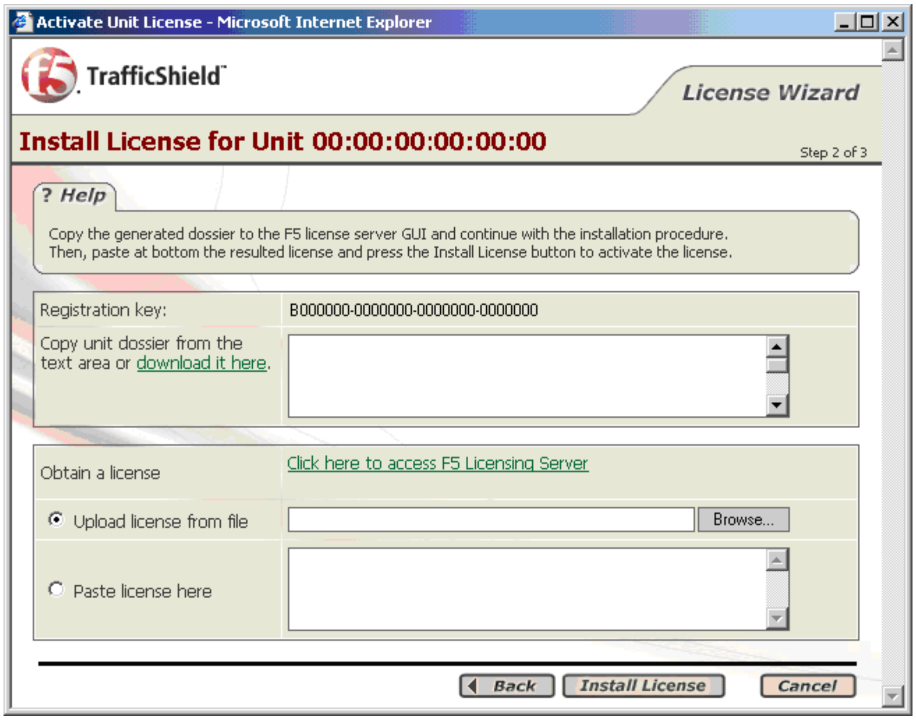
Registration Key:	B000000-0000000-0000000-0000000
Registration Method:	● Manual ○ Automatic

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

4. 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.



Install License for Unit 00:00:00:00:00:00

Step 2 of 3

Copy the generated dossier to the F5 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: B000000-0000000-0000000-0000000

Copy unit dossier from the text area or download it here.

Obtain a license: Click here to access F5 Licensing Server

● Upload license from file

○ Paste license here

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

Note

Dossier: This is an encryption of a string containing a set of physical hardware elements of the machine.

5. 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 Licenses Activation Screen:

     a) Click the “download it here” link.

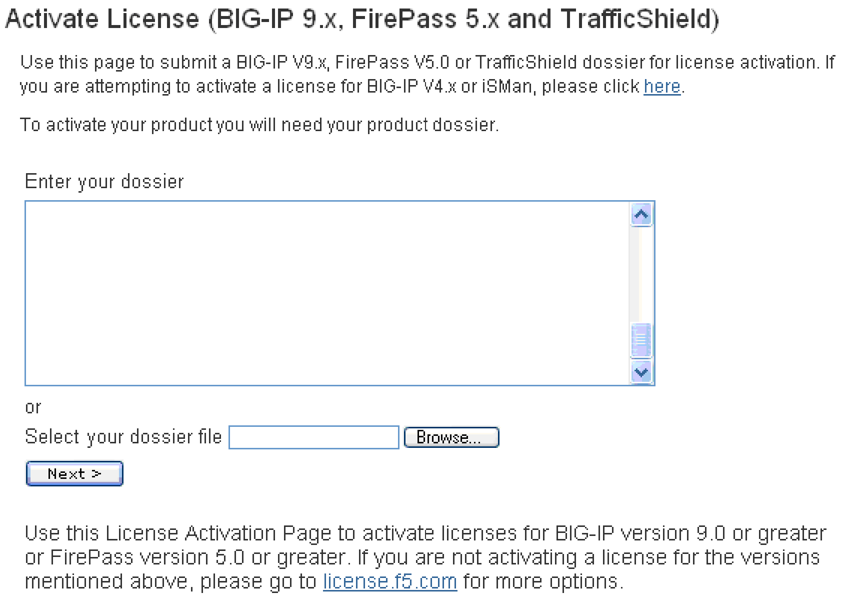
     b) A “save as” box opens.

     c) 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.

6. 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 for more options.

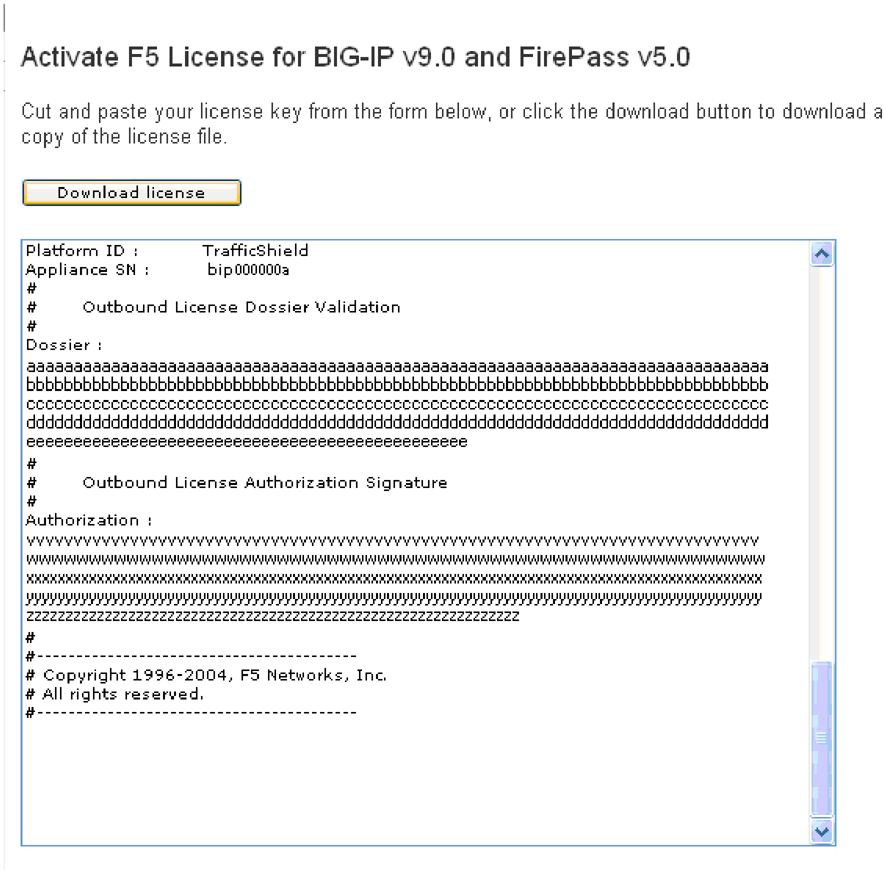
7. Save your information in the way consistent with your previous choice:

   - 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.

8. Choose Next to continue.

9. The dossier information is processed and the following F5 Networks licensing screen is displayed:



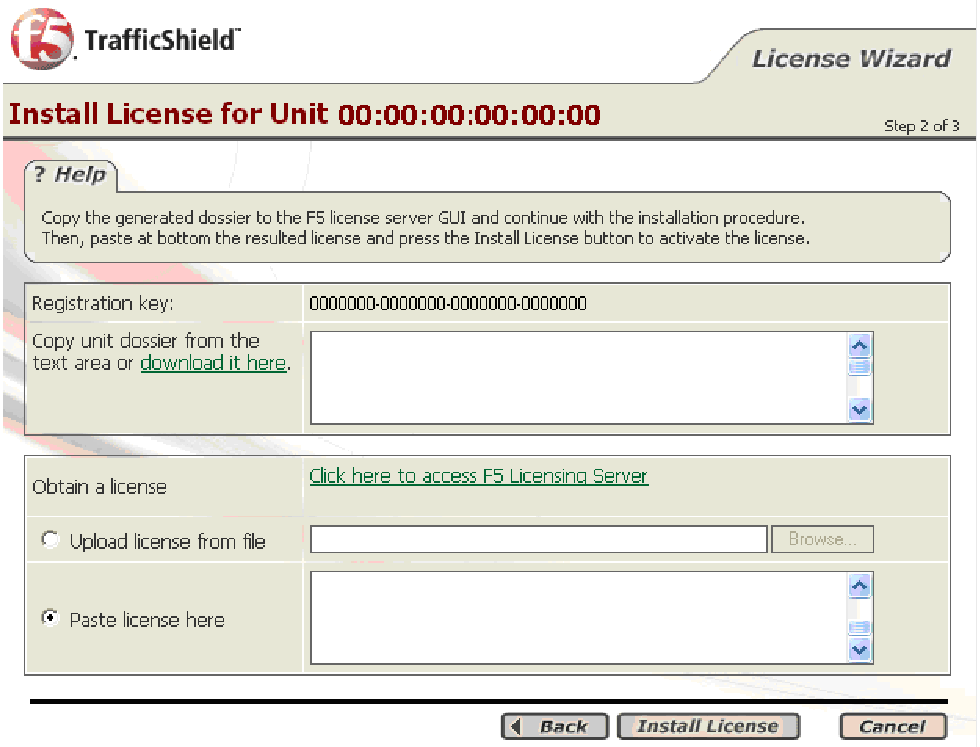
Activate F5 License for BIG-IP v9.0 and FirePass v5.0

