- Static NAT is configured for a network object (for information, see ***Using Network Objects*** on page 185)
- NAT rules are received from the Service Center

Implicitly defined NAT rules can only be edited or deleted indirectly. For example, in order to remove a NAT rule created when a certain network object was defined, you must modify the relevant network object.

The Address Translation page displays both custom NAT rules and implicitly defined NAT rules, and it allows you to create, edit, and delete custom NAT rules.

How Does Hide NAT Work?

In Hide NAT, traffic to and from the internal networks traverses an enforcement module. When a packet from an internal network passes through the gateway, the source IP address is changed to the hiding IP address, and the source port is changed to a dynamically assigned port that uniquely identifies the connection. The relationship between the dynamically assigned port and the internal IP address is recorded in the gateway's state tables. When reply packets arrive, the enforcement module uses the destination port to determine to which connection the packet belongs, and then adjusts the destination port and IP address accordingly.

Adding and Editing NAT Rules

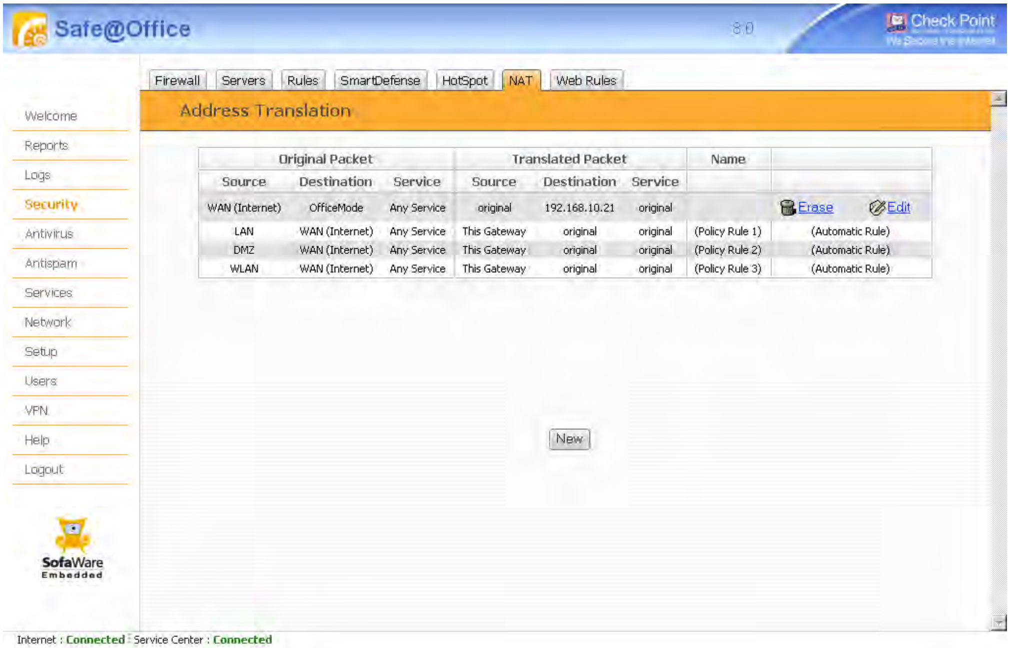
500

This procedure explains how to add and edit *custom* NAT rules. You cannot add or edit an implicitly defined NAT rule directly.

To add or edit a custom NAT rule

1. Click **Security** in the main menu, and click the **NAT** tab.

   The **Address Translation** page appears.



Address Translation

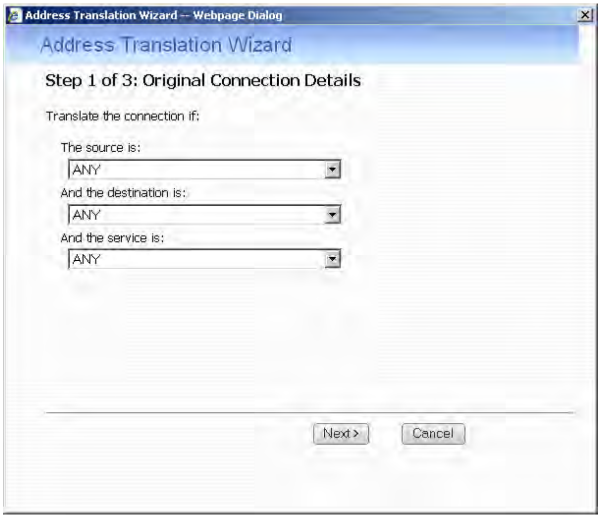
Original Packet			Translated Packet			Name	
Source	Destination	Service	Source	Destination	Service		
WAN (Internet)	OfficeMode	Any Service	original	192.168.10.21	original		Erase Edit
LAN	WAN (Internet)	Any Service	This Gateway	original	original	(Policy Rule 1)	(Automatic Rule)
DMZ	WAN (Internet)	Any Service	This Gateway	original	original	(Policy Rule 2)	(Automatic Rule)
WLAN	WAN (Internet)	Any Service	This Gateway	original	original	(Policy Rule 3)	(Automatic Rule)

Internet : Connected Service Center : Connected

2. Do one of the following:

   - To add a new rule, click **New**.
   - To edit an existing rule, click ✎ next to the desired rule.

The **Address Translation** wizard opens, with the **Step 1 of 3: Original Connection Details** dialog box displayed.



Address Translation Wizard -- Webpage Dialog

Address Translation Wizard

Step 1 of 3: Original Connection Details

Translate the connection if:

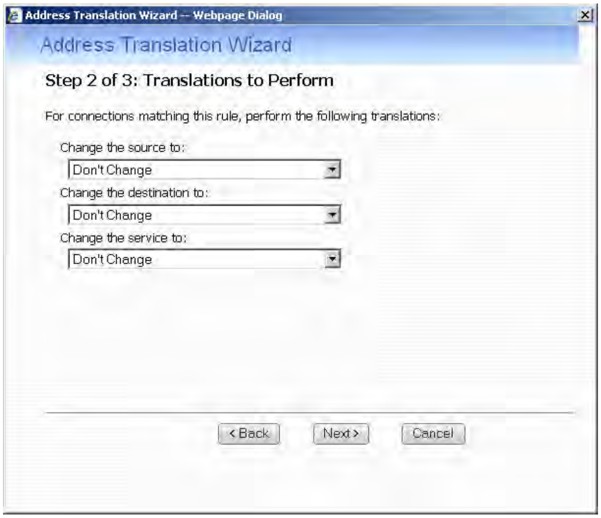
The source is: ANY

And the destination is: ANY

And the service is: ANY

3. Complete the fields using the relevant information in the following table.
4. Click **Next**.

   The **Step 2 of 3: Translations to Perform** dialog box appears.



Address Translation Wizard -- Webpage Dialog

Address Translation Wizard

Step 2 of 3: Translations to Perform

For connections matching this rule, perform the following translations:

Change the source to: Don't Change

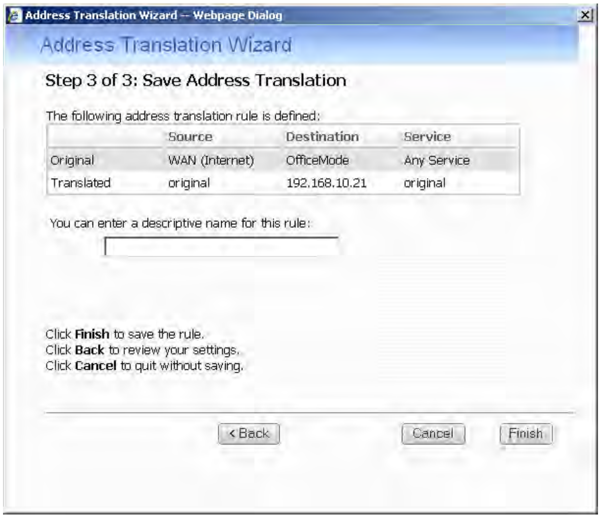
Change the destination to: Don't Change

Change the service to: Don't Change

5. Complete the fields using the relevant information in the following table.

6. Click **Next.**

   The **Step 3 of 3: Save Address Translation** dialog box appears.



Address Translation Wizard -- Webpage Dialog
Address Translation Wizard

Step 3 of 3: Save Address Translation

The following address translation rule is defined:

	Source	Destination	Service
Original	WAN (Internet)	OfficeMode	Any Service
Translated	original	192.168.10.21	original

You can enter a descriptive name for this rule:

Click **Finish** to save the rule.
Click **Back** to review your settings.
Click **Cancel** to quit without saving.

7. If desired, type a description of the rule in the field provided.
8. Click **Finish.**

   The new rule appears in the **Address Translation** page.

Table 67: Address Translation Wizard Fields

Field	Description
The source is	Select the original source of the connections you want to translate. This list includes network objects. To specify an IP address, select **Specified IP** and type the desired IP address in the field provided. To specify an IP address range, select **Specified Range** and type the desired IP address range in the fields provided.

Field	Description
And the destination is	Select the original destination of the connections you want to translate. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify the Safe@Office IP addresses, select This Gateway. To specify any destination *except* the Safe@Office Portal IP addresses, select ANY.
And the service is	Select the original service used for the connections you want to translate. This list includes network service objects.
Change the source to	Select the new source to which the original source should be translated. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify that the original source should not be translated, select Don't Change.

Field	Description
Change the destination to	Select the new destination to which the original destination should be translated. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify that the original destination should not be translated, select Don't Change.
Change the service to	Select the new service to which the original service should be translated. This list includes network service objects. To specify that the original service should not be translated, select Don't Change.

Viewing and Deleting NAT Rules

500

This procedure explains how to view *all* NAT rules and how to delete *custom* NAT rules. You cannot delete implicitly defined NAT rules directly.

To view and delete NAT rules

1. Click Security in the main menu, and click the NAT tab.

   The Address Translation page appears with a list of all existing NAT rules.

   Implicitly defined NAT rules are marked Automatic Rule in the right-most column.

2. To delete a custom NAT rule, do the following.

   a. In the desired rule's row, click 🗑.

A confirmation message appears.

b. Click OK.

The rule is deleted.

Using the EAP Authenticator

Wi-Fi Protected Access Enterprise (WPA-Enterprise) and 802.1x are Network Access Control (NAC) protocols that can be used to authenticate users connecting to the Check Point Safe@Office appliance. Both WPA-Enterprise and 802.1x can be used to control access to the wireless network; however, WPA-Enterprise has the added capability of encrypting transmitted data, and 802.1x can be used to secure connections to the Safe@Office appliance's LAN and DMZ ports as well.

Traditionally, WPA-Enterprise and 802.1x require installing an external Remote Authentication Dial-In User Service (RADIUS) server. When a user tries to authenticate using 802.1x or WPA-Enterprise, the Safe@Office appliance sends the entered user credentials to the RADIUS server. The server then checks whether the RADIUS database contains a matching set of credentials. If so, then the user is logged in.

While purchasing and configuring a RADIUS server may pose little challenge for a large enterprise, such a solution may be costly and complex, and may therefore be unsuitable for smaller networks. In such cases, it is recommended to configure the Safe@Office appliance's built-in Extended Authentication Protocol (EAP) authenticator, which allows using the local user database, enabling the use of WPA-Enterprise or 802.1x without an external RADIUS server.

Workflows

The Safe@Office built-in EAP authenticator can be used to authenticate wireless clients or wired clients connecting to appliance ports.

Using the EAP Authenticator for Authentication of Wireless Clients

500W

To use the EAP authenticator for authentication of wireless clients

1. Configure the Safe@Office appliance as follows:

   a. Configure the desired wireless network for use with the EAP authenticator.

   For information on configuring the primary WLAN, see ***Manually Configuring a Wireless Network*** on page 280. For information on configuring a VAP, see ***Configuring Virtual Access Points*** on page 294.

   Note: The Security field must set to 802.1x or WPA-Enterprise, and the Authentication Server field must be set to Internal User Database.

   b. Ensure that the Safe@Office appliance has a certificate installed in the Safe@Office Portal's VPN > Certificate page.

   The certificate can be any of the following:

   - A self-signed certificate generated by the Safe@Office appliance, version 8.0 or later.

     If a self-signed certificate is installed on the appliance, but was generated by an earlier firmware version, you must generate a new certificate. For instructions on generating a self-signed certificate, see ***Generating a Certificate*** on page 621.

   - A certificate received from the Service Center.

   c. Export the Safe@Office appliance's CA certificate.

   See ***Exporting the Safe@Office Appliance CA Certificate*** on page 630.

d. For each client that should be allowed to connect to the Safe@Office appliance, add a user with Network Access permissions to the local user database.

   See ***Adding and Editing Users*** on page 643.

e. Provide each of the users with the authentication credentials you configured for them.

2. Configure each wireless client as follows:

   a. Configure the client for server authentication.

      See ***Configuring Clients for Server Authentication on Wireless Connections*** on page 398.

   b. Install the Safe@Office appliance's CA certificate as a trusted root CA.

      See ***Installing the Safe@Office Appliance's CA Certificate on Clients*** on page 403.

3. Connect the wireless client to the wireless network.

   See ***Connecting Clients to the Safe@Office Appliance*** on page 408.

Using the EAP Authenticator for Authentication of Wired Clients

Power Pack

To use the EAP authenticator for authentication of wired clients

1. Configure the Safe@Office appliance as follows:

   a. Configure the desired port for port-based security using the Safe@Office EAP authenticator.

      See ***Configuring Port-Based Security*** on page 375.

> Note: The Port Security field must set to 802.1x, and the Authentication Server field must be set to Internal User Database.

   b. Ensure that the Safe@Office appliance has a certificate installed in the Safe@Office Portal's VPN > Certificate page.

The certificate can be any of the following:

- A self-signed certificate generated by the Safe@Office appliance, version 8.0 or later.

  If a self-signed certificate is installed on the appliance, but was generated by an earlier firmware version, you must generate a new certificate. For instructions on generating a self-signed certificate, see ***Generating a Certificate*** on page 621.

- A certificate received from the Service Center.

c. Export the Safe@Office appliance's CA certificate.

See ***Exporting the Safe@Office Appliance CA Certificate*** on page 630.

d. For each client that should be allowed to connect to the Safe@Office appliance, add a user with Network Access permissions to the local user database.

See ***Adding and Editing Users*** on page 643.

e. Provide each of the users with the authentication credentials you configured for them.

2. Configure each wireless client as follows:

a. Configure the client for server authentication.

See ***Configuring Clients for Server Authentication on Wired Connections*** on page 401.

b. Install the Safe@Office appliance's CA certificate as a trusted root CA.

See ***Installing the Safe@Office Appliance's CA Certificate on Clients*** on page 403.

3. Connect the client directly to the port, and enter the Network Access user's authentication credentials when prompted.

Configuring Clients for Server Authentication on Wireless Connections

500W

To configure a Microsoft Windows client for server authentication

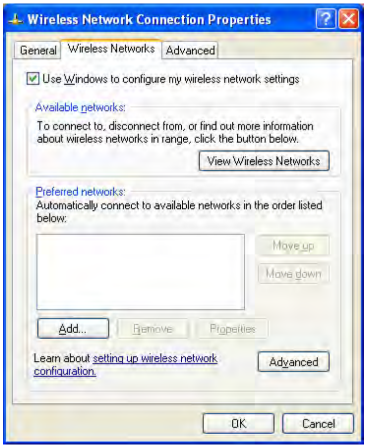
1. In the START menu, click Control Panel.
2. Click Network Connections.
3. Double-click on the wireless network connection.
4. Do one of the following:

   - If the Choose a Wireless Network screen appears, click Change Advanced Settings.
   - If you are already connected to a wireless network, click Properties.

   The Wireless Network Connection Properties dialog box appears displaying the General tab.

5. Click the Wireless Networks tab.

   The Wireless Networks tab appears.



☑ Use Windows to configure my wireless network settings

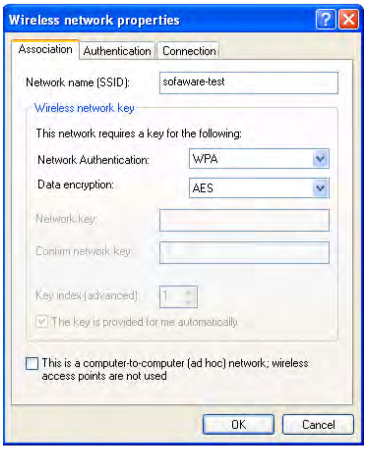
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

6. Click Add and add your network.

The **Wireless network properties** dialog box appears displaying the **Association** tab.



Network name (SSID): sofaware-test

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: AES

Network key:

Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

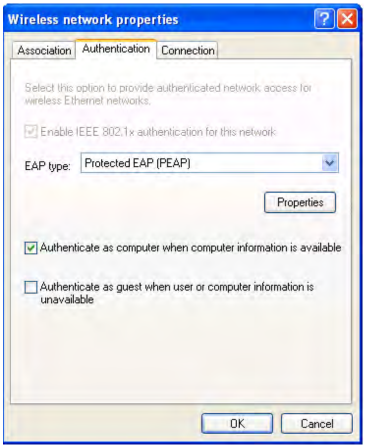
□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

7. In the **Network name (SSID)** field, type the Safe@Office appliance wireless network name.
8. In the **Network Authentication** drop-down list, select **WPA**.

Note: You must select WPA, regardless of whether the Safe@Office appliance is configured to use the WPA-Enterprise or 802.1x security protocol.

9. In the **Data encryption** drop-down list, select **AES**.
10. Click the **Authentication** tab.

The **Authentication** tab appears.



Wireless network properties

Association | Authentication | Connection

Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

Properties

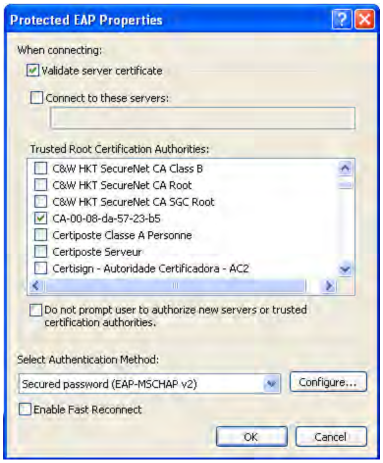
☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

OK | Cancel

11. In the EAP type drop-down list, select **Protected EAP (PEAP)**.
12. Select the **Authenticate as computer when computer information is available** check box.
13. Click **Properties**.

    The **Protected EAP Properties** dialog box appears.



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ C&W HKT SecureNet CA Class B
□ C&W HKT SecureNet CA Root
□ C&W HKT SecureNet CA SGC Root
☑ CA-00-08-da-57-23-b5
□ Certiposte Classe A Personne
□ Certiposte Serveur
□ Certisign - Autoridade Certificadora - AC2

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2) | Configure...

□ Enable Fast Reconnect

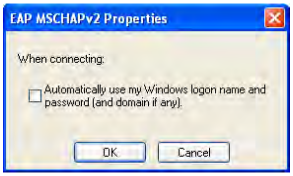
OK | Cancel

14. Make sure that the **Validate server certificate** check box is selected.

15. In the Select Authentication Method drop-down list, select Secured password (EAP-MSCHAP v2).
16. If the user credentials for connecting to the Safe@Office appliance differ from the user credentials for connecting to Windows, do the following:

    a. Click Configure.

    The EAP MSCHAPv2 Properties dialog box appears.

    
    EAP MSCHAPv2 Properties

    When connecting:

    □ Automatically use my Windows logon name and password (and domain if any).

    b. Clear the check box.

    c. Click OK.
17. Click OK in all open windows.

Configuring Clients for Server Authentication on Wired Connections

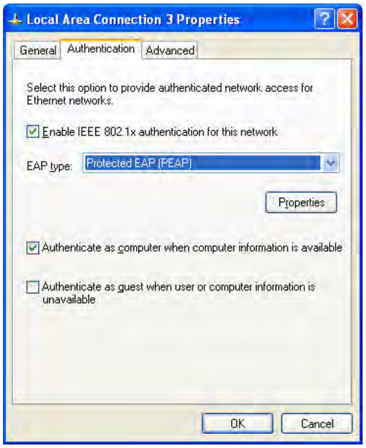
Power Pack

To configure a Microsoft Windows client for server authentication

1. In the START menu, click Control Panel.
2. Click Network Connections.
3. Right-click on Local Area Connection, and click Properties in the popup menu that appears.

   The Local Area Connection Properties dialog box appears displaying the General tab.
4. Click the Authentication tab.

The **Authentication** tab appears.



Local Area Connection 3 Properties

General | Authentication | Advanced

Select this option to provide authenticated network access for Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

Properties

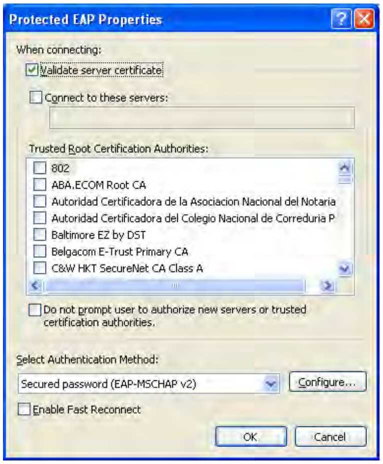
☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

OK | Cancel

5. Select the **Enable IEEE 802.1x authentication for this network** check box.
6. In the **EAP type** drop-down list, select **Protected EAP (PEAP)**.
7. Select the **Authenticate as computer when computer information is available** check box.
8. Click **Properties**.

   The **Protected EAP Properties** dialog box appears.



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ 802
□ ABA.ECOM Root CA
□ Autoridad Certificadora de la Asociacion Nacional del Notaria
□ Autoridad Certificadora del Colegio Nacional de Correduria P
□ Baltimore EZ by DST
□ Belgacom E-Trust Primary CA
□ C&W HKT SecureNet CA Class A

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2) | Configure...

□ Enable Fast Reconnect

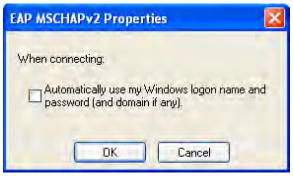
OK | Cancel

9. Make sure that the **Validate server certificate** check box is selected.

10. In the Select Authentication Method drop-down list, select Secured password (EAP-MSCHAP v2).
11. If the user credentials for connecting to the Safe@Office appliance differ from the user credentials for connecting to Windows, do the following:

    a. Click Configure.

    The EAP MSCHAPv2 Properties dialog box appears.



EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

    b. Clear the check box.

    c. Click OK.

12. Click OK in all open windows.

Installing the Safe@Office Appliance's CA Certificate on Clients

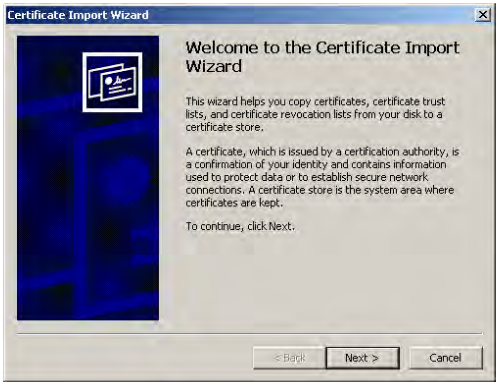
500

To install the Safe@Office appliance's CA certificate on a Microsoft Windows client

1. On the client, right-click on the Safe@Office appliance's CA certificate you exported, and click Install PFX in the pop-up menu that appears.

   For information on exporting the CA certificate, see ***Exporting the Safe@Office Appliance CA Certificate*** on page 630.

The **Certificate Import Wizard** opens displaying the **Welcome to Certificate Import Wizard** screen.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

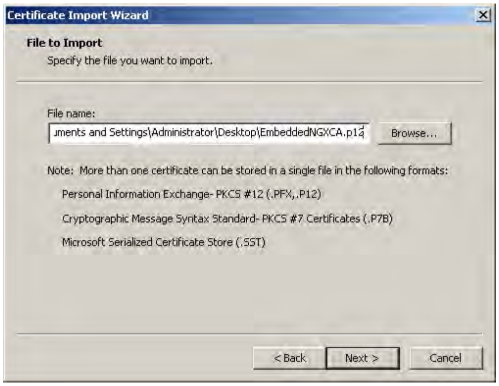
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

2. Click **Next.**

   The **File to Import** dialog box appears.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

ıments and Settings\Administrator\Desktop\EmbeddedNGXCA.p12

Note: More than one certificate can be stored in a single file in the following formats:

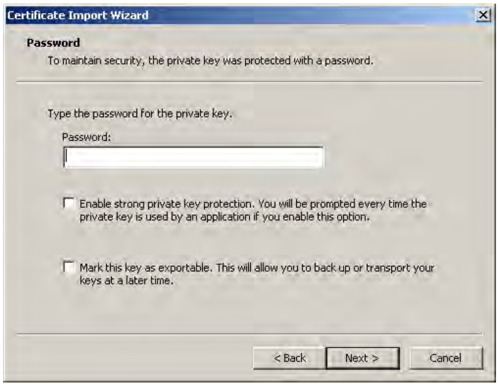
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

3. Browse to the Safe@Office appliance's CA certificate (*.p12 file).
4. Click **Next.**

The **Password** dialog box appears.



To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

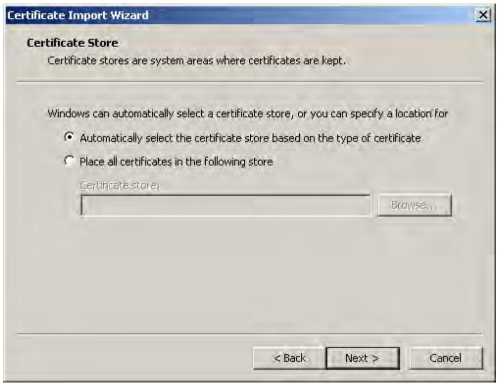
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

Do not type a password.

5. Click **Next**.

   The **Certificate Store** dialog box appears.



Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

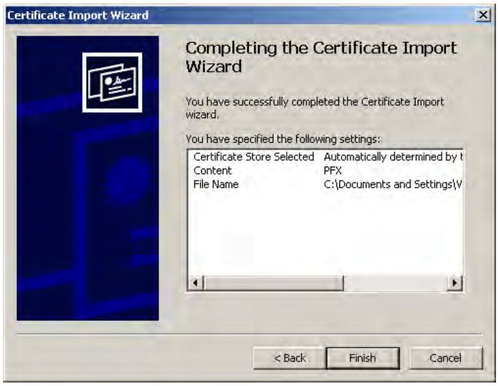
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

6. Click **Automatically select the certificate store based on the type of certificate.**
7. Click **Next.**

The **Completing the Certificate Import Wizard** screen appears.



Completing the Certificate Import Wizard

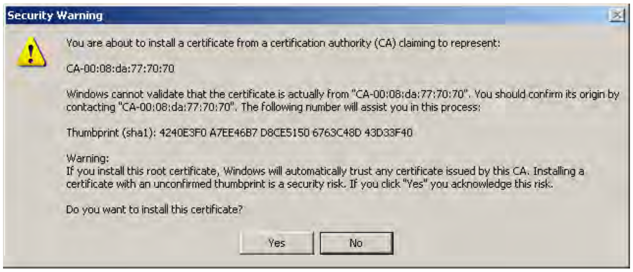
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	C:\Documents and Settings\V

8. Click **Finish.**

   If the Safe@Office appliance certificate was self-signed, a warning message appears.



You are about to install a certificate from a certification authority (CA) claiming to represent:

CA-00:08:da:77:70:70

Windows cannot validate that the certificate is actually from "CA-00:08:da:77:70:70". You should confirm its origin by contacting "CA-00:08:da:77:70:70". The following number will assist you in this process:

Thumbprint (sha1): 4240E3F0 A7EE46B7 D8CE5150 6763C48D 43D33F40

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Do the following:

a. Click **Yes.**

   A success message appears.

b. Click **OK.**

9. To check that the certificate was successfully installed as a trusted root CA, do the following:

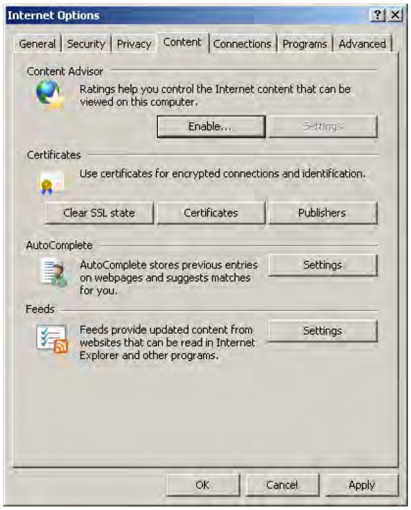
a. On the client, open Internet Explorer.

b. In the **Tools** menu, click **Internet Options.**

   The **Internet Options** dialog box appears displaying the **General** tab.

c. Click the **Content** tab.

The **Content** tab appears.



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

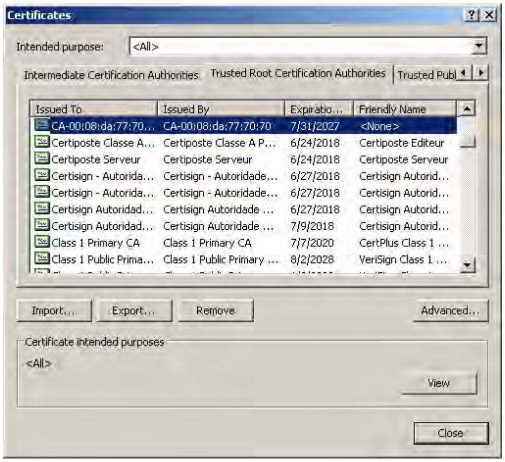
Feeds provide updated content from websites that can be read in Internet Explorer and other programs.

d. Click **Certificates.**

The **Certificates** dialog box appears.

e. Click the **Trusted Root Certification Authorities** tab.

The **Trusted Root Certification Authorities** tab appears.


Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
CA-00:08:da:77:70...	CA-00:08:da:77:70:70	7/31/2027	<None>
Certiposte Classe A...	Certiposte Classe A P...	6/24/2018	Certiposte Editeur
Certiposte Serveur	Certiposte Serveur	6/24/2018	Certiposte Serveur
Certisign - Autorida...	Certisign - Autoridade...	6/27/2018	Certisign Autorid...
Certisign - Autorida...	Certisign - Autoridade...	6/27/2018	Certisign Autorid...
Certisign Autoridad...	Certisign Autoridade ...	6/27/2018	Certisign Autorid...
Certisign Autoridad...	Certisign Autoridade ...	7/9/2018	Certisign Autorid...
Class 1 Primary CA	Class 1 Primary CA	7/7/2020	CertPlus Class 1 ...
Class 1 Public Prima...	Class 1 Public Primary ...	8/2/2028	VeriSign Class 1 ...

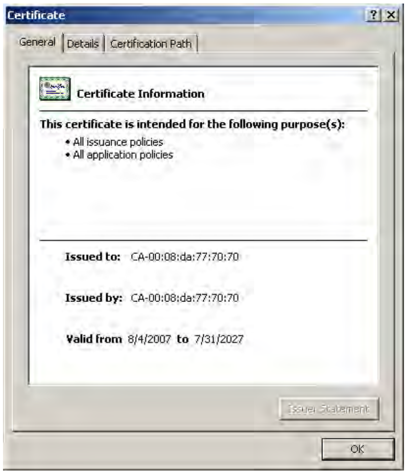
<All>

f. In the list, locate the Safe@Office appliance's CA certificate.

The certificate's name is in the format `CA-<Identifier>`, where `<Identifier>` is the Safe@Office appliance's MAC address or gateway name.

g. To view further information about the certificate, double-click on it.

The Certificate dialog box appears with additional information.



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: CA-00:08:da:77:70:70

Issued by: CA-00:08:da:77:70:70

Valid from 8/4/2007 to 7/31/2027

Connecting Wireless Clients to the Safe@Office Appliance

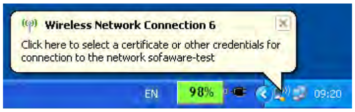
500W

To connect a Microsoft Windows wireless client to the Safe@Office appliance with WPA Enterprise authentication

1. In the START menu, click Control Panel.
2. Click Network Connections.

   A list of wireless networks appears.
3. Select the Safe@Office appliance wireless network.
4. Click Connect.

A popup message appears asking you to supply credentials.

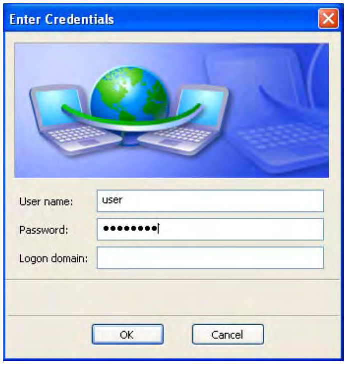


Wireless Network Connection 6

Click here to select a certificate or other credentials for connection to the network sofaware-test

5. Click on the popup message.

The **Enter Credentials** dialog box appears.



User name: user

Password: ••••••••

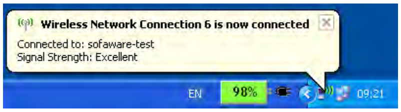
Logon domain:

6. Type the Network Access user's user name and password in the fields provided.

7. Click **OK**.

The wireless client attempts to connect to the network.

Upon successful connection, the client indicates that it is connected to the network.



Wireless Network Connection 6 is now connected

Connected to: sofaware-test
Signal Strength: Excellent

Chapter 14

Using SmartDefense

This chapter explains how to use Check Point SmartDefense Services.

This chapter includes the following topics:

Overview

The Safe@Office appliance includes Check Point SmartDefense Services, based on Check Point Application Intelligence. SmartDefense provides a combination of attack safeguards and attack-blocking tools that protect your network in the following ways:

- Validating compliance to standards
- Validating expected usage of protocols (Protocol Anomaly Detection)
- Limiting application ability to carry malicious data
- Controlling application-layer operations

In addition, SmartDefense aids proper usage of Internet resources, such as FTP, instant messaging, Peer-to-Peer (P2P) file sharing, file-sharing operations, and File Transfer Protocol (FTP) uploading, among others.

Configuring SmartDefense

500

You can configure SmartDefense using the following tools:

- **SmartDefense Wizard.** Resets all SmartDefense settings to their defaults, and then creates a SmartDefense security policy according to your network and security preferences. See ***Using the SmartDefense Wizard*** on page 411.
- **SmartDefense Tree.** Enables you to fine tune individual settings in the SmartDefense policy. You can use the SmartDefense tree instead of, or in addition to, the wizard. See ***Using the SmartDefense Tree*** on page 417.

Using the SmartDefense Wizard

500

The SmartDefense Wizard allows you to configure your SmartDefense security policy quickly and easily through its user-friendly interface.

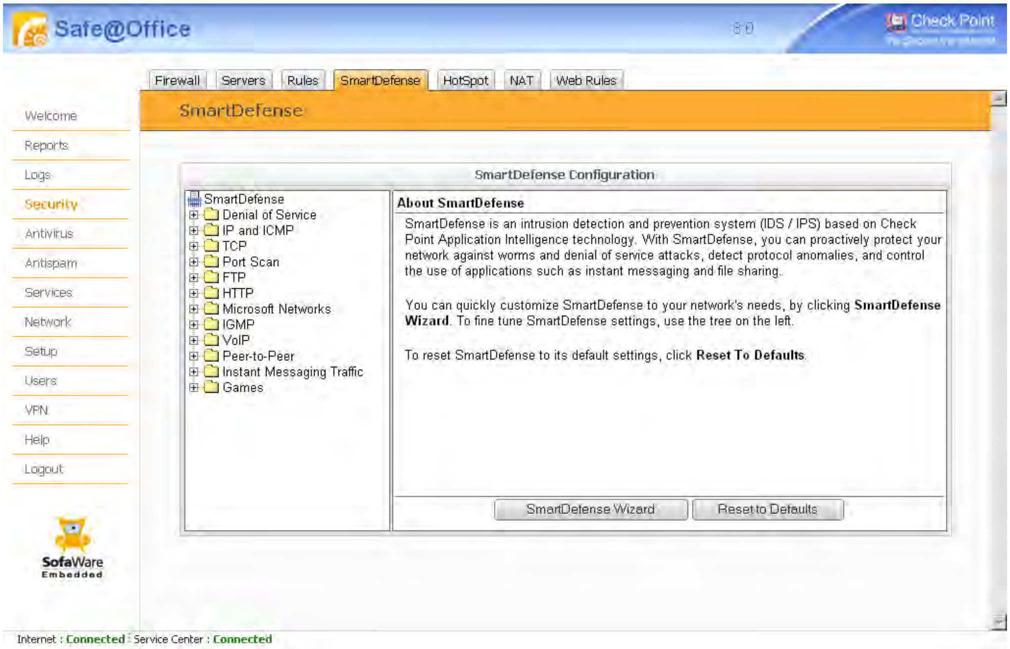
Note: The SmartDefense wizard clears any existing SmartDefense settings.