Cut and paste your license key from the form below, or click the download button to download a copy of the license file.

```
Platform ID :         TrafficShield
Appliance SN :        bip000000a
#
#       Outbound License Dossier Validation
#
Dossier :
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
dddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
#
#       Outbound License Authorization Signature
#
Authorization :
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
#
#----------------------------------------
# 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.



Install License for Unit 00:00:00:00:00:00

Step 2 of 3

? Help

Copy the generated dossier to the F5 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.

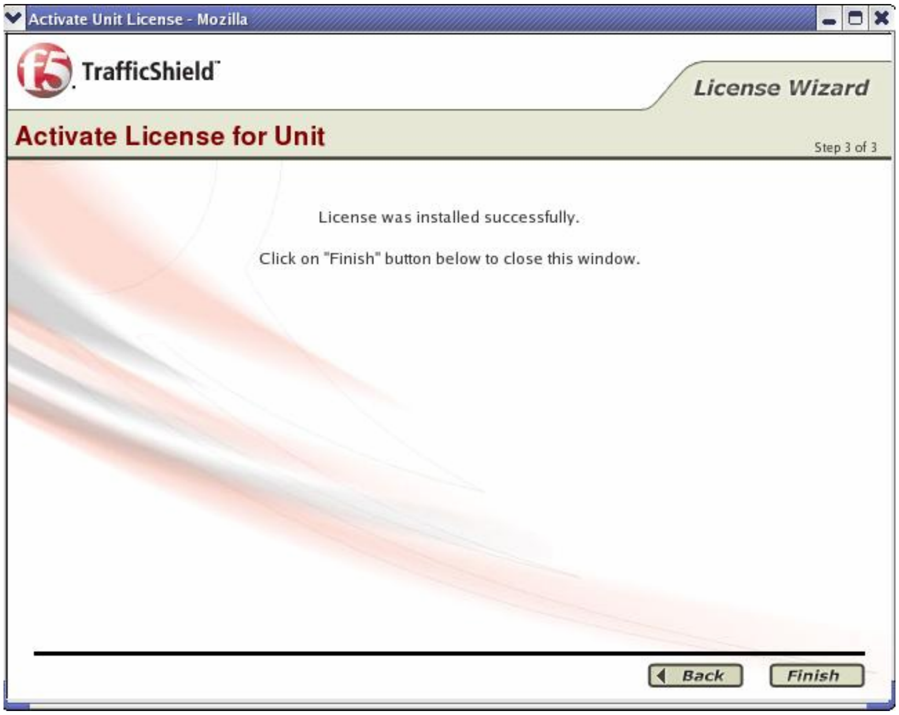
Registration key:	0000000-0000000-0000000-0000000
Copy unit dossier from the text area or download it here.	

Obtain a license	Click here to access F5 Licensing Server
○ Upload license from file	Browse...
● 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.



Activate License for Unit

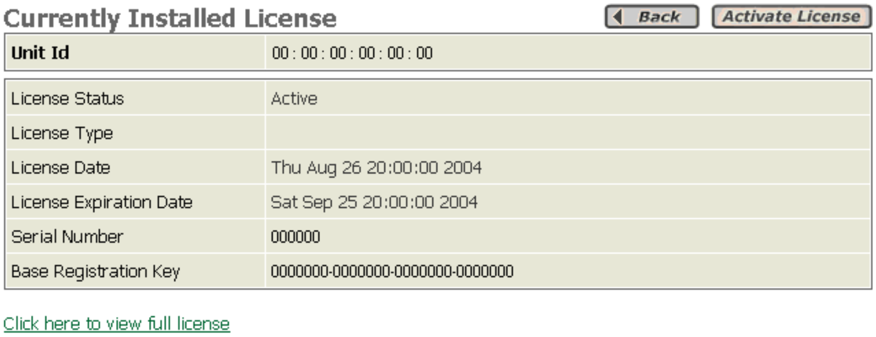
License was installed successfully.

Click on "Finish" button below to close this window.

- Click the *Back* button to return to previous step.
- Click the *Finish* button to close this 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.



Currently Installed License

Unit Id	00 : 00 : 00 : 00 : 00 : 00
License Status	Active
License Type	
License Date	Thu Aug 26 20:00:00 2004
License Expiration Date	Sat Sep 25 20:00:00 2004
Serial Number	000000
Base Registration Key	0000000-0000000-0000000-0000000

Click here to view full license

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

Chapter 4 Web Applications

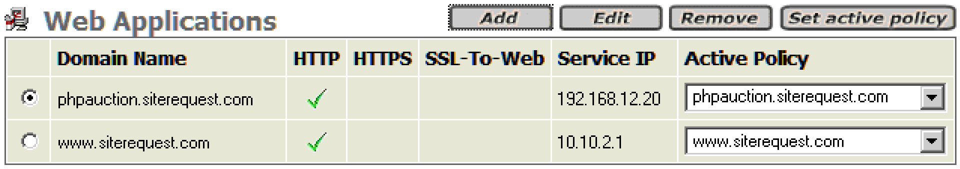
This chapter explains how to create a new Web application definition in TrafficShield Management Station (TSMS) and how to configure it and how to maintain and remove exiting Web Applications definitions as well.

Defining a new Web application

To define a new Web application:

1. Select Administration -> Configuration -> Web Applications tab at the top of the TSMS page. (Web Application is selected by default).

2. If this is not the first time you are defining a Web application and you have already defined one or more Web applications in the past, a list of the existing Web application definitions will appear.



	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. Open the Web Application Wizard by clicking the icon in the Web Applications tab or choosing the Add button.

4. Enter the information described below. The Wizard will

ask you at the end whether you would like to continue automatically to the Configure Crawler Wizard or to return to the TSMS.

Note

This also creates a default policy for the Web application.

Tip

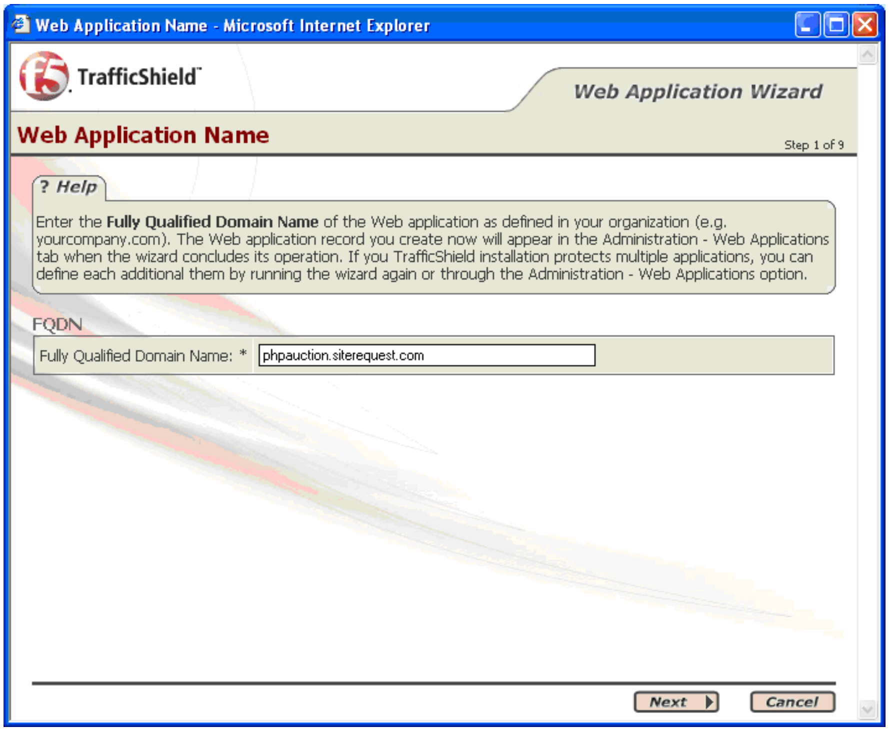
Regardless of your choice (Return to TSMS or Run the Crawler Wizard), we recommend that you activate your default policy before using it. Choose the *Set active Policy* located in the Administration->Configuration->Web Application Window.

Web Application Wizard

Note

All information entered to the Wizard's fields in the various screens are examples only.

Step 1: Web Application Name



Web Application Name

Step 1 of 9

? Help

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 each additional them by running the wizard again or through the Administration - Web Applications option.

FQDN

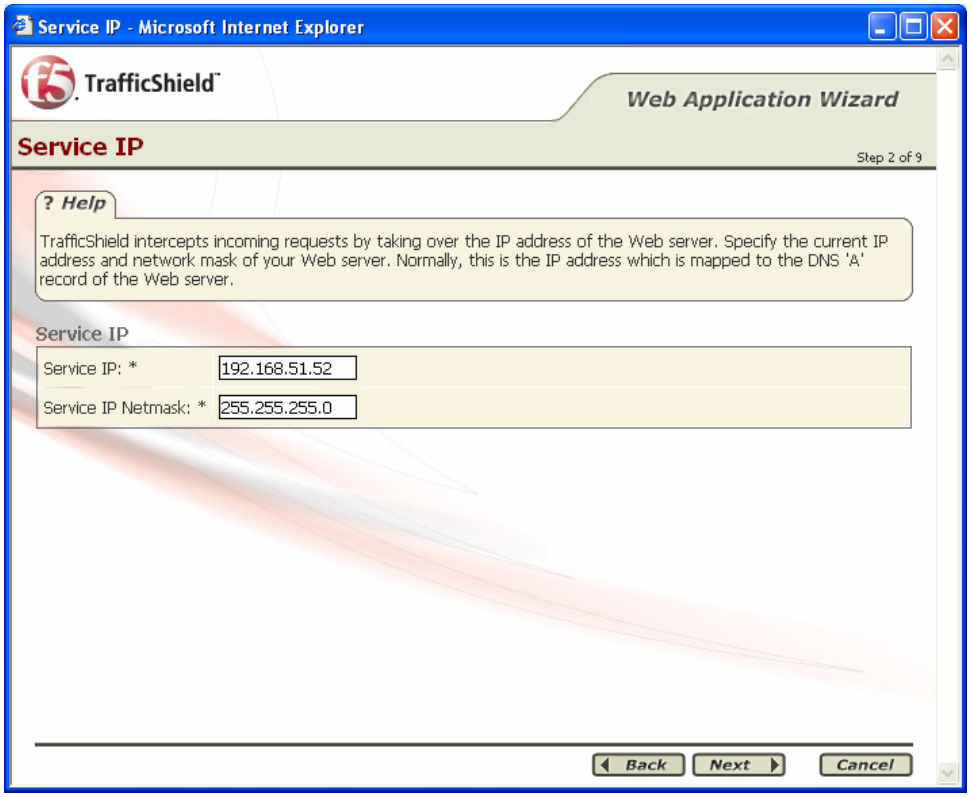
Fully Qualified Domain Name: * phpauction.siterequest.com

FQDN Fully Qualified Domain Name

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

- Click the *Next* button to continue.

Step 2: Service IP



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: *	192.168.51.52
Service IP Netmask: *	255.255.255.0

Service IP, Service IP Netmask

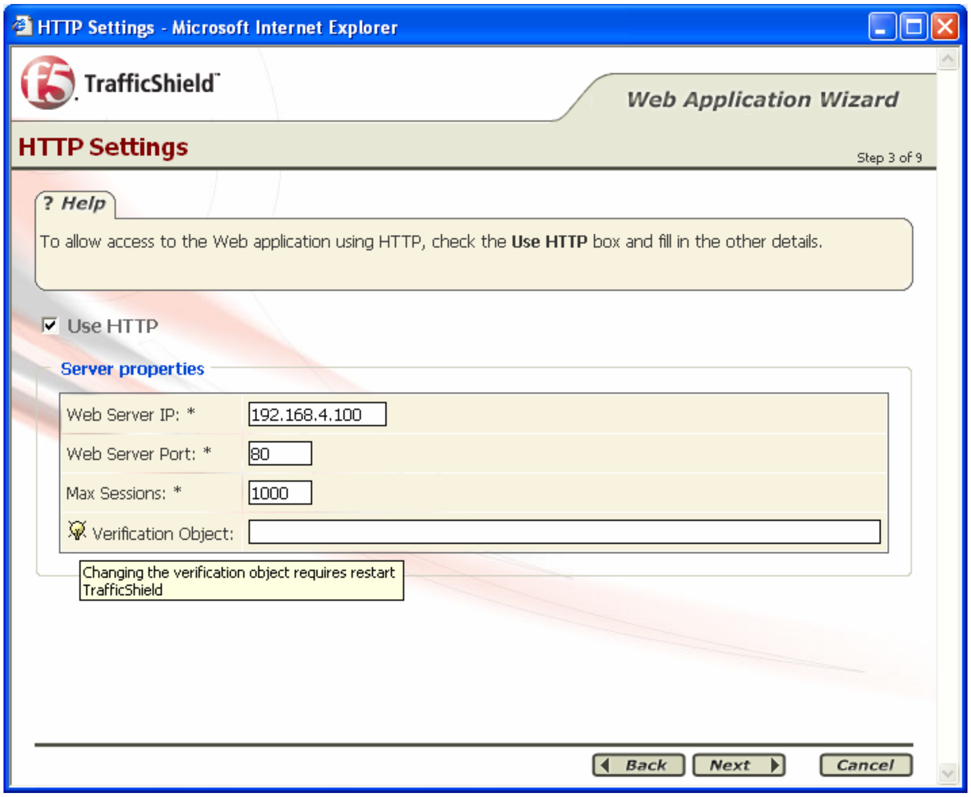
Specify the Web Application IP address and the corresponding network mask.

- Click the *Back* button to go to the previous step.

Or

- Choose *Next* to continue.

Step 3: HTTP Settings



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: *	192.168.4.100
Web Server Port: *	80
Max Sessions: *	1000
Verification Object:	

Changing the verification object requires restart TrafficShield