After using the wizard, you can fine tune the policy settings using the SmartDefense tree. See ***Using the SmartDefense Tree*** on page 417.

To configure the SmartDefense policy using the wizard

1. Click Security in the main menu, and click the SmartDefense tab.

   The SmartDefense page appears.



About SmartDefense

SmartDefense is an intrusion detection and prevention system (IDS / IPS) based on Check Point Application Intelligence technology. With SmartDefense, you can proactively protect your network against worms and denial of service attacks, detect protocol anomalies, and control the use of applications such as instant messaging and file sharing.

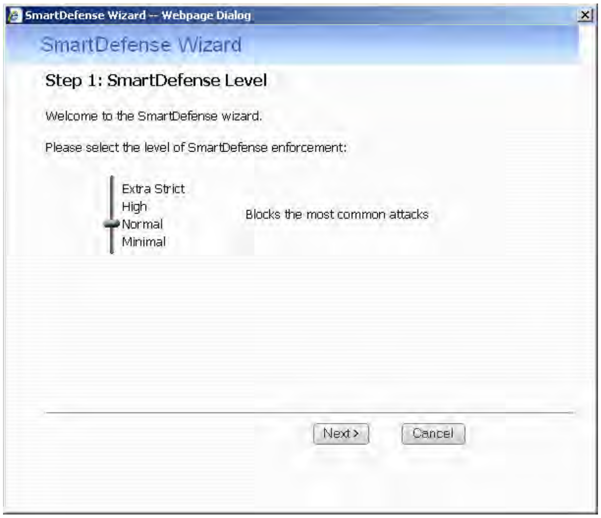
You can quickly customize SmartDefense to your network's needs, by clicking **SmartDefense Wizard**. To fine tune SmartDefense settings, use the tree on the left.

To reset SmartDefense to its default settings, click **Reset To Defaults**.

Internet : Connected : Service Center : Connected

2. Click SmartDefense Wizard.

The **SmartDefense Wizard** opens, with the **Step 1: SmartDefense Level** dialog box displayed.



SmartDefense Wizard -- Webpage Dialog

SmartDefense Wizard

Step 1: SmartDefense Level

Welcome to the SmartDefense wizard.

Please select the level of SmartDefense enforcement:

Extra Strict
High
Normal
Minimal

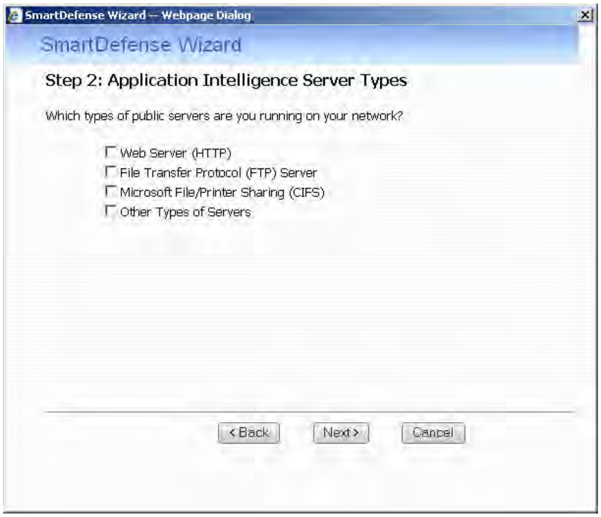
Blocks the most common attacks

3. Drag the lever to the desired level of SmartDefense enforcement.

   For information on the levels, see the following table.

4. Click **Next**.

   The **Step 2: Application Intelligence Server Types** dialog box appears.



SmartDefense Wizard -- Webpage Dialog

SmartDefense Wizard

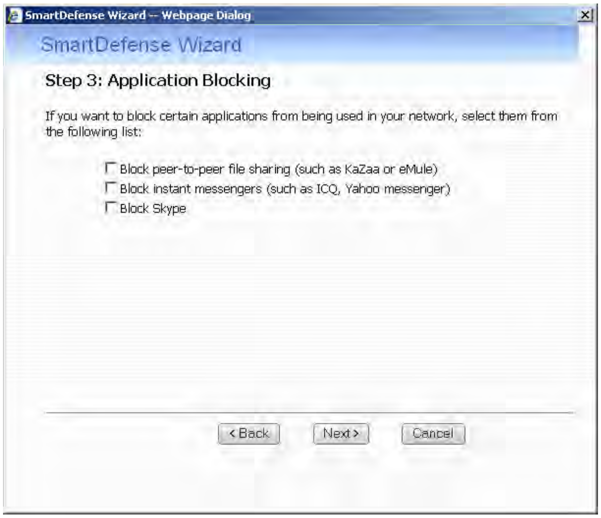
Step 2: Application Intelligence Server Types

Which types of public servers are you running on your network?

□ Web Server (HTTP)
□ File Transfer Protocol (FTP) Server
□ Microsoft File/Printer Sharing (CIFS)
□ Other Types of Servers

5. Select the check boxes next to the types of public servers that are running on your network.
6. Click **Next**.

   The **Step 3: Application Blocking** dialog box appears.



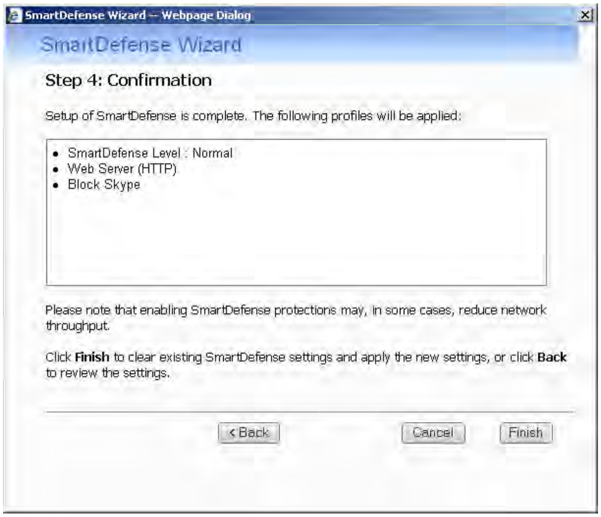
Step 3: Application Blocking

If you want to block certain applications from being used in your network, select them from the following list:

□ Block peer-to-peer file sharing (such as KaZaa or eMule)
□ Block instant messengers (such as ICQ, Yahoo messenger)
□ Block Skype

7. Select the check boxes next to the types of applications you want to block from running on your network.
8. Click **Next**.

The **Step 4: Confirmation** dialog box appears.



Step 4: Confirmation

Setup of SmartDefense is complete. The following profiles will be applied:

- SmartDefense Level : Normal
- Web Server (HTTP)
- Block Skype

Please note that enabling SmartDefense protections may, in some cases, reduce network throughput.

Click **Finish** to clear existing SmartDefense settings and apply the new settings, or click **Back** to review the settings.

9. Click **Finish**.

   Existing SmartDefense settings are cleared, and the security policy is applied.

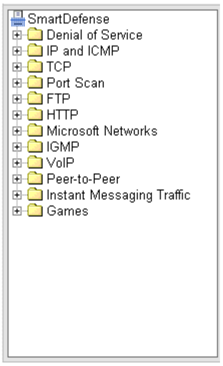
Table 68: SmartDefense Security Levels

This level...	Does this...
Minimal	Disables all SmartDefense protections, except those that cannot be disabled.
Normal	Enables the following: • Teardrop • Ping of Death • LAND • Packet Sanity • Max Ping Size (set to 1500) • Welchia • Cisco IOS • Null Payload • IGMP • Small PMTU (Log Only) This level blocks the most common attacks.
High	Enables the same protections as Normal level, as well as the following: • Host Port Scan • Sweep Scan • HTTP Header Rejection • Strict TCP (Log Only)
Extra Strict	Enables the same protections as High level, as well as the following: • Strict TCP (Log + Block) • Small PMTU (Log + Block) • Max Ping Size (set to 512) • Network Quota

Using the SmartDefense Tree

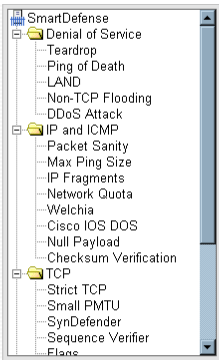
500

For convenience, SmartDefense is organized as a tree, in which each branch represents a category of settings.



- SmartDefense
  - Denial of Service
  - IP and ICMP
  - TCP
  - Port Scan
  - FTP
  - HTTP
  - Microsoft Networks
  - IGMP
  - VoIP
  - Peer-to-Peer
  - Instant Messaging Traffic
  - Games

When a category is expanded, the settings it contains appear as nodes. For information on each category and the nodes it contains, see ***SmartDefense Categories*** on page 419.



- SmartDefense
  - Denial of Service
    - Teardrop
    - Ping of Death
    - LAND
    - Non-TCP Flooding
    - DDoS Attack
  - IP and ICMP
    - Packet Sanity
    - Max Ping Size
    - IP Fragments
    - Network Quota
    - Welchia
    - Cisco IOS DOS
    - Null Payload
    - Checksum Verification
  - TCP
    - Strict TCP
    - Small PMTU
    - SynDefender
    - Sequence Verifier
    - Flags

Each node represents an attack type, a sanity check, or a protocol or service that is vulnerable to attacks. To control how SmartDefense handles a specific attack, you must configure the relevant node's settings.

To configure a SmartDefense node

1. Click **Security** in the main menu, and click the **SmartDefense** tab.

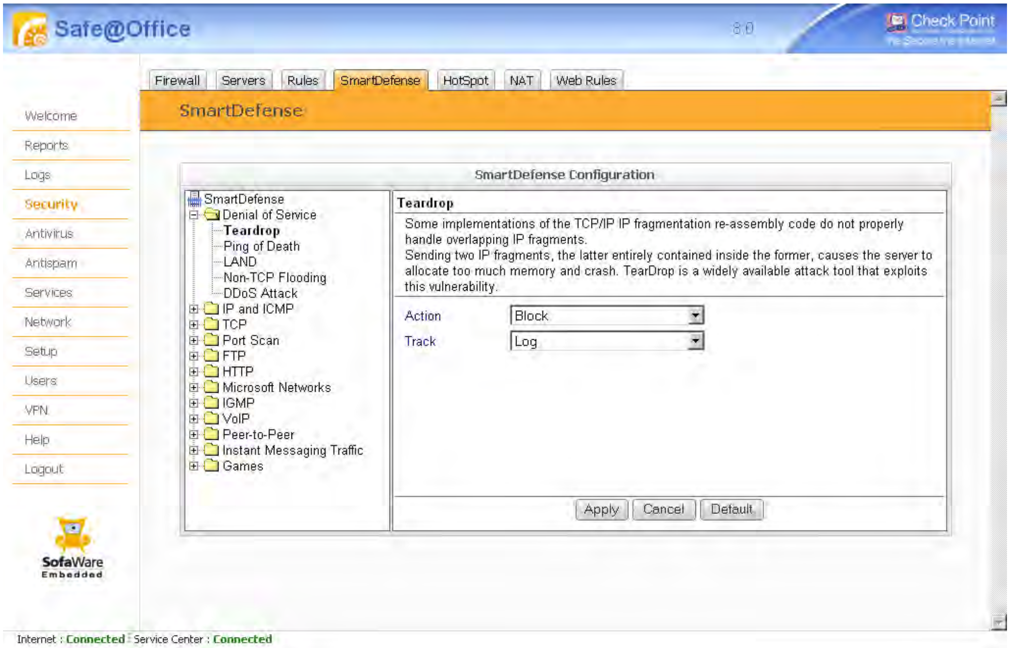
   The **SmartDefense** page appears.

   The left pane displays a tree containing SmartDefense categories.

   - To expand a category, click the ⊞ icon next to it.
   - To collapse a category, click the ⊟ icon next to it.

2. Expand the relevant category, and click on the desired node.

   The right pane displays a description of the node, followed by fields.



Teardrop

Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments.
Sending two IP fragments, the latter entirely contained inside the former, causes the server to allocate too much memory and crash. TearDrop is a widely available attack tool that exploits this vulnerability.

Action: Block

Track: Log

Internet : Connected Service Center : Connected

3. To modify the node's current settings, do the following:

   a) Complete the fields using the relevant information in ***SmartDefense Categories*** on page 419.

   b) Click **Apply**.

4. To reset the node to its default values:

   a) Click **Default**.

      A confirmation message appears.

   b) Click **OK**.

      The fields are reset to their default values, and your changes are saved.

SmartDefense Categories

SmartDefense includes the following categories:

- ***Denial of Service*** on page 420
- ***FTP*** on page 446
- ***HTTP*** on page 451
- ***IGMP*** on page 455
- ***Instant Messaging Traffic*** on page 461
- ***IP and ICMP*** on page 426
- ***Microsoft Networks*** on page 453
- ***Peer-to-Peer*** on page 459
- ***Port Scan*** on page 444
- ***TCP*** on page 437
- ***VoIP*** on page 456
- ***Games*** on page 463

Denial of Service

Denial of Service (DoS) attacks are aimed at overwhelming the target with spurious data, to the point where it is no longer able to respond to legitimate service requests.

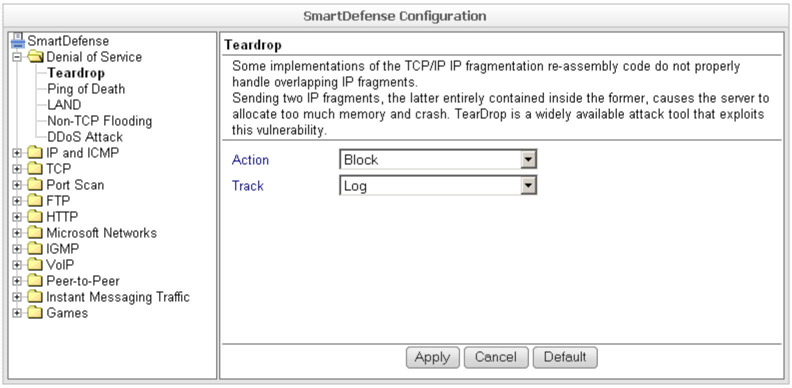
This category includes the following attacks:

- ***DDoS Attack*** on page 425
- ***LAND*** on page 422
- ***Non-TCP Flooding*** on page 423
- ***Ping of Death*** on page 421
- ***Teardrop*** on page 420

Teardrop

In a Teardrop attack, the attacker sends two IP fragments, the latter entirely contained within the former. This causes some computers to allocate too much memory and crash.

You can configure how Teardrop attacks should be handled.



SmartDefense Configuration

Teardrop

Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments.
Sending two IP fragments, the latter entirely contained inside the former, causes the server to allocate too much memory and crash. TearDrop is a widely available attack tool that exploits this vulnerability.

Action: Block
Track: Log

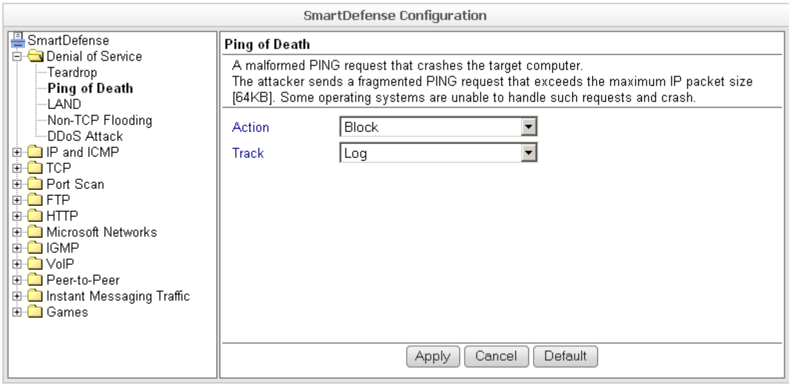
Table 69: Teardrop Fields

In this field...	Do this...
Action	Specify what action to take when a Teardrop attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Teardrop attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Ping of Death

In a Ping of Death attack, the attacker sends a fragmented PING request that exceeds the maximum IP packet size (64KB). Some operating systems are unable to handle such requests and crash.

You can configure how Ping of Death attacks should be handled.



SmartDefense Configuration

Ping of Death

A malformed PING request that crashes the target computer.
The attacker sends a fragmented PING request that exceeds the maximum IP packet size [64KB]. Some operating systems are unable to handle such requests and crash.

Action: Block

Track: Log

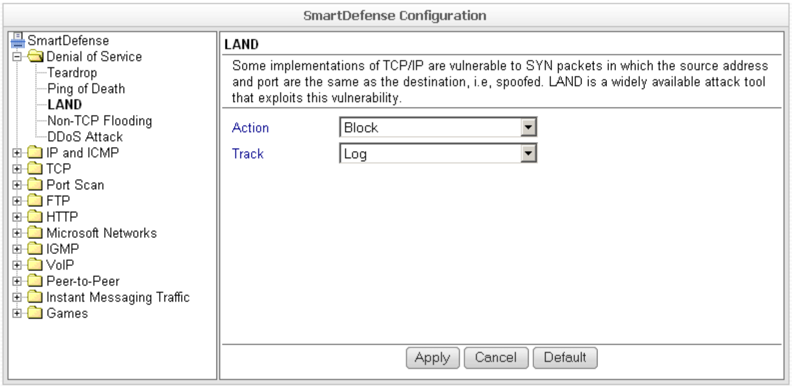
Table 70: Ping of Death Fields

In this field…	Do this…
Action	Specify what action to take when a Ping of Death attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Ping of Death attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

LAND

In a LAND attack, the attacker sends a SYN packet, in which the source address and port are the same as the destination (the victim computer). The victim computer then tries to reply to itself and either reboots or crashes.

You can configure how LAND attacks should be handled.



SmartDefense Configuration

LAND

Some implementations of TCP/IP are vulnerable to SYN packets in which the source address and port are the same as the destination, i.e, spoofed. LAND is a widely available attack tool that exploits this vulnerability.

Action: Block

Track: Log

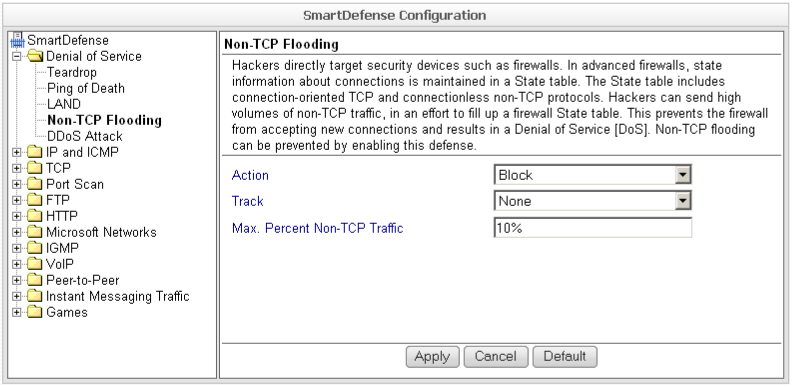
Table 71: LAND Fields

In this field...	Do this...
Action	Specify what action to take when a LAND attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log LAND attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Non-TCP Flooding

Advanced firewalls maintain state information about connections in a State table. In Non-TCP Flooding attacks, the attacker sends high volumes of non-TCP traffic. Since such traffic is connectionless, the related state information cannot be cleared or reset, and the firewall State table is quickly filled up. This prevents the firewall from accepting new connections and results in a Denial of Service (DoS).

You can protect against Non-TCP Flooding attacks by limiting the percentage of state table capacity used for non-TCP connections.



Non-TCP Flooding

Hackers directly target security devices such as firewalls. In advanced firewalls, state information about connections is maintained in a State table. The State table includes connection-oriented TCP and connectionless non-TCP protocols. Hackers can send high volumes of non-TCP traffic, in an effort to fill up a firewall State table. This prevents the firewall from accepting new connections and results in a Denial of Service [DoS]. Non-TCP flooding can be prevented by enabling this defense.

Action	Block
Track	None
Max. Percent Non-TCP Traffic	10%

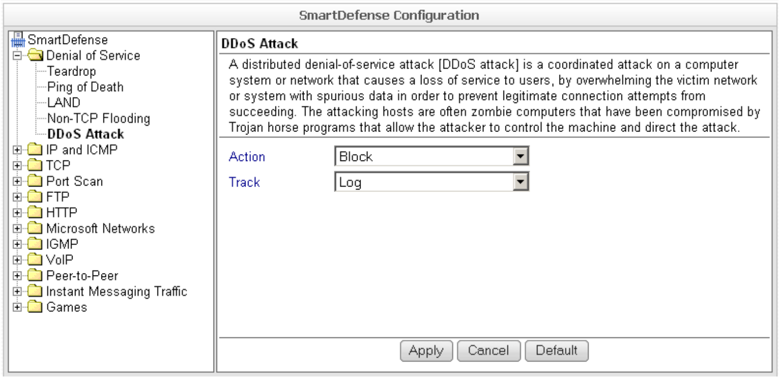
Table 72: Non-TCP Flooding Fields

In this field…	Do this…
Action	Specify what action to take when the percentage of state table capacity used for non-TCP connections reaches the Max. percent non TCP traffic threshold. Select one of the following: • Block. Block any additional non-TCP connections. • None. No action. This is the default.
Track	Specify whether to log non-TCP connections that exceed the Max. Percent Non-TCP Traffic threshold, by selecting one of the following: • Log. Log the connections. • None. Do not log the connections. This is the default.
Max. Percent Non-TCP Traffic	Type the maximum percentage of state table capacity allowed for non-TCP connections. The default value is 10%.

DDoS Attack

In a distributed denial-of-service attack (DDoS attack), the attacker directs multiple hosts in a coordinated attack on a victim computer or network. The attacking hosts send large amounts of spurious data to the victim, so that the victim is no longer able to respond to legitimate service requests.

You can configure how DDoS attacks should be handled.



SmartDefense Configuration

DDoS Attack

A distributed denial-of-service attack [DDoS attack] is a coordinated attack on a computer system or network that causes a loss of service to users, by overwhelming the victim network or system with spurious data in order to prevent legitimate connection attempts from succeeding. The attacking hosts are often zombie computers that have been compromised by Trojan horse programs that allow the attacker to control the machine and direct the attack.

Action: Block

Track: Log

Table 73: Distributed Denial of Service Fields

In this field…	Do this…
Action	Specify what action to take when a DDoS attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log DDoS attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

IP and ICMP

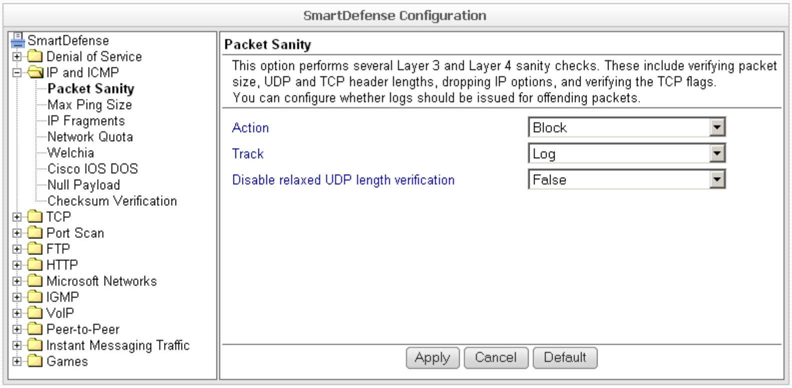
This category allows you to enable various IP and ICMP protocol tests, and to configure various protections against IP and ICMP-related attacks. It includes the following:

- ***Checksum Verification*** on page 436
- ***Cisco IOS DOS*** on page 433
- ***IP Fragments*** on page 429
- ***Max Ping Size*** on page 428
- ***Network Quota*** on page 431
- ***Null Payload*** on page 435
- ***Packet Sanity*** on page 426
- ***Welchia*** on page 432

Packet Sanity

Packet Sanity performs several Layer 3 and Layer 4 sanity checks. These include verifying packet size, UDP and TCP header lengths, dropping IP options, and verifying the TCP flags.

You can configure whether logs should be issued for offending packets.



Packet Sanity

This option performs several Layer 3 and Layer 4 sanity checks. These include verifying packet size, UDP and TCP header lengths, dropping IP options, and verifying the TCP flags.
You can configure whether logs should be issued for offending packets.

Action	Block
Track	Log
Disable relaxed UDP length verification	False

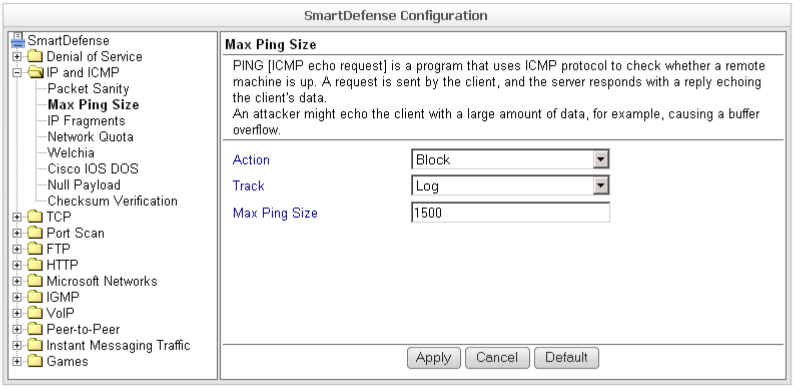
Table 74: Packet Sanity Fields

In this field…	Do this…
Action	Specify what action to take when a packet fails a sanity test, by selecting one of the following: • Block. Block the packet. This is the default. • None. No action.
Track	Specify whether to issue logs for packets that fail the packet sanity tests, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs.
Disable relaxed UDP length verification	The UDP length verification sanity check measures the UDP header length and compares it to the UDP header length specified in the UDP header. If the two values differ, the packet may be corrupted. However, since different applications may measure UDP header length differently, the Safe@Office appliance relaxes the UDP length verification sanity check by default, performing the check but not dropping offending packets. This is called relaxed UDP length verification. Specify whether the Safe@Office appliance should relax the UDP length verification sanity check or not, by selecting one of the following: • True. Disable relaxed UDP length verification. The Safe@Office appliance will drop packets that fail the UDP length verification check. • False. Do not disable relaxed UDP length verification. The Safe@Office appliance will not drop packets that fail the UDP length verification check. This is the default.

Max Ping Size

PING (ICMP echo request) is a program that uses ICMP protocol to check whether a remote machine is up. A request is sent by the client, and the server responds with a reply echoing the client's data.

An attacker can echo the client with a large amount of data, causing a buffer overflow. You can protect against such attacks by limiting the allowed size for ICMP echo requests.



Max Ping Size

PING [ICMP echo request] is a program that uses ICMP protocol to check whether a remote machine is up. A request is sent by the client, and the server responds with a reply echoing the client's data.
An attacker might echo the client with a large amount of data, for example, causing a buffer overflow.

Action: Block
Track: Log
Max Ping Size: 1500

Table 75: Max Ping Size Fields

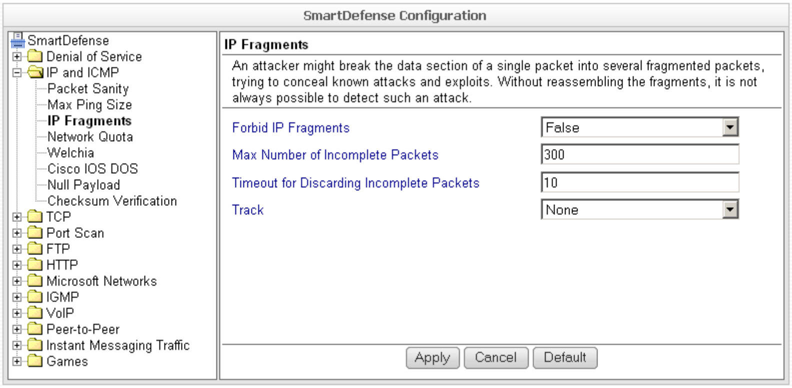
In this field...	Do this...
Action	Specify what action to take when an ICMP echo response exceeds the Max Ping Size threshold, by selecting one of the following: • Block. Block the request. This is the default. • None. No action.
Track	Specify whether to log ICMP echo responses that exceed the Max Ping Size threshold, by selecting one of the following: • Log. Log the responses. This is the default. • None. Do not log the responses.

In this field...	Do this...
Max Ping Size	Specify the maximum data size for ICMP echo response. The default value is 548.

IP Fragments

When an IP packet is too big to be transported by a network link, it is split into several smaller IP packets and transmitted in fragments. To conceal a known attack or exploit, an attacker might imitate this common behavior and break the data section of a single packet into several fragmented packets. Without reassembling the fragments, it is not always possible to detect such an attack. Therefore, the Safe@Office appliance always reassembles all the fragments of a given IP packet, before inspecting it to make sure there are no attacks or exploits in the packet.

You can configure how fragmented packets should be handled.



IP Fragments

An attacker might break the data section of a single packet into several fragmented packets, trying to conceal known attacks and exploits. Without reassembling the fragments, it is not always possible to detect such an attack.

Forbid IP Fragments: False
Max Number of Incomplete Packets: 300
Timeout for Discarding Incomplete Packets: 10
Track: None

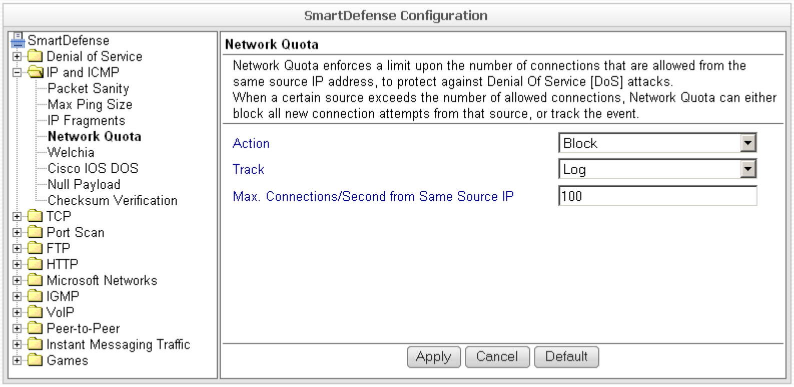
Table 76: IP Fragments Fields

In this field…	Do this…
Forbid IP Fragments	Specify whether all fragmented packets should be dropped, by selecting one of the following: • True. Drop all fragmented packets. • False. No action. This is the default. Under normal circumstances, it is recommended to leave this field set to False. Setting this field to True may disrupt Internet connectivity, because it does not allow any fragmented packets.
Max Number of Incomplete Packets	Type the maximum number of fragmented packets allowed. Packets exceeding this threshold will be dropped. The default value is 300.
Timeout for Discarding Incomplete Packets	When the Safe@Office appliance receives packet fragments, it waits for additional fragments to arrive, so that it can reassemble the packet. Type the number of seconds to wait before discarding incomplete packets. The default value is 10.
Track	Specify whether to log fragmented packets, by selecting one of the following: • Log. Log all fragmented packets. • None. Do not log the fragmented packets. This is the default.

Network Quota

An attacker may try to overload a server in your network by establishing a very large number of connections per second. To protect against Denial Of Service (DoS) attacks, Network Quota enforces a limit upon the number of connections per second that are allowed from the same source IP address.

You can configure how connections that exceed that limit should be handled.



SmartDefense Configuration

Network Quota

Network Quota enforces a limit upon the number of connections that are allowed from the same source IP address, to protect against Denial Of Service [DoS] attacks. When a certain source exceeds the number of allowed connections, Network Quota can either block all new connection attempts from that source, or track the event.

Action	Block
Track	Log
Max. Connections/Second from Same Source IP	100

Table 77: Network Quota Fields

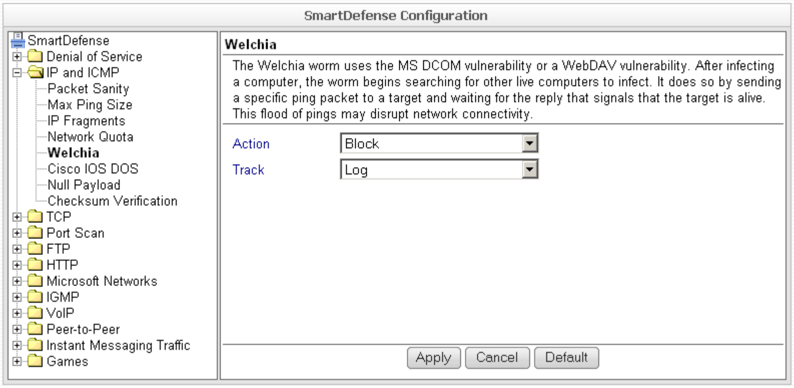
In this field…	Do this…
Action	Specify what action to take when the number of network connections from the same source reaches the Max. Connections/Second per Source IP threshold. Select one of the following: • Block. Block all new connections from the source. Existing connections will not be blocked. This is the default. • None. No action.
Track	Specify whether to log connections from a specific source that exceed the Max. Connections/Second per Source IP threshold, by selecting one of the following: • Log. Log the connections. This is the default. • None. Do not log the connections.

In this field…	Do this…
Max. Connections/Second from Same Source IP	Type the maximum number of network connections allowed per second from the same source IP address. The default value is 100. Set a lower threshold for stronger protection against DoS attacks. Note: Setting this value too low can lead to false alarms.

Welchia

The Welchia worm uses the MS DCOM vulnerability or a WebDAV vulnerability. After infecting a computer, the worm begins searching for other live computers to infect. It does so by sending a specific ping packet to a target and waiting for the reply that signals that the target is alive. This flood of pings may disrupt network connectivity.

You can configure how the Welchia worm should be handled.



SmartDefense Configuration

Welchia

The Welchia worm uses the MS DCOM vulnerability or a WebDAV vulnerability. After infecting a computer, the worm begins searching for other live computers to infect. It does so by sending a specific ping packet to a target and waiting for the reply that signals that the target is alive. This flood of pings may disrupt network connectivity.

Action: Block

Track: Log

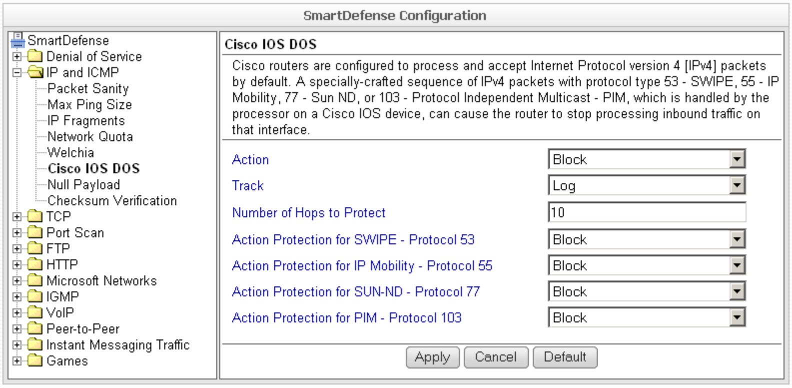
Table 78: Welchia Fields

In this field...	Do this...
Action	Specify what action to take when the Welchia worm is detected, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Welchia worm attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Cisco IOS DOS

Cisco routers are configured to process and accept Internet Protocol version 4 (IPv4) packets by default. When a Cisco IOS device is sent a specially crafted sequence of IPv4 packets (with protocol type 53 - SWIPE, 55 - IP Mobility, 77 - Sun ND, or 103 - Protocol Independent Multicast - PIM), the router will stop processing inbound traffic on that interface.

You can configure how Cisco IOS DOS attacks should be handled.



SmartDefense Configuration

Cisco IOS DOS

Cisco routers are configured to process and accept Internet Protocol version 4 [IPv4] packets by default. A specially-crafted sequence of IPv4 packets with protocol type 53 - SWIPE, 55 - IP Mobility, 77 - Sun ND, or 103 - Protocol Independent Multicast - PIM, which is handled by the processor on a Cisco IOS device, can cause the router to stop processing inbound traffic on that interface.