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 unit.

Note

The distributed Application feature is not supported at this time.

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, you need to consult with your system administrator about the maximum number of simultaneous clients, connection time-out definitions, etc.

Verification Object

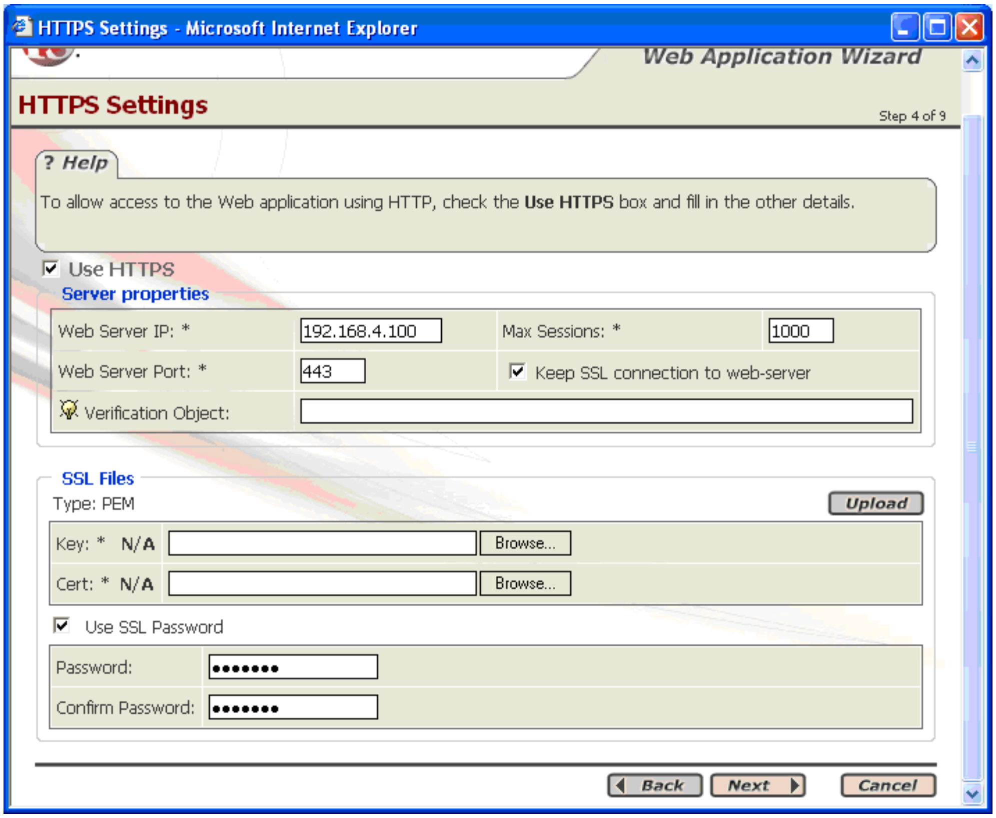
This is an optional field that enables the user to verify that the TrafficShield security application is responding correctly to a pre-defined test object.

- Click the *Back* button, to go to the previous step.

Or

- Choose *Next* to continue.

Step 4: HTTPS Settings



HTTPS Settings

Step 4 of 9

? Help

To allow access to the Web application using HTTP, 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

Key: *	N/A	
Cert: *	N/A	

☑ Use SSL Password

Password:	•••••••
Confirm Password:	•••••••

Use HTTPS

To allow HTTPS access to the Web application, check 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" 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 the requests to the Web server.

Note

Requests will flow to the server more quickly 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 checkbox.

Password

Specify the password for key file.

Confirm Password

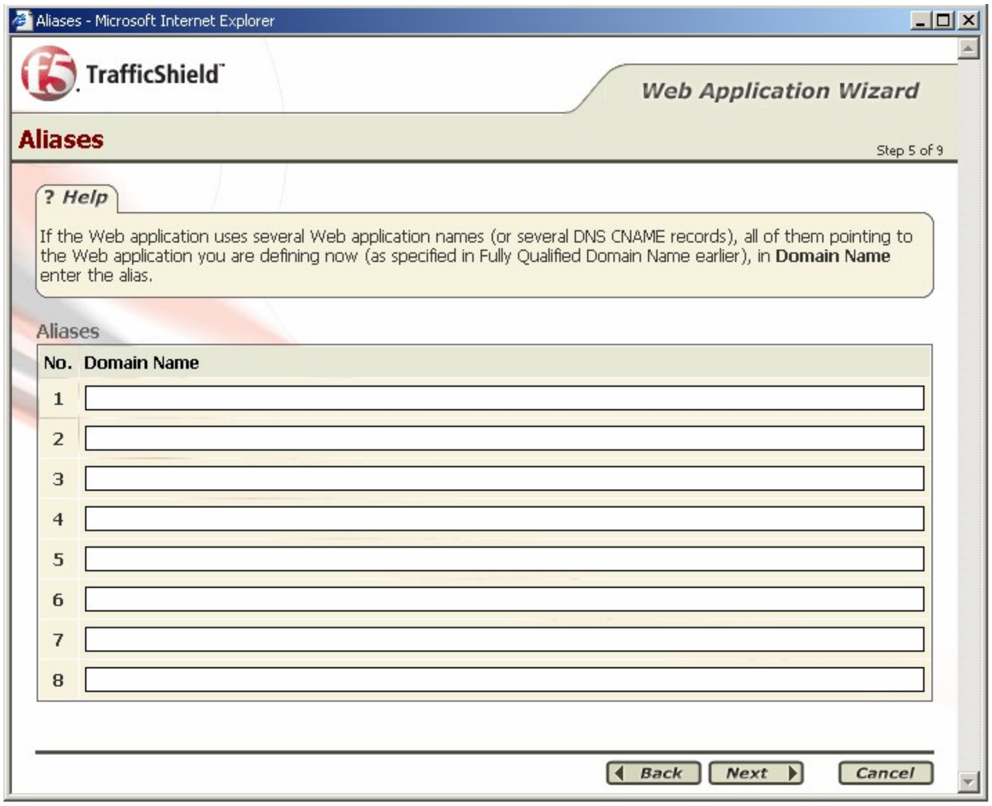
Type the password again for confirmation

- Click the *Back* button, to go to the previous step.

Or

- Choose *Next* to continue.

Step 5: Aliases



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	
2	
3	
4	
5	
6	
7	
8	

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

Check the checkbox 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).

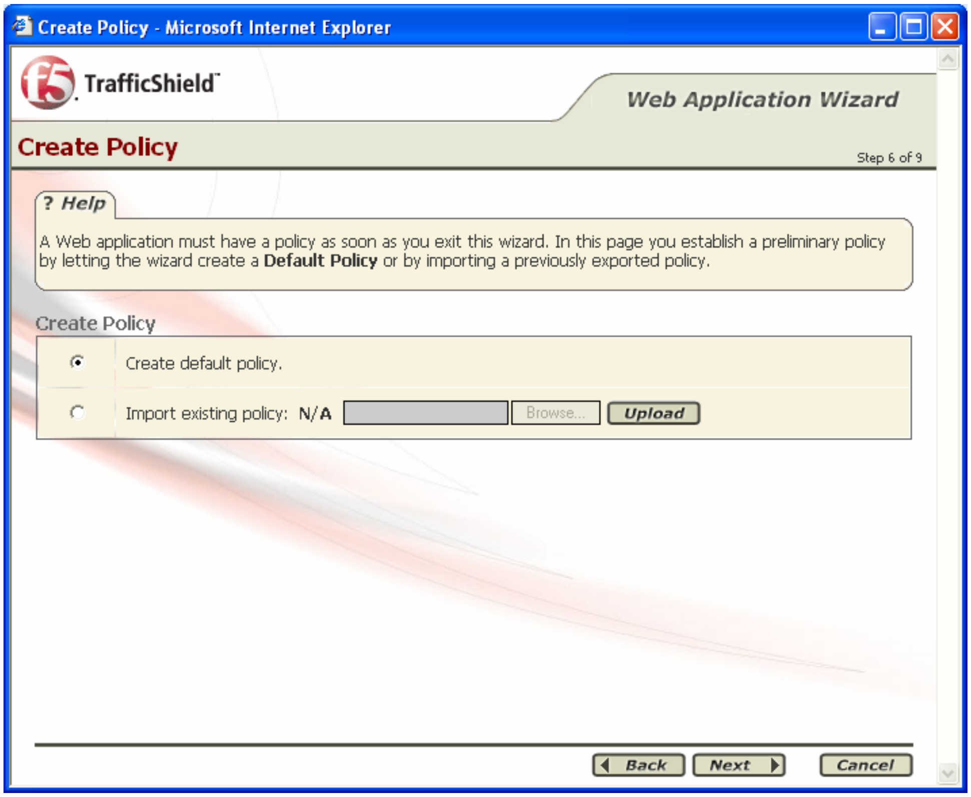
You need to define in advance all of the aliases that might appear in requests addressed to this Web application. TrafficShield security application will block requests containing undefined destinations.

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.

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

Step 6: Create Policy



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.

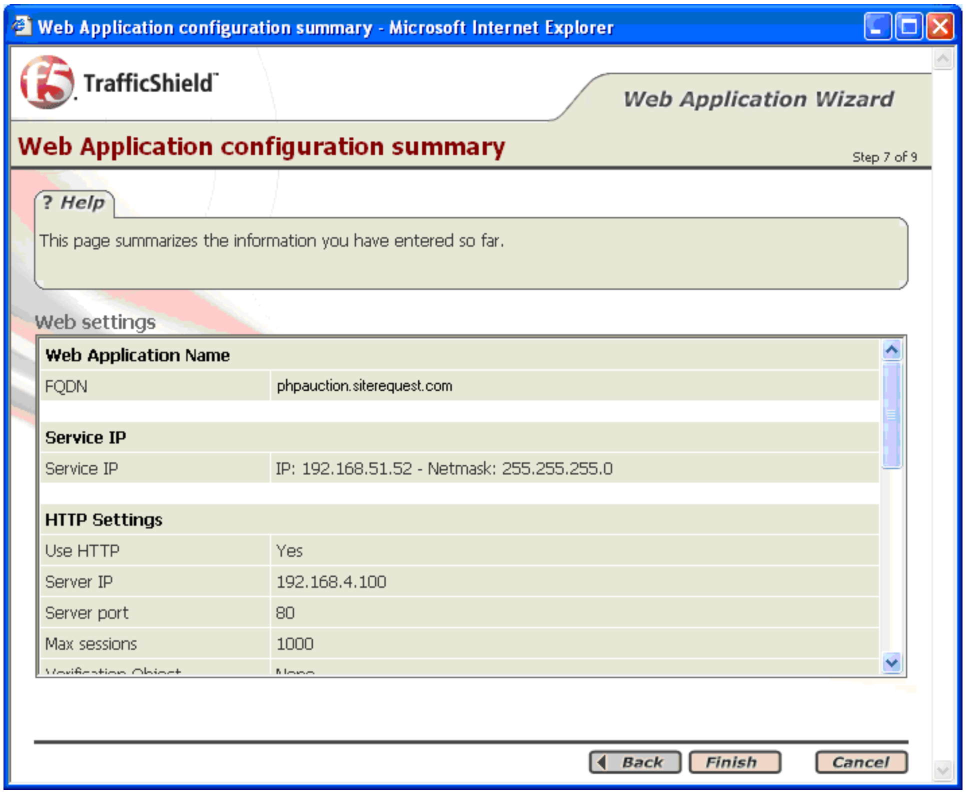
● Create default policy.

○ Import existing policy: N/A

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 Default Policy or by importing a previously exported policy.

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

Step 7: Web Application configuration summary


Web Application configuration summary - Microsoft Internet Explorer
TrafficShield
Web Application Wizard
Web Application configuration summary
Step 7 of 9
? Help
Back
Finish
Cancel

This page summarizes the information you have entered so far.

Web settings

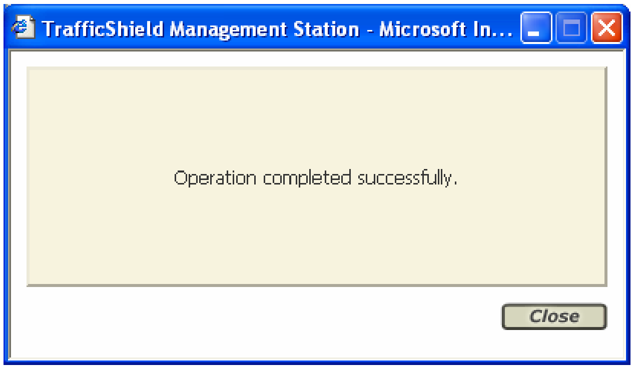
Web Application Name	
FQDN	phpauction.siterequest.com
Service IP	
Service IP	IP: 192.168.51.52 - Netmask: 255.255.255.0
HTTP Settings	
Use HTTP	Yes
Server IP	192.168.4.100
Server port	80
Max sessions	1000
Verification Object	None

Upon completion of the wizard configuration, the Web Application configuration summary window is displayed. Review this information and use the:

- *Back* button to go to the previous step.

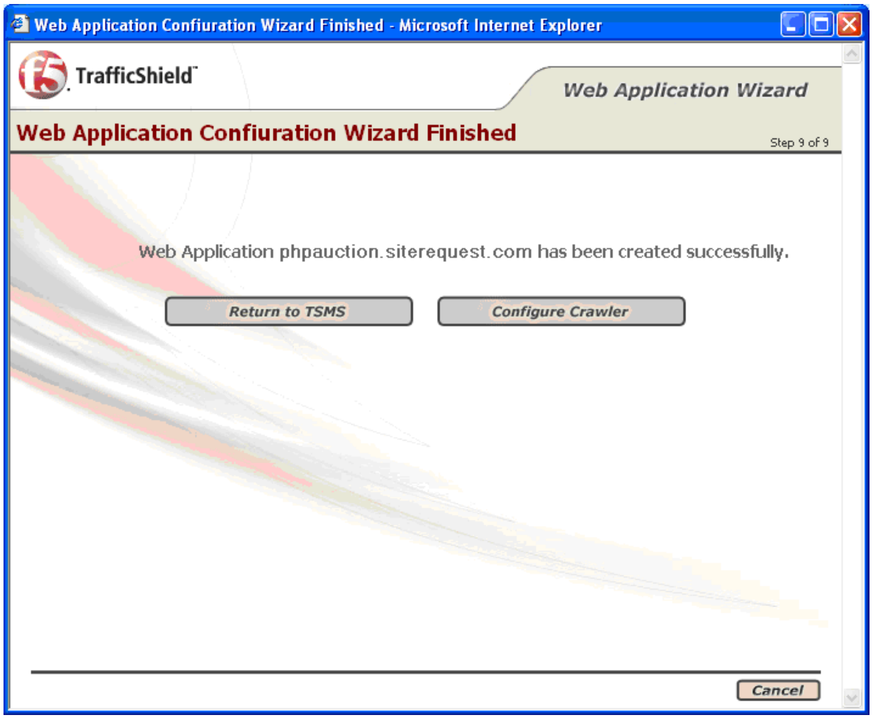
- *Cancel* to exit without saving.
- *Finish* button to save and exit the Wizard.

After Clicking the *Finish* button the following successful completion message is displayed:



Operation completed successfully.

Step 8: Web Application Wizard Finished


Web Application Confiuration Wizard Finished - Microsoft Internet Explorer
TrafficShield
Web Application Wizard
Web Application Confiuration Wizard Finished
Step 9 of 9

Web Application phpauction.siterequest.com has been created successfully.

Return to TSMS
Configure Crawler
Cancel

This screen offers 2 options:

- Return to TSMS – Returns to the TSMS window.
- Configure Crawler – Automatically opens the Crawler configuration Wizard.

Tip

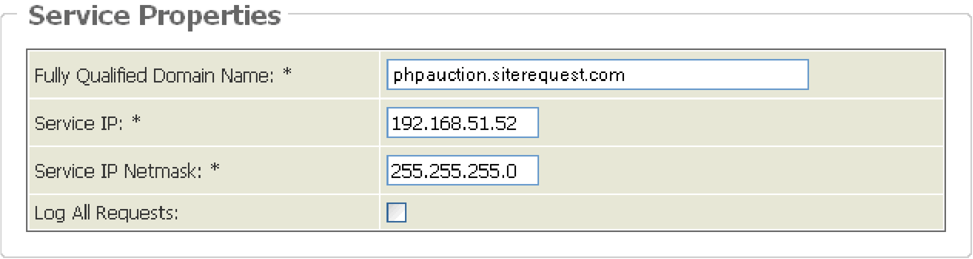
Regardless of your choice (Return to TSMS or Run the Crawler Wizard), we recommend that you activate your default policy before using it. Choose the *Set active Policy* located in the Administration->Configuration->Web Application Window.

Or click the *Close* button to exit the wizard.