Action	Block
Track	Log
Number of Hops to Protect	10
Action Protection for SWIPE - Protocol 53	Block
Action Protection for IP Mobility - Protocol 55	Block
Action Protection for SUN-ND - Protocol 77	Block
Action Protection for PIM - Protocol 103	Block

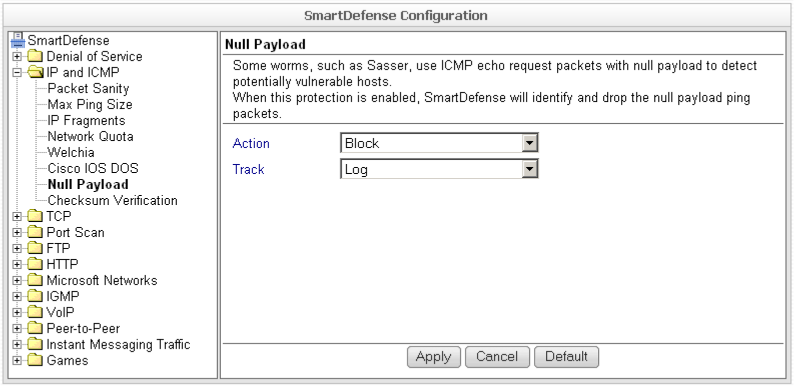
Table 79: Cisco IOS DOS

In this field...	Do this...
Action	Specify what action to take when a Cisco IOS DOS attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Cisco IOS DOS attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.
Number of Hops to Protect	Type the number of hops from the enforcement module that Cisco routers should be protected. The default value is 10.
Action Protection for SWIPE - Protocol 53 / IP Mobility - Protocol 55 / SUN-ND - Protocol 77 / PIM - Protocol 103	Specify what action to take when an IPv4 packet of the specific protocol type is received, by selecting one of the following: • Block. Drop the packet. This is the default. • None. No action.

Null Payload

Some worms, such as Sasser, use ICMP echo request packets with null payload to detect potentially vulnerable hosts.

You can configure how null payload ping packets should be handled.



Null Payload

Some worms, such as Sasser, use ICMP echo request packets with null payload to detect potentially vulnerable hosts.
When this protection is enabled, SmartDefense will identify and drop the null payload ping packets.

Action: Block

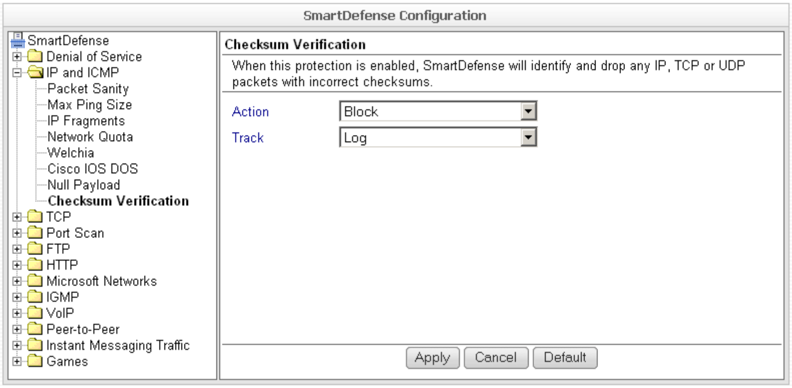
Track: Log

Table 80: Null Payload Fields

In this field…	Do this…
Action	Specify what action to take when null payload ping packets are detected, by selecting one of the following: • Block. Block the packets. This is the default. • None. No action.
Track	Specify whether to log null payload ping packets, by selecting one of the following: • Log. Log the packets. This is the default. • None. Do not log the packets.

Checksum Verification

SmartDefense identifies any IP, TCP, or UDP packets with incorrect checksums. You can configure how these packets should be handled.



Checksum Verification

When this protection is enabled, SmartDefense will identify and drop any IP, TCP or UDP packets with incorrect checksums.

Action: Block

Track: Log

Table 81: Checksum Verification Fields

In this field…	Do this…
Action	Specify what action to take when packets with incorrect checksums are detected, by selecting one of the following: • Block. Block the packets. This is the default. • None. No action.
Track	Specify whether to log packets with incorrect checksums, by selecting one of the following: • Log. Log the packets. • None. Do not log the packets. This is the default.

TCP

This category allows you to configure various protections related to the TCP protocol. It includes the following:

- ***Flags*** on page 443
- ***Sequence Verifier*** on page 442
- ***Small PMTU*** on page 438
- ***Strict TCP*** on page 437
- ***SynDefender*** on page 440

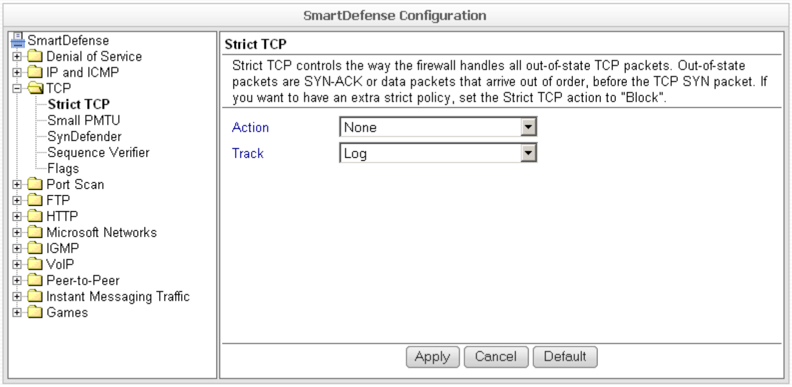
Strict TCP

Out-of-state TCP packets are SYN-ACK or data packets that arrive out of order, before the TCP SYN packet.

Note: In normal conditions, out-of-state TCP packets can occur after the Safe@Office restarts, since connections which were established prior to the reboot are unknown. This is normal and does not indicate an attack.

Note: Certain SmartDefense protections implicitly apply the Strict TCP protection to relevant connections. In such cases, "TCP Out-of-State" log messages may appear in the Security Log, even though the Strict TCP protection is disabled.

You can configure how out-of-state TCP packets should be handled.



SmartDefense Configuration

Strict TCP

Strict TCP controls the way the firewall handles all out-of-state TCP packets. Out-of-state packets are SYN-ACK or data packets that arrive out of order, before the TCP SYN packet. If you want to have an extra strict policy, set the Strict TCP action to "Block".

Action: None

Track: Log

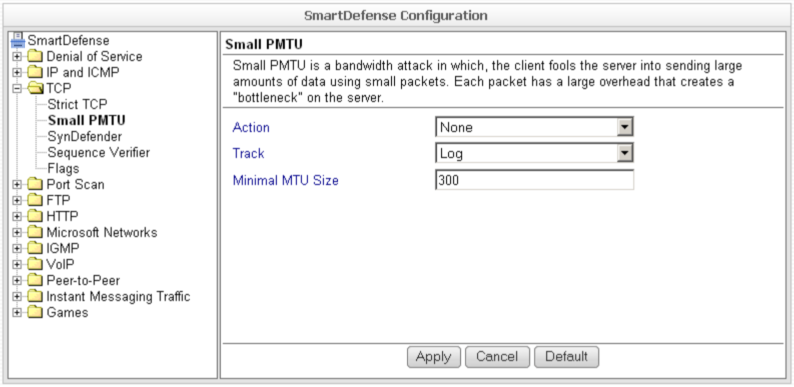
Table 82: Strict TCP

In this field...	Do this...
Action	Specify what action to take when an out-of-state TCP packet arrives, by selecting one of the following: • Block. Block the packets. • None. No action. This is the default.
Track	Specify whether to log null payload ping packets, by selecting one of the following: • Log. Log the packets. This is the default. • None. Do not log the packets.

Small PMTU

Small PMTU (Packet MTU) is a bandwidth attack in which the client fools the server into sending large amounts of data using small packets. Each packet has a large overhead that creates a "bottleneck" on the server.

You can protect against this attack by specifying a minimum packet size for data sent over the Internet.



SmartDefense Configuration

Small PMTU

Small PMTU is a bandwidth attack in which, the client fools the server into sending large amounts of data using small packets. Each packet has a large overhead that creates a "bottleneck" on the server.

Action: None

Track: Log

Minimal MTU Size: 300

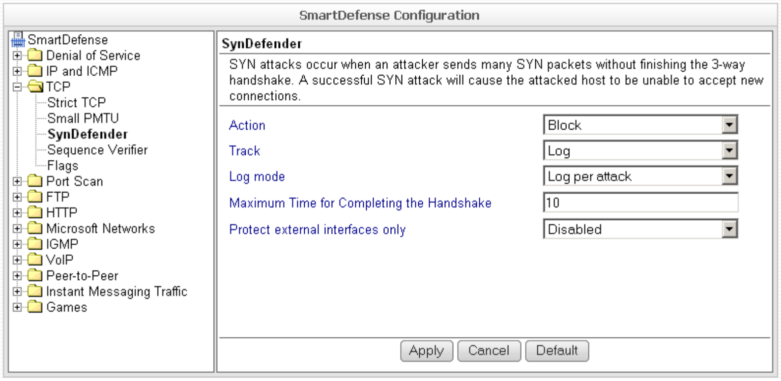
Table 83: Small PMTU Fields

In this field...	Do this...
Action	Specify what action to take when a packet is smaller than the Minimal MTU Size threshold, by selecting one of the following: • Block. Block the packet. • None. No action. This is the default.
Track	Specify whether to issue logs for packets are smaller than the Minimal MTU Size threshold, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs.
Minimal MTU Size	Type the minimum value allowed for the MTU field in IP packets sent by a client. An overly small value will not prevent an attack, while an overly large value might degrade performance and cause legitimate requests to be dropped. The default value is 300.

SynDefender

In a SYN attack, the attacker sends many SYN packets without finishing the three-way handshake. This causes the attacked host to be unable to accept new connections.

You can protect against this attack by specifying a maximum amount of time for completing handshakes.



SynDefender

SYN attacks occur when an attacker sends many SYN packets without finishing the 3-way handshake. A successful SYN attack will cause the attacked host to be unable to accept new connections.

Action	Block
Track	Log
Log mode	Log per attack
Maximum Time for Completing the Handshake	10
Protect external interfaces only	Disabled

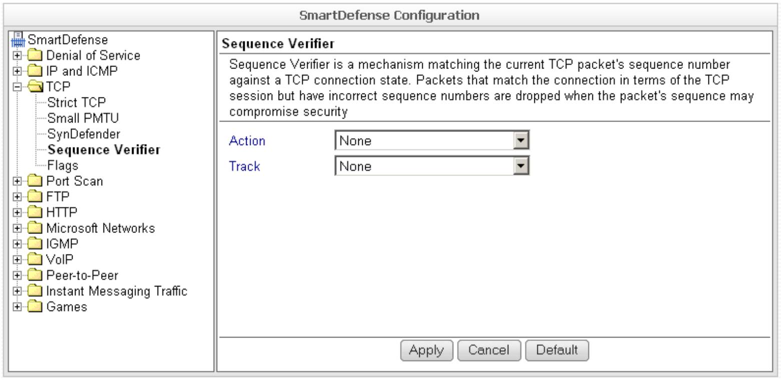
Table 84: SynDefender Fields

In this field...	Do this...
Action	Specify what action to take when a SYN attack occurs, by selecting one of the following: • Block. Block the packet. This is the default. • None. No action. A SYN attack is when more than 5 incomplete TCP handshakes are detected within 10 seconds. A handshake is considered incomplete when it exceeds the Maximum time for completing the handshake threshold.
Track	Specify whether to issue logs for the events specified by the Log Mode parameter, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs.

In this field…	Do this…
Log mode	Specify upon which events logs should be issued, by selecting one of the following: • None. Do not issue logs. • Log per attack. Issue logs for each SYN attack. This is the default. • Log individual unfinished handshakes. Issue logs for each incomplete handshake. This field is only relevant if the Track field is set to Log.
Maximum Time for Completing the Handshake	Type the maximum amount of time in seconds after which a TCP handshake is considered incomplete. The default value is 10 seconds.
Protect external interfaces only	Specify whether SynDefender should be enabled for external (WAN) interfaces only, by selecting one of the following: • Disabled. Enable SynDefender for all the firewall interfaces. This is the default. • Enabled. Enable SynDefender for external interfaces only.

Sequence Verifier

The Safe@Office appliance examines each TCP packet's sequence number and checks whether it matches a TCP connection state. You can configure how the appliance handles packets that match a TCP connection in terms of the TCP session but have incorrect sequence numbers.



Sequence Verifier

Sequence Verifier is a mechanism matching the current TCP packet's sequence number against a TCP connection state. Packets that match the connection in terms of the TCP session but have incorrect sequence numbers are dropped when the packet's sequence may compromise security

Action: None

Track: None

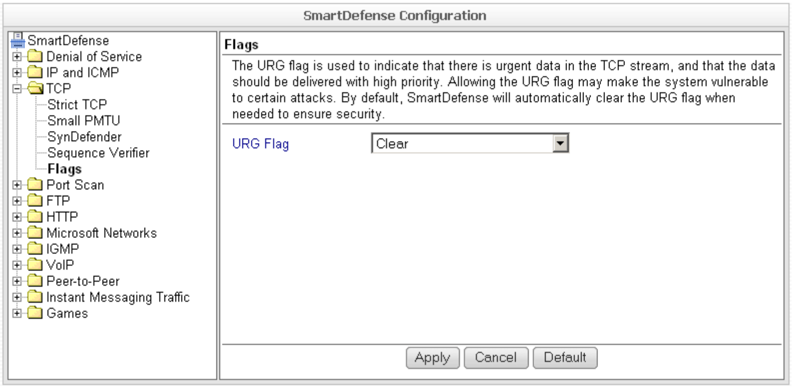
Table 85: Strict TCP

In this field...	Do this...
Action	Specify what action to take when TCP packets with incorrect sequence numbers arrive, by selecting one of the following: • Block. Block the packets. • None. No action. This is the default.
Track	Specify whether to log TCP packets with incorrect sequence numbers, by selecting one of the following: • Log. Log the packets. This is the default. • None. Do not log the packets.

Flags

The URG flag is used to indicate that there is urgent data in the TCP stream, and that the data should be delivered with high priority. Since handling of the URG flag is inconsistent between different operating systems, an attacker can use the URG flag to conceal certain attacks.

You can configure how the URG flag should be handled.



Flags

The URG flag is used to indicate that there is urgent data in the TCP stream, and that the data should be delivered with high priority. Allowing the URG flag may make the system vulnerable to certain attacks. By default, SmartDefense will automatically clear the URG flag when needed to ensure security.

URG Flag: Clear

Table 86: Flags Fields

In this field...	Do this...
URG Flag	Specify whether to clear or allow the URG flag, by selecting one of the following: • Clear. Clear the URG flag on all incoming packets. This is the default. • Allow. Allow the URG flag.

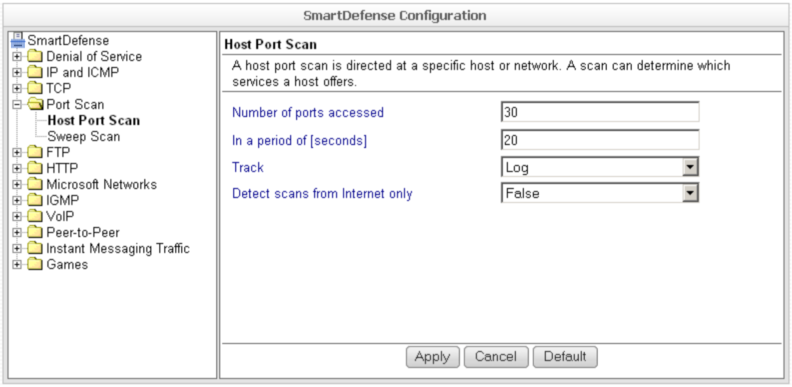
Port Scan

An attacker can perform a port scan to determine whether ports are open and vulnerable to an attack. This is most commonly done by attempting to access a port and waiting for a response. The response indicates whether or not the port is open.

This category includes the following types of port scans:

- Host Port Scan. The attacker scans a specific host's ports to determine which of the ports are open.
- Sweep Scan. The attacker scans various hosts to determine where a specific port is open.

You can configure how the Safe@Office appliance should react when a port scan is detected.



SmartDefense Configuration

Host Port Scan

A host port scan is directed at a specific host or network. A scan can determine which services a host offers.

Number of ports accessed: 30

In a period of [seconds]: 20

Track: Log

Detect scans from Internet only: False

Table 87: Port Scan Fields

In this field...	Do this...
Number of ports accessed	SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the Number of ports accessed value, within the number of seconds specified by the In a period of [seconds] value, in order for SmartDefense to consider the activity a scan. Type the minimum number of ports that must be accessed within the In a period of [seconds] period, in order for SmartDefense to detect the activity as a port scan. For example, if this value is 30, and 40 ports are accessed within a specified period of time, SmartDefense will detect the activity as a port scan. For Host Port Scan, the default value is 30. For Sweep Scan, the default value is 50.
In a period of [seconds]	SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the Number of ports accessed value, within the number of seconds specified by the In a period of [seconds] value, in order for SmartDefense to consider the activity a scan. Type the maximum number of seconds that can elapse, during which the Number of ports accessed threshold is exceeded, in order for SmartDefense to detect the activity as a port scan. For example, if this value is 20, and the Number of ports accessed threshold is exceeded for 15 seconds, SmartDefense will detect the activity as a port scan. If the threshold is exceeded for 30 seconds, SmartDefense will not detect the activity as a port scan. The default value is 20 seconds.

In this field…	Do this…
Track	Specify whether to issue logs for scans, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs. This is the default.
Detect scans from Internet only	Specify whether to detect only scans originating from the Internet, by selecting one of the following: • False. Do not detect only scans from the Internet. This is the default. • True. Detect only scans from the Internet.

FTP

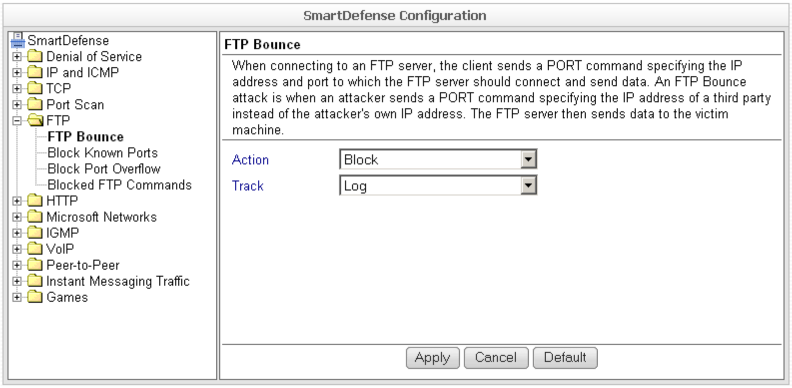
This category allows you to configure various protections related to the FTP protocol. It includes the following:

- ***Block Known Ports*** on page 448
- ***Block Port Overflow*** on page 449
- ***Blocked FTP Commands*** on page 450
- ***FTP Bounce*** on page 447

FTP Bounce

When connecting to an FTP server, the client sends a PORT command specifying the IP address and port to which the FTP server should connect and send data. An FTP Bounce attack is when an attacker sends a PORT command specifying the IP address of a third party instead of the attacker's own IP address. The FTP server then sends data to the victim machine.

You can configure how FTP bounce attacks should be handled.



SmartDefense Configuration

FTP Bounce

When connecting to an FTP server, the client sends a PORT command specifying the IP address and port to which the FTP server should connect and send data. An FTP Bounce attack is when an attacker sends a PORT command specifying the IP address of a third party instead of the attacker's own IP address. The FTP server then sends data to the victim machine.

Action: Block

Track: Log

Table 88: FTP Bounce Fields

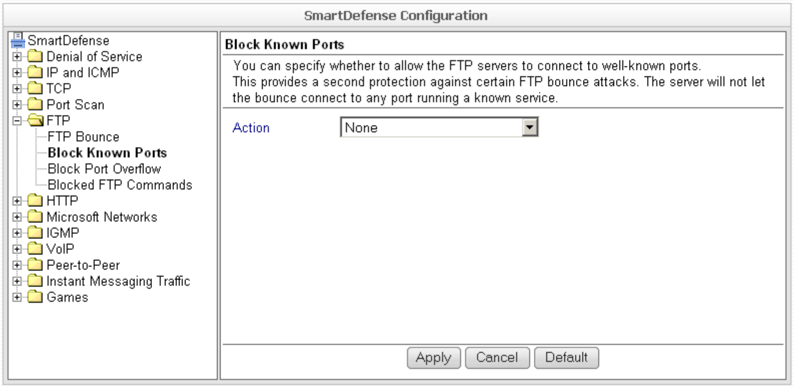
In this field...	Do this...
Action	Specify what action to take when an FTP Bounce attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log FTP Bounce attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Block Known Ports

You can choose to block the FTP server from connecting to well-known ports.

Note: Known ports are published ports associated with services (for example, SMTP is port 25).

This provides a second layer of protection against FTP bounce attacks, by preventing such attacks from reaching well-known ports.


SmartDefense Configuration

Block Known Ports

You can specify whether to allow the FTP servers to connect to well-known ports.
This provides a second protection against certain FTP bounce attacks. The server will not let the bounce connect to any port running a known service.

Action: None

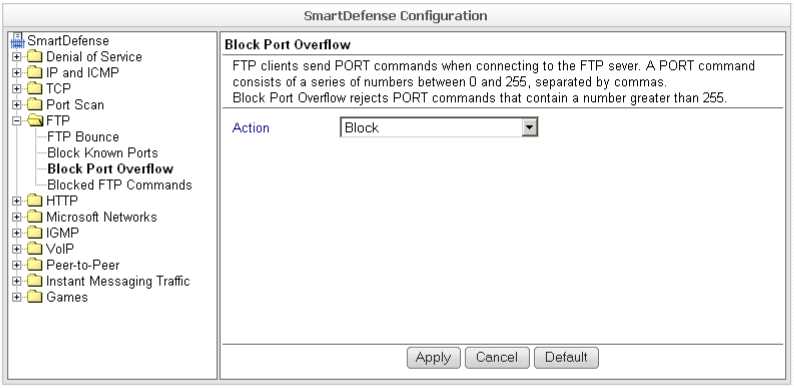
Table 89: Block Known Ports Fields

In this field…	Do this…
Action	Specify what action to take when the FTP server attempts to connect to a well-known port, by selecting one of the following: • Block. Block the connection. • None. No action. This is the default.

Block Port Overflow

FTP clients send PORT commands when connecting to the FTP sever. A PORT command consists of a series of numbers between 0 and 255, separated by commas.

To enforce compliance to the FTP standard and prevent potential attacks against the FTP server, you can block PORT commands that contain a number greater than 255.



SmartDefense Configuration

Block Port Overflow

FTP clients send PORT commands when connecting to the FTP sever. A PORT command consists of a series of numbers between 0 and 255, separated by commas.
Block Port Overflow rejects PORT commands that contain a number greater than 255.

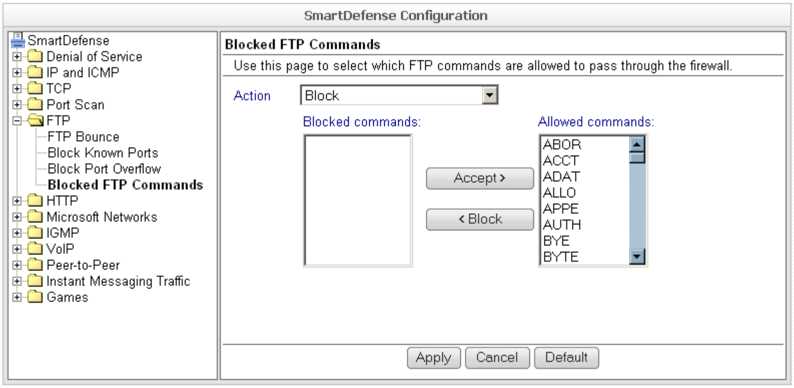
Action: Block

Table 90: Block Port Overflow

In this field...	Do this...
Action	Specify what action to take for PORT commands containing a number greater than 255, by selecting one of the following: • Block. Block the PORT command. This is the default. • None. No action.

Blocked FTP Commands

Some seldom-used FTP commands may compromise FTP server security and integrity. You can specify which FTP commands should be allowed to pass through the security server, and which should be blocked.



SmartDefense Configuration

Blocked FTP Commands

Use this page to select which FTP commands are allowed to pass through the firewall.

Action: Block

To enable FTP command blocking

- In the **Action** drop-down list, select **Block**.

  The FTP commands listed in the **Blocked Commands** box will be blocked.

  FTP command blocking is enabled by default.

To disable FTP command blocking

- In the **Action** drop-down list, select **None**.

  All FTP commands are allowed, including those in the **Blocked Commands** box.

To block a specific FTP command

1. In the **Allowed Commands** box, select the desired FTP command.
2. Click **Block**.

   The FTP command appears in the **Blocked Commands** box.
3. Click **Apply**.

   When FTP command blocking is enabled, the FTP command will be blocked.

To allow a specific FTP command

1. In the **Blocked Commands** box, select the desired FTP command.
2. Click **Accept.**

   The FTP command appears in the **Allowed Commands** box.
3. Click **Apply.**

   The FTP command will be allowed, regardless of whether FTP command blocking is enabled or disabled.

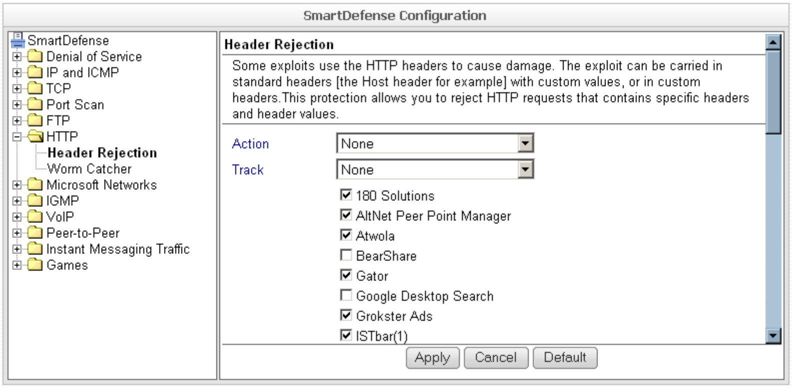
HTTP

This category allows you to configure various protections related to the HTTP protocol. It includes the following:

- ***Header Rejection*** on page 451
- ***Worm Catcher*** on page 452

Header Rejection

Some exploits are carried in standard HTTP headers with custom values (for example, in the Host header), or in custom HTTP headers. You can protect against such exploits by rejecting HTTP requests that contain specific headers and header values.



Header Rejection

Some exploits use the HTTP headers to cause damage. The exploit can be carried in standard headers [the Host header for example] with custom values, or in custom headers.This protection allows you to reject HTTP requests that contains specific headers and header values.

Action: None

Track: None

☑ 180 Solutions
☑ AltNet Peer Point Manager
☑ Atwola
□ BearShare
☑ Gator
□ Google Desktop Search
☑ Grokster Ads
☑ ISTbar(1)

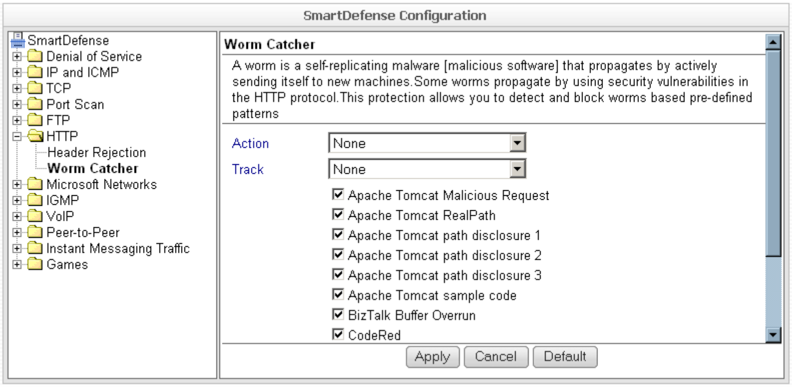
Table 91: Header Rejection Fields

In this field…	Do this…
Action	Specify what action to take when an HTTP header-based exploit is detected, by selecting one of the following: • Block. Block the attack. • None. No action. This is the default.
Track	Specify whether to log HTTP header-based exploits, by selecting one of the following: • Log. Log the attack. • None. Do not log the attack. This is the default.
HTTP header values list	Select the HTTP header values to detect.

Worm Catcher

A worm is a self-replicating malware (malicious software) that propagates by actively sending itself to new machines. Some worms propagate by using security vulnerabilities in the HTTP protocol.

You can specify how HTTP-based worm attacks should be handled.



SmartDefense Configuration

Worm Catcher

A worm is a self-replicating malware [malicious software] that propagates by actively sending itself to new machines.Some worms propagate by using security vulnerabilities in the HTTP protocol.This protection allows you to detect and block worms based pre-defined patterns

Action: None

Track: None

☑ Apache Tomcat Malicious Request
☑ Apache Tomcat RealPath
☑ Apache Tomcat path disclosure 1
☑ Apache Tomcat path disclosure 2
☑ Apache Tomcat path disclosure 3
☑ Apache Tomcat sample code
☑ BizTalk Buffer Overrun
☑ CodeRed

Table 92: Worm Catcher Fields

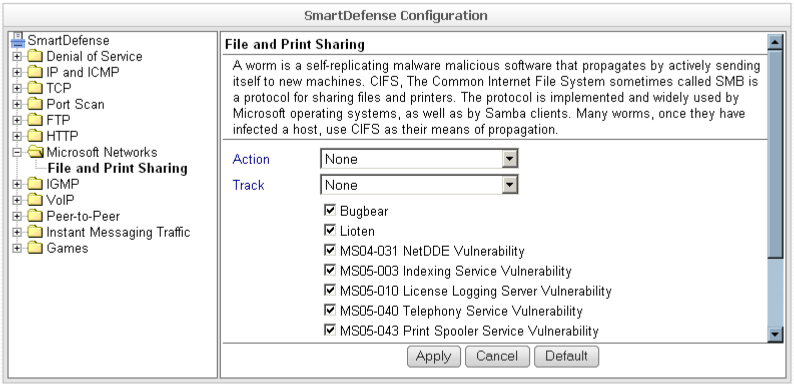
In this field...	Do this...
Action	Specify what action to take when an HTTP-based worm attack is detected, by selecting one of the following: • Block. Block the attack. • None. No action. This is the default.
Track	Specify whether to log HTTP-based worm attacks, by selecting one of the following: • Log. Log the attack. • None. Do not log the attack. This is the default.
HTTP-based worm patterns list	Select the worm patterns to detect.

Microsoft Networks

This category includes File and Print Sharing.

Microsoft operating systems and Samba clients rely on Common Internet File System (CIFS), a protocol for sharing files and printers. However, this protocol is also widely used by worms as a means of propagation.

You can configure how CIFS worms should be handled.



File and Print Sharing

A worm is a self-replicating malware malicious software that propagates by actively sending itself to new machines. CIFS, The Common Internet File System sometimes called SMB is a protocol for sharing files and printers. The protocol is implemented and widely used by Microsoft operating systems, as well as by Samba clients. Many worms, once they have infected a host, use CIFS as their means of propagation.

Action: None

Track: None

☑ Bugbear
☑ Lioten
☑ MS04-031 NetDDE Vulnerability
☑ MS05-003 Indexing Service Vulnerability
☑ MS05-010 License Logging Server Vulnerability
☑ MS05-040 Telephony Service Vulnerability
☑ MS05-043 Print Spooler Service Vulnerability

Table 93: File Print and Sharing Fields

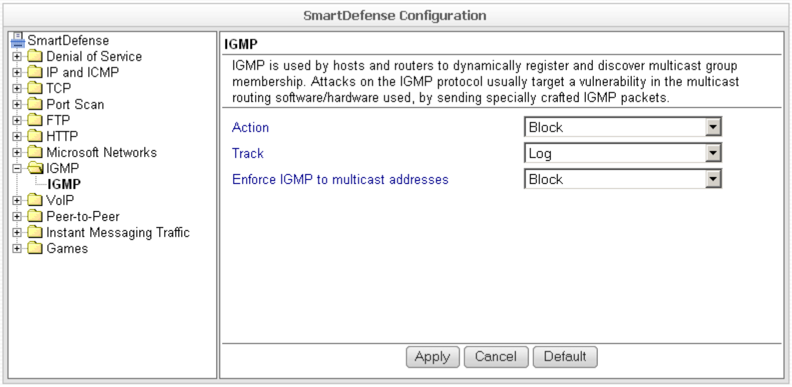
In this field…	Do this…
Action	Specify what action to take when a CIFS worm attack is detected, by selecting one of the following: • Block. Block the attack. • None. No action. This is the default.
Track	Specify whether to log CIFS worm attacks, by selecting one of the following: • Log. Log the attack. • None. Do not log the attack. This is the default.
CIFS worm patterns list	Select the worm patterns to detect. Patterns are matched against file names (including file paths but excluding the disk share name) that the client is trying to read or write from the server.

IGMP

This category includes the IGMP protocol.

IGMP is used by hosts and routers to dynamically register and discover multicast group membership. Attacks on the IGMP protocol usually target a vulnerability in the multicast routing software/hardware used, by sending specially crafted IGMP packets.

You can configure how IGMP attacks should be handled.



IGMP

IGMP is used by hosts and routers to dynamically register and discover multicast group membership. Attacks on the IGMP protocol usually target a vulnerability in the multicast routing software/hardware used, by sending specially crafted IGMP packets.

Action: Block

Track: Log

Enforce IGMP to multicast addresses: Block

Table 94: IGMP Fields

In this field…	Do this…
Action	Specify what action to take when an IGMP attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log IGMP attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

In this field...	Do this...
Enforce IGMP to multicast addresses	According to the IGMP specification, IGMP packets must be sent to multicast addresses. Sending IGMP packets to a unicast or broadcast address might constitute and attack; therefore the Safe@Office appliance blocks such packets. Specify whether to allow or block IGMP packets that are sent to non-multicast addresses, by selecting one of the following: • Block. Block IGMP packets that are sent to non-multicast addresses. This is the default. • None. No action.

VoIP

Voice over IP (VoIP) traffic is subject to various threats, such as:

- Call redirections, in which calls intended for one recipient are redirected to another
- Stealing calls, where the caller pretends to be someone else
- System hacking, using ports that were opened for VoIP connections

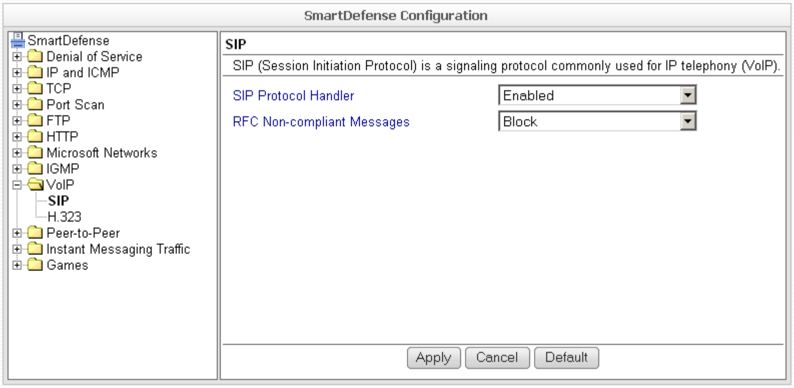
This category allows you to configure various protections related to VoIP protocols. It includes the following:

- ***SIP*** on page 457
- ***H.323*** on page 458

SIP

The SmartDefense SIP Application Level Gateway (ALG) processes the SIP protocol, allows firewall and NAT traversal, and enables Traffic Shaper to operate on SIP connections.

By default, the SIP ALG checks SIP sessions for RFC compliance. If desired, you can allow non-RFC-compliant SIP connections, so that VoIP devices that initiate non-standard SIP calls can communicate through the firewall. You can also disable the SIP ALG altogether, if it is not needed by your SIP clients, or if it interferes with their operation.



SIP

SIP (Session Initiation Protocol) is a signaling protocol commonly used for IP telephony (VoIP).

SIP Protocol Handler: Enabled

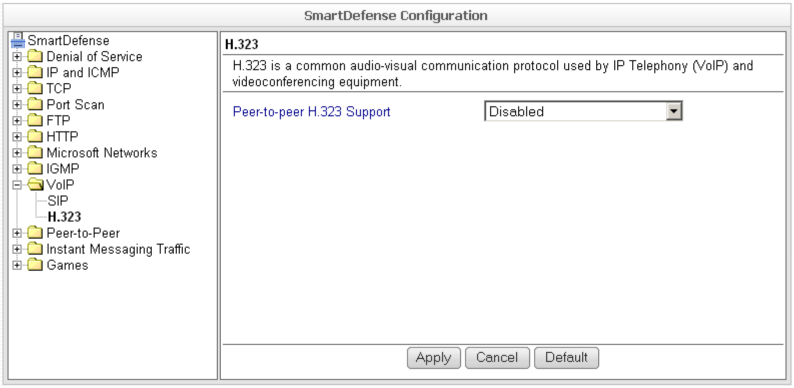
RFC Non-compliant Messages: Block

Table 95: SIP Fields

In this field...	Do this...
SIP Protocol Handler	Specify whether to enable SIP support, by selecting one of the following: • Enabled. Enable SIP support. This is the default. • Disabled. Disable SIP support.
RFC Non-compliant Messages	Specify what action to take when non-RFC-compliant SIP packets arrive, by selecting one of the following: • Block. Block the packets. This is the default. • None. No action.