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: *	phpauction.siterequest.com
Service IP: *	192.168.51.52
Service IP Netmask: *	255.255.255.0
Log All Requests:	□

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.*yourcompany*.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.

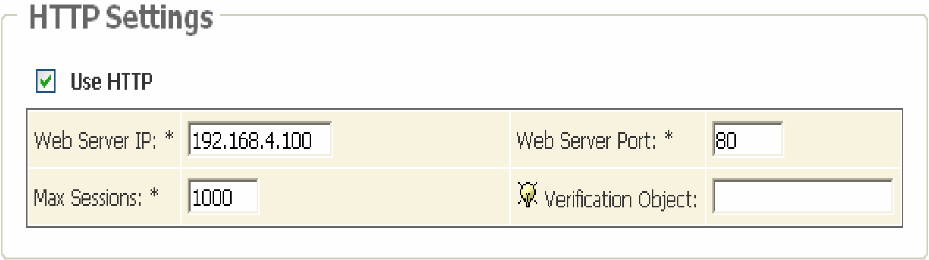
Log All Requests

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

☑ Use HTTP

Web Server IP: *	192.168.4.100	Web Server Port: *	80
Max Sessions: *	1000	Verification Object:	

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.

Note

The distributed Application feature is not supported at this time.

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

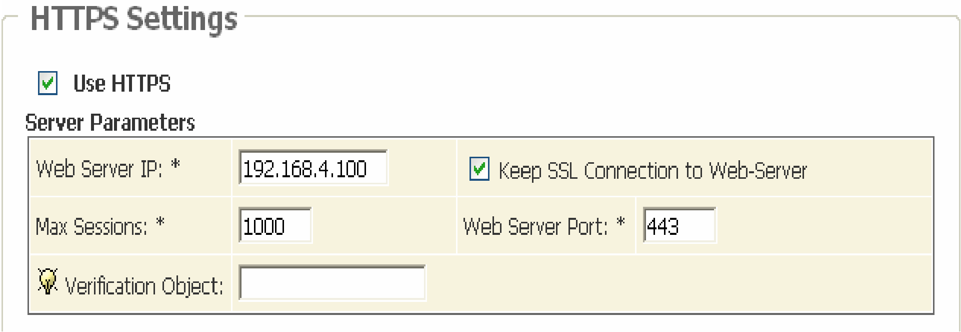
If you are not familiar with your server configuration, you need to consult with your system administrator about the maximum number of simultaneous clients, connection time-out definitions, etc.

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: *	192.168.4.100	☑ Keep SSL Connection to Web-Server	
Max Sessions: *	1000	Web Server Port: *	443
Verification Object:			

Use HTTPS

To allow HTTPS access to the Web application, check 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” 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.

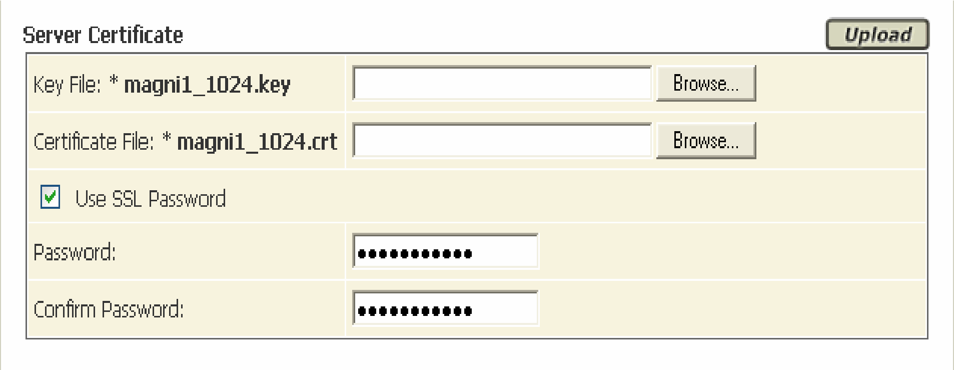
Keep SSL connection to web-server

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: * magni1_1024.key

Certificate File: * magni1_1024.crt

☑ Use SSL Password

Password: ●●●●●●●●●●●●

Confirm 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 PEM format.

Use SSL Password checkbox

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

Password

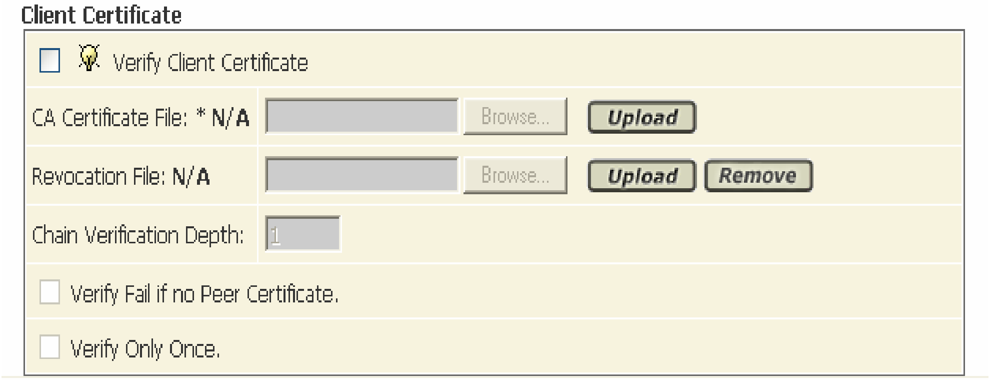
Specify the password for key file.

Confirm Password

Type password again for conformation.

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: 1

□ Verify Fail if no Peer Certificate.

□ Verify Only Once.

Enter the following information:

Verify Client Certificate

Check the Verify Client Certificate checkbox 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 checkbox to terminate the SSL handshake if no client certificate was provided.

Verify Only Once

Check this checkbox 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" checkbox 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 checkbox 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).

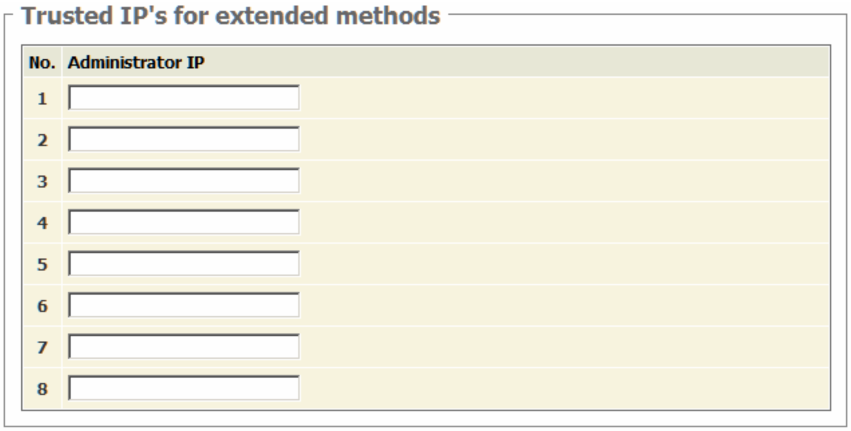
You need to define in advance all of the aliases that might appear in requests addressed to this Web application. TrafficShield security application will block requests containing undefined destinations.

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.



Trusted IP's for extended methods

No.	Administrator IP
1	
2	
3	
4	
5	
6	
7	
8	

Chapter 5 Administration

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.

Users

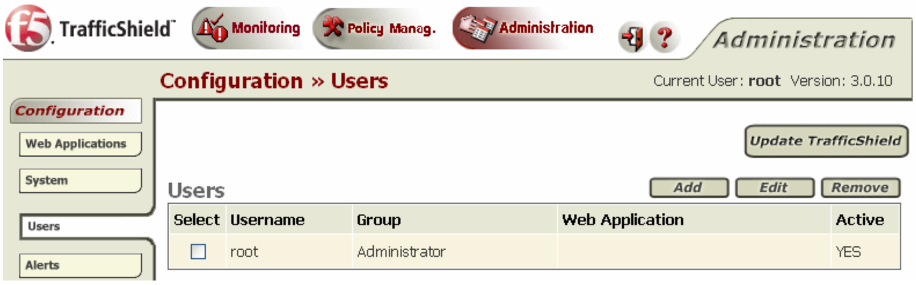
During the installation stage you were asked to define the TSMS Administrator as the initial super user. It is possible to add additional users who are authorized to access the TrafficShield security application and back up TrafficShield data.

To add users:

1. Select the Administration button.

2. In the Configuration menu, select the Users tab.

   The Users page appears.



Configuration » Users

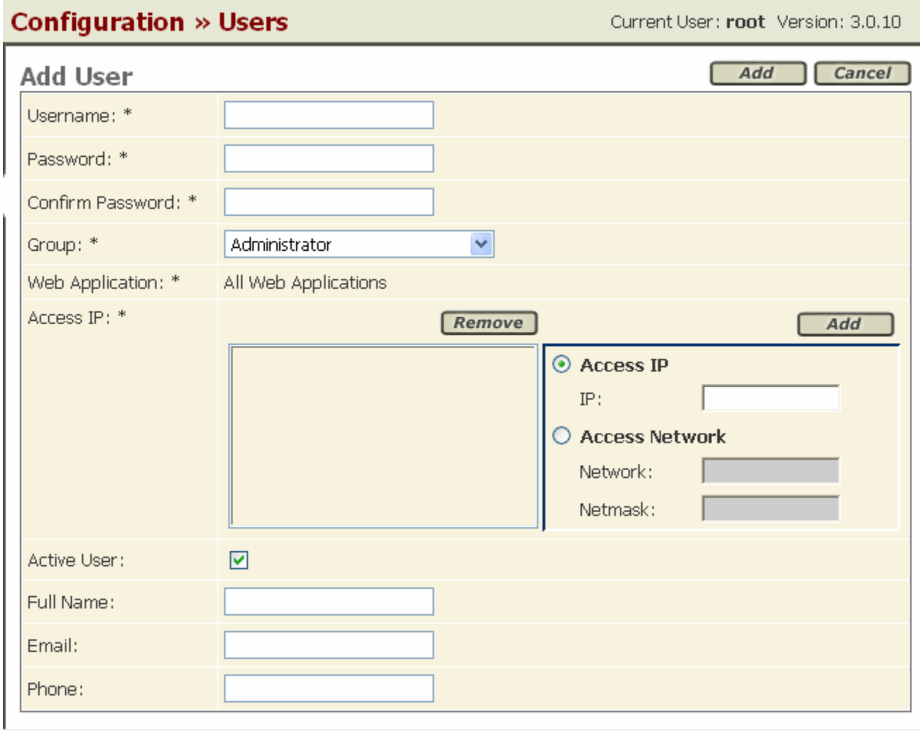
Current User: **root** Version: 3.0.10

Users

Select	Username	Group	Web Application	Active
□	root	Administrator		YES

3. Click the Add button.

The Add User page opens.



Configuration » Users   Current User: **root** Version: 3.0.10

Add User

Username: *	
Password: *	
Confirm Password: *	
Group: *	Administrator
Web Application: *	All Web Applications
Access IP: *	● Access IP IP: ○ Access Network Network: Netmask:
Active User:	☑
Full Name:	
Email:	
Phone:	

4. Enter the information described below:

Username

Enter the name that the user should specify when accessing TSMS.

Password

Enter the password that the user should specify when accessing TSMS.

Confirm Password

Enter the password again.

Group

The group determines the operations that this user will be allowed to perform in the TrafficShield security application. Select the group to which this user belongs. 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 Administrator	Access 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 module 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 module only. Users in this group can only view data.

Web Application

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.

Access IP

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.

Active User

Clear this box to withdraw this user's access permissions without deleting the user record. Check the box again to re-enable the user.

Full Name, E-mail, Phone

Enter the full name, e-mail address and the telephone number of this user.

5. Do one of the following:

   - To allow access from individual IP addresses, select the Access IP radio button.
   - To allow access from any IP address in a network, select the Access Network radio button.

6. Enter the IP address or the network address.
7. Click the Add button.

   The address moves to the box on the left.

   You can remove an address by selecting it in the left box and clicking the Remove button.

8. Repeat the procedure for all relevant addresses.
9. Click the Add button.

   This closes the Add User page. The user record appears in the main page.

10. Click the Update TrafficShield button.

Alerts

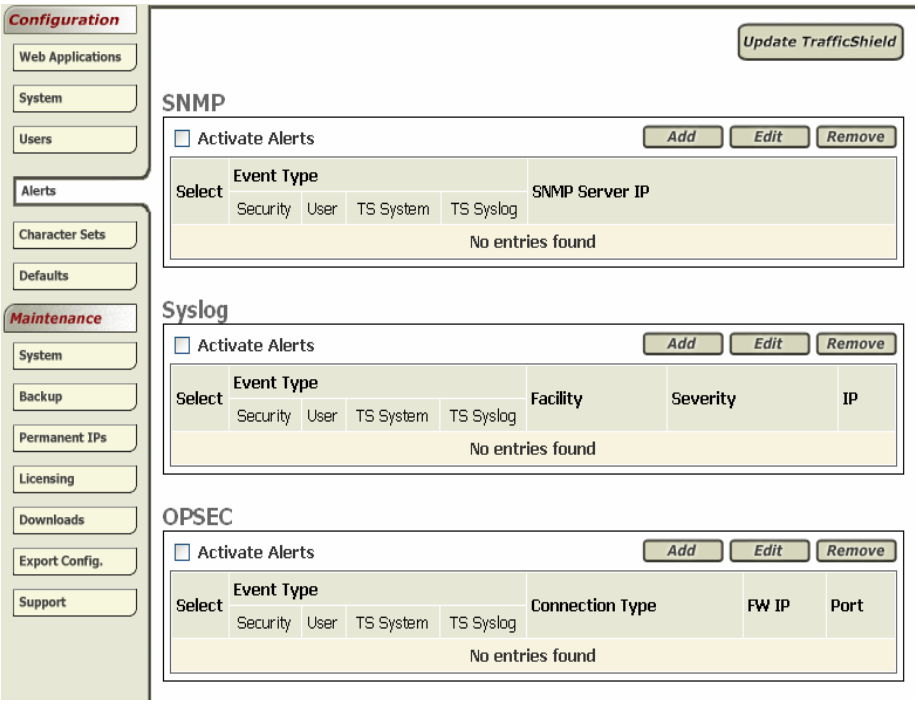
The alerts feature allows you to collect events and to send them to SNMP, Syslog or/and OPSEC. The TrafficShield alerts mechanism can collect events of different types.

To collect alerts:

1. Select the Administration button.

2. In the Configuration menu, select Alerts.

   The Alerts page opens. 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.



SNMP

□ Activate Alerts

Select	Event Type				SNMP Server IP
	Security	User	TS System	TS Syslog	
No entries found					

Syslog

□ Activate Alerts

Select	Event Type				Facility	Severity	IP
	Security	User	TS System	TS Syslog			
No entries found							

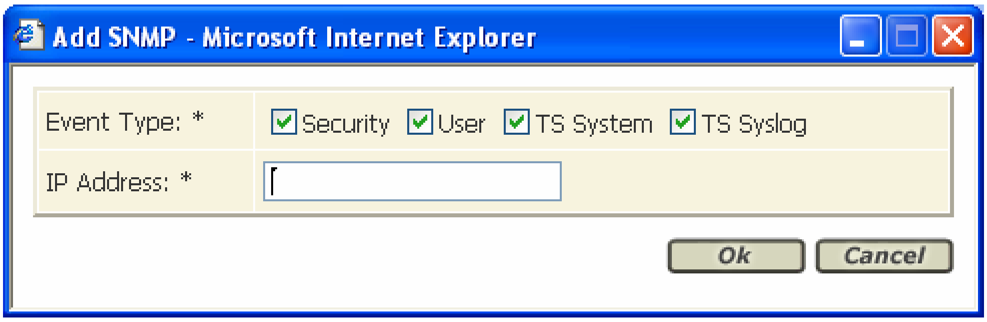
OPSEC

□ Activate Alerts

Select	Event Type				Connection Type	FW IP	Port
	Security	User	TS System	TS Syslog			
No entries found							

3. Click the Add button in a section.

   The "add" box opens.



Event Type: *	☑ Security ☑ User ☑ TS System ☑ TS Syslog
IP Address: *	

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

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

5. Enter the server IP address relating to the server that will receive the events.

6. If necessary, repeat the operation to create alert collection records that combine different types of alerts and/or send alerts to different servers.

7. Click the "Update TrafficShield" button.

Character Sets

The TrafficShield security application can be set to allow certain characters to appear in certain sections of a request. For example, you can allow letters, digits and the slash (/) in a path to an object but exclude the “@” character from it. Such exclusion causes TrafficShield security application to apply the Alarm/Blocking policy to the request that contains the excluded character.

Character sets can be defined for header values, object paths and user input (key value pairs).

For example, a path to an object may include the “/“character but not the name of a parameter. Therefore, a set should be defined for paths, which allows the “/” character, and another set should be defined for parameters, which excludes the “/” character.

In addition, you can define the valid character set for the data expected to be entered by the Web application users in a supported language. For example, if your application contains a form where users can type information in French, you can determine which characters are allowed when entering information in French; data entered in a form that contains characters not included in the French character set, as you have defined it, will activate the Alarm/Blocking mechanism.

Although the TrafficShield Application Firewall is shipped with default character sets for each such element, you can change them if you want. This section shows you how to enter such changes. When building a policy you can further fine-tune the character set for input languages.

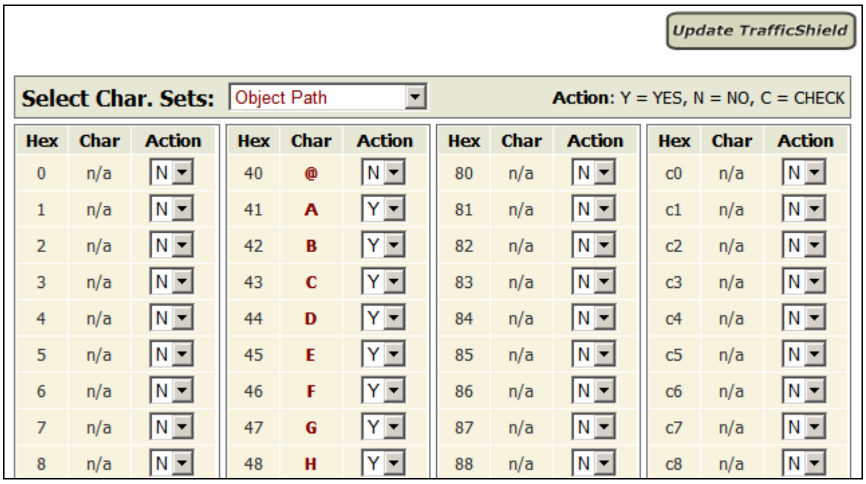
To build character sets:

1. Select the Administration button.
2. Click the Character Sets tab.