H.323

H.323 telephony is used by various devices and applications, such as Microsoft Netmeeting. SmartDefense allows you to choose whether to disable or enable the H.323 Application Level Gateway (ALG), which allows firewall and NAT traversal of H.323 calls.



SmartDefense Configuration

H.323

H.323 is a common audio-visual communication protocol used by IP Telephony (VoIP) and videoconferencing equipment.

Peer-to-peer H.323 Support: Disabled

Table 96: H.323 Fields

In this field…	Do this…
Peer-to-peer H.323 Support	Specify whether to enable H.323 support, by selecting one of the following: • Enabled. Enable H.323 support. • Disabled. Disabled H.323 support. This is the default.

Peer-to-Peer

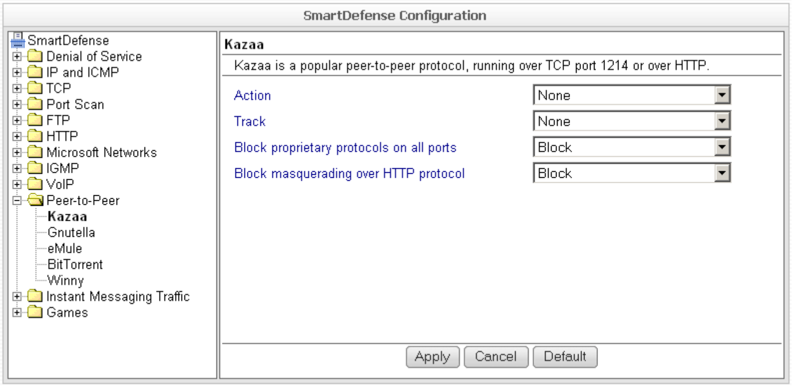
SmartDefense can block peer-to-peer file-sharing traffic, by identifying the proprietary protocols and preventing the initial connection to the peer-to-peer networks. This prevents not only downloads, but also search operations.

This category includes the following nodes:

- BitTorrent
- eMule
- Gnutella
- KaZaA
- Winny

Note: SmartDefense can detect peer-to-peer traffic regardless of the TCP port being used to initiate the session.

In each node, you can configure how peer-to-peer connections of the selected type should be handled, using the following table.



SmartDefense Configuration

Kazaa

Kazaa is a popular peer-to-peer protocol, running over TCP port 1214 or over HTTP.

Action	None
Track	None
Block proprietary protocols on all ports	Block
Block masquerading over HTTP protocol	Block

Table 97: Peer to Peer Fields

In this field…	Do this…
Action	Specify what action to take when a connection is attempted, by selecting one of the following: • Block. Block the connection. • None. No action. This is the default.
Track	Specify whether to log peer-to-peer connections, by selecting one of the following: • Log. Log the connection. • None. Do not log the connection. This is the default.
Block proprietary protocols on all ports	Specify whether proprietary protocols should be blocked on all ports, by selecting one of the following: • Block. Block the proprietary protocol on all ports. This in effect prevents all communication using this peer-to-peer application. This is the default. • None. Do not block the proprietary protocol on all ports.
Block masquerading over HTTP protocol	Specify whether to block using the peer-to-peer application over HTTP, by selecting one of the following: • Block. Block using the application over HTTP. This is the default. • None. Do not block using the application over HTTP. This field is not relevant for eMule and Winny.

Instant Messaging Traffic

SmartDefense can block instant messaging applications that use VoIP protocols, by identifying the messaging application's fingerprints and HTTP headers.

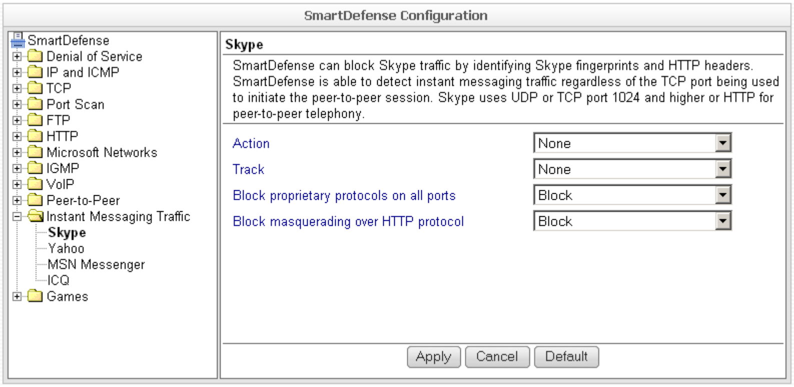
This category includes the following nodes:

- ICQ
- MSN Messenger
- Skype
- Yahoo

Note: SmartDefense can detect instant messaging traffic regardless of the TCP port being used to initiate the session.

Note: Skype versions up to 2.0.0.103 are supported.

In each node, you can configure how instant messaging connections of the selected type should be handled, using the following table.



Skype

SmartDefense can block Skype traffic by identifying Skype fingerprints and HTTP headers. SmartDefense is able to detect instant messaging traffic regardless of the TCP port being used to initiate the peer-to-peer session. Skype uses UDP or TCP port 1024 and higher or HTTP for peer-to-peer telephony.

Action	None
Track	None
Block proprietary protocols on all ports	Block
Block masquerading over HTTP protocol	Block

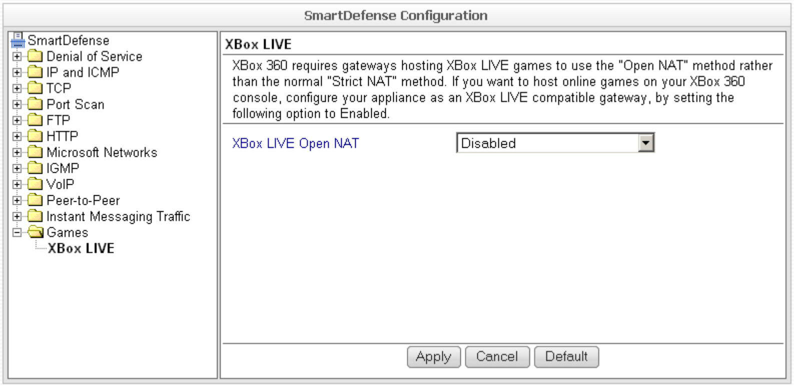
Table 98: Instant Messengers Fields

In this field...	Do this...
Action	Specify what action to take when a connection is attempted, by selecting one of the following: • Block. Block the connection. • None. No action. This is the default.
Track	Specify whether to log instant messenger connections, by selecting one of the following: • Log. Log the connection. • None. Do not log the connection. This is the default.
Block proprietary protocol / Block proprietary protocols on all ports	Specify whether proprietary protocols should be blocked on all ports, by selecting one of the following: • Block. Block the proprietary protocol on all ports. This in effect prevents all communication using this instant messenger application. This is the default. • None. Do not block the proprietary protocol on all ports.
Block masquerading over HTTP protocol	Specify whether to block using the instant messenger application over HTTP, by selecting one of the following: • Block. Block using the application over HTTP. This is the default. • None. Do not block using the application over HTTP.

Games

This category includes XBox LIVE.

XBox 360 requires gateways hosting XBox LIVE games to use the "Open NAT" method rather than the normal "Strict NAT" method. Therefore, if you want to host online games on an XBox 360 console, you must first configure your Safe@Office appliance to use the "Open NAT" method.



SmartDefense Configuration

XBox LIVE

XBox 360 requires gateways hosting XBox LIVE games to use the "Open NAT" method rather than the normal "Strict NAT" method. If you want to host online games on your XBox 360 console, configure your appliance as an XBox LIVE compatible gateway, by setting the following option to Enabled.

XBox LIVE Open NAT: Disabled

Table 99: XBox LIVE Fields

In this field…	Do this…
Xbox Live OpenNAT	Specify whether the Safe@Office appliance should use the "Open NAT" method, by selecting one of the following: • Enabled. Use the "Open NAT" method. You will be able to host XBox LIVE games and join existing ones. • Disabled. Do not use the "Open NAT" method. You will not be able to host XBox LIVE games, but you will still be able to join existing ones. This is the default.

Resetting SmartDefense to its Defaults

500

If desired, you can reset the SmartDefense security policy to its default settings. For information on the default value of each SmartDefense setting, see ***SmartDefense Categories*** on page 419.

For information on resetting individual nodes in the SmartDefense tree to their default settings, see ***Using the SmartDefense Tree*** on page 417.

To reset SmartDefense to its defaults

1. Click Security in the main menu, and click the SmartDefense tab.

   The SmartDefense page appears.

2. Click Reset to Defaults.

   A confirmation message appears.

3. Click OK.

   The SmartDefense policy is reset to its default settings.

Chapter 15

Using Antivirus and Antispam Filtering

This chapter explains how to use antivirus and antispam filtering.

This chapter includes the following topics:

Overview

The Safe@Office appliance enables you to perform both antivirus and antispam filtering, to ensure your network remains secure.

Antivirus Filtering Solutions

You can scan connections for viruses, by using VStream Antivirus and/or the Email Antivirus subscription service (part of the centralized Email Filtering service). The following table describes the main differences between VStream Antivirus and the Email Antivirus service:

Table 100: Comparison of Antivirus Filtering Methods

	VStream Antivirus	Email Antivirus
Supported Protocols	VStream Antivirus supports multiple protocols, including incoming SMTP and outgoing POP3 connections.	Email Antivirus is specific to email, scanning incoming POP3 and outgoing SMTP connections only.

	VStream Antivirus	Email Antivirus
Point of Enforcement	VStream Antivirus scans for viruses in the Safe@Office gateway itself.	Email Antivirus is centralized, redirecting traffic through the Service Center for scanning.

You can use either antivirus solution, or both in conjunction.

Antispam Filtering Solutions

You can scan email messages for spam, by using VStream Antispam and/or the Email Antispam subscription service (part of the centralized Email Filtering service). The following table describes the main differences between VStream Antispam and the Email Antispam service:

Table 101: Comparison of Antispam Filtering Methods

	VStream Antispam	Email Antispam
Supported Protocols	VStream Antispam supports both incoming and outgoing POP3 and SMTP, as well as POP3 and SMTP connections between internal networks.	Email Antispam scans incoming POP3 and outgoing SMTP connections only.
Point of Enforcement	VStream Antispam scans for spam in the Safe@Office gateway itself.	Email Antispam is centralized, redirecting traffic through the Service Center for scanning.

You can use either antispam solution, or both in conjunction.

Using VStream Antivirus

500

The Safe@Office appliance includes VStream Antivirus, an embedded stream-based antivirus engine based on Check Point Stateful Inspection and Application Intelligence technologies, that performs virus scanning at the kernel level.

VStream Antivirus scans files for malicious content on the fly, without downloading the files into intermediate storage. This means minimal added latency and support for unlimited file sizes; and since VStream Antivirus stores only minimal state information per connection, it can scan thousands of connections concurrently. In order to scan archive files on the fly, VStream Antivirus performs real-time decompression and scanning of ZIP, TAR, and GZ archive files, with support for nested archive files.

If you are subscribed to the VStream Antivirus subscription service, VStream Antivirus virus signatures are automatically updated, so that security is always up-to-date, and your network is always protected.

VStream Antivirus Actions

When VStream Antivirus detects malicious content, the action it takes depends on the protocol in which the virus was found. See the following table. In each case, VStream Antivirus blocks the file and writes a log to the Event Log.

Table 102: VStream Antivirus Actions

If a virus if found in this protocol...	VStream Antivirus does this...	The protocol is detected on this port...
HTTP	• Terminates the connection	All ports on which VStream Antivirus is enabled by the policy, not only port 80

If a virus if found in this protocol...	VStream Antivirus does this...	The protocol is detected on this port...
POP3	• Terminates the connection • Deletes the virus-infected email from the server	The standard TCP port 110.
IMAP	• Terminates the connection • Replaces the virus-infected email with a message notifying the user that a virus was found	The standard TCP port 143
SMTP	• Rejects the virus-infected email with error code 554 • Sends a "Virus detected" message to the sender	The standard TCP port 25
FTP	• Terminates the data connection • Sends a "Virus detected" message to the FTP client	The standard TCP port 21
TCP and UDP	• Terminates the connection	Generic TCP and UDP ports, other than those listed above

Note: In protocols that are not listed in this table, VStream Antivirus uses a "best effort" approach to detect viruses. In such cases, detection of viruses is not guaranteed and depends on the specific encoding used by the protocol.

Default Antivirus Policy

The VStream Antivirus default policy includes the following rules:

- All SMTP connections are scanned, regardless of the connection's direction.
- All POP3 connections are scanned, regardless of the connection's direction.
- All IMAP connections are scanned, regardless of the connection's direction.

You can easily override the default antivirus policy, by creating user-defined rules. For further information, see ***Configuring the VStream Antivirus Policy*** on page 471.

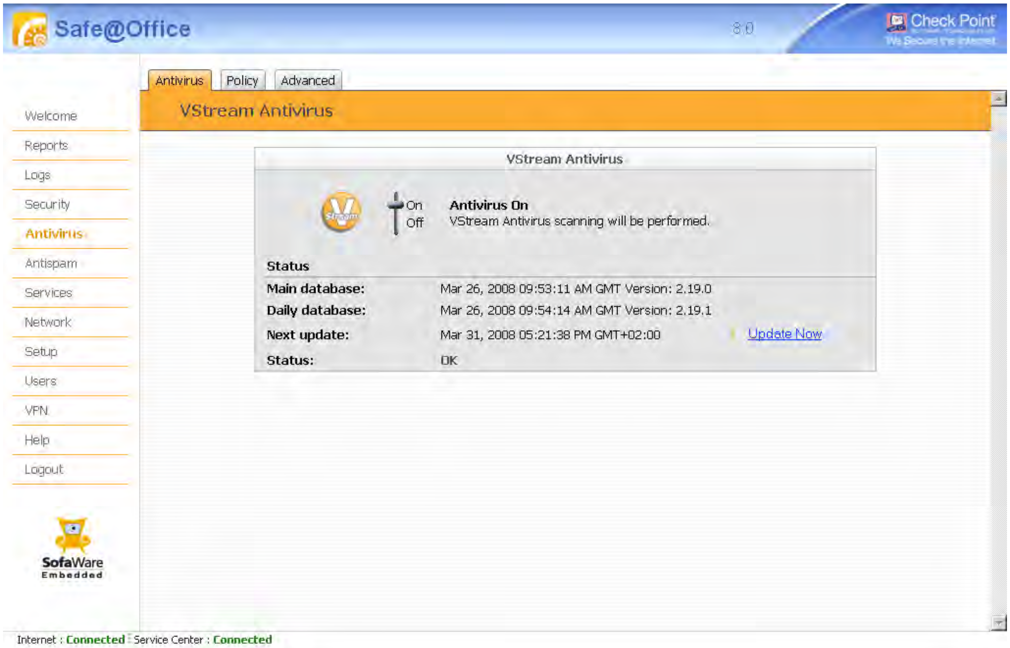
Enabling/Disabling VStream Antivirus

500

To enable/disable VStream Antivirus

1. Click Antivirus in the main menu, and click the Antivirus tab.

The VStream Antivirus page appears.



VStream Antivirus

VStream Antivirus

Antivirus On
VStream Antivirus scanning will be performed.

Status

Main database:	Mar 26, 2008 09:53:11 AM GMT Version: 2.19.0
Daily database:	Mar 26, 2008 09:54:14 AM GMT Version: 2.19.1
Next update:	Mar 31, 2008 05:21:38 PM GMT+02:00
Status:	OK

Internet : Connected | Service Center : Connected

2. Drag the On/Off lever upwards or downwards.

   VStream Antivirus is enabled/disabled for all internal network computers.

Viewing VStream Antivirus Signature Database Information

500

VStream Antivirus maintains two databases: a daily database and a main database. The daily database is updated frequently with the newest virus signatures. Periodically, the contents of the daily database are moved to the main database, leaving the daily database empty. This system of incremental updates to the main database allows for quicker updates and saves on network bandwidth.

You can view information about the VStream Antivirus signature databases currently in use, in the VStream Antivirus page.

Table 103: VStream Antivirus Page Fields

This field...	Displays...
Main database	The date and time at which the main database was last updated, followed by the version number.
Daily database	The date and time at which the daily database was last updated, followed by the version number.
Next update	The next date and time at which the Safe@Office appliance will check for updates.
Status	The current status of the database. This includes the following statuses: • Database Not Installed • OK

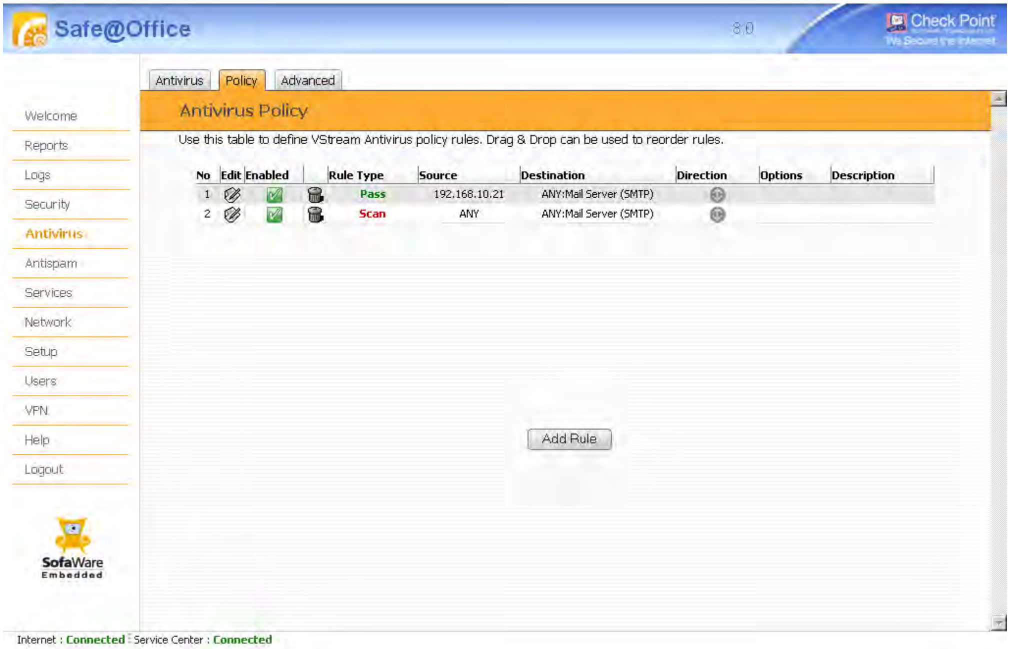
Configuring the VStream Antivirus Policy

500

VStream Antivirus includes a flexible mechanism that allows the user to define exactly which traffic should be scanned, by specifying the protocol, ports, and source and destination IP addresses.

VStream Antivirus processes policy rules in the order they appear in the Antivirus Policy table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the Rules table.

For example, if you want to scan all outgoing SMTP traffic, except traffic from a specific IP address, you can create a rule scanning all outgoing SMTP traffic and move the rule down in the **Antivirus Policy** table. Then create a rule passing SMTP traffic from the desired IP address and move this rule to a higher location in the **Antivirus Policy** table than the first rule. In the figure below, the general rule is rule number 2, and the exception is rule number 1.



Antivirus Policy

Use this table to define VStream Antivirus policy rules. Drag & Drop can be used to reorder rules.

No	Edit	Enabled		Rule Type	Source	Destination	Direction	Options	Description
1		✓		Pass	192.168.10.21	ANY:Mail Server (SMTP)			
2		✓		Scan	ANY	ANY:Mail Server (SMTP)			

Internet : Connected : Service Center : Connected

The Safe@Office appliance will process rule 1 first, passing outgoing SMTP traffic from the specified IP address, and only then it will process rule 2, scanning all outgoing SMTP traffic.

The following rule types exist:

Table 104: VStream Antivirus Rule Types

Rule	Description
Pass	This rule type enables you to specify that VStream Antivirus should not scan traffic matching the rule.
Scan	This rule type enables you to specify that VStream Antivirus should scan traffic matching the rule. If a virus is found, it is blocked and logged.

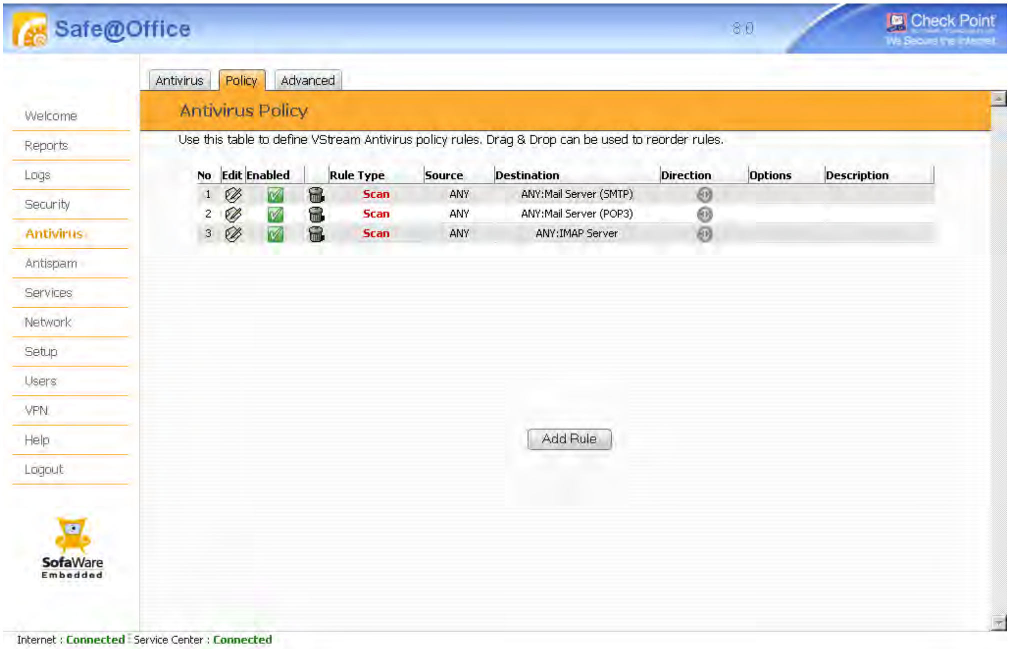
Adding and Editing VStream Antivirus Rules

500

To add or edit a VStream Antivirus rule

1. Click Antivirus in the main menu, and click the Policy tab.

The **Antivirus Policy** page appears.



Antivirus Policy

Use this table to define VStream Antivirus policy rules. Drag & Drop can be used to reorder rules.

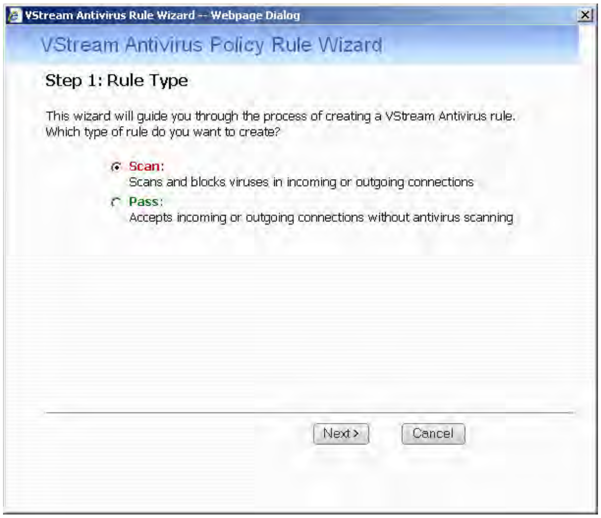
No	Edit	Enabled		Rule Type	Source	Destination	Direction	Options	Description
1	✎	☑	🗑	Scan	ANY	ANY:Mail Server (SMTP)	○		
2	✎	☑	🗑	Scan	ANY	ANY:Mail Server (POP3)	○		
3	✎	☑	🗑	Scan	ANY	ANY:IMAP Server	○		

Internet : Connected Service Center : Connected

2. Do one of the following:

- To add a new rule, click **Add Rule**.
- To edit an existing rule, click ✎ next to the desired rule.

The **VStream Policy Rule Wizard** opens, with the **Step 1: Rule Type** dialog box displayed.



VStream Antivirus Rule Wizard -- Webpage Dialog
VStream Antivirus Policy Rule Wizard

Step 1: Rule Type

This wizard will guide you through the process of creating a VStream Antivirus rule.
Which type of rule do you want to create?

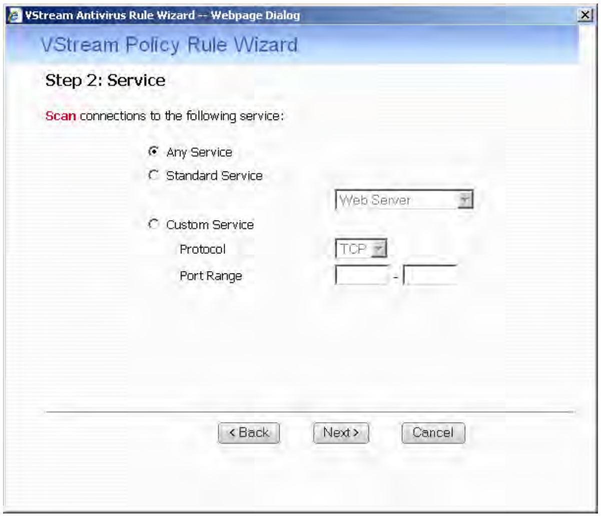
● Scan:
Scans and blocks viruses in incoming or outgoing connections

○ Pass:
Accepts incoming or outgoing connections without antivirus scanning

3. Select the type of rule you want to create.
4. Click **Next**.

The **Step 2: Service** dialog box appears.

The example below shows a Scan rule.



VStream Antivirus Rule Wizard -- Webpage Dialog
VStream Policy Rule Wizard

Step 2: Service

Scan connections to the following service:

● Any Service

○ Standard Service — Web Server

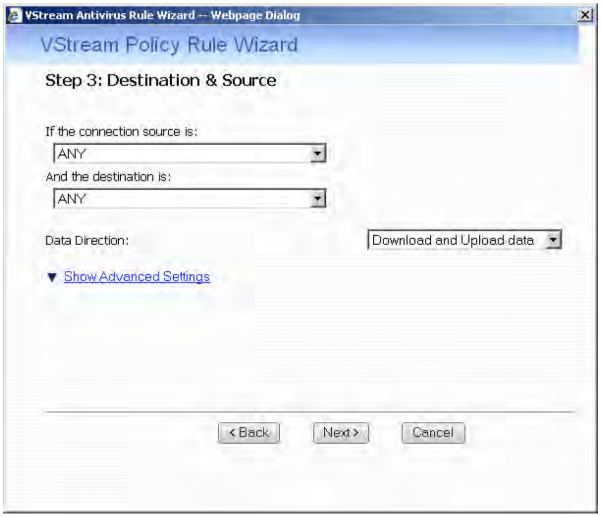
○ Custom Service

Protocol — TCP

Port Range — [ ] - [ ]

5. Complete the fields using the relevant information in the following table.
6. Click **Next**.

   The **Step 3: Destination & Source** dialog box appears.



VStream Antivirus Rule Wizard -- Webpage Dialog

VStream Policy Rule Wizard

Step 3: Destination & Source

If the connection source is: ANY

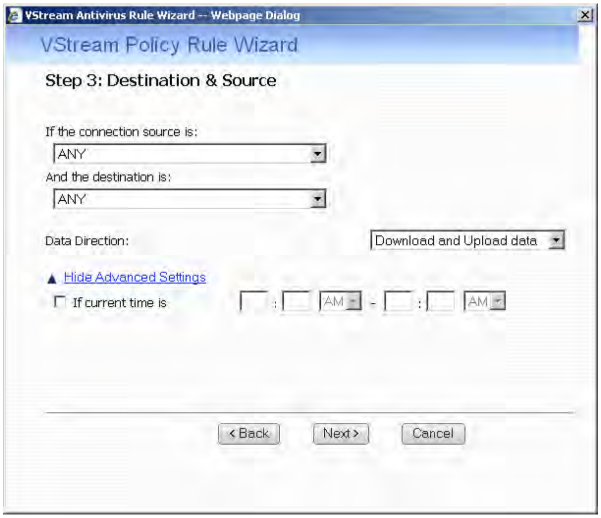
And the destination is: ANY

Data Direction: Download and Upload data

▼ Show Advanced Settings

7. To configure advanced settings, click **Show Advanced Settings**.

   New fields appear.



VStream Antivirus Rule Wizard -- Webpage Dialog

VStream Policy Rule Wizard

Step 3: Destination & Source

If the connection source is: ANY

And the destination is: ANY

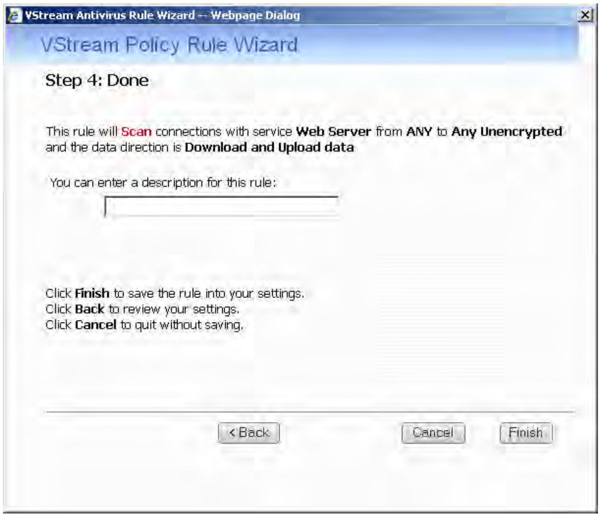
Data Direction: Download and Upload data

▲ Hide Advanced Settings

□ If current time is : AM - : AM

8. Complete the fields using the relevant information in the following table.
9. Click Next.

   The Step 4: Done dialog box appears.



VStream Antivirus Rule Wizard -- Webpage Dialog
VStream Policy Rule Wizard
Step 4: Done

This rule will Scan connections with service **Web Server** from **ANY** to **Any Unencrypted** and the data direction is **Download and Upload data**

You can enter a description for this rule:

Click **Finish** to save the rule into your settings.
Click **Back** to review your settings.
Click **Cancel** to quit without saving.

10. If desired, type a description of the rule in the field provided.
11. Click Finish.

    The new rule appears in the Antivirus Policy page.

Table 105: VStream Antivirus Rule Fields

In this field...	Do this...
Any Service	Click this option to specify that the rule should apply to any service.
Standard Service	Click this option to specify that the rule should apply to a specific standard service or network service object. You must then select the desired service or network service object from the drop-down list.
Custom Service	Click this option to specify that the rule should apply to a specific non-standard service. The Protocol and Port Range fields are enabled. You must fill them in.
Protocol	Select the protocol (TCP, UDP, or ANY) for which the rule should apply.
Port Range	To specify the port range to which the rule applies, type the start port number in the left text box, and the end port number in the right text box. Note: If you do not enter a port range, the rule will apply to all ports. If you enter only one port number, the range will include only that port.
If the connection source is	Select the source of the connections you want to allow/block. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify any source, select ANY.

In this field…	Do this…
And the destination is	Select the destination of the connections you want to allow or block. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify the Safe@Office IP addresses, select This Gateway. To specify any destination *except* the Safe@Office Portal IP addresses, select ANY.
Data Direction	Select the direction of connections to which the rule should apply: • Download and Upload data. The rule applies to downloaded and uploaded data. This is the default. • Download data. The rule applies to downloaded data, that is, data flowing from the destination of the connection to the source of the connection. • Upload data. The rule applies to uploaded data, that is, data flowing from the source of the connection to the destination of the connection.
If the current time is	Select this option to specify that the rule should be applied only during certain hours of the day. You must then use the fields and drop-down lists provided, to specify the desired time range.

Enabling/Disabling VStream Antivirus Rules

500

You can temporarily disable a VStream Antivirus rule.

To enable/disable a VStream Antivirus rule

1. Click **Antivirus** in the main menu, and click the **Policy** tab.

   The **Antivirus Policy** page appears.

2. Next to the desired rule, do one of the following:

   - To enable the rule, click ☒.

     The button changes to ☑ and the rule is enabled.

   - To disable the rule, click ☑.

     The button changes to ☒ and the rule is disabled.

Reordering VStream Antivirus Rules

500

To reorder VStream Antivirus rules

1. Click **Antivirus** in the main menu, and click the **Policy** tab.

   The **Antivirus Policy** page appears.

2. For each rule you want to move, click on the rule and drag it to the desired location in the table.

Viewing and Deleting VStream Antivirus Rules

500

To view or delete an existing VStream Antivirus rule

1. Click **Antivirus** in the main menu, and click the **Policy** tab.

   The **Antivirus Policy** page appears with a list of existing VStream Antivirus rules.

2. To resize a column, drag the relevant column divider right or left.

3. To delete a rule, do the following.

   a. In the desired rule's row, click 🗑.

      A confirmation message appears.

   b. Click **OK**.

      The rule is deleted.

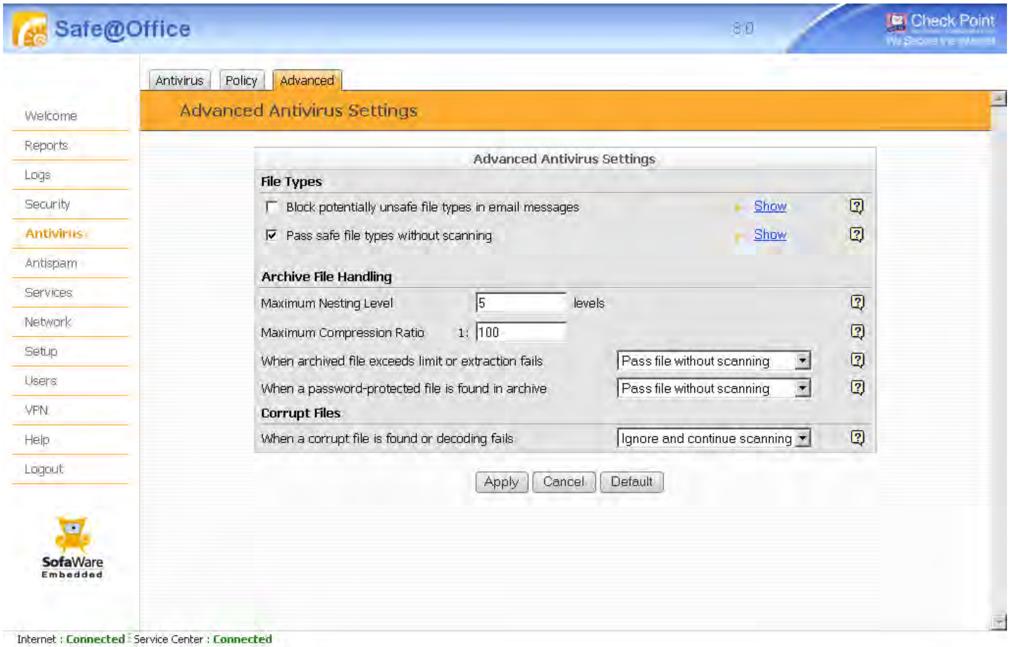
Configuring VStream Antivirus Advanced Settings

500

To configure VStream Antivirus advanced settings

1. Click **Antivirus** in the main menu, and click the **Advanced** tab.

   The **Advanced Antivirus Settings** page appears.



Advanced Antivirus Settings

Advanced Antivirus Settings

File Types

☐ Block potentially unsafe file types in email messages

☑ Pass safe file types without scanning

Archive File Handling

Maximum Nesting Level	5 levels
Maximum Compression Ratio	1: 100
When archived file exceeds limit or extraction fails	Pass file without scanning
When a password-protected file is found in archive	Pass file without scanning

Corrupt Files

When a corrupt file is found or decoding fails	Ignore and continue scanning

Internet : Connected : Service Center : Connected

2. Complete the fields using the following table.
3. Click **Apply**.
4. To restore the default VStream Antivirus settings, do the following:

   a) Click **Default**.

      A confirmation message appears.

   b) Click **OK**.

The VStream Antivirus settings are reset to their defaults. For information on the default values, refer to the following table.

Table 106: Advanced Antivirus Settings Fields

In this field…	Do this…
File Types	
Block potentially unsafe file types in email messages	Select this option to block all emails containing potentially unsafe attachments. Unsafe file types are: • DOS/Windows executables, libraries and drivers • Compiled HTML Help files • VBScript encoded files • Files with {CLSID} in their name • The following file extensions: ade, adp, bas, bat, chm, cmd,com, cpl, crt, exe, hlp, hta, inf, ins, isp, js, jse, lnk, mdb, mde, msc, msi, msp, mst, pcd, pif, reg, scr, sct, shs,shb, url, vb, vbe, vbs, wsc, wsf, wsh. To view a list of unsafe file types and their descriptions, click Show next to this option.