3. In Select Char. Set list, open the list and select the application element or input language for which you want to define a valid character set.

   The options are:

Option	**Allows you to determine the characters allowed in**
Object Path	The path to an object.
Param Name	Parameter names.
HTTP Headers	The header section of an HTTP request.
Language names	User input in a specific language. For example, if your Web application supports French and you select User Input: French, data typed in by Web application users in form fields is verified against the French character set.

After selecting an option, TrafficShield security application displays an entire character set.



Update TrafficShield

Select Char. Sets: Object Path ▾ Action: Y = YES, N = NO, C = CHECK

Hex	Char	Action	Hex	Char	Action	Hex	Char	Action	Hex	Char	Action
0	n/a	N	40	@	N	80	n/a	N	c0	n/a	N
1	n/a	N	41	A	Y	81	n/a	N	c1	n/a	N
2	n/a	N	42	B	Y	82	n/a	N	c2	n/a	N
3	n/a	N	43	C	Y	83	n/a	N	c3	n/a	N
4	n/a	N	44	D	Y	84	n/a	N	c4	n/a	N
5	n/a	N	45	E	Y	85	n/a	N	c5	n/a	N
6	n/a	N	46	F	Y	86	n/a	N	c6	n/a	N
7	n/a	N	47	G	Y	87	n/a	N	c7	n/a	N
8	n/a	N	48	H	Y	88	n/a	N	c8	n/a	N

4. In the Action field of each character, select one of the following:

Action	Means
N	No. The character is invalid. An incoming request that contains this character will be blocked.
Y	Yes. The character is valid. An incoming request that contains this character will be let through.
C	Check, is equal to N, unless its explicitly defined as allowed in the Parameter Characteristics table under Application Flow (Policy Management module). If the character is allowed there, then the request is valid. **Note** C isn't available for headers, URI, etc.

5. Repeat the above procedure for other application sections or input languages, if necessary.
6. Click the Update TrafficShield button.

Defaults

Negative Regular Expressions Policy Defaults

TrafficShield 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

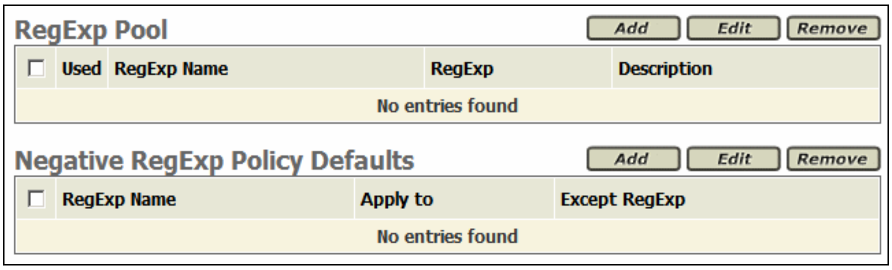
When you create an expression it goes to a pool of expressions. Subsequently, you can select expressions from the pool and assign them to various application elements.

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.



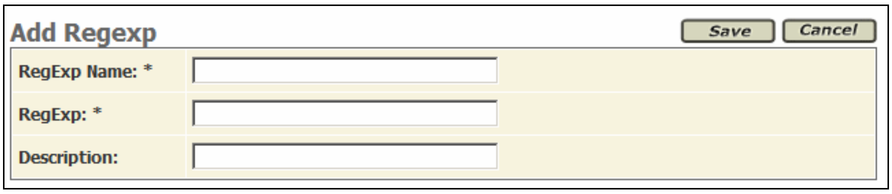
RegExp Pool

☐	Used	RegExp Name	RegExp	Description
		No entries found		

Negative RegExp Policy Defaults

☐	RegExp Name	Apply to	Except RegExp
		No entries found	

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



Add Regexp

RegExp Name: *	
RegExp: *	
Description:	

4. In RexExp Name, enter a name that will help you identify the regular expressions when creating policies.

5. In RegExp, type the expression by following the standard Regular Expression syntax.

6. In Description, optionally type a few words that describe the expression.

7. Click the Save button.
   The regular expression definition appears on the main page.

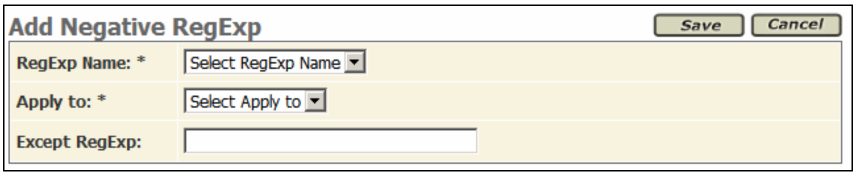
8. Repeat the above procedure for all the expressions you intend to use.

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:

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



RegExp Name: *	Select RegExp Name
Apply to: *	Select Apply to
Except RegExp:	

4. 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:

Option	Applies the regular expression to
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 follows 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.

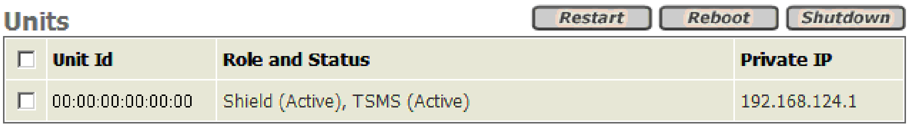
8. Repeat the above procedure for all the expressions you intend to use.

System

You can shutdown or reboot a TrafficShield unit, or restart the TSMS from within the TSMS GUI. Some modifications in the configuration require you to restart the units. The modifications that require restarting are explained in the appropriate sections of this manual.

To restart, reboot, or shutdown TrafficShield system:

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



Units

□	Unit Id	Role and Status	Private IP
□	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].

Reboot

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

Note

If you have a hot backup unit installed, it will become the active unit and the other re-booted unit will become the hot backup unit.

Shutdown

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

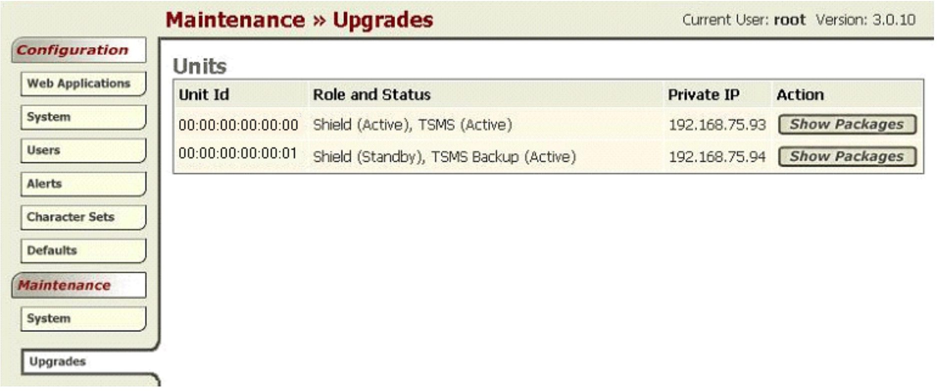
Upgrades

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 asked to restart or reboot the TrafficShield unit.

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 a main unit and a hot backup

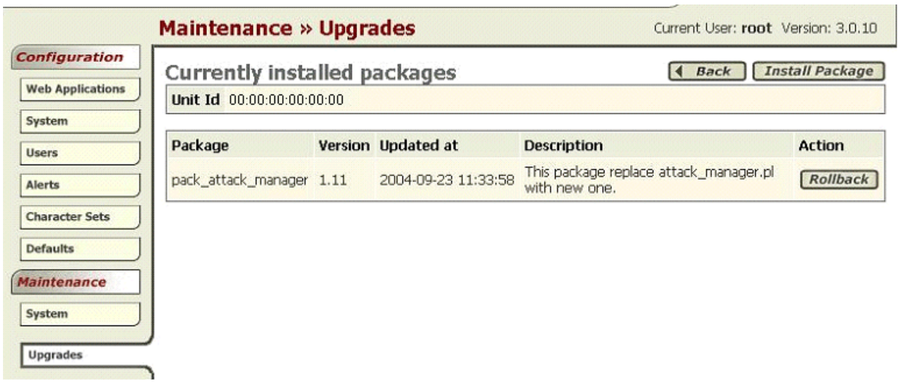
unit, you will need to upgrade each unit separately.



Units

Unit Id	Role and Status	Private IP	Action
00:00:00:00:00:00	Shield (Active), TSMS (Active)	192.168.75.93	Show Packages
00:00:00:00:00:01	Shield (Standby), TSMS Backup (Active)	192.168.75.94	Show Packages

3. Choose the relevant unit to upgrade and click the *Show Packages* button. The Currently Installed packages window will be displayed.



Currently installed packages

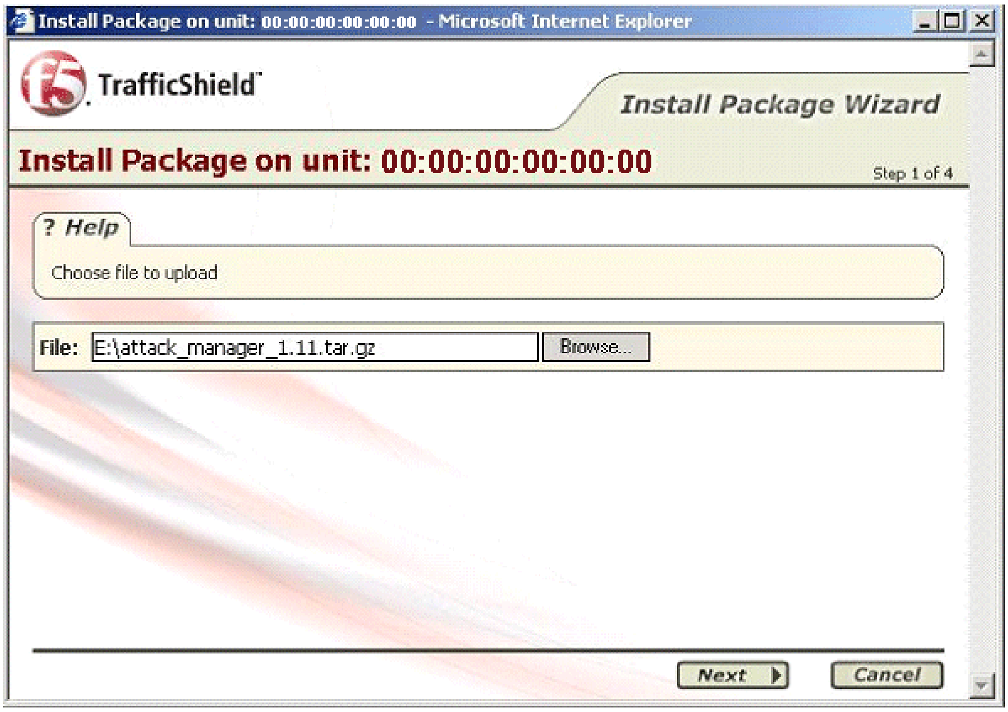
Unit Id 00:00:00:00:00:00

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

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

Install Package Wizard

Step 1: Upload the package file



Install Package on unit: 00:00:00:00:00:00 - Microsoft Internet Explorer
TrafficShield
Install Package Wizard
Step 1 of 4
? Help
Browse...
Next
Cancel

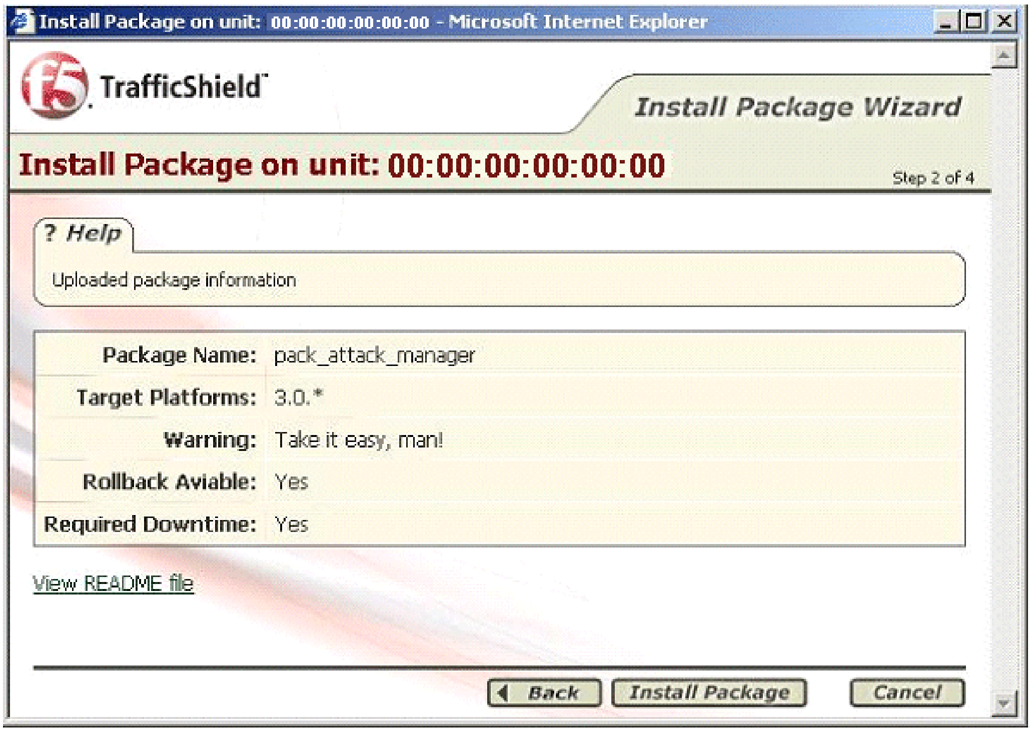
Install Package on unit: 00:00:00:00:00:00

Choose file to upload

File: E:\attack_manager_1.11.tar.gz

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

Step 2: Package Information uploaded and displayed


Install Package on unit: 00:00:00:00:00:00 - Microsoft Internet Explorer
TrafficShield
Install Package Wizard

Install Package on unit: 00:00:00:00:00:00

Step 2 of 4

? Help

Uploaded package information

Package Name:	pack_attack_manager
Target Platforms:	3.0.*
Warning:	Take it easy, man!
Rollback Aviable:	Yes
Required Downtime:	Yes

View README file

Back
Install Package
Cancel

Package Name

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

Target Platforms

This is the TrafficShield software 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 click the Set Active Policy button to activate this package).

Rollback Available

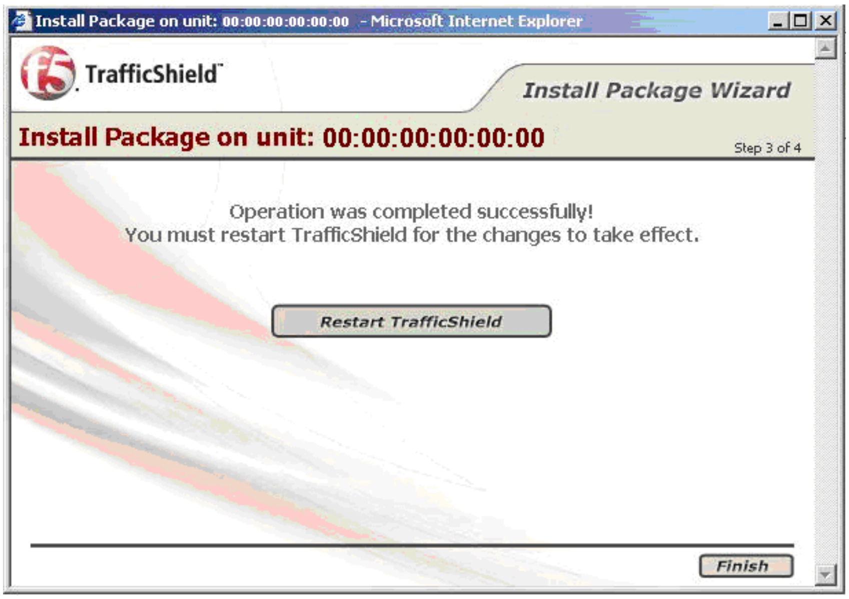
This field indicates whether it is possible to roll back to previous status after installation, should problems occur.

Required Downtime

Sometimes the new package must be installed only after the TrafficShield unit has been put in standby mode. 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



Install Package on unit: 00:00:00:00:00:00

Operation was completed successfully!
You must restart TrafficShield for the changes to take effect.

- 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.

Rollback

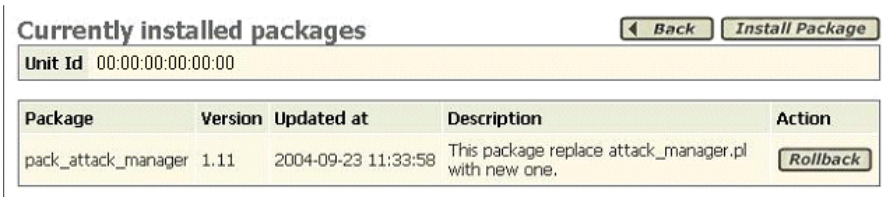
After installing a new software package, problems may occur due to unforeseen circumstances. In some cases it is possible to roll back after installing a new software package. If you have already installed five sequential packages and you roll back the fifth package, you will roll back to the fourth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

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 a main unit and a hot backup 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

Note

If you have already installed five sequential packages, and you roll back the third package, you will roll back to the second package.

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 username 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, for example if it was configured with a request “all logs” feature, it can reach a very large size, close to 100MB.

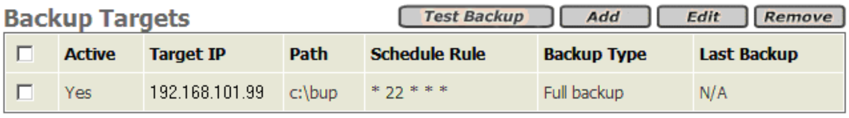
A built in test backup feature enables you to check the accuracy of your settings. See below for details.

Defining Schedules

To schedule backups:

1. Select the Administration button.
2. In the Maintenance menu, select the Backup tab.

   The Backup page opens.

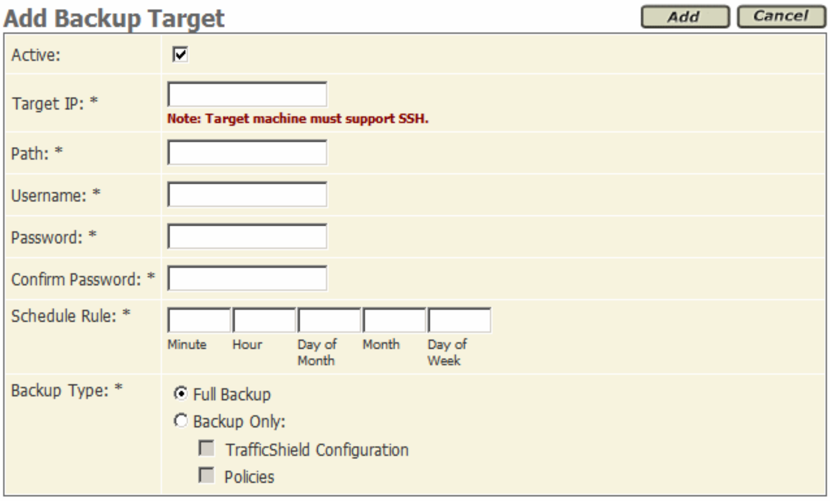


Backup Targets

□	Active	Target IP	Path	Schedule Rule	Backup Type	Last Backup
□	Yes	192.168.101.99	c:\bup	* 22 * * *	Full backup	N/A

3. Click the Add button.

   The Add Backup Target page opens.



Add Backup Target

Active:	☑
Target IP: *	Note: Target machine must support SSH.
Path: *	
Username: *	
Password: *	
Confirm Password: *	
Schedule Rule: *	
Backup Type: *	● Full Backup ○ Backup Only: □ TrafficShield Configuration □ Policies

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 username and the password that are needed to access the backup computer.