In this field…	Do this…
Pass safe file types without scanning	Select this option to accept common file types that are known to be safe, without scanning them. Safe files types are: • GIF • BMP • JFIF standard • EXIF standard • PNG • MPEG video stream • MPEG sys stream • Ogg Stream • MP3 file with ID3 version 2 • MP3 • PDF • PostScript • WMA/WMV/ASF • RealMedia file • JPEG - only the header is scanned, and the rest of the file is skipped To view a list of safe file types, click Show next to this option. Selecting this option reduces the load on the gateway by skipping safe file types. This option is selected by default.

In this field…	Do this…
Archive File Handling	
Maximum Nesting Level	Type the maximum number of nested content levels that VStream Antivirus should scan. Setting a higher number increases security. Setting a lower number prevents attackers from overloading the gateway by sending extremely nested archive files. The default value is 5 levels.
Maximum Compression Ratio 1:x	Fill in the field to complete the maximum compression ratio of files that VStream Antivirus should scan. For example, to specify a 1:80 maximum compression ratio, type 80. Setting a higher number allows the scanning of highly compressed files, but creates a potential for highly compressible files to create a heavy load on the appliance. Setting a lower number prevents attackers from overloading the gateway by sending extremely compressible files. The default value is 100.
When archived file exceeds limit or extraction fails	Specify how VStream Antivirus should handle files that exceed the Maximum nesting level or the Maximum compression ratio, and files for which scanning fails. Select one of the following: • Pass file without scanning. Scan only the number of levels specified, and skip the scanning of more deeply nested archives. Furthermore, skip scanning highly compressible files, and skip scanning archives that cannot be extracted because they are corrupt. This is the default. • Block file. Block the file.

In this field…	Do this…
When a password-protected file is found in archive	VStream Antivirus cannot extract and scan password-protected files inside archives. Specify how VStream Antivirus should handle such files, by selecting one of the following: • Pass file without scanning. Accept the file without scanning it. This is the default. • Block file. Block the file.
Corrupt Files	
When a corrupt file is found or decoding fails	Specify how VStream Antivirus should handle corrupt files and protocol anomalies, by selecting one of the following: • Ignore and continue scanning. Log the corrupt file or protocol anomaly, and scan the information on a best-effort basis. This is the default. • Block file. Block and log the corrupt file or protocol anomaly.

Updating VStream Antivirus

500

When you are subscribed to the VStream Antivirus updates service, VStream Antivirus virus signatures are automatically updated, keeping security up-to-date with no need for user intervention. However, you can still check for updates manually, if needed.

To update the VStream Antivirus virus signature database

1. Click Antivirus in the main menu, and click the Antivirus tab.

   The VStream Antivirus page appears.

2. Click Update Now.

   The VStream Antivirus database is updated with the latest virus signatures.

Using VStream Antispam

500

The Safe@Office appliance includes VStream Antispam, an embedded antispam engine that scans emails for spam. VStream Antispam is composed three antispam engines, each of which can be enabled or disabled separately:

- IP Reputation

  The IP Reputation engine protects mail servers by checking the email sender's IP address against an online and constantly updated IP reputation database, before accepting the SMTP email connection. If the IP address belongs to a known spammer, the connection can be immediately blocked at the TCP connection level, thereby stopping the spam before it reaches your mail server.

Note: If you have a mail server in your network, it is recommended to enable the IP Reputation engine as a first line of defense for incoming SMTP connections. When enabled, the IP Reputation engine blocks emails that would otherwise reach your mail server and require extensive analysis by the Content Based Antispam and Block List engines, both of which examine email content and consume network, gateway, and mail server resources. By reducing the amount of emails that require in-depth analysis, the IP Reputation engine helps prevent Denial of Service (DoS) attacks on your gateway or mail server.

If you do not have a mail server in your network, there is no need to enable the IP Reputation engine. (If you do enable this engine anyway, it will have no negative effects.)

- Block List

  VStream Antispam allows configuring a list of senders whose emails should be blocked. When an email reaches your mail server, the Block List engine determines whether the sender's email address appears on the list. If so, then VStream Antispam blocks the emails.

- Content Based Antispam

  The Content Based Antispam engine calculates a "spam fingerprint" for each incoming email message. The fingerprint is then sent to a VStream Antispam data center and compared to a constantly updated database of spam messages. The data center returns a "spam score", which is a value in percentages indicating the likelihood that the message is spam. If the spam score exceeds a user-configurable threshold called the “confidence level”, the message can be flagged as spam, or the message can be deleted altogether.

In addition, VStream Antispam allows you to define a Safe Sender List, which consists of senders who are exempt from the Block List and Content Based Antispam engines.

The following table provides a comparison of the VStream Antispam engines.

Table 107: Comparison of VStream Antispam Engines

	IP Reputation	Content Based Antispam and Block List
Supported Protocols	Protects mail servers only, and applies to the SMTP protocol only	Protects both mail servers and mail clients, and applies to both POP3 and SMTP protocols
Email Scanning Time	Scans the email before accepting the connection	Scans the email after accepting the connection
Detection Method	Examines the sender's IP address	Content Based Antispam examines the email's content, and Block List examines the email's Sender field.
SMTP Error Message	Does not return an SMTP error message to the email sender	Returns an SMTP error message to the email sender
Mail Rejection Method	Resets the TCP connection	Marks the email Subject line, marks the email header, rejects the email (SMTP only), or deletes the email (POP3 only)
Server Overload Protection	Prevents spammers from overloading gateway and mail server resources	Does not prevent spammers from overloading gateway and mail server resources

Important: In order to use VStream Antispam, your Safe@Office appliance must be subscribed to a Service Center.

How VStream Antispam Works

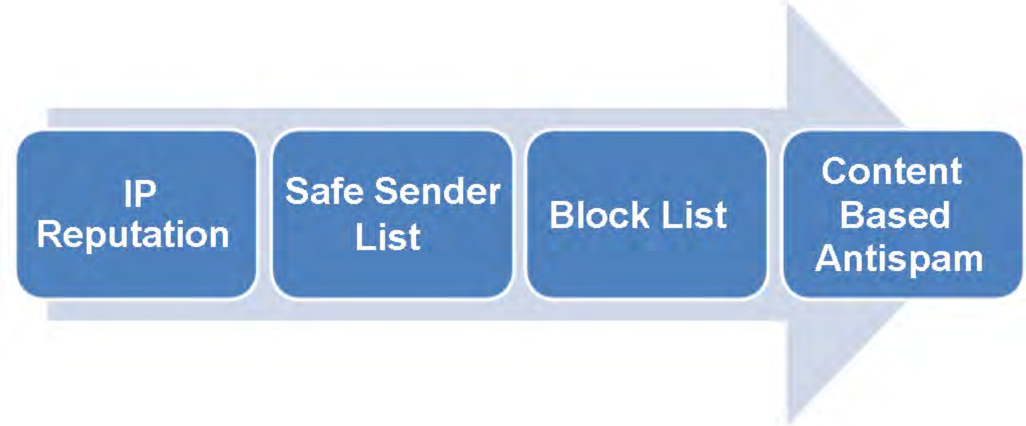


Figure 26: VStream Antispam Flow

VStream Antispam works as follows:

1. A TCP connection arrives at the SMTP port (TCP 25) or the POP3 port (TCP 110).
2. The connection is checked against the VStream Antispam policy, to determine whether it should be scanned.
3. If the IP Reputation engine is enabled, and the connection is an SMTP connection:
   a. VStream Antispam sends the connection's source IP address to a VStream Antispam data center.
   b. The VStream Antispam data center checks the reputation of this IP address against a list of known spam sender IP addresses, and then returns a spam score.
   c. One of the following things happens:

        - If the spam score does not exceed the configured confidence level, the email passes to the next enabled VStream Antispam engine for processing.
        - If the spam score exceeds the configured confidence level, VStream Antispam determines that the email is spam and handles it as specified by the IP Reputation engine's settings.

    d. VStream Antispam caches the results of the IP Reputation check.

4. VStream Antispam checks whether the email sender appears on the Safe Sender List. If so, then the email is accepted.
5. If the Block List engine is enabled:

    a. VStream Antispam examines the email content and compares the sender to the list of blocked senders.

    b. One of the following things happens:

        - If the sender is not on the list of blocked senders, the email passes to the next enabled VStream Antispam engine for processing.
        - If the sender is on the list of blocked senders, VStream Antispam determines that the email is spam and handles it as specified by the Block List engine's settings.

          By default, VStream Antispam marks the email subject.

6. If the Content Based Antispam engine is enabled:

    a. VStream Antispam examines the email content and creates a spam fingerprint.

    b. VStream Antispam sends the fingerprint to a VStream Antispam data center, where it is checked against an online database of spam messages.

    c. The VStream Antispam data center returns a spam score.

    d. One of the following things happens:

        - If the spam score does not exceed the configured confidence level, the email is accepted.
        - If the spam score exceeds the configured confidence level, VStream Antispam determines that email is spam and handles it and handles it as specified by the Content Based Antispam engine's settings.

By default, VStream Antispam marks the email as spam.

7. One of the following things happen:

   - If the connection is an SMTP connection, the mail server forwards the email to the recipient.
   - If the connection is a POP3 connection, the email client receives the email.

Header Marking

VStream Antispam adds the following headers to each email that is scanned by the Content Based Antispam or Block List engine, but not blocked:

- `X-VStream-Spam-Level`. Contains an integer between 0 and 100, where 100 indicates the highest likelihood that the email is spam.
- `X-VStream-Engine`. The VStream Antispam engine, (either "Content Based Antispam" or "Block List")
- `X-Spam-Level`. Contains one to five asterisks, where five asterisks indicates the highest likelihood that the email is spam.
- `X-Spam-Flag`. Contains `YES` if the email is deemed to be spam, according to the currently configured thresholds.

For example:

```
X-VStream-Spam-Level: 81%
X-VStream-Engine: Content Based Antispam
X-Spam-Level: ***
X-Spam-Flag: YES
```

If your email client allows defining rules based on message headers, you can create rules specifying that emails with certain headers should be moved to specific folders. For example, you can configure your email client to move all emails with the `X-Spam-Flag: YES` header directly to a "Spam Email" folder.

Default Antispam Policy

The VStream Antispam default policy includes the following rules:

- All incoming SMTP connections are scanned, unless they originate from VPN. This protects mail servers in your network.
- All outgoing POP3 connections are scanned. This protects mail clients in your network.

You can easily override the default antispam policy, for example to exclude certain addresses or networks from spam scanning, by creating user-defined rules. For further information, see ***Configuring the VStream Antispam Policy*** on page 510.

Enabling/Disabling VStream Antispam

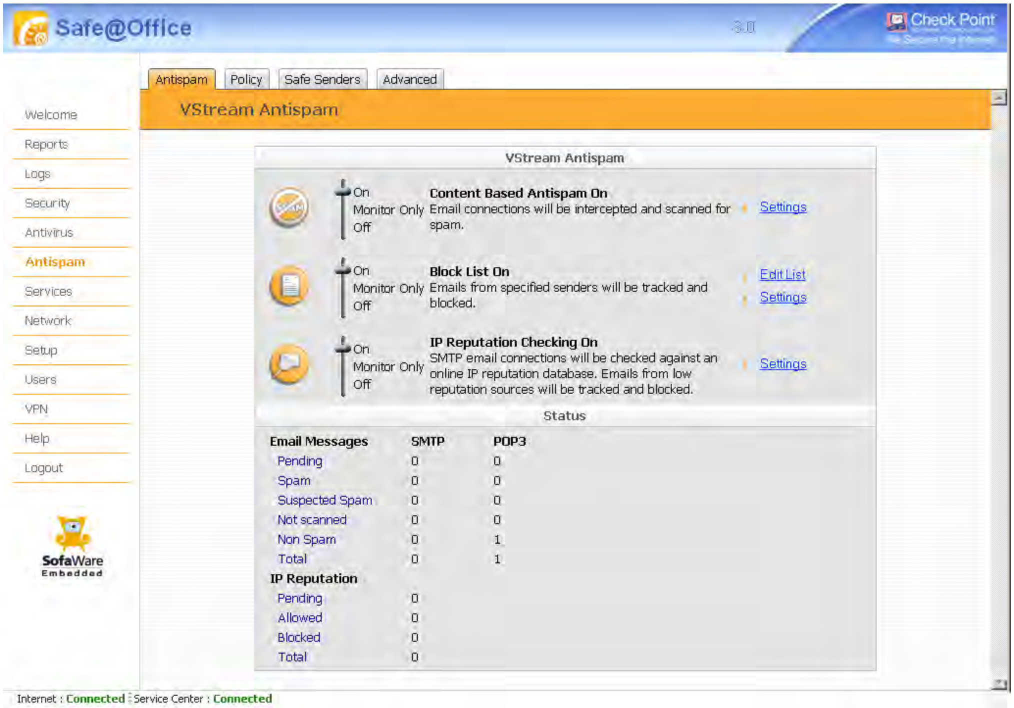
500

You must enable *at least one* VStream Antispam engine in order for VStream Antispam to work. Once you have enabled the desired engines, you must configure them, using the relevant sections in this guide.

To enable/disable VStream Antispam

1. Click Antispam in the main menu, and click the Antispam tab.

The VStream Antispam page appears.



VStream Antispam

VStream Antispam

On / Monitor Only / Off

Content Based Antispam On
Email connections will be intercepted and scanned for spam.
Settings

On / Monitor Only / Off

Block List On
Emails from specified senders will be tracked and blocked.
Edit List
Settings

On / Monitor Only / Off

IP Reputation Checking On
SMTP email connections will be checked against an online IP reputation database. Emails from low reputation sources will be tracked and blocked.
Settings

Status

Email Messages	SMTP	POP3
Pending	0	0
Spam	0	0
Suspected Spam	0	0
Not scanned	0	0
Non Spam	0	1
Total	0	1
IP Reputation		
Pending	0	
Allowed	0	
Blocked	0	
Total	0	

Internet : Connected Service Center : Connected

2. Complete the fields using the information in the following table.

Table 108: VStream Antispam Fields

In this field…	Do this…
Content Based Antispam	Specify the Content Based Antispam engine's mode, by dragging the lever to one of the following: • On. The Content Based Antispam engine is on. VStream Antispam will check email fingerprints against an online spam detection database. Emails that fail the check will be handled according to configured Content Based Antispam settings. • Monitor Only. The Content Based Antispam engine is on. VStream Antispam will check email fingerprints against an online spam detection database. Emails that fail the check will be *logged only*, and any action configured in the Content Based Antispam Settings page will *not* be performed. • Off. The Content Based Antispam engine is off. You can then click Settings to configure the Content Based Antispam settings. For further information, see ***Configuring the Content Based Antispam Engine*** on page 497.
Block List	Specify the Block List engine's mode, by dragging the lever to one of the following: • On. The Block List engine is on. VStream Antispam will check email messages against a list of blocked senders. Emails that fail the check will be handled according to configured Block List settings. • Monitor Only. The Block List engine is on. VStream Antispam will check email messages against a list of blocked senders. Emails that fail the check will be *logged only*, and any action configured in the Antispam Block List Settings page will *not* be performed. • Off. The Block List engine is off. You can then click Settings to configure the Block List settings. For further information, see ***Configuring the Block List Engine Settings*** on page 504.

In this field...	Do this...
IP Reputation Checking	Specify the IP Reputation engine's mode for SMTP connections, by dragging the lever to one of the following: • On. The IP Reputation engine is on. VStream Antispam will check the reputation of email senders against an online IP reputation database prior to accepting the TCP connection. Emails that fail the check will be handled according to configured IP Reputation settings. • Monitor Only. The IP Reputation engine is on. VStream Antispam will check the reputation of email senders against an online IP reputation database. Emails that fail the check will be *logged only*, and any action configured in the Antispam IP Reputation Settings page will *not* be performed. • Off. The IP Reputation engine is off. You can then click Settings to configure the IP Reputation settings. For further information, see ***Configuring the IP Reputation Engine*** on page 507.

Viewing VStream Antispam Statistics

500

To view VStream Antispam statistics

- Click Antispam in the main menu, and click the Antispam tab.

  The VStream Antispam page appears.

Table 109: VStream Antispam Status Fields

This field...	Displays...
Email Messages	Statistics for the Content Based Antispam and Block List engines.
Pending	The number of SMTP and POP3 email messages pending for the Content Based Antispam and Block List engines.
Spam	The number of SMTP and POP3 email messages that the Content Based Antispam and Block List engines determined to be spam.
Suspected Spam	The number of SMTP and POP3 email messages that the Content Based Antispam and Block List engines determined to be suspected spam.
Not scanned	The number of SMTP and POP3 email messages that were not scanned, due to temporary loss of contact with the VStream Antispam data center, or due to gateway resource overload.
Non Spam	The number of SMTP and POP3 email messages that the Content Based Antispam and Block List engines determined to be legitimate.
Total	The total number of SMTP and POP3 email messages scanned by the Content Based Antispam and Block List engines.
IP Reputation	Statistics for the IP Reputation engine.
Pending	The number of SMTP email connections currently pending for handling by the IP Reputation engine.
Allowed	The number of SMTP email connections allowed by the IP Reputation engine.
Blocked	The number of SMTP email connections blocked by the IP Reputation engine.

This field...	Displays...
Total	The total number of SMTP email connections scanned by the IP Reputation engine.

Configuring the Content Based Antispam Engine

500

You can configure how VStream Antispam should handle spam and suspected spam that is detected by the Content Based Antispam engine.

For information on enabling this engine, see ***Enabling/Disabling VStream Antispam*** on page 492.

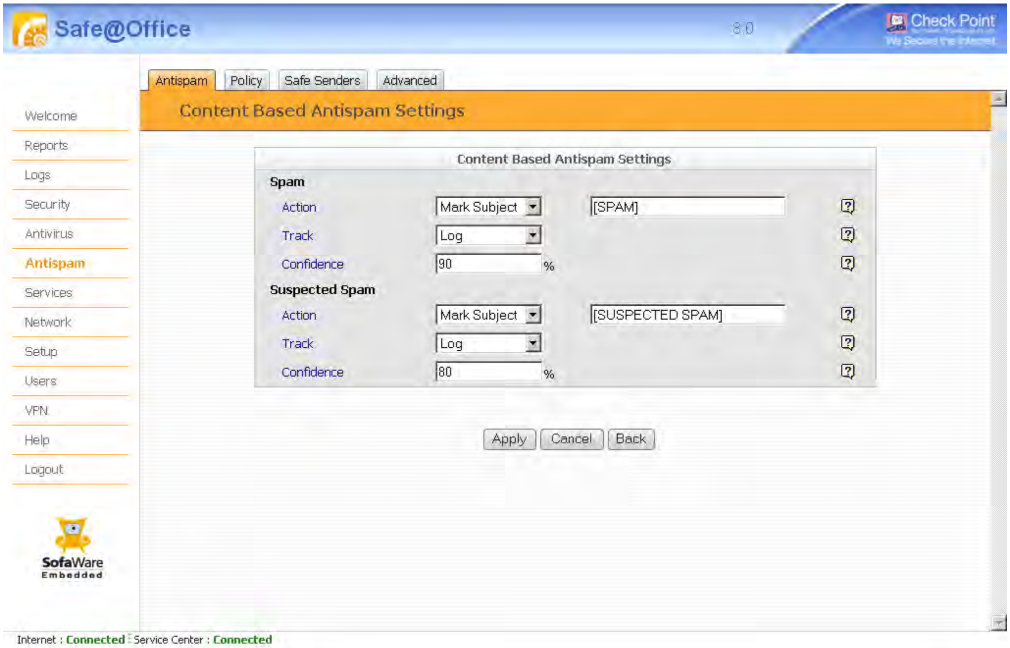
To configure Content Based Antispam engine settings

1. Click Antispam in the main menu, and click the Antispam tab.

   The VStream Antispam page appears.

2. Next to the Content Based Antispam lever, click Settings.

The **Content Based Antispam Settings** page appears.



Content Based Antispam Settings

Content Based Antispam Settings

Spam

Action	Mark Subject	[SPAM]
Track	Log	
Confidence	90 %	

Suspected Spam

Action	Mark Subject	[SUSPECTED SPAM]
Track	Log	
Confidence	80 %	

Internet : Connected | Service Center : Connected

3. Complete the fields using the information in the following table.
4. Click **Apply**.

Table 110: Content Based Antispam Settings Fields

In this field…	Do this…
Spam	Configure how VStream Antispam should handle spam that is detected using the Content Based Antispam engine.

In this field...	Do this...
Action	Specify the action VStream Antispam should take upon detecting spam, by selecting one of the following: • None. Take no action. • Reject. Block the email. The email will be permanently deleted. • Mark Subject. Mark the email's Subject line. If you select Mark Subject, the Mark Text field appears. Note: If the Content Based Antispam engine is in Monitor Only mode, this setting is ignored. For information on changing the engine's mode, see ***Enabling/Disabling VStream Antispam*** on page 492.
Mark Text	Type the prefix to the text appearing in the Subject field of the spam notification email. For example, if you type `[SPAM]` and the original email's Subject field displays "Earn Money the Easy Way", the spam notification email's Subject field will display: "[SPAM] Earn Money the Easy Way". The default value is `[SPAM]`. Note: If your email client allows defining rules based on the Subject field, you can create rules specifying that emails whose Subject field contains certain words should be moved to specific folders. For example, you can configure your email client to move all emails whose Subject field contains `[SPAM]` directly to the Deleted Items folder.
Track	Specify whether VStream Antispam should log spam, by selecting one of the following: • Log. VStream Antispam should log spam. • None. VStream Antispam should not log spam.

In this field...	Do this...
Confidence	Type the minimum spam confidence level (SCL). If an email's SCL matches or exceeds this threshold, the email is considered spam. Setting a higher SCL reduces the number of legitimate emails erroneously identified as spam. Setting a lower SCL increases the amount of spam that is identified as legitimate email. The default value is 90.
Suspected Spam	Configure how VStream Antispam should handle suspected spam that is detected using the Content Based Antispam engine.
Action	Specify the action VStream Antispam should take upon detecting potential spam, by selecting one of the following: • None. Take no action. • Reject. Block the email. The email will be permanently deleted. • Mark Subject. Mark the email's Subject line. If you select Mark Subject, the Mark Text field appears. Note: If the Content Based Antispam engine is in Monitor Only mode, this setting is ignored. For information on changing the engine's mode, see ***Enabling/Disabling VStream Antispam*** on page 492.

In this field...	Do this...
Mark Text	Type the prefix to the text appearing in the Subject field of the suspected spam notification email. For example, if you type `[SUSPECTED SPAM]` and the original email's Subject field displays "Earn Money the Easy Way", the suspected spam notification email's Subject field will display: "[SUSPECTED SPAM] Earn Money the Easy Way". The default value is `[SUSPECTED SPAM]`. Note: If your email client allows defining rules based on the Subject field, you can create rules specifying that emails whose Subject field contains certain words should be moved to specific folders. For example, you can configure your email client to move all emails whose Subject field contains `[SUSPECTED SPAM]` directly to a Quarantine folder.
Track	Specify whether VStream Antispam should log suspected spam, by selecting one of the following: • Log. VStream Antispam should log suspected spam. • None. VStream Antispam should not log suspected spam.
Confidence	Type the minimum spam confidence level (SCL). If an email's SCL matches or exceeds this threshold, the email is considered suspected spam. Setting a higher SCL reduces the number of legitimate emails erroneously identified as suspected spam. Setting a lower SCL increases the amount of potential spam that is identified as legitimate email. The default value is 80.

Configuring the Block List Engine

500

You can configure a list of email addresses and domain names that VStream Antispam should automatically block, if the Block List engine is enabled.

For information on enabling the Block List engine, see ***Enabling/Disabling VStream Antispam*** on page 492.

Adding Blocked Senders

500

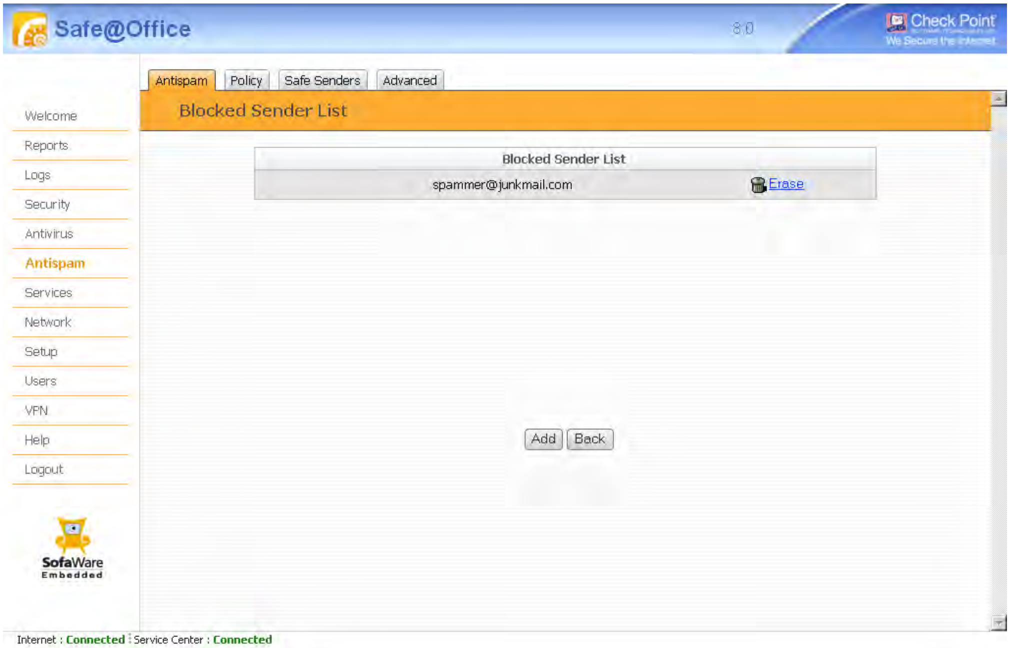
To add a blocked sender

1. Click Antispam in the main menu, and click the Antispam tab.

   The VStream Antispam page appears.

2. Next to the Block List lever, click Edit List.

The **Blocked Sender List** page appears.



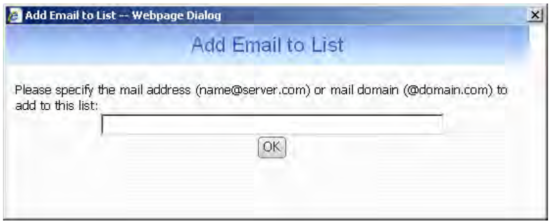
Blocked Sender List

Blocked Sender List	
spammer@junkmail.com	Erase

Internet : Connected | Service Center : Connected

3. Click **Add**.

   The **Add Email to List** dialog box appears.



Add Email to List

Please specify the mail address (name@server.com) or mail domain (@domain.com) to add to this list:

4. In the field provided, do one of the following:

   - To block all email from a specific sender, type the sender's email address.
   - To block all email from addresses ending with a specific domain, type the domain name.

     For example, if you type "@special-offers.com", then email addresses such as johns@special-offers.com and sarahm@special-offers.com will be blocked.

5. Click **OK**.

   The sender appears in the **Block Sender List** table.

Viewing and Deleting Blocked Senders

500

To delete a blocked sender

1. Click **Antispam** in the main menu, and click the **Antispam** tab.

   The **VStream Antispam** page appears.

2. Next to the **Block List** lever, click **Edit List**.

   The **Blocked Sender List** page appears.

3. In the desired sender's row, click 🗑.

   The sender is deleted.

Configuring the Block List Engine Settings

500

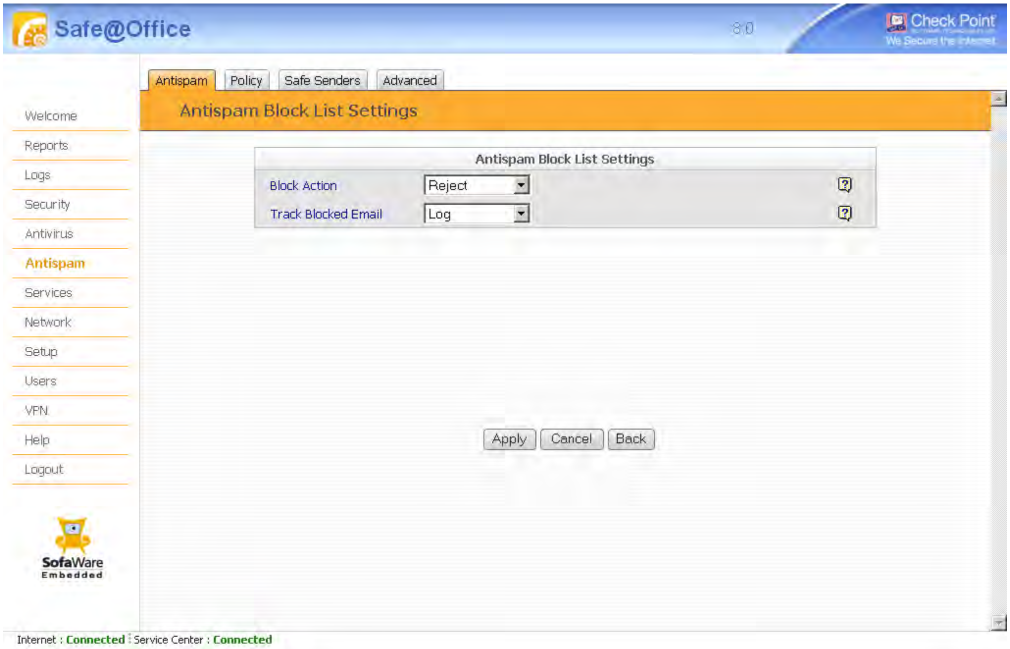
To configure Block List engine settings

1. Click **Antispam** in the main menu, and click the **Antispam** tab.

   The **VStream Antispam** page appears.

2. Next to the **Block List** lever, click **Settings**.

The **Antispam Block List Settings** page appears.



Antispam Block List Settings

Antispam Block List Settings

Block Action	Reject
Track Blocked Email	Log

Internet : Connected Service Center : Connected

3. Complete the fields using the information in the following table.
4. Click **Apply**.

Table 111: Antispam Block List Settings Fields

In this field…	Do this…
Block Action	Specify the action VStream Antispam should take upon receiving an email from a blocked sender, by selecting one of the following: • None. Take no action. • Reject. Block the email. • Mark Subject. Mark the email's Subject line. If you select Mark Subject, the Mark Text field appears. Note: If the Block List engine is in Monitor Only mode, this setting is ignored. For information on changing the engine's mode, see ***Enabling/Disabling VStream Antispam*** on page 492.
Mark Text	Type the prefix to the text appearing in the Subject field of the spam notification email. For example, if you type `[SPAM]` and the original email's Subject field displays "Earn Money the Easy Way", the spam notification email's Subject field will display: "[SPAM] Earn Money the Easy Way". The default value is `[SPAM]`. Note: If your email client allows defining rules based on the Subject field, you can create rules specifying that emails whose Subject field contains certain words should be moved to specific folders. For example, you can configure your email client to move all emails whose Subject field contains `[SPAM]` directly to the Deleted Items folder.
Track Blocked Email	Specify whether VStream Antispam should log emails from blocked senders, by selecting one of the following: • Log. VStream Antispam should log emails from blocked senders. • None. VStream Antispam should not log emails from blocked senders.

Configuring the IP Reputation Engine

500

You can configure how VStream Antispam should handle spam and suspected spam that is detected by the IP Reputation engine.

For information on enabling this engine, see ***Enabling/Disabling VStream Antispam*** on page 492.

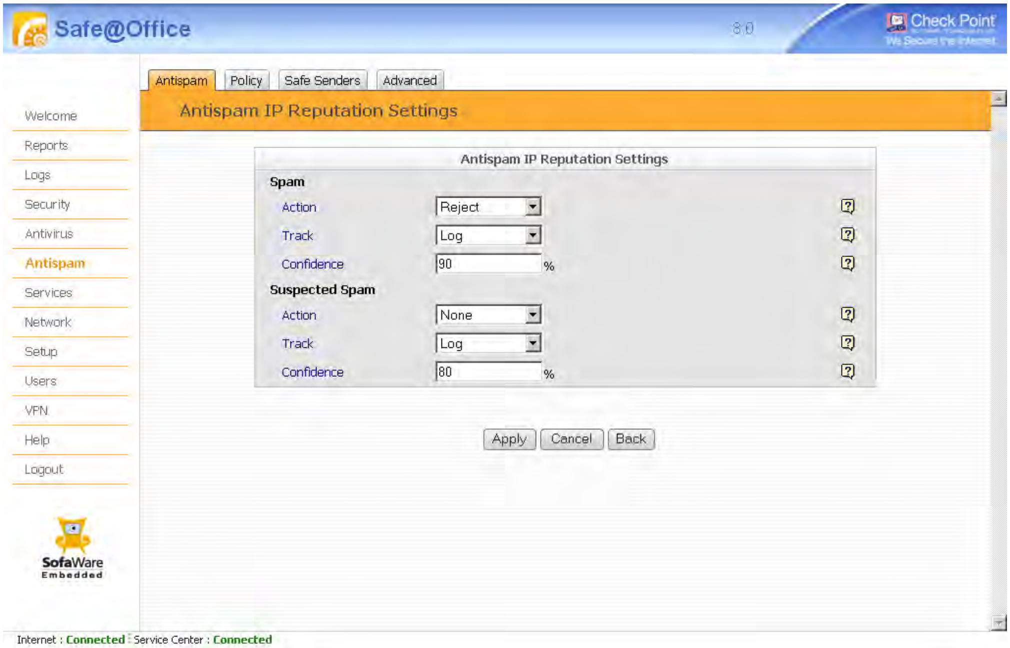
To configure IP Reputation engine settings

1. Click Antispam in the main menu, and click the Antispam tab.

   The VStream Antispam page appears.

2. Next to the IP Reputation Checking lever, click Settings.

   The Antispam IP Reputation Settings page appears.



Antispam IP Reputation Settings

Antispam IP Reputation Settings		
Spam		
Action	Reject	
Track	Log	
Confidence	90	%
Suspected Spam		
Action	None	
Track	Log	
Confidence	80	%

Internet : Connected Service Center : Connected

3. Complete the fields using the information in the following table.

4. Click **Apply**.

Table 112: Antispam IP Reputation Settings Fields

In this field…	Do this…
Spam	Configure how VStream Antispam should handle spam that is detected using the IP Reputation engine.
Action	Specify the action VStream Antispam should take upon detecting spam, by selecting one of the following: • Reject. Block the email. • None. Take no action. Note: If the IP Reputation engine is in Monitor Only mode, this setting is ignored. For information on changing the engine's mode, see ***Enabling/Disabling VStream Antispam*** on page 492.
Track	Specify whether VStream Antispam should log spam, by selecting one of the following: • Log. VStream Antispam should log spam. • None. VStream Antispam should not log spam.
Confidence	Type the minimum spam confidence level (SCL) needed to fail this check. If an email's SCL matches or exceeds this threshold, the email is considered spam. Setting a higher SCL reduces the number of legitimate emails erroneously identified as spam. Setting a lower SCL increases the amount of spam that is identified as legitimate email. The default value is 90.
Suspected Spam	Configure how VStream Antispam should handle suspected spam that is detected using the IP Reputation engine.

In this field...	Do this...
Action	Specify the action VStream Antispam should take upon detecting potential spam, by selecting one of the following: • Reject. Block the email. • None. Take no action. Note: If the IP Reputation engine is in Monitor Only mode, this setting is ignored. For information on changing the engine's mode, see ***Enabling/Disabling VStream Antispam*** on page 492.
Track	Specify whether VStream Antispam should log suspected spam, by selecting one of the following: • Log. VStream Antispam should log suspected spam. • None. VStream Antispam should not log suspected spam.
Confidence	Type the minimum spam confidence level (SCL) needed to fail this check. If an email's SCL matches or exceeds this threshold, the email is considered suspected spam. Setting a higher SCL reduces the number of legitimate emails erroneously identified as suspected spam. Setting a lower SCL increases the amount of potential spam that is identified as legitimate email. The default value is 80.