Confirm Password

Type the password again.

Schedule Rule

Specify the schedule using the UNIX cron syntax.

Note

Format: *minute hour day month weekday command*

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.

   To select an entry, mark its checkbox on the leftmost column. You can test one backup entry at a time.

2. Click the Test Backup button.

   If all data is correct, a confirmation message appears.

Permanent IPs

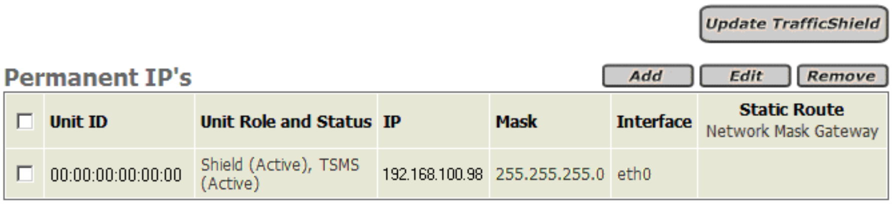
Each TrafficShield security application unit may have one or more permanent IP addresses that remain usable even when TrafficShield processes are down. This is not mandatory. If you need permanent addresses, define them as explained below.

To set a permanent IP address:

1. Select the Administration button at the top of the TSMS window.

2. In the Maintenance menu, select Permanent IPs.

   The Permanent IP's page opens.

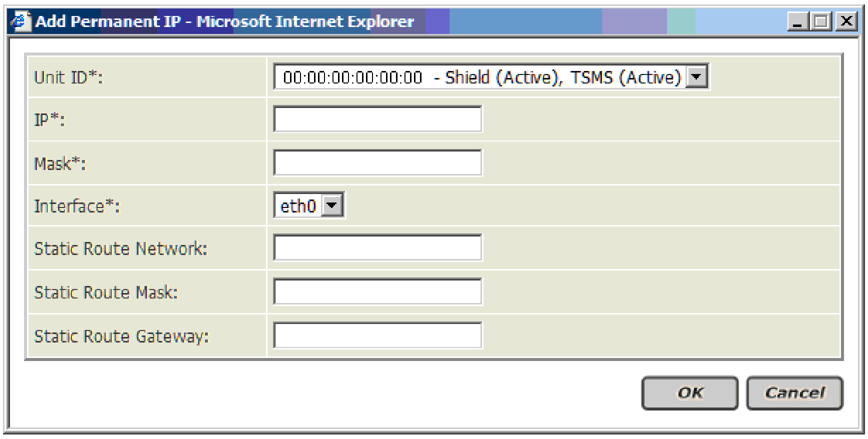


Permanent IP's

☐	Unit ID	Unit Role and Status	IP	Mask	Interface	Static Route Network Mask Gateway
☐	00:00:00:00:00:00	Shield (Active), TSMS (Active)	192.168.100.98	255.255.255.0	eth0	

3. Click the Add button.

   The Add Permanent IP box opens.



Unit ID*:	00:00:00:00:00:00 - Shield (Active), TSMS (Active)
IP*:	
Mask*:	
Interface*:	eth0
Static Route Network:	
Static Route Mask:	
Static Route Gateway:	

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.

Static Route

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

Item	Description
Static Route Network	The destination network address
Static Route Mask	The netmask of the destination network address
Static Route Gateway	The IP address of the gateway

5. Click OK.

   The permanent IP address definition appears on the main page. Repeat the above procedure for all the permanent IP addresses you need to define.

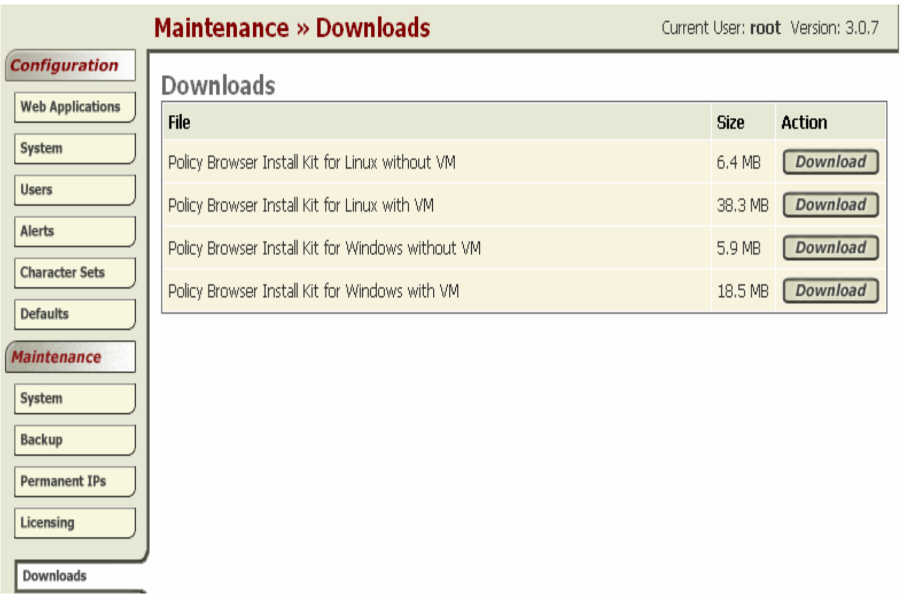
6. Click the Update TrafficShield button to update the unit.

Downloads

Policy Browser

To download the Policy Browser software:

1. In the Administration module, select the Downloads tab under Maintenance.



Maintenance » Downloads

Current User: root Version: 3.0.7

Downloads

File	Size	Action
Policy Browser Install Kit for Linux without VM	6.4 MB	Download
Policy Browser Install Kit for Linux with VM	38.3 MB	Download
Policy Browser Install Kit for Windows without VM	5.9 MB	Download
Policy Browser Install Kit for Windows with VM	18.5 MB	Download

2. Select the relevant Policy Browser Installation Kit from the Downloads list.

3. Choose 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.

Export Configuration

Purpose:

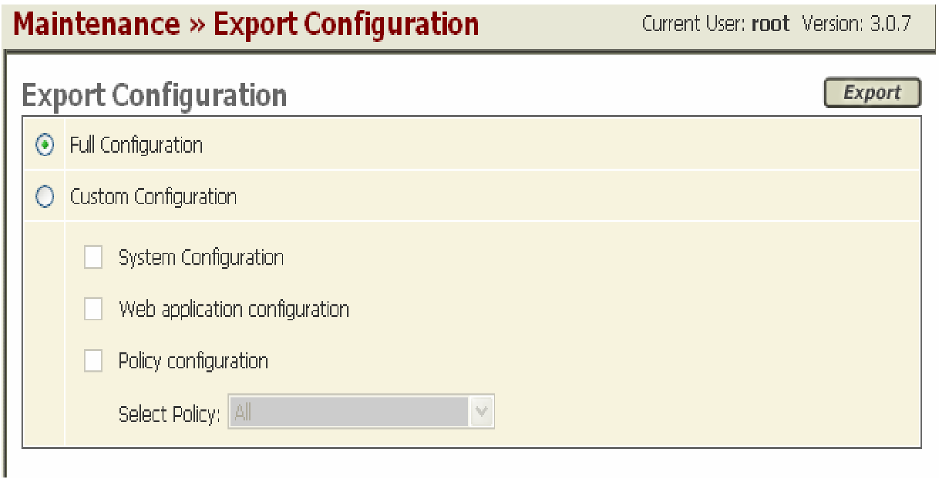
This feature is intended to reproduce a TrafficShield security application unit's existing configuration for troubleshooting customer problems.

Note

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

To export your configuration to a disk:

1. In the Administration module, select the Maintenance -> Export Config. tab.



Maintenance » Export Configuration

Current User: root Version: 3.0.7

Export Configuration

Export

● Full Configuration

○ Custom Configuration

□ System Configuration

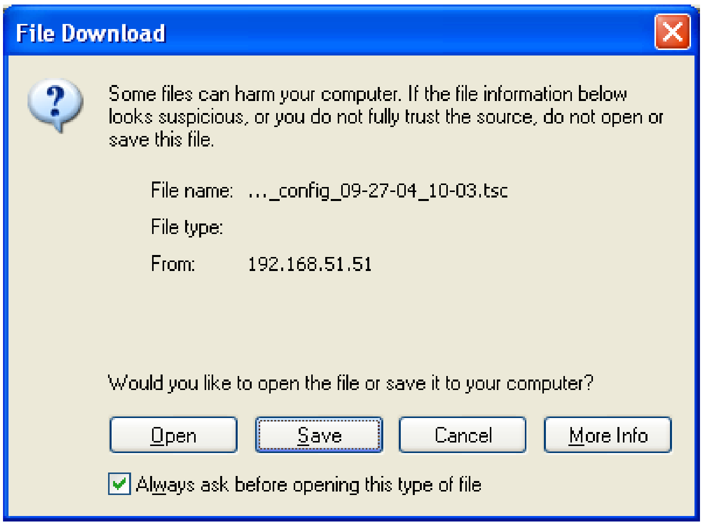
□ Web application configuration

□ Policy configuration

Select Policy: All

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

3. Click the *Export* button. The file Download screen will appear.



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: ..._config_09-27-04_10-03.tsc

File type:

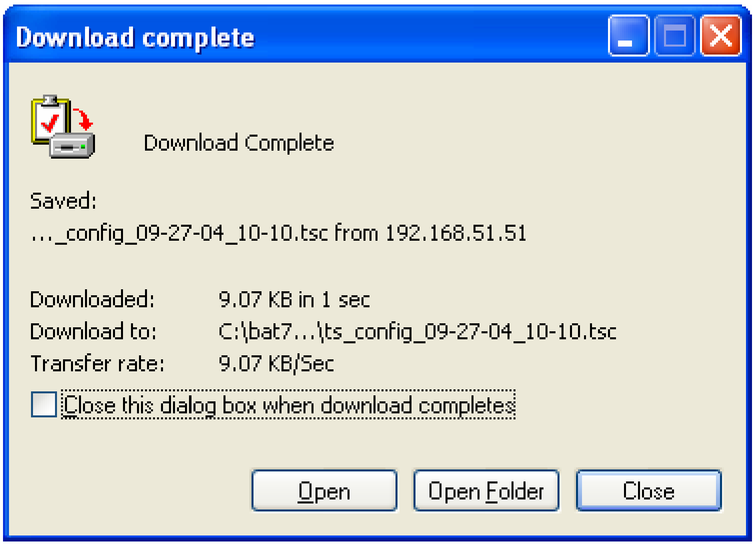
From: 192.168.51.51

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

4. Choose Save to open the browser and select the target folder where you wish to save the exported file.

5. The file is saved to the disk and the Download complete window is opened.



Download complete

Download Complete

Saved:
..._config_09-27-04_10-10.tsc from 192.168.51.51

Downloaded: 9.07 KB in 1 sec
Download to: C:\bat7...\ts_config_09-27-04_10-10.tsc
Transfer rate: 9.07 KB/Sec

□ Close this dialog box when download completes

6. Choose Close to return to the TrafficShield security application.

7. The file was saved with a default name: ts_config_mm-dd-yy_hh-mm.tsc that the user can change before saving.