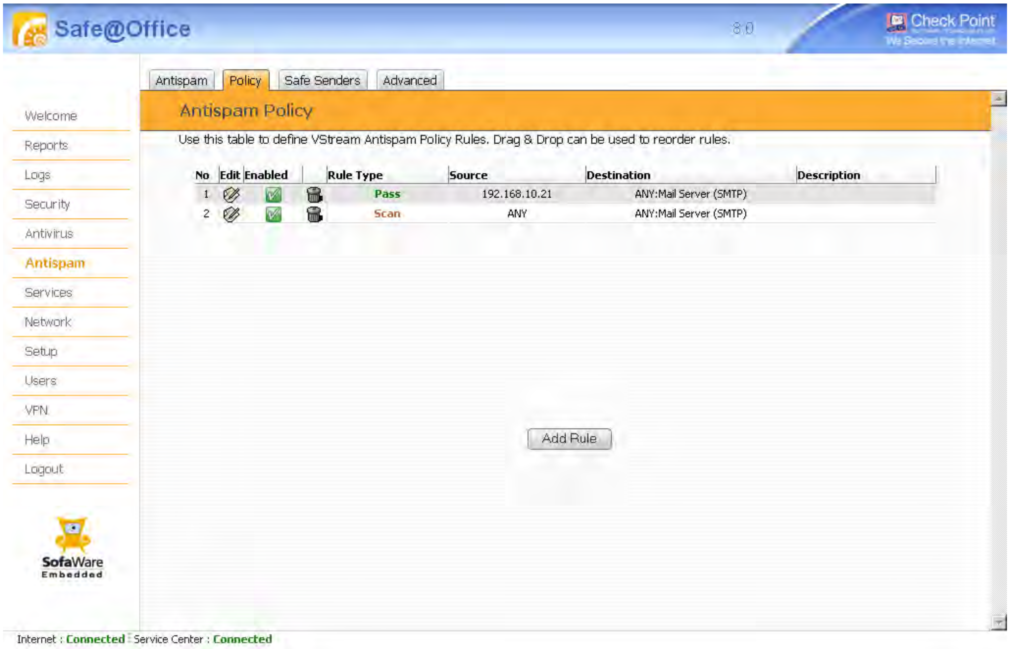
Configuring the VStream Antispam Policy

500

VStream Antispam includes a flexible mechanism that allows the user to define exactly which emails should be scanned for spam and which should be considered safe, by specifying the protocol, and the source and destination IP addresses.

VStream Antispam processes policy rules in the order they appear in the Antispam Policy table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the Rules table.

For example, if you want to scan all outgoing SMTP traffic, except traffic from a specific IP address, you can create a rule scanning all outgoing SMTP traffic and move the rule down in the Antispam Policy table. Then create a rule passing SMTP traffic from the desired IP address and move this rule to a higher location in the Antispam Policy table than the first rule. In the figure below, the general rule is rule number 2, and the exception is rule number 1.



Antispam Policy

Use this table to define VStream Antispam Policy Rules. Drag & Drop can be used to reorder rules.

No	Edit	Enabled		Rule Type	Source	Destination	Description
1	✎	☑	🗑	Pass	192.168.10.21	ANY:Mail Server (SMTP)	
2	✎	☑	🗑	Scan	ANY	ANY:Mail Server (SMTP)	

Internet : Connected Service Center : Connected

The Safe@Office appliance will process rule 1 first, passing outgoing SMTP traffic from the specified IP address, and only then it will process rule 2, scanning all outgoing SMTP traffic.

The following rule types exist:

Table 113: VStream Antispam Rule Types

Rule	Description
Pass	This rule type enables you to specify that VStream Antispam should allow all emails matching the rule, without scanning the emails.
Scan	This rule type enables you to specify that VStream Antispam should scan all emails matching the rule.
Reject	This rule type enables you to specify that VStream Antispam should reject all emails matching the rule, without scanning the emails.

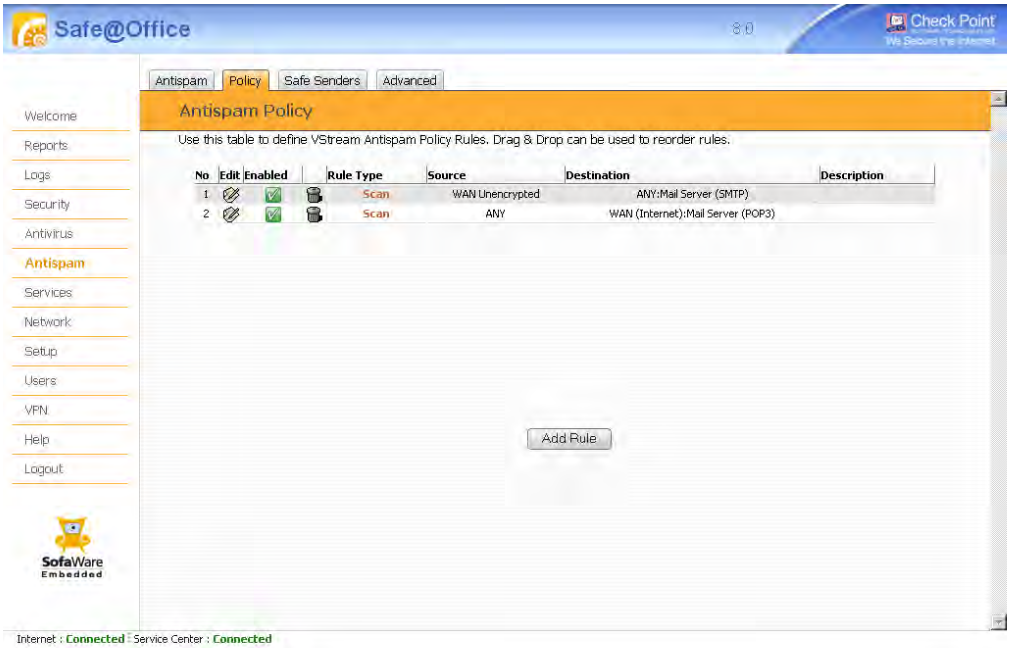
Adding and Editing VStream Antispam Rules

500

To add or edit a VStream Antispam rule

1. Click **Antispam** in the main menu, and click the **Policy** tab.

   The **Antispam Policy** page appears.



Antispam Policy

Use this table to define VStream Antispam Policy Rules. Drag & Drop can be used to reorder rules.

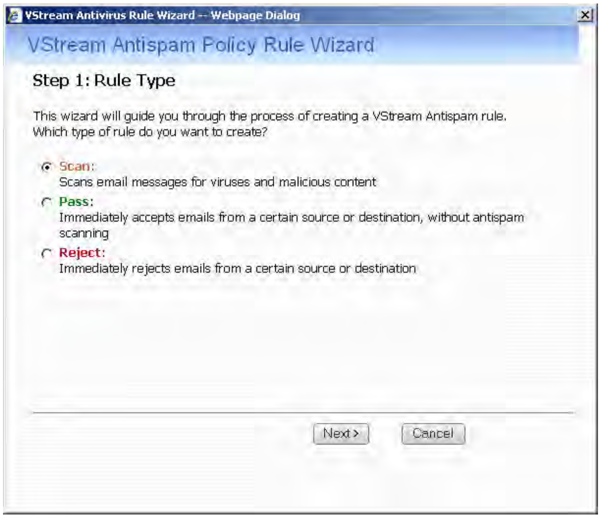
No	Edit	Enabled		Rule Type	Source	Destination	Description
1	✎	☑	🗑	Scan	WAN Unencrypted	ANY:Mail Server (SMTP)	
2	✎	☑	🗑	Scan	ANY	WAN (Internet):Mail Server (POP3)	

Internet : Connected Service Center : Connected

2. Do one of the following:

   - To add a new rule, click **Add Rule**.
   - To edit an existing rule, click ✎ next to the desired rule.

The **VStream Antispam Policy Rule Wizard** opens, with the **Step 1: Rule Type** dialog box displayed.



VStream Antivirus Rule Wizard -- Webpage Dialog
VStream Antispam Policy Rule Wizard

Step 1: Rule Type

This wizard will guide you through the process of creating a VStream Antispam rule. Which type of rule do you want to create?

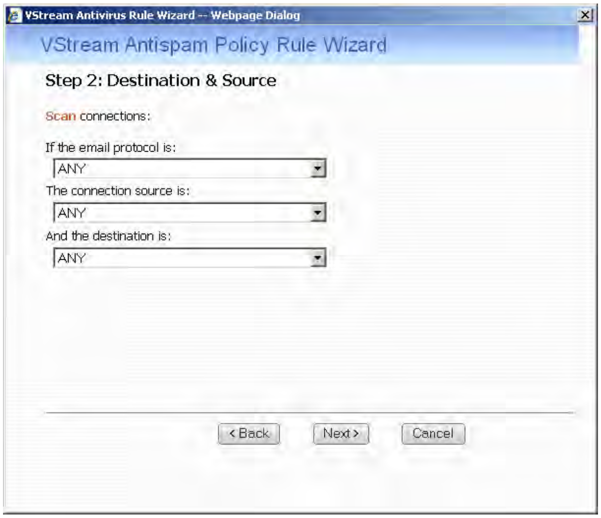
● Scan:
Scans email messages for viruses and malicious content

○ Pass:
Immediately accepts emails from a certain source or destination, without antispam scanning

○ Reject:
Immediately rejects emails from a certain source or destination

3. Select the type of rule you want to create.
4. Click **Next.**

The **Step 2: Destination & Source** dialog box appears.



VStream Antivirus Rule Wizard -- Webpage Dialog
VStream Antispam Policy Rule Wizard

Step 2: Destination & Source

Scan connections:

If the email protocol is: ANY

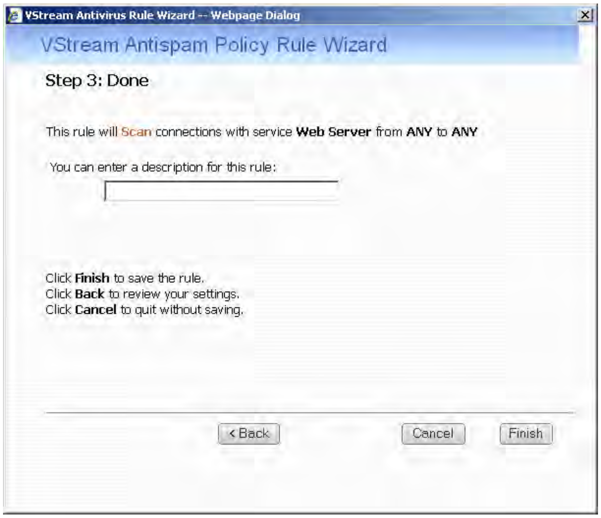
The connection source is: ANY

And the destination is: ANY

5. Complete the fields using the relevant information in the following table.

6. Click **Next**.

   The **Step 3: Done** dialog box appears.



VStream Antivirus Rule Wizard -- Webpage Dialog

VStream Antispam Policy Rule Wizard

Step 3: Done

This rule will Scan connections with service **Web Server** from **ANY** to **ANY**

You can enter a description for this rule:

Click **Finish** to save the rule.
Click **Back** to review your settings.
Click **Cancel** to quit without saving.

7. If desired, type a description of the rule in the field provided.
8. Click **Finish**.

   The new rule appears in the **Antispam Policy** page.

Table 114: VStream Antispam Policy Rule Wizard Fields

In this field…	Do this…
If the email protocol is	Select the email protocol to which the rule should apply. The supported protocols are SMTP and POP3. To specify both SMTP and POP3, select ANY. Note: When defining a Reject rule, this field is set to Mail Server (SMTP).

In this field…	Do this…
The connection source is	Select the source of the connections to which the rule should apply. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify connections originating from this gateway, select This Gateway. To specify any source *except* this gateway, select ANY.
And the destination is	Select the destination of the connections to which the rule should apply. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify the Safe@Office IP addresses, select This Gateway. To specify any destination *except* the Safe@Office Portal IP addresses, select ANY.
Description	Type a description of the rule.

Enabling/Disabling VStream Antispam Rules

500

You can temporarily disable a VStream Antispam rule.

To enable/disable a VStream Antispam rule

1. Click Antispam in the main menu, and click the Policy tab.

   The Antispam Policy page appears.

2. Next to the desired rule, do one of the following:

   - To enable the rule, click ☒.

     The button changes to ☑ and the rule is enabled.

   - To disable the rule, click ☑.

     The button changes to ☒ and the rule is disabled.

Reordering VStream Antispam Rules

500

To reorder VStream Antispam rules

1. Click Antispam in the main menu, and click the Policy tab.

   The Antispam Policy page appears.

2. For each rule you want to move, click on the rule and drag it to the desired location in the table.

Viewing and Deleting VStream Antispam Rules

500

To view or delete an existing VStream Antispam rule

1. Click Antispam in the main menu, and click the Policy tab.

   The Antispam Policy page appears with a list of existing VStream Antispam rules.

2. To resize a column, drag the relevant column divider right or left.

3. To delete a rule, do the following.

   a. In the desired rule's row, click 🗑.

      A confirmation message appears.

   b. Click OK.

      The rule is deleted.

Configuring the Safe Sender List

500

You can configure a list of email addresses and domain names that are "safe". VStream Antispam will treat all emails sent from these addresses or domains as legitimate (non-spam) mail.

Note: The IP Reputation check is performed *before* accepting the TCP connection, at which point the sender’s email address is not yet available. Therefore, if the IP Reputation engine is enabled, and an SMTP session is received from an IP address that is reputed to be a source of spam, VStream Antispam will block the connection, regardless of whether the sender's email address is on the Safe Sender List.

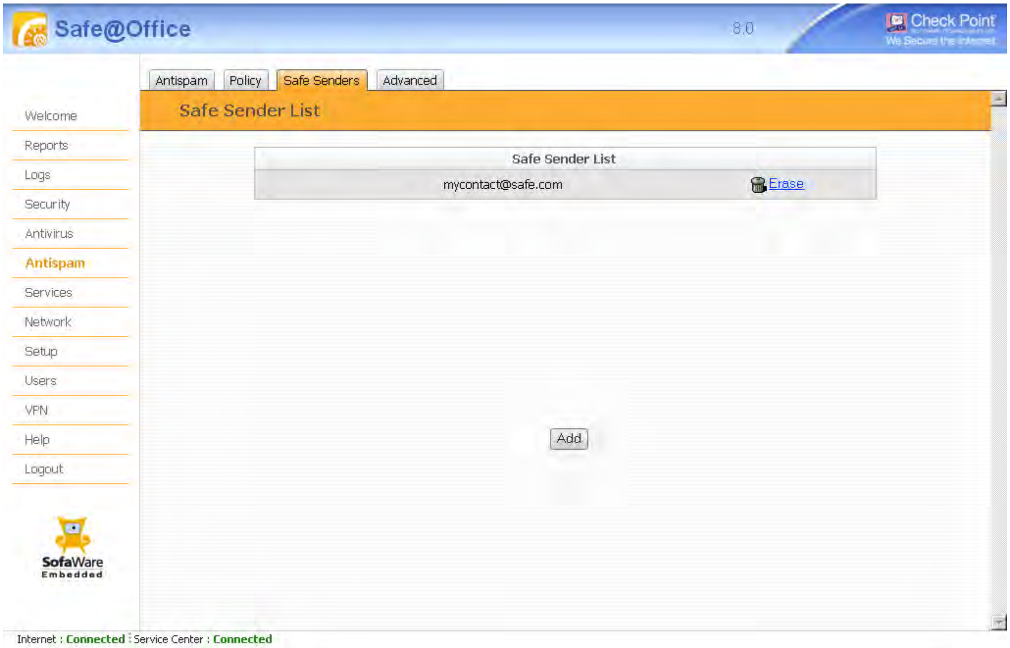
Adding Safe Senders

500

To add a safe sender

1. Click **Antispam** in the main menu, and click the **Safe Senders** tab.

   The **Safe Sender List** page appears.



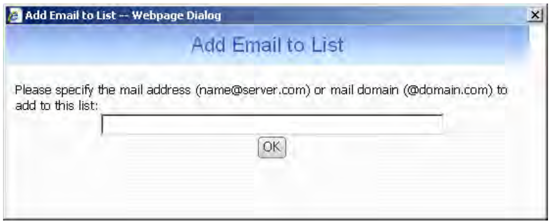
Safe Sender List

Safe Sender List	
mycontact@safe.com	Erase

Internet : Connected | Service Center : Connected

2. Click **Add**.

   The **Add Email to List** dialog box appears.



Add Email to List

Please specify the mail address (name@server.com) or mail domain (@domain.com) to add to this list:

3. In the field provided, do one of the following:

   - To allow all email from a specific sender, type the sender's email address.
   - To allow all email from addresses ending with a specific domain, type the domain name.

     For example, if you type "@mycompany.com", then email addresses such as johns@mycompany.com and sarahm@mycompany.com will be allowed.

4. Click **OK**.

   The sender appears in the **Safe Senders** table.

Viewing and Deleting Safe Senders

500

To view or delete a safe sender

1. Click **Antispam** in the main menu, and click the **Safe Senders** tab.

   The **Safe Sender List** page appears.

2. In the desired sender's row, click **Erase**.

   The sender is deleted.

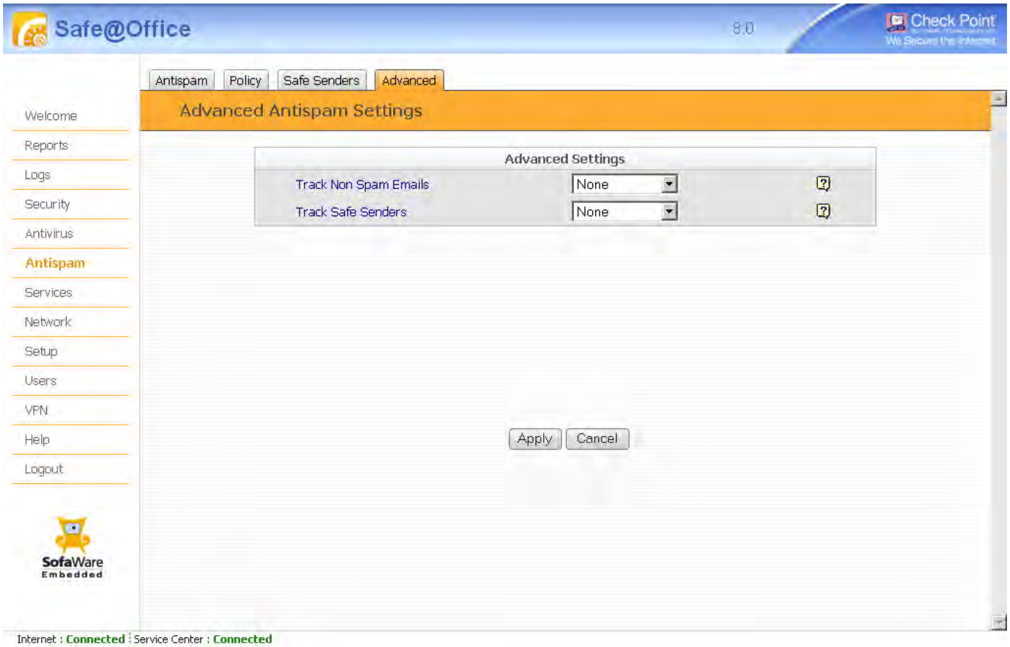
Configuring VStream Antispam Advanced Settings

500

To configure VStream Antispam advanced settings

1. Click Antispam in the main menu, and click the Advanced tab.

   The Advanced Antispam Settings page appears.



Advanced Antispam Settings

Advanced Settings

Track Non Spam Emails: None

Track Safe Senders: None

Internet : Connected | Service Center : Connected

2. In the Track Non Spam Emails drop-down list, do one of the following:

   - To specify that VStream Antispam should log email that is detected as legitimate mail, select Log.
   - To specify that VStream Antivirus should not log email that is detected as legitimate mail, select None.

3. In the Track Safe Senders drop-down list, do one of the following:

- To specify that VStream Antispam should log email sent by addresses on the Safe Sender List, select Log.
- To specify that VStream Antivirus should not log email sent by addresses on the Safe Sender List, select None.

4. Click Apply.

Using Centralized Email Filtering

500

There are two centralized Email Filtering services:

- Email Antivirus

  When the Email Antivirus service is enabled, your email is automatically scanned for the detection and elimination of all known viruses and vandals. If a virus is detected, it is removed and replaced with a warning message.

- Email Antispam

  When the Email Antispam service is enabled, your email is automatically scanned for the detection of spam. If spam is detected, the email's Subject line is modified to indicate that it is suspected spam. If your email client allows defining rules based on the Subject field, you can create rules to divert such messages to a special folder.

Note: Email Filtering services are only available if you are connected to a Service Center and subscribed to the services. For information on using subscription services, see ***Using Subscription Services*** on page 551.

Note: For information on the differences between the centralized Email Filtering services and VStream Antivirus or VStream Antispam, see ***Overview*** on page 465.

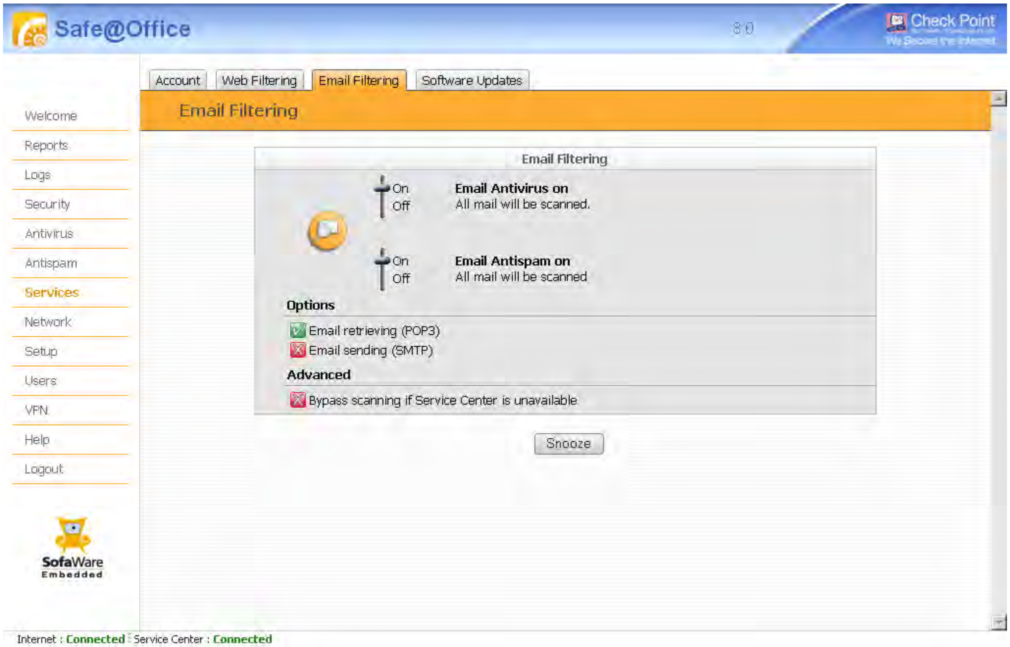
Enabling/Disabling Email Filtering

500

To enable/disable Email Filtering

1. Click **Services** in the main menu, and click the **Email Filtering** tab.

   The **Email Filtering** page appears.



Email Filtering

Email Filtering

On / Off — **Email Antivirus on**
All mail will be scanned.

On / Off — **Email Antispam on**
All mail will be scanned

Options

☑ Email retrieving (POP3)
☒ Email sending (SMTP)

Advanced

☒ Bypass scanning if Service Center is unavailable

Internet : Connected | Service Center : Connected

2. Next to **Email Antivirus**, drag the **On/Off** lever upwards or downwards.

   Email Antivirus is enabled/disabled.

Selecting Protocols for Scanning

500

If you are locally managed, you can define which protocols should be scanned for viruses and spam:

- Email retrieving (POP3). If enabled, all incoming email in the POP3 protocol will be scanned.
- Email sending (SMTP). If enabled, all outgoing email will be scanned.

Protocols marked with ☑ will be scanned, while those marked with ☒ will not.

Note: If the Safe@Office appliance is remotely managed, contact your Service Center administrator to change these settings.

To enable virus and spam scanning for a protocol

1. Click Services in the main menu, and click the Email Filtering tab.

   The Email Filtering page appears.

2. In the Options area, click ☑ or ☒ next to the desired protocol.

Configuring Email Filtering Advanced Settings

500

Note: If the Safe@Office appliance is remotely managed, contact your Service Center administrator to change these settings.

To configure Email Filtering advanced settings

1. Click **Services** in the main menu, and click the **Email Filtering** tab.

   The **Email Filtering** page appears.

2. Next to the **Bypass scanning if Service Center is unavailable** option, specify how the gateway should handle Email Filtering when the service is enabled and the Service Center is unavailable, by doing do one of the following:

   - To temporarily block all email traffic, click ☒.

     This ensures constant protection from spam and viruses.

     The button changes to ☑.

   - To temporarily allow all email traffic, click ☑.

     This ensures continuous access to email; however, it does not protect against viruses and spam, so use this option cautiously.

     The button changes to ☒.

   When the Service Center is available again, the gateway will enforce the configured Email Filtering policy.

Temporarily Disabling Email Filtering

500

If you are having problems sending or receiving email you can temporarily disable the Email Filtering services.

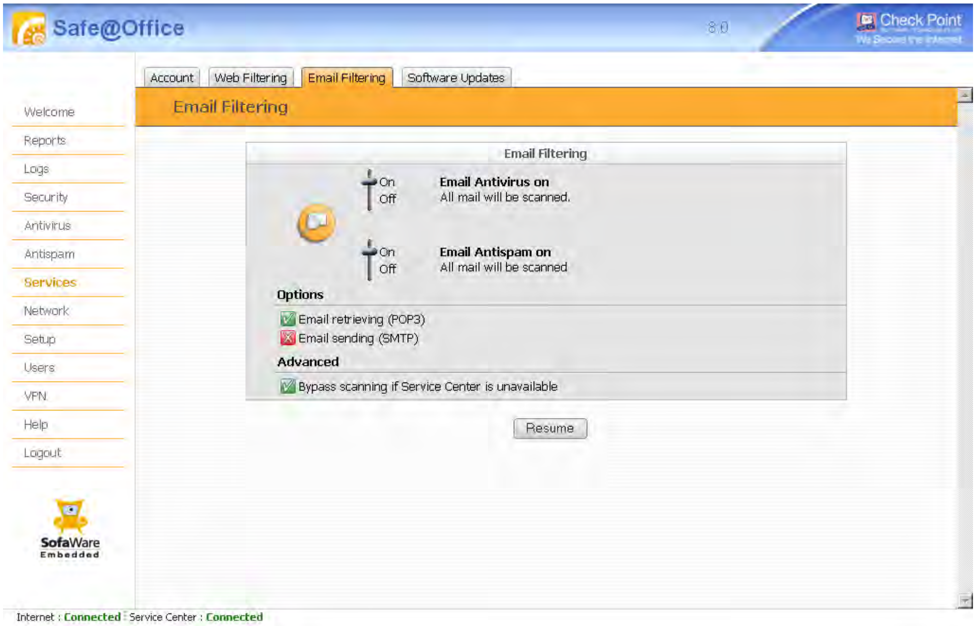
To temporarily disable Email Filtering

1. Click **Services** in the main menu, and click the **Email Filtering** tab.

   The **Email Filtering** page appears.

2. Click **Snooze**.

   - Email Antivirus and Email Antispam are temporarily disabled for all internal network computers.
   - The **Snooze** button changes to **Resume**.



Email Filtering

Email Filtering

Email Antivirus on
All mail will be scanned.

Email Antispam on
All mail will be scanned

Options

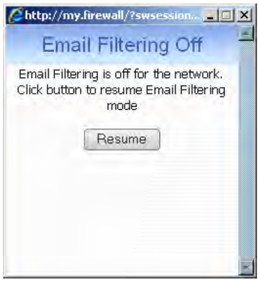
☑ Email retrieving (POP3)
☒ Email sending (SMTP)

Advanced

☑ Bypass scanning if Service Center is unavailable

Internet : Connected Service Center : Connected

- The **Email Filtering Off** popup window opens.



http://my.firewall/?swsession...

Email Filtering Off

Email Filtering is off for the network. Click button to resume Email Filtering mode

3. To re-enable Email Antivirus and Email Antispam, click **Resume**, either in the popup window, or on the **Email Filtering** page.

- The services are re-enabled for all internal network computers.
- If you clicked **Resume** in the **Email Filtering** page, the button changes to **Snooze**.
- If you clicked **Resume** in the **Email Filtering Off** popup window, the popup window closes.

Chapter 16

Using Web Content Filtering

This chapter explains how to use Web content filtering.

This chapter includes the following topics:

Overview

You can allow or block users from accessing Web content, by configuring Web rules and/or the Web Filtering service. The following table describes the main differences between Web rules and the Web Filtering service:

Table 115: Comparison of Web Content Filtering Methods

	Web Rules	Web Filtering
Filtering Action	Web rules allow and block specific URLs.	The Web Filtering service is category based; that is, it filters Web sites based on the category to which they belong.
Point of Enforcement	HTTP requests are analyzed in the gateway, by comparing each request against a list of rules.	HTTP requests are analyzed in the gateway, by extracting each request's URL and then sending the URL to the Service Center, to determine to which categories the URL belongs. The request is then allowed or denied according to the configured list of allowed categories.

	Web Rules	Web Filtering
Subscription and Connection Requirement	Web rules are included with the Safe@Office appliance and do not require a Service Center subscription or connection.	The Web Filtering service is subscription-based and requires a connection to the Service Center.

You can use either Web content filtering solution or both in conjunction. When a user attempts to access a Web site, the Safe@Office appliance first evaluates the Web rules. If the site is not blocked or allowed by the Web rules, the Web Filtering service is then consulted.

Regardless of which method is used, if a user attempts to access a blocked page, the Access Denied page appears. For information on customizing this page, see ***Customizing the Access Denied Page*** on page 543.

If desired, you can permit specific users to override Web content filtering, by granting them Web Filtering Override permissions. Such users will be able to view Web pages without restriction, after they have provided their username password via the Access Denied page. For information on granting Web Filtering Override permissions, see ***Adding and Editing Users*** on page 643.

In addition, you can choose to exclude specific network objects from Web content filtering enforcement. Users connecting from these network objects will be able to view Web pages without restriction, regardless of whether they have Web Filtering Override permissions. For information on configuring network objects, see ***Using Network Objects*** on page 185.

Using Web Rules

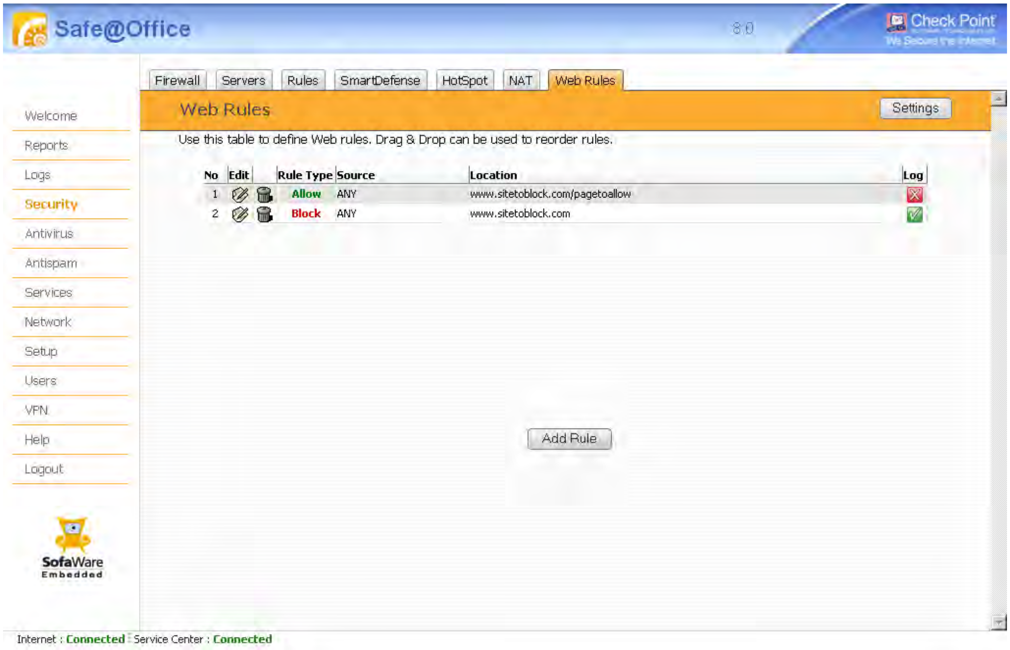
500

You can block or allow access to specific Web pages, by defining Web rules.

Note: Web rules affect outgoing traffic only and cannot be used to allow or limit access from the Internet to internal Web servers.

The Safe@Office appliance processes Web rules in the order they appear in the **Web Rules** table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the **Web Rules** table.

For example, if you want to block all the pages of a particular Web site, except a specific page, you can create a rule blocking access to all of the Web site's pages and move the rule down in the **Web Rules** table. Then create a rule allowing access to the desired page and move this rule to a higher location in the **Web Rules** table than the first rule. In the figure below, the general rule is rule number 2, and the exception is rule number 1.



Web Rules

Use this table to define Web rules. Drag & Drop can be used to reorder rules.

No	Edit	Rule Type	Source	Location	Log
1		Allow	ANY	www.sitetoblock.com/pagetoallow	☒
2		Block	ANY	www.sitetoblock.com	☑

Internet : Connected Service Center : Connected

The Safe@Office appliance will process rule 1 first, allowing access to the desired page, and only then it will process rule 2, blocking access to the rest of the site.

The following rule types exist:

Table 116: Web Rule Types

Rule	Description
Allow	This rule type enables you to specify that a specific Web page should be allowed.
Block	This rule type enables you to specify that a specific Web page should be blocked.

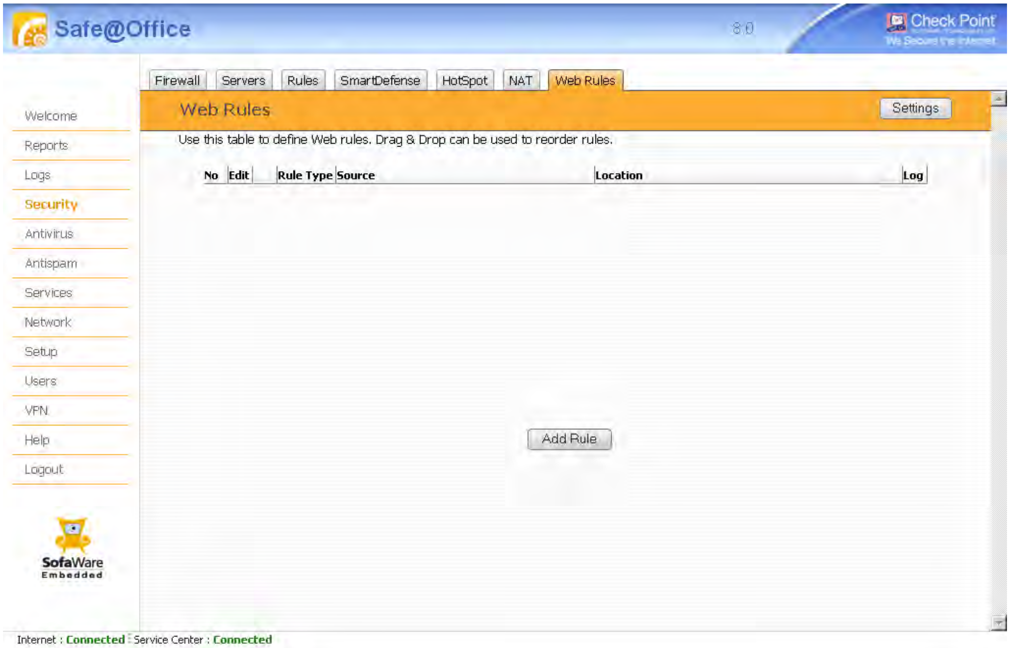
Adding and Editing Web Rules

500

To add or edit a Web rule

1. Click Security in the main menu, and click the Web Rules tab.

The **Web Rules** page appears.



Web Rules

Use this table to define Web rules. Drag & Drop can be used to reorder rules.

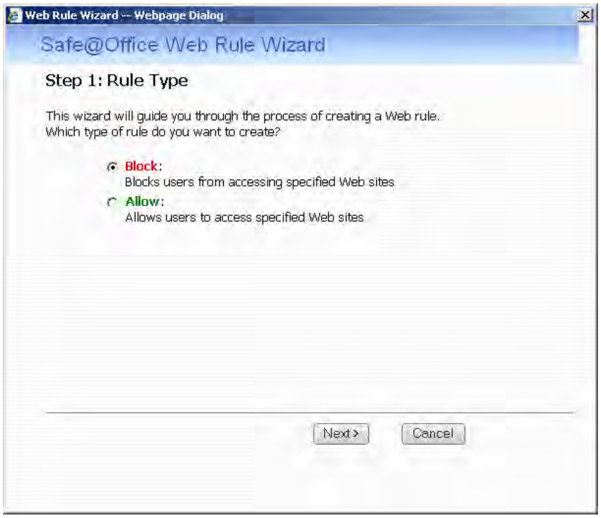
No	Edit	Rule Type	Source	Location	Log

Internet : Connected | Service Center : Connected

2. Do one of the following:

- To add a new rule, click **Add Rule**.
- To edit an existing rule, click ✎ next to the desired rule.

The **Safe@Office Web Rule Wizard** opens, with the **Step 1: Rule Type** dialog box displayed.



Web Rule Wizard -- Webpage Dialog

Safe@Office Web Rule Wizard

Step 1: Rule Type

This wizard will guide you through the process of creating a Web rule.
Which type of rule do you want to create?

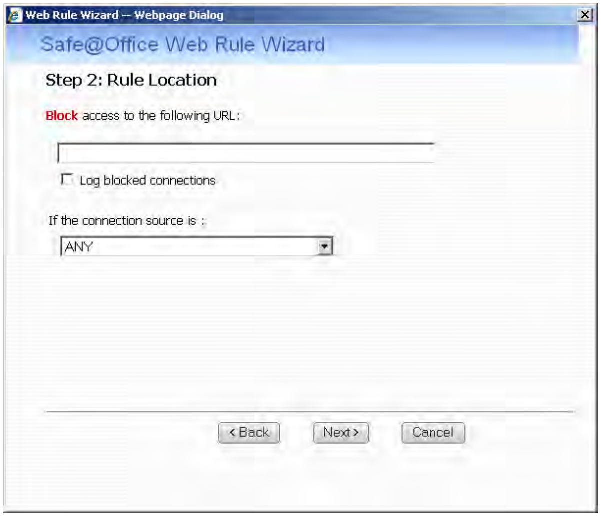
● Block:
Blocks users from accessing specified Web sites

○ Allow:
Allows users to access specified Web sites

3. Select the type of rule you want to create.
4. Click **Next**.

   The **Step 2: Rule Location** dialog box appears.

   The example below shows a Block rule.



Web Rule Wizard -- Webpage Dialog

Safe@Office Web Rule Wizard

Step 2: Rule Location

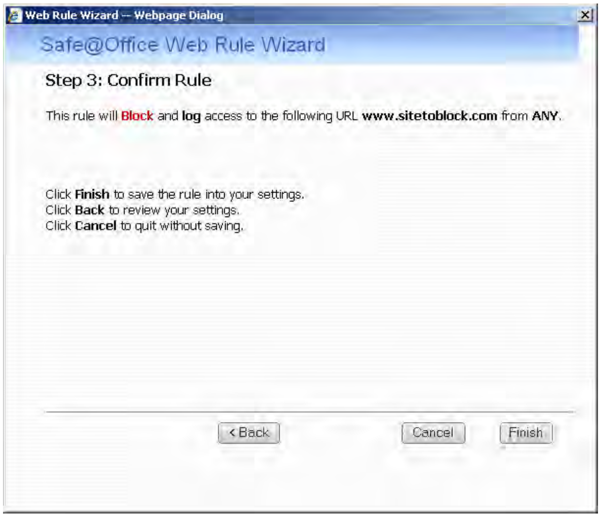
Block access to the following URL:

□ Log blocked connections

If the connection source is :
ANY

5. Complete the fields using the relevant information in the following table.
6. Click **Next**.

   The **Step 3: Confirm Rule** dialog box appears.



Web Rule Wizard -- Webpage Dialog

Safe@Office Web Rule Wizard

Step 3: Confirm Rule

This rule will **Block** and **log** access to the following URL **www.sitetoblock.com** from **ANY**.

Click **Finish** to save the rule into your settings.
Click **Back** to review your settings.
Click **Cancel** to quit without saving.

7. Click **Finish**.

   The new rule appears in the **Web Rules** page.

Table 117: Web Rules Fields

In this field...	Do this...
Block/Allow access to the following URL	Type the URL or IP address to which the rule should apply. Wildcards (*) are supported. For example, to block all URLs that start with "http://www.casino-", set this field's value to: `http://www.casino-*` **Note**: If you block a Web site based on its domain name (http://<domain_name>), the Web site is not automatically blocked when surfing to the Web server's IP address (http://<IP_address>). Likewise, if you block a Web site based on its IP address, the Web site is not automatically blocked when surfing to the domain name. To prevent access to both the domain name and the IP address, you must block both.
Log allowed connections / Log blocked connections	Select this option to log the specified blocked or allowed connections. By default, allowed Web pages are not logged, and blocked Web pages are logged.
If the connection source is	Select the source of the connections you want to allow/block. This list includes network objects. To specify an IP address, select **Specified IP** and type the desired IP address in the field provided. To specify an IP address range, select **Specified Range** and type the desired IP address range in the fields provided.

Reordering Web Rules

500

To reorder Web rules

1. Click **Security** in the main menu, and click the **Web Rules** tab.

   The **Web Rules** page appears.

2. For each rule you want to move, click on the rule and drag it to the desired location in the table.

Enabling/Disabling Web Rule Logging

500

You can enable or disable logging for a Web rule, by using the information in ***Adding and Editing Web Rules*** on page 530, or by using the following shortcut.

To enable/disable logging for a Web rule

1. Click **Security** in the main menu, and click the **Web Rules** tab.

   The **Web Rules** page appears.

2. Next to the desired rule, in the **Log** column, do one of the following:

   - To enable logging, click ☒.

     The button changes to ☑ and logging is enabled for the rule.

   - To disable logging, click ☑.

     The button changes to ☒ and logging is disabled for the rule.

Viewing and Deleting Web Rules

500

To view or delete an existing Web rule

1. Click Security in the main menu, and click the Web Rules tab.

   The Web Rules page appears with a list of existing Web rules.

2. To resize a column, drag the relevant column divider right or left.

3. To delete a rule, do the following.

   a. In the desired rule's row, click 🗑.

      A confirmation message appears.

   b. Click OK.

      The rule is deleted.

Using Web Filtering

500

When the Web Filtering service is enabled, access to Web content is restricted according to the categories specified in the Allow Categories area of the Web Filtering page.

Note: The Web Filtering service is only available if you are connected to a Service Center and subscribed to this service. For information on using subscription services, see ***Using Subscription Services*** on page 551.

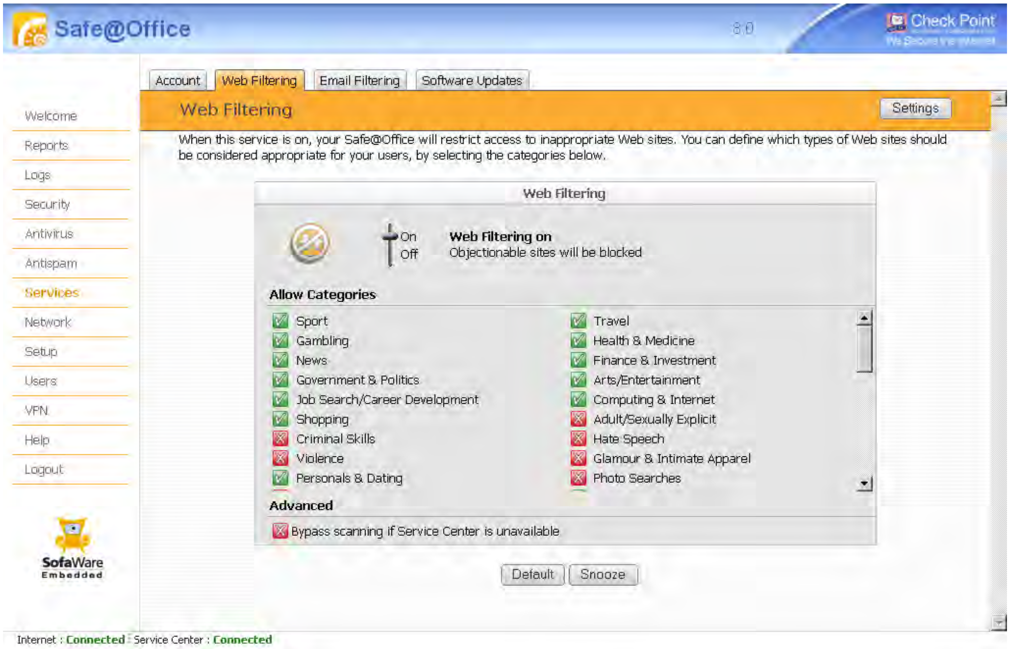
Enabling/Disabling Web Filtering

500

To enable/disable Web Filtering

1. Click Services in the main menu, and click the Web Filtering tab.

The **Web Filtering** page appears.



Web Filtering

When this service is on, your Safe@Office will restrict access to inappropriate Web sites. You can define which types of Web sites should be considered appropriate for your users, by selecting the categories below.

Web Filtering

Web Filtering on
Objectionable sites will be blocked

Allow Categories

☑ Sport	☑ Travel
☑ Gambling	☑ Health & Medicine
☑ News	☑ Finance & Investment
☑ Government & Politics	☑ Arts/Entertainment
☑ Job Search/Career Development	☑ Computing & Internet
☑ Shopping	☒ Adult/Sexually Explicit
☒ Criminal Skills	☒ Hate Speech
☒ Violence	☒ Glamour & Intimate Apparel
☑ Personals & Dating	☒ Photo Searches

Advanced

☒ Bypass scanning if Service Center is unavailable

Internet : Connected | Service Center : Connected

2. Drag the **On/Off** lever upwards or downwards.

Web Filtering is enabled/disabled.

Selecting Categories for Blocking

500

You can define which types of Web sites should be considered appropriate for your family or office members, by selecting the categories. Categories marked with ☑ will remain visible, while categories marked with ☒ will be blocked and will require the administrator password for viewing.

Note: If the Safe@Office appliance is remotely managed, contact your Service Center administrator to change these settings.

Note: The list of supported categories may vary, depending on the Service Center to which the Safe@Office appliance is connected.

To allow/block a category

1. Click **Services** in the main menu, and click the **Web Filtering** tab.

   The **Web Filtering** page appears.

2. In the **Allow Categories** area, use the scroll bar to scroll through all of the categories.

3. Click ☑ or ☒ next to the desired category.

Configuring Web Filtering Advanced Settings

500

Note: If the Safe@Office appliance is remotely managed, contact your Service Center administrator to change these settings.

To configure Web Filtering advanced settings

1. Click **Services** in the main menu, and click the **Web Filtering** tab.

   The **Web Filtering** page appears.

2. Next to the **Bypass scanning if Service Center is unavailable** option, specify how the gateway should handle Web Filtering when the service is enabled and the Service Center is unavailable, by doing do one of the following:

   - To temporarily block all connections to the Internet, click ☒.

     This ensures that users will not gain access to undesirable Web sites, even when the Service Center is unavailable.

     The button changes to ☑.

   - To temporarily allow all connections to the Internet, click ☑.

     This ensures continuous access to the Internet.

     The button changes to ☒.

   When the Service Center is available again, the gateway will enforce the configured Web Filtering policy.

Temporarily Disabling Web Filtering

500

If desired, you can temporarily disable the Web Filtering service.

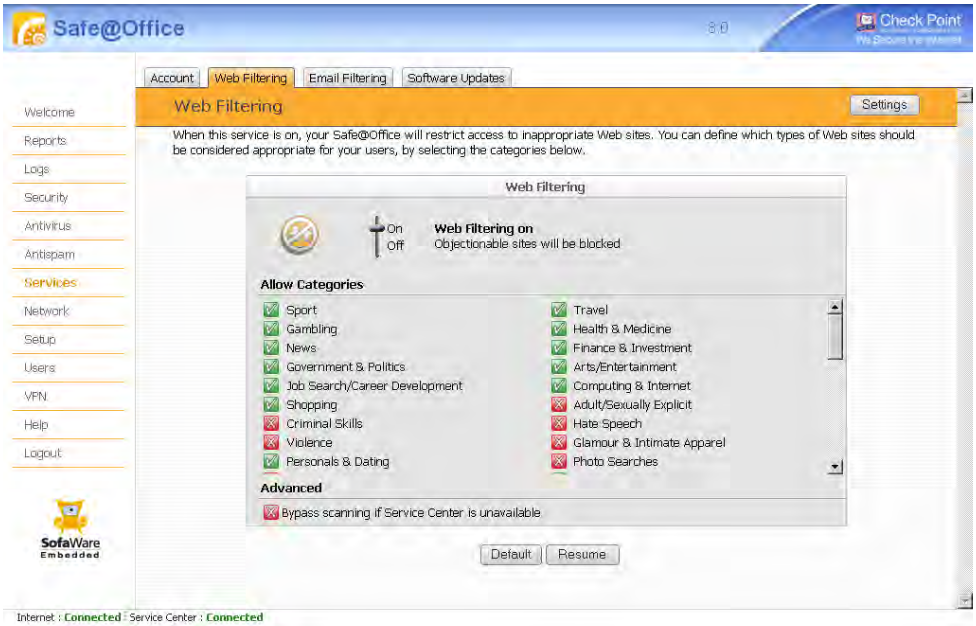
To temporarily disable Web Filtering

1. Click **Services** in the main menu, and click the **Web Filtering** tab.

   The **Web Filtering** page appears.

2. Click **Snooze**.

   - Web Filtering is temporarily disabled for all internal network computers.
   - The **Snooze** button changes to **Resume**.



Web Filtering

When this service is on, your Safe@Office will restrict access to inappropriate Web sites. You can define which types of Web sites should be considered appropriate for your users, by selecting the categories below.

Web Filtering

Web Filtering on
Objectionable sites will be blocked

Allow Categories

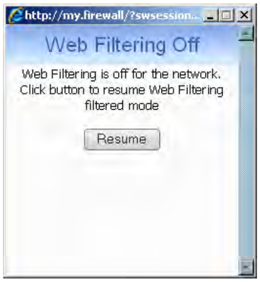
☑ Sport
☑ Gambling
☑ News
☑ Government & Politics
☑ Job Search/Career Development
☑ Shopping
☒ Criminal Skills
☒ Violence
☑ Personals & Dating
☑ Travel
☑ Health & Medicine
☑ Finance & Investment
☑ Arts/Entertainment
☑ Computing & Internet
☒ Adult/Sexually Explicit
☒ Hate Speech
☒ Glamour & Intimate Apparel
☒ Photo Searches

Advanced

☒ Bypass scanning if Service Center is unavailable

Internet : Connected Service Center : Connected

- The **Web Filtering Off** popup window opens.



Web Filtering Off

Web Filtering is off for the network. Click button to resume Web Filtering filtered mode

3. To re-enable the service, click **Resume**, either in the popup window, or on the **Web Filtering** page.

   - The service is re-enabled for all internal network computers.
   - If you clicked **Resume** in the **Web Filtering** page, the button changes to **Snooze**.
   - If you clicked **Resume** in the **Web Filtering Off** popup window, the popup window closes.

Resetting Web Filtering Categories to Defaults

500

If desired, you can reset the Web Filtering categories to their default settings.

To restore Web Filtering defaults

1. Click **Services** in the main menu, and click the **Web Filtering** tab.

   The **Web Filtering** page appears.

2. Click **Defaults**

   A confirmation message appears.

3. Click **OK**.

Customizing the Access Denied Page

Power Pack

The **Access Denied** page appears when a user attempts to access a page that is blocked either by a Web rule or by the Web Filtering service. You can customize this page using the following procedure.

To customize the Access Denied page

1. Do one of the following:

   - Click **Security** in the main menu, and click the **Web Rules** tab.

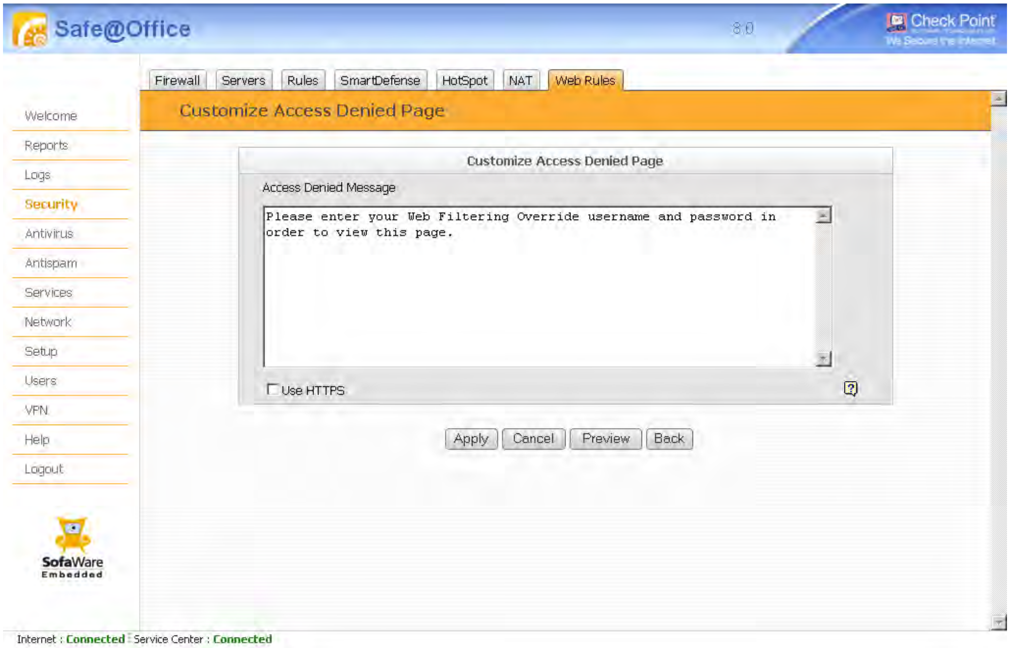
     The **Web Rules** page appears.

   - Click **Services** in the main menu, and click the **Web Filtering** tab.

     The **Web Filtering** page appears.

2. Click **Settings**.

The **Customize Access Denied Page** page appears. In the following example, this page was accessed via the **Web Rules** page.



Customize Access Denied Page

Customize Access Denied Page

Access Denied Message

```
Please enter your Web Filtering Override username and password in
order to view this page.
```

□ Use HTTPS

Internet : Connected Service Center : Connected

3. In the text box, type the message that should appear when a user attempts to access a blocked Web page.

   You can use HTML tags as needed.

4. To display the Access Denied page using HTTPS, select the **Use HTTPS** check box.

5. To preview the Access Denied page, click **Preview**.

   A browser window opens displaying the Access Denied page.

6. Click **Apply**.

   Your changes are saved.

Chapter 17

Updating the Firmware

This chapter explains how to update the Safe@Office appliance's firmware.

This chapter includes the following topics:

Overview

You can update your Safe@Office appliance with new product features and protection against new security threats. To do so, you must update your appliance's firmware, by using one of the following methods:

- Software Updates. This subscription service allows checking for new security and software updates, either automatically or manually. Detected updates are downloaded and installed without user intervention.
- Manual updates. If you are not subscribed to the Software Updates service, you must update the firmware manually.

Using Software Updates

500

Note: Software Updates are only available if you are connected to a Service Center and subscribed to this service. For information on using subscription services, see ***Using Subscription Services*** on page 551.

Checking for Software Updates when Remotely Managed

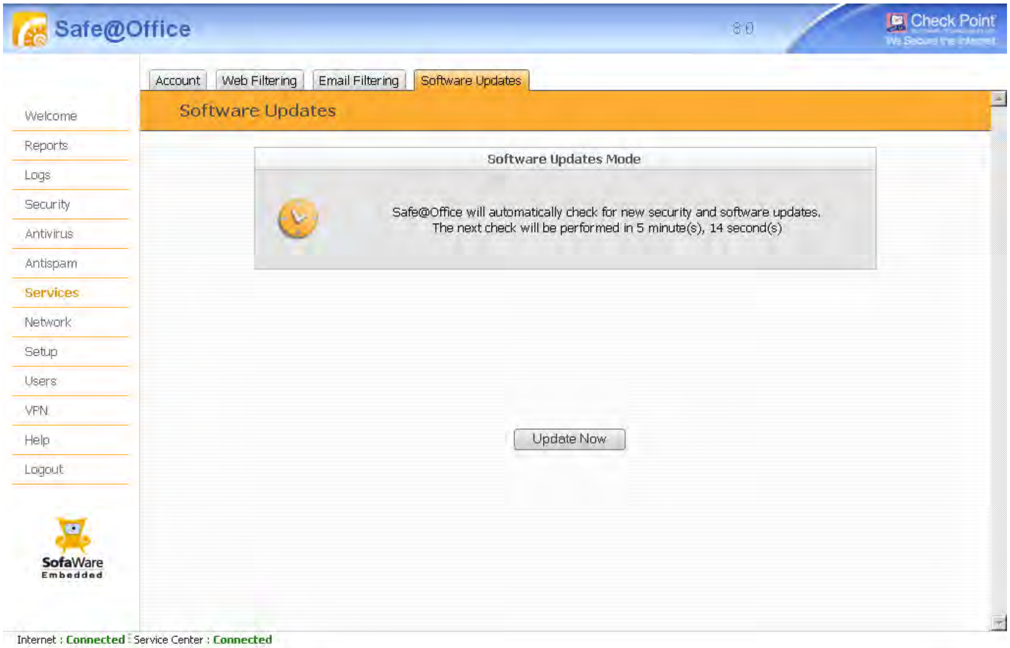
500

If your Safe@Office appliance is remotely managed, it automatically checks for software updates and installs them without user intervention. However, you can still check for updates manually, if needed.

To manually check for security and software updates

1. Click Services in the main menu, and click the Software Updates tab.

The **Software Updates** page appears.



Software Updates

Software Updates Mode

Safe@Office will automatically check for new security and software updates.
The next check will be performed in 5 minute(s), 14 second(s)

Internet : Connected | Service Center : Connected

2. Click **Update Now**.

   The system checks for new updates and installs them.

Checking for Software Updates when Locally Managed

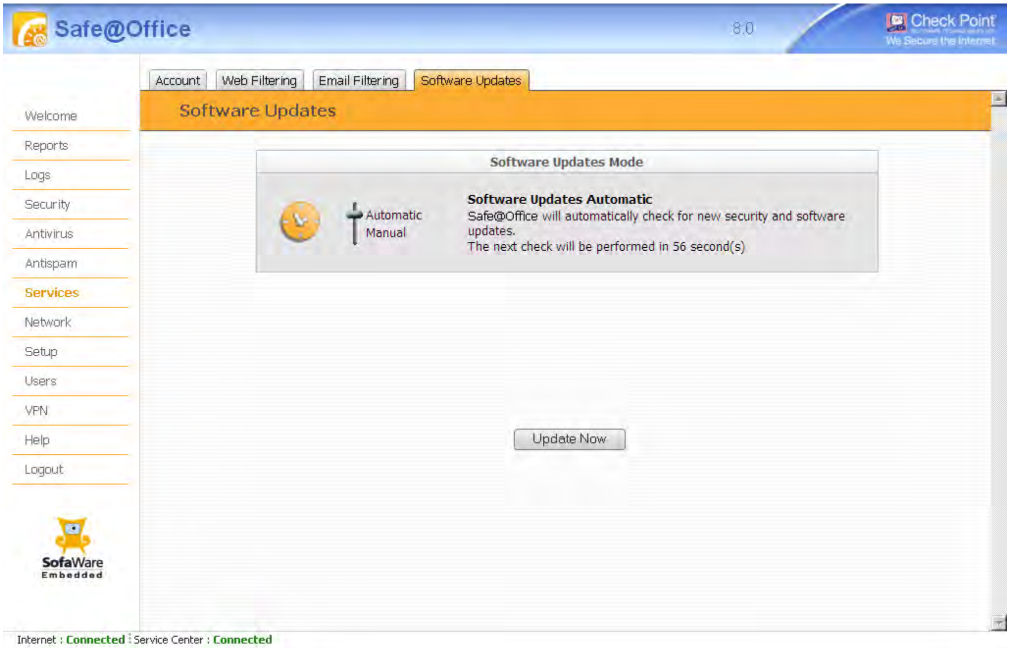
500

If your Safe@Office appliance is locally managed, you can set it to automatically check for software updates, or you can set it so that software updates must be checked for manually.

To configure software updates when locally managed

1. Click **Services** in the main menu, and click the **Software Updates** tab.

   The **Software Updates** page appears.



Software Updates

Software Updates Mode

Automatic
Manual

Software Updates Automatic
Safe@Office will automatically check for new security and software updates.
The next check will be performed in 56 second(s)

Internet : Connected | Service Center : Connected

2. To set the Safe@Office appliance to automatically check for and install new software updates, drag the **Automatic/Manual** lever upwards.

   The Safe@Office appliance checks for new updates and installs them according to its schedule.

Note: When the Software Updates service is set to Automatic, you can still manually check for updates.

3. To set the Safe@Office appliance so that software updates must be checked for manually, drag the Automatic/Manual lever downwards.

   The Safe@Office appliance does not check for software updates automatically.

4. To manually check for software updates, click Update Now.

   The system checks for new updates and installs them.

Updating the Firmware Manually

500

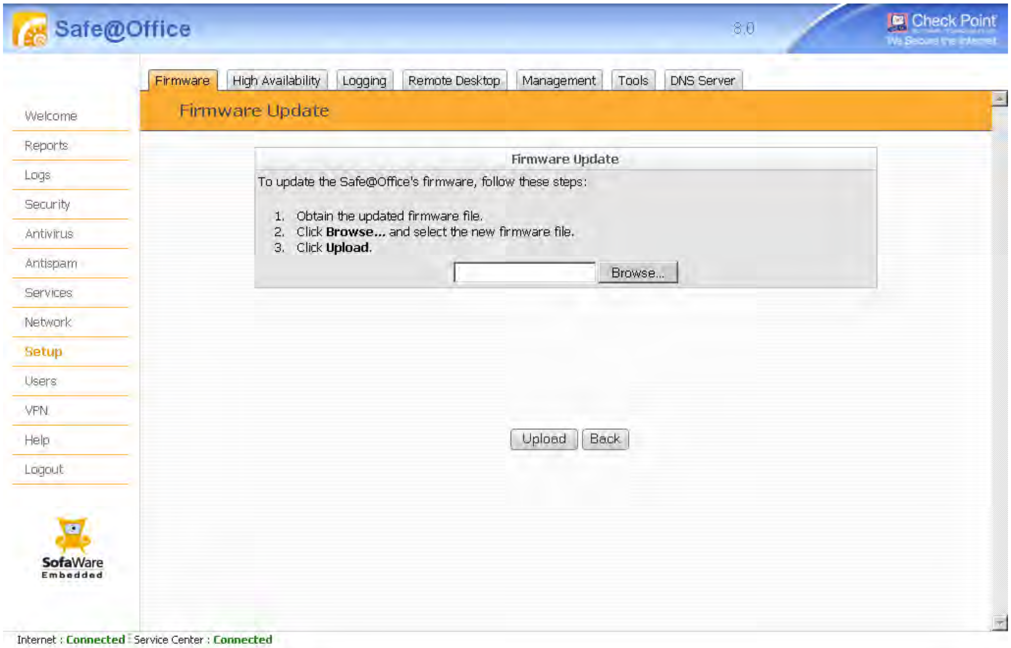
To update your Safe@Office firmware manually

1. Click Setup in the main menu, and click the Firmware tab.

   The Firmware page appears.

2. Click Firmware Update.

The **Firmware Update** page appears.



Firmware Update

Firmware Update

To update the Safe@Office's firmware, follow these steps:

1. Obtain the updated firmware file.
2. Click **Browse...** and select the new firmware file.
3. Click **Upload**.

Internet : Connected Service Center : Connected

3. Click **Browse**.

   A browse window appears.

4. Select the image file and click **Open**.

   The **Firmware Update** page reappears. The path to the firmware update image file appears in the **Browse** text box.

5. Click **Upload**.

   Your Safe@Office appliance firmware is updated.

   Updating may take a few minutes. Do not power off the appliance.

   At the end of the process the Safe@Office appliance restarts automatically.

Chapter 18

Using Subscription Services

This chapter explains how to connect your Safe@Office appliance to a Service Center and start subscription services.

Note: Check with your reseller regarding availability of subscription services, or surf to www.sofaware.com/servicecenters to locate a Service Center in your area.

This chapter includes the following topics:

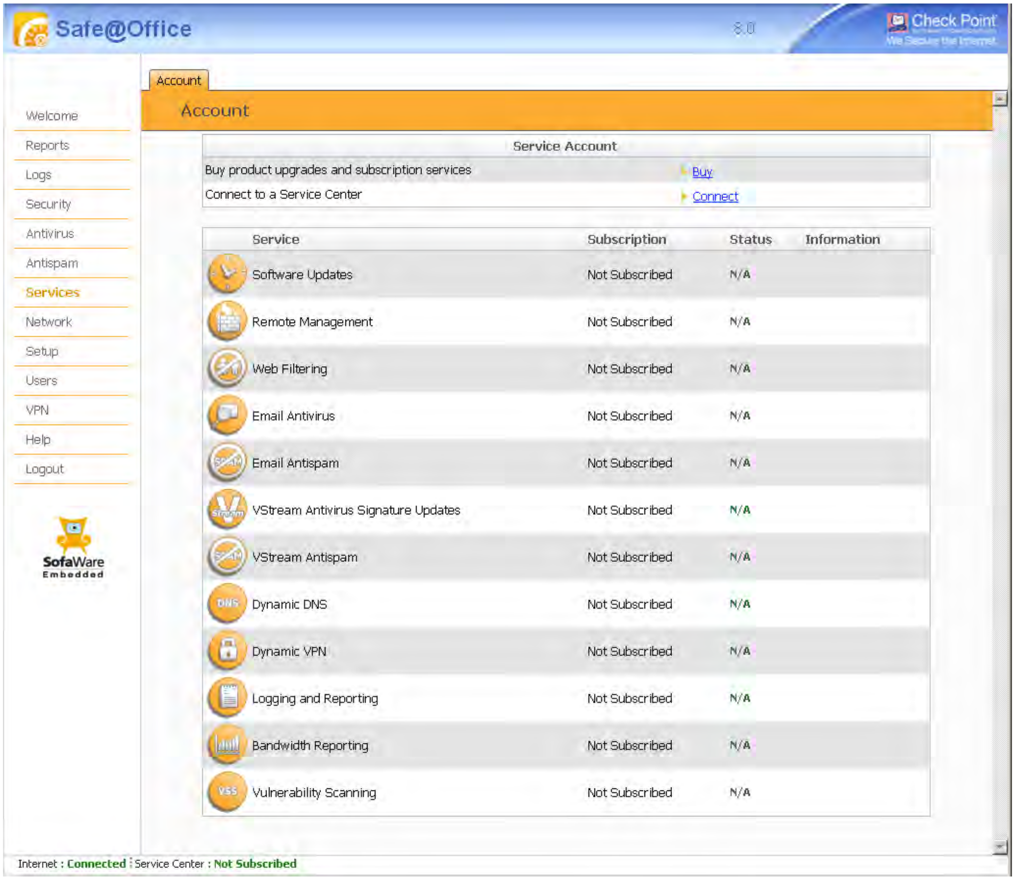
Connecting to a Service Center

500

To connect to a Service Center

1. Click **Services** in the main menu, and click the **Account** tab.

The **Account** page appears.



Account

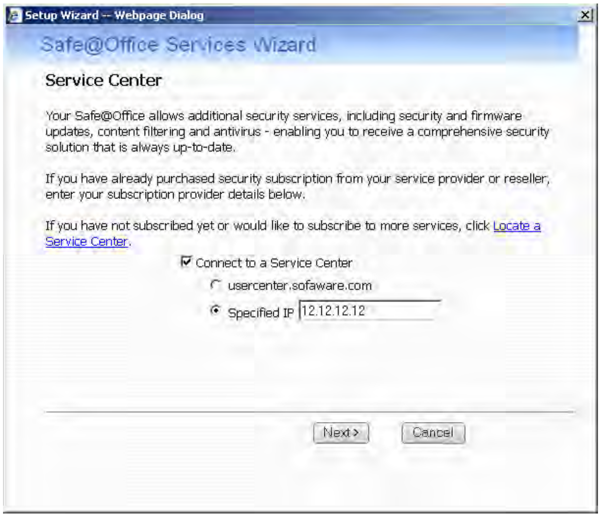
Service Account	
Buy product upgrades and subscription services	Buy
Connect to a Service Center	Connect

Service	Subscription	Status	Information
Software Updates	Not Subscribed	N/A	
Remote Management	Not Subscribed	N/A	
Web Filtering	Not Subscribed	N/A	
Email Antivirus	Not Subscribed	N/A	
Email Antispam	Not Subscribed	N/A	
VStream Antivirus Signature Updates	Not Subscribed	N/A	
VStream Antispam	Not Subscribed	N/A	
Dynamic DNS	Not Subscribed	N/A	
Dynamic VPN	Not Subscribed	N/A	
Logging and Reporting	Not Subscribed	N/A	
Bandwidth Reporting	Not Subscribed	N/A	
Vulnerability Scanning	Not Subscribed	N/A	

Internet : Connected | Service Center : Not Subscribed

2. In the **Service Account** area, click **Connect**.

The **Safe@Office Services Wizard** opens, with the **Service Center** dialog box displayed.



Service Center

Your Safe@Office allows additional security services, including security and firmware updates, content filtering and antivirus - enabling you to receive a comprehensive security solution that is always up-to-date.

If you have already purchased security subscription from your service provider or reseller, enter your subscription provider details below.

If you have not subscribed yet or would like to subscribe to more services, click Locate a Service Center.

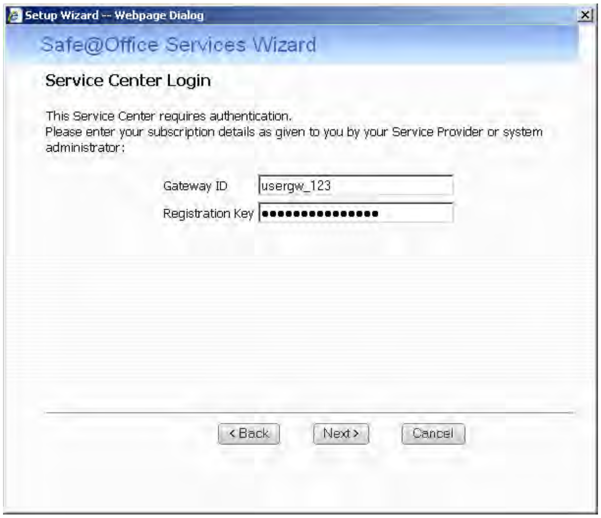
☑ Connect to a Service Center

○ usercenter.sofaware.com

● Specified IP 12.12.12.12

3. Make sure the **Connect to a Service Center** check box is selected.
4. Do one of the following:
   - To connect to the SofaWare Service Center, choose **usercenter.sofaware.com**.
   - To specify a Service Center, choose **Specified IP** and then in the **Specified IP** field, enter the desired Service Center's IP address, as given to you by your system administrator.
5. Click **Next**.
   - The **Connecting** screen appears.

- If the Service Center requires authentication, the **Service Center Login** dialog box appears.



Service Center Login

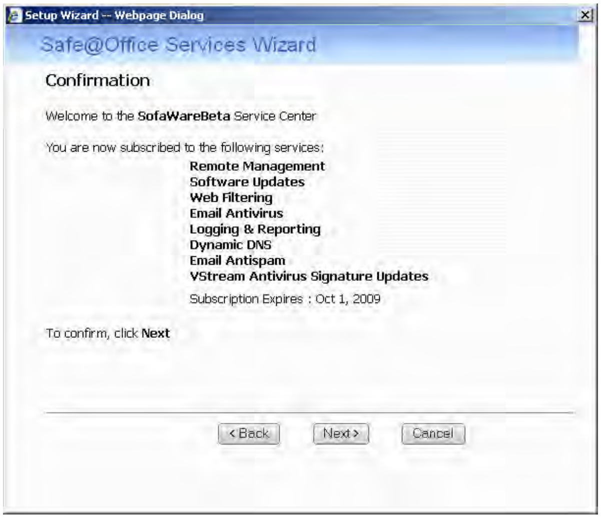
This Service Center requires authentication.
Please enter your subscription details as given to you by your Service Provider or system administrator:

Gateway ID: usergw_123
Registration Key: ●●●●●●●●●●●●●●●●

Enter your gateway ID and registration key in the appropriate fields, as given to you by your service provider, then click **Next**.

- The **Connecting** screen appears.

- The **Confirmation** dialog box appears with a list of services to which you are subscribed.



Confirmation

Welcome to the **SofaWareBeta** Service Center

You are now subscribed to the following services:

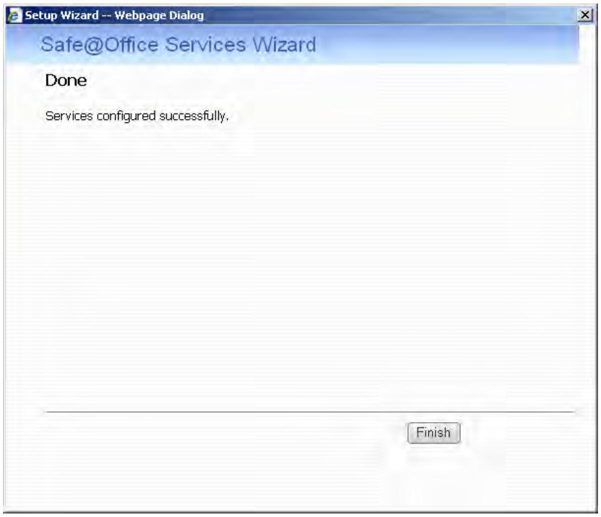
Remote Management
Software Updates
Web Filtering
Email Antivirus
Logging & Reporting
Dynamic DNS
Email Antispam
VStream Antivirus Signature Updates

Subscription Expires : Oct 1, 2009

To confirm, click **Next**

6. Click **Next.**

   The **Done** screen appears with a success message.



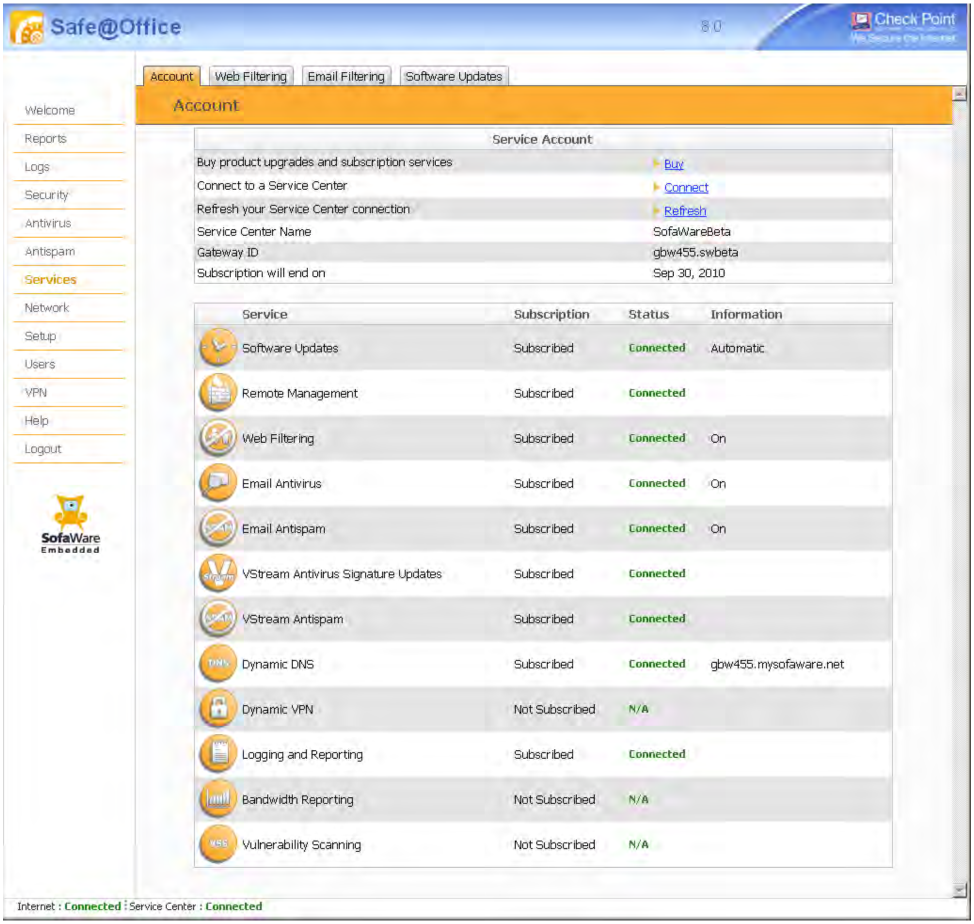
Done

Services configured successfully.

7. Click **Finish.**

   The following things happen:

- If a new firmware is available, the Safe@Office appliance may start downloading it. This may take several minutes. Once the download is complete, the Safe@Office appliance restarts using the new firmware.
- The Welcome page appears.
- The services to which you are subscribed are now available on your Safe@Office appliance and listed as such on the Account page. See ***Viewing Services Information*** on page 557 for further information.



Account

Service Account	
Buy product upgrades and subscription services	Buy
Connect to a Service Center	Connect
Refresh your Service Center connection	Refresh
Service Center Name	SofaWareBeta
Gateway ID	gbw455.swbeta
Subscription will end on	Sep 30, 2010

Service	Subscription	Status	Information
Software Updates	Subscribed	Connected	Automatic
Remote Management	Subscribed	Connected	
Web Filtering	Subscribed	Connected	On
Email Antivirus	Subscribed	Connected	On
Email Antispam	Subscribed	Connected	On
VStream Antivirus Signature Updates	Subscribed	Connected	
VStream Antispam	Subscribed	Connected	
Dynamic DNS	Subscribed	Connected	gbw455.mysofaware.net
Dynamic VPN	Not Subscribed	N/A	
Logging and Reporting	Subscribed	Connected	
Bandwidth Reporting	Not Subscribed	N/A	
Vulnerability Scanning	Not Subscribed	N/A	

Internet : Connected ⁞ Service Center : Connected

- The Services submenu includes the services to which you are subscribed.

Viewing Services Information

500

The Account page displays the following information about your subscription.

Table 118: Account Page Fields

This field...	Displays...
Service Center Name	The name of the Service Center to which you are connected (if known).
Gateway ID	Your gateway ID.
Subscription will end on	The date on which your subscription to services will end.
Service	The services available in your service plan.
Subscription	The status of your subscription to each service: • Subscribed • Not Subscribed
Status	The status of each service: • Connected. You are connected to the service through the Service Center. • Connecting. Connecting to the Service Center. • N/A. The service is not available.

This field...	Displays...
Information	The mode to which each service is set. If you are subscribed to Dynamic DNS, this field displays your gateway's domain name. For further information, see ***Web Filtering*** on page 537, ***Virus Scanning*** on page 521, and ***Automatic and Manual Updates*** on page 546.

Refreshing Your Service Center Connection

500

This option restarts your Safe@Office appliance’s connection to the Service Center and refreshes your Safe@Office appliance’s service settings.

To refresh your Service Center connection

1. Click Services in the main menu, and click the Account tab.

   The Account page appears.

2. In the Service Account area, click Refresh.

   The Safe@Office appliance reconnects to the Service Center.

   Your service settings are refreshed.

Configuring Your Account

500

This option allows you to access your Service Center's Web site, which may offer additional configuration options for your account. Contact your Service Center for a user ID and password.

To configure your account

1. Click **Services** in the main menu, and click the **Account** tab.

   The **Account** page appears.

2. In the **Service Account** area, click **Configure**.

   Note: If no additional settings are available from your Service Center, this button will not appear.

   Your Service Center's Web site opens.

3. Follow the on-screen instructions.

Disconnecting from Your Service Center

500

If desired, you can disconnect from your Service Center.

To disconnect from your Service Center

1. Click **Services** in the main menu, and click the **Account** tab.

   The **Account** page appears.

2. In the **Service Account** area, click **Connect**.

   The **Safe@Office Services Wizard** opens, with the first **Subscription Services** dialog box displayed.

3. Clear the **Connect to a Service Center** check box.
4. Click **Next.**

   The **Done** screen appears with a success message.
5. Click **Finish.**

   The following things happen:

   - You are disconnected from the Service Center.
   - The services to which you were subscribed are no longer available on your Safe@Office appliance.

Chapter 19

Working With VPNs

This chapter describes how to use your Safe@Office appliance as a Remote Access VPN Client, server, or gateway.

This chapter includes the following topics:

Overview

You can configure your Safe@Office appliance as part of a virtual private network (VPN). A VPN is a private data network consisting of a group of gateways that can securely connect to each other. Each member of the VPN is called a *VPN site*, and a connection between two VPN sites is called a *VPN tunnel*. VPN tunnels encrypt and authenticate all traffic passing through them. Through these tunnels, employees can safely use their company’s network resources when working at home. For example, they can securely read email, use the company’s intranet, or access the company’s database from home.

The are four types of VPN sites:

- SecuRemote Remote Access VPN Server. Makes a network remotely available to authorized users who connect to the Remote Access VPN Server using the Check Point SecuRemote VPN Client (provided for free with your Safe@Office) or another Safe@Office.

- **SecuRemote Internal VPN Server.** SecuRemote can also be used from your internal networks, allowing you to secure your wired or wireless network with strong encryption and authentication.
- **L2TP VPN Server.** Makes a network available to authorized users who connect from the Internet or from your internal networks using an L2TP client such as the Microsoft L2TP IPSec VPN Client.
- **Site-to-Site VPN Gateway.** Can connect with another Site-to-Site VPN Gateway in a permanent, bi-directional relationship.
- **Remote Access VPN Client.** Can connect to a Remote Access VPN Server, but other VPN sites cannot initiate a connection to the Remote Access VPN Client. Defining a Remote Access VPN Client is a hardware alternative to using SecuRemote software.

All Safe@Office models provide full VPN functionality. They can act as a Remote Access VPN Client, a Remote Access VPN Server for multiple users, or a Site-to-Site VPN Gateway.

A virtual private network (VPN) must include at least one Remote Access VPN Server or gateway. The type of VPN sites you include in a VPN depends on the type of VPN you want to create, Site-to-Site or Remote Access.

Note: A locally managed Remote Access VPN Server or gateway must have a static IP address. If you need a Remote Access VPN Server or gateway with a dynamic IP address, you must use SofaWare Security Management Portal (SMP) management.

A SecuRemote/SecureClient or Safe@Office Remote Access VPN Client can have a dynamic IP address, regardless of whether it is locally or remotely managed.

Note: This chapter explains how to define a VPN locally. However, if your appliance is centrally managed by a Service Center, then the Service Center can automatically deploy VPN configuration for your appliance.

Site-to-Site VPNs

A Site-to-Site VPN consists of two or more Site-to-Site VPN Gateways that can communicate with each other in a bi-directional relationship. The connected networks function as a single network. You can use this type of VPN to mesh office branches into one corporate network.

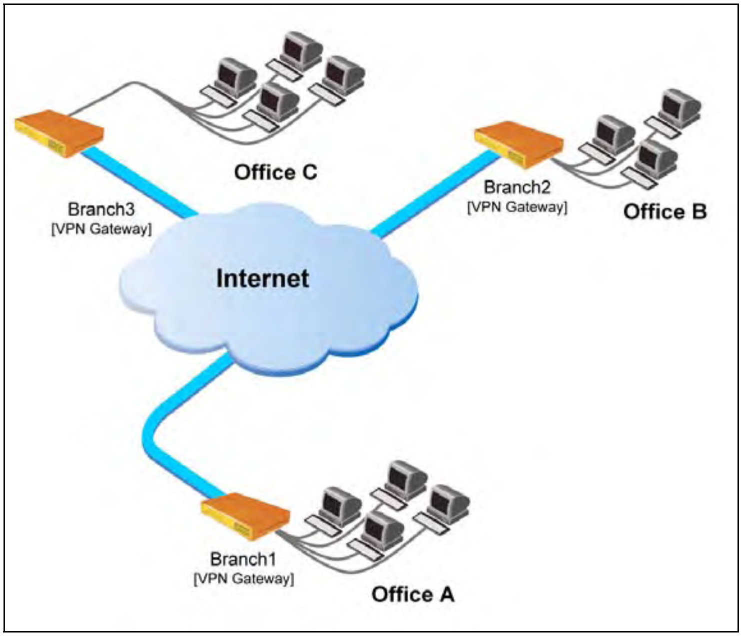


Figure 27: Site-to-Site VPN

To create a Site-to-Site VPN with two VPN sites

1. On the first VPN site's Safe@Office appliance, do the following:

    a. Define the second VPN site as a Site-to-Site VPN Gateway, using the procedure ***Adding and Editing VPN Sites*** on page 581.

    b. Enable a Remote Access VPN Server using the procedure ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 567.

2. On the second VPN site's Safe@Office appliance, do the following:

    a. Define the first VPN site as a Site-to-Site VPN Gateway, using the procedure ***Adding and Editing VPN Sites*** on page 581.

    b. Enable a Remote Access VPN Server using the procedure ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 567.

Note: You can manually configure each VPN site's internal encryption domain via the CLI. For information, refer to the *Embedded NGX CLI Reference Guide*.

Remote Access VPNs

A Remote Access VPN consists of one Remote Access VPN Server or Site-to-Site VPN Gateway, and one or more Remote Access VPN Clients. You can use this type of VPN to make an office network remotely available to authorized users, such as employees working from home, who connect to the office Remote Access VPN Server with their Remote Access VPN Clients.

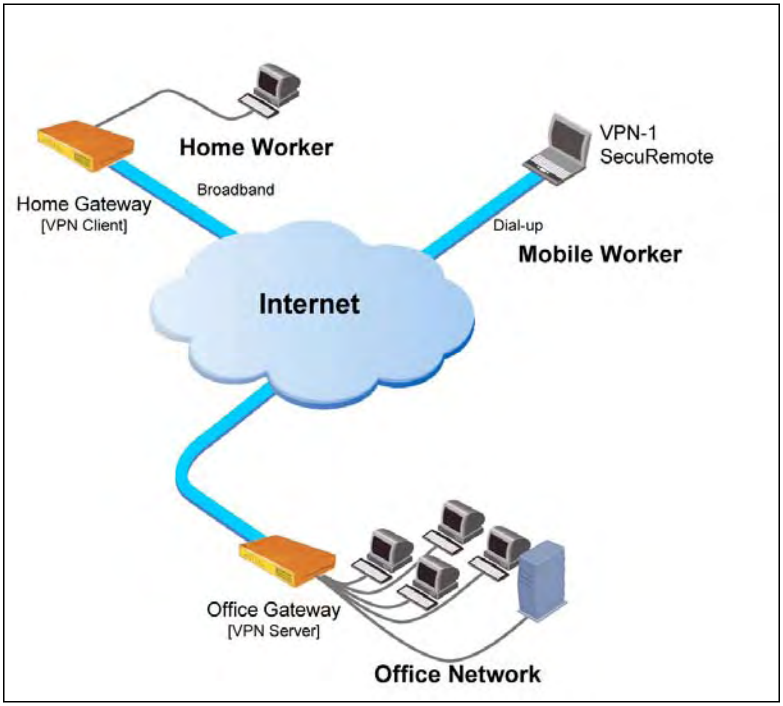


Figure 28: Remote Access VPN

To create a Remote Access VPN with two VPN sites

1. On the remote user VPN site's Safe@Office appliance, add the office Remote Access VPN Server as a Remote Access VPN site.

   See ***Adding and Editing VPN Sites*** on page 581.

   The remote user's Safe@Office appliance will act as a Remote Access VPN Client.

2. On the office VPN site's Safe@Office appliance, enable a Remote Access VPN Server.

   See ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 567.

Internal VPN Server

You can use your Safe@Office appliance as an internal VPN Server, for enhanced wired and wireless security. When an internal VPN Server is enabled, internal network PCs and PDAs with the appropriate software installed can establish a Remote Access VPN session to the gateway. This means that connections from internal network users to the gateway can be encrypted and authenticated.

The benefits of using an internal VPN Server are two-fold:

- Accessibility

  Using SecuRemote/SecureClient or L2TP, you can enjoy a secure connection from anywhere—in your wireless network or on the road—without changing any settings. The standard is completely transparent and allows you to access company resources the same way, whether you are sitting at your desk or anywhere else.

- Security

  Many of today's attacks are increasingly introduced from inside the network. Internal security threats cause outages, downtime, and lost revenue. Wired networks that deal with highly sensitive information—especially networks in public places, such as classrooms—are vulnerable to users trying to hack the internal network.

  Using an internal VPN Server, along with a strict security policy for non-VPN users, can enhance security both for wired networks and for wireless networks, which are particularly vulnerable to security breaches.

For information on setting up your Safe@Office appliance as an internal VPN Server, see ***Configuring the Internal VPN Server*** on page 571.

Setting Up Your Safe@Office Appliance as a VPN Server

500

You can make your network available to authorized users connecting from the Internet or from your internal networks, by setting up your Safe@Office appliance as a VPN Server.

When the SecuRemote Remote Access VPN Server or SecuRemote Internal VPN Server is enabled, users can connect to the server via Check Point SecuRemote/SecureClient or via a Safe@Office appliance in Remote Access VPN mode. When the L2TP (Layer 2 Tunneling Protocol) VPN Server is enabled, users can connect to the server using an L2TP client such as the Microsoft Windows L2TP IPSEC VPN Client. L2TP users are automatically assigned to the OfficeMode network, enabling you to configure special security rules for them.

SecuRemote/SecureClient supports split tunneling, which means that VPN Clients can connect directly to the Internet, while traffic to and from VPN sites passes through the VPN Server. In contrast, the L2TP VPN Client does not support split tunneling, meaning that all Internet traffic to and from a VPN Client passes through the VPN Server and is routed to the Internet.

Enabling the Safe@Office VPN Server for users connecting from your internal networks adds a layer of security to such connections. For example, while you could create a firewall rule allowing a specific user on the DMZ to access the LAN, enabling VPN access for the user means that such connections can be encrypted and authenticated. For more information, see ***Internal VPN Server*** on page 566.

To set up your Safe@Office appliance as a VPN Server

1. Configure the VPN Server in one or more of the following ways:

   - To accept SecuRemote/SecureClient or Safe@Office remote access connections from the Internet.

     See ***Configuring the SecuRemote Remote Access VPN Server*** on page 569.

   - To accept SecuRemote/SecureClient connections from your internal networks.

     See ***Configuring the Internal VPN Server*** on page 571.

   - To accept L2TP remote access connections from the Internet, as well L2TP connections from your internal networks.

     See ***Configuring the L2TP VPN Server*** on page 572.

2. If you configured the SecuRemote Internal VPN Server, install SecuRemote/SecureClient on the desired internal network computers.

   See ***Installing SecuRemote*** on page 573.

3. If you configured the L2TP VPN Server, do the following:

   a. Configure the OfficeMode network.

      See ***Configuring the OfficeMode Network*** on page 172.

      All users connecting via L2TP will be assigned to the OfficeMode network.

   b. Configure L2TP VPN Clients on the desired internal network computers.

      See ***Configuring L2TP VPN Clients*** on page 574.

4. Set up remote VPN access for users.

   See ***Setting Up Remote VPN Access for Users*** on page 650.

Note: Disabling the VPN Server for a specific type of connection (from SecuRemote/SecureClient clients on the Internet, from SecuRemote/SecureClient clients on internal networks, or from L2TP clients) will cause all existing VPN tunnels of that type to disconnect.

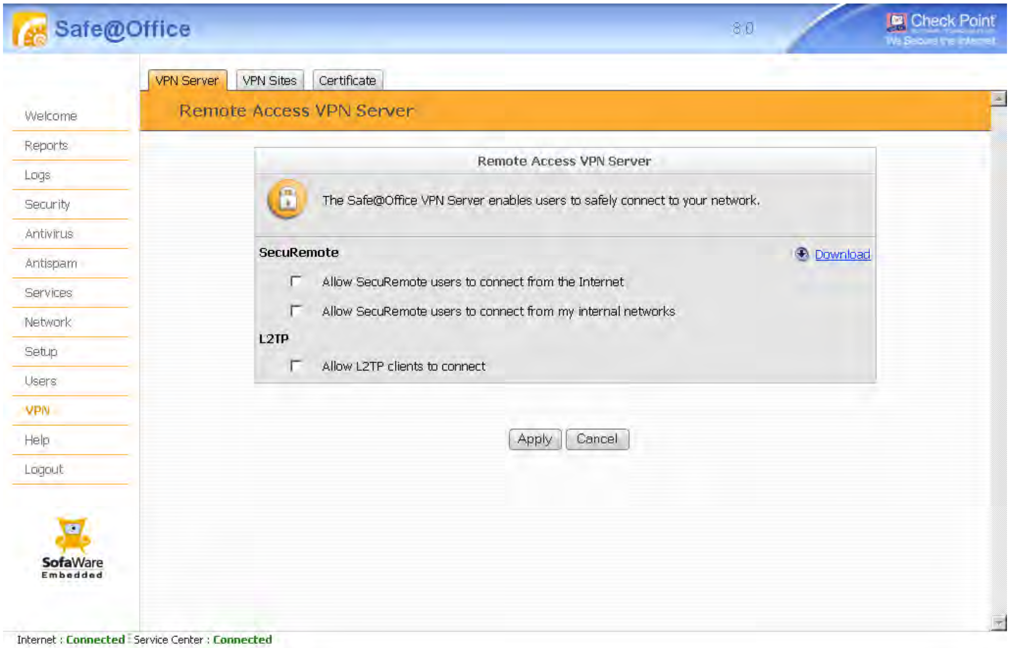
Configuring the SecuRemote Remote Access VPN Server

500

To configure the SecuRemote Remote Access VPN Server

1. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.



Remote Access VPN Server

Remote Access VPN Server

The Safe@Office VPN Server enables users to safely connect to your network.

SecuRemote

□ Allow SecuRemote users to connect from the Internet

□ Allow SecuRemote users to connect from my internal networks

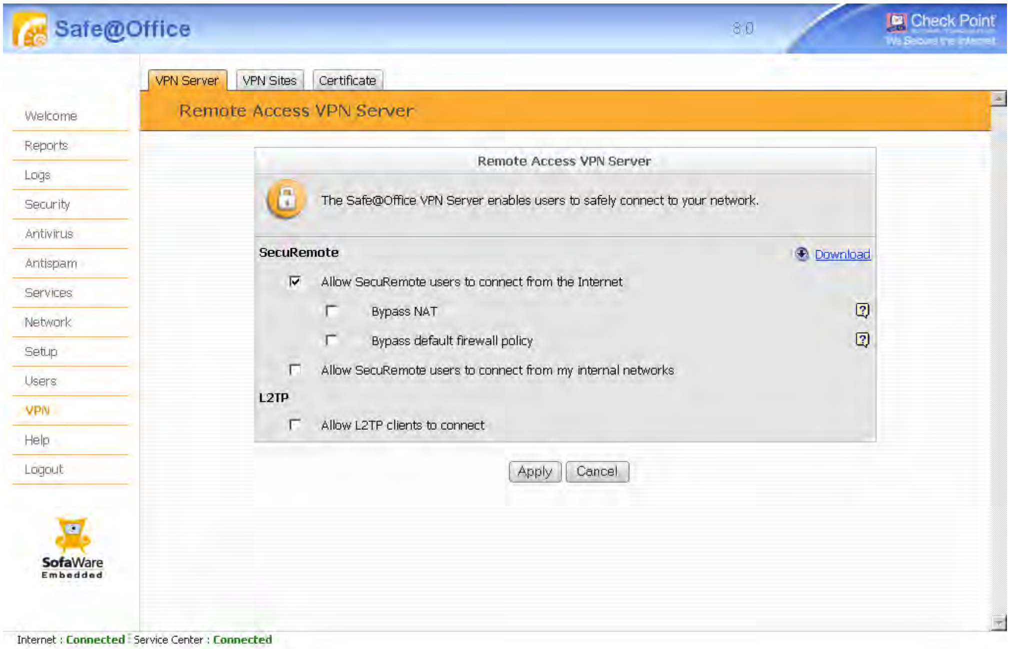
L2TP

□ Allow L2TP clients to connect

Internet : Connected | Service Center : Connected

2. Select the Allow SecuRemote users to connect from the Internet check box.

New check boxes appear.



Remote Access VPN Server

Remote Access VPN Server

The Safe@Office VPN Server enables users to safely connect to your network.

SecuRemote

☑ Allow SecuRemote users to connect from the Internet

□ Bypass NAT

□ Bypass default firewall policy

□ Allow SecuRemote users to connect from my internal networks

L2TP

□ Allow L2TP clients to connect

Internet : Connected | Service Center : Connected

3. To allow authenticated users connecting from the Internet to bypass NAT when connecting to your internal network, select the Bypass NAT check box.

4. To allow authenticated users connecting from the Internet to bypass the default firewall policy and access your internal network without restriction, select the Bypass default firewall policy check box.

   User-defined rules will still apply to the authenticated users.

5. Click Apply.

   The SecuRemote Remote Access VPN Server is enabled for the specified connection types.

Configuring the Internal VPN Server

500

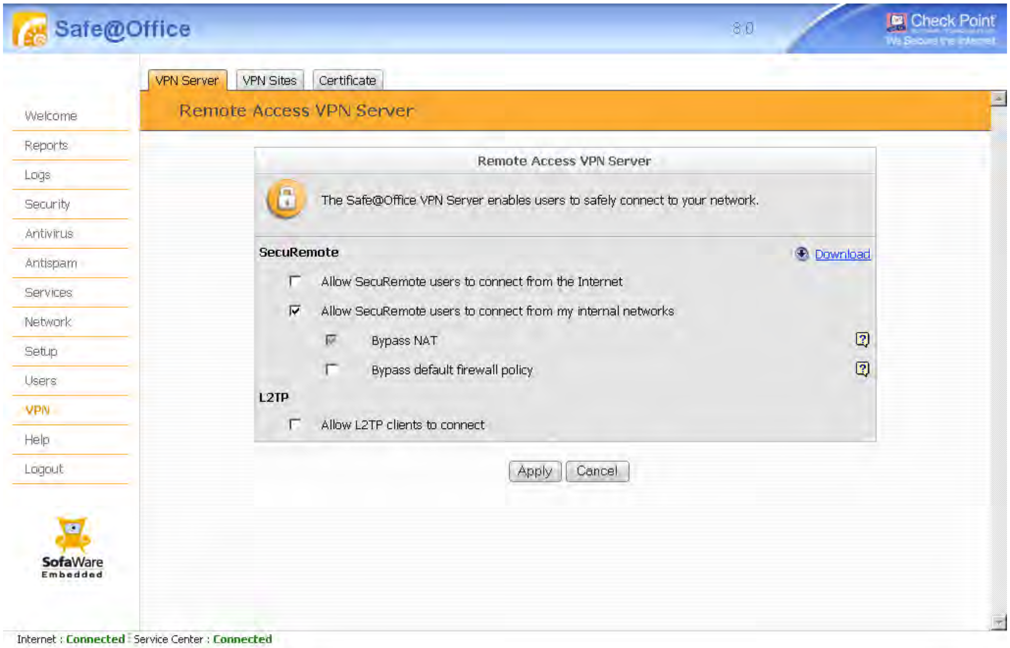
To configure the internal VPN Server

1. Click VPN in the main menu, and click the VPN Server tab.

   The SecuRemote VPN Server page appears.

2. Select the Allow SecuRemote users to connect from my internal networks check box.

   New check boxes appear.



Remote Access VPN Server

Remote Access VPN Server

The Safe@Office VPN Server enables users to safely connect to your network.

SecuRemote

□ Allow SecuRemote users to connect from the Internet

☑ Allow SecuRemote users to connect from my internal networks

☑ Bypass NAT

□ Bypass default firewall policy

L2TP

□ Allow L2TP clients to connect

Internet : Connected Service Center : Connected

3. To allow authenticated users connecting from internal networks to bypass the default firewall policy and access your internal network without restriction, select the Bypass default firewall policy check box.

   User-defined rules will still apply to the authenticated users.

Note: Bypass NAT is always enabled for the internal VPN Server, and cannot be disabled.

4. Click Apply.

   The internal VPN Server is enabled for the specified connection types.

Configuring the L2TP VPN Server

500

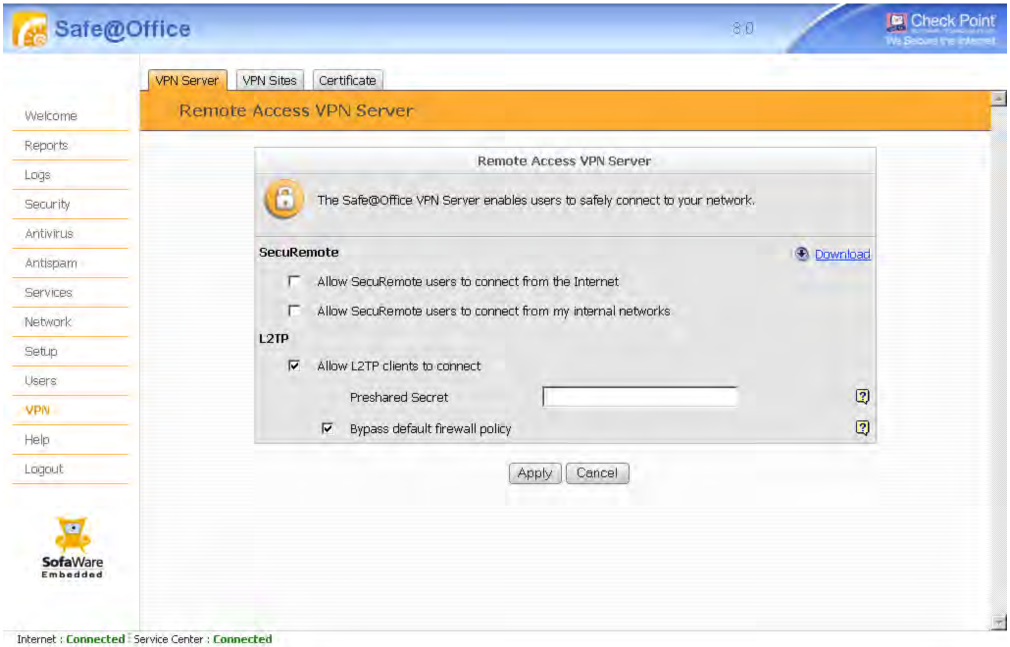
To configure the L2TP VPN Server

1. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.

2. Select the Allow L2TP clients to connect check box.

   New check boxes appear.



Remote Access VPN Server

Remote Access VPN Server

The Safe@Office VPN Server enables users to safely connect to your network.

SecuRemote

☐ Allow SecuRemote users to connect from the Internet

☐ Allow SecuRemote users to connect from my internal networks

L2TP

☑ Allow L2TP clients to connect

Preshared Secret

☑ Bypass default firewall policy

Internet : Connected | Service Center : Connected

3. In the Preshared Secret field, type the preshared secret to use for secure communications between the L2TP clients and the VPN Server.

   The secret can contain spaces and special characters. It is used to secure L2TP connections for all users.

   In addition to entering this secret, each L2TP user will have to authenticate with a username and password.

   For information on defining users with VPN access permissions, see ***Setting Up Remote VPN Access for Users*** on page 650.

4. To allow authenticated users to bypass the default firewall policy and access your internal network without restriction, select the Bypass default firewall policy check box.

   User-defined rules will still apply to the authenticated users.

5. Click Apply.

   The L2TP VPN Server is enabled for the specified connection types.

Installing SecuRemote

500

If you configured the SecuRemote Internal VPN Server, you must install the SecuRemote/SecureClient VPN Client on all internal network computers that should be allowed to remotely access your network via SecuRemote connections.

To install SecureClient/SecuRemote

1. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.

2. Click the Download link.

   The VPN-1 SecuRemote for Safe@Office page opens in a new window.

3. Follow the online instructions to complete installation.

   SecureClient/SecuRemote is installed.

For information on using SecureClient/SecuRemote, see the User Help. To access SecureClient/SecuRemote User Help, right-click on the VPN Client icon in the taskbar, select **Settings**, and then click **Help**.

Configuring L2TP VPN Clients

500

If you configured the L2TP VPN Server, you must configure the L2TP VPN Client on all computers that should be allowed to remotely access your network via L2TP connections.

This procedure is relevant for computers with a Windows XP operating system.

Note: The Safe@Office appliance supports the following authentication methods:

- PAP. For both local users and RADIUS users
- EAP-MD5, CHAP. For local users, but not for RADIUS users

To configure L2TP VPN Clients on Microsoft Windows

1. Click **Start** > **Settings** > **Control Panel**.

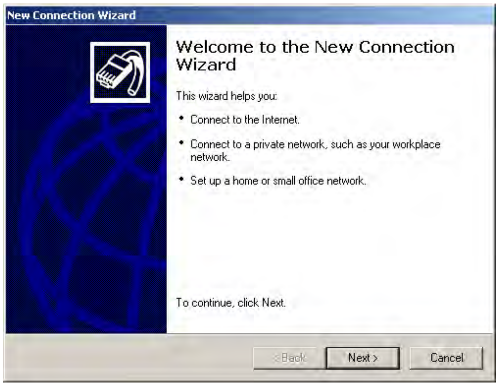
   The **Control Panel** window appears.

2. Double-click the **Network and Dial-up Connections** icon.

   The **Network and Dial-up Connections** window appears.

3. Click **File** > **New Connection**.

The **New Connection Wizard** opens displaying the **Welcome to the New Connection Wizard** screen.


New Connection Wizard

Welcome to the New Connection Wizard

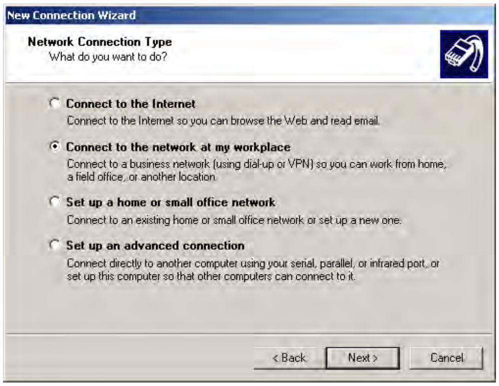
This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

To continue, click Next.

4. Click **Next.**

   The **Network Connection Type** dialog box appears.


New Connection Wizard

Network Connection Type
What do you want to do?

○ Connect to the Internet
Connect to the Internet so you can browse the Web and read email.

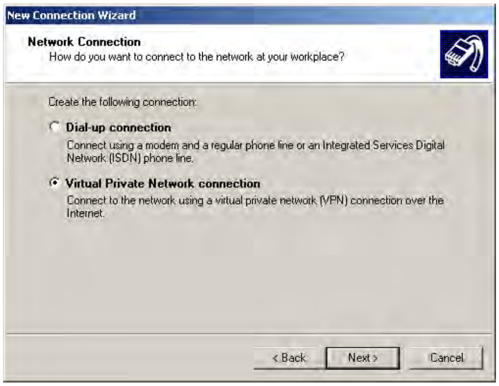
● Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ Set up a home or small office network
Connect to an existing home or small office network or set up a new one.

○ Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

5. Choose **Connect to the network at my workplace.**
6. Click **Next.**

7. The **Network Connection** dialog box appears.



New Connection Wizard

Network Connection
How do you want to connect to the network at your workplace?

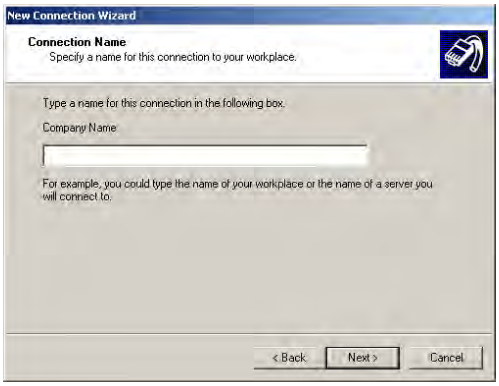
Create the following connection:

○ Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.

8. Choose **Virtual Private Network connection.**
9. Click **Next.**

   The **Connection Name** dialog box appears.



New Connection Wizard

Connection Name
Specify a name for this connection to your workplace.

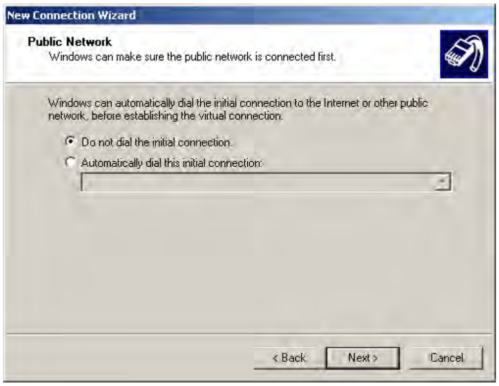
Type a name for this connection in the following box.

Company Name

For example, you could type the name of your workplace or the name of a server you will connect to.

10. In the **Company Name** field, type your company's name.
11. Click **Next.**

The **Public Network** dialog box appears.



New Connection Wizard

Public Network

Windows can make sure the public network is connected first.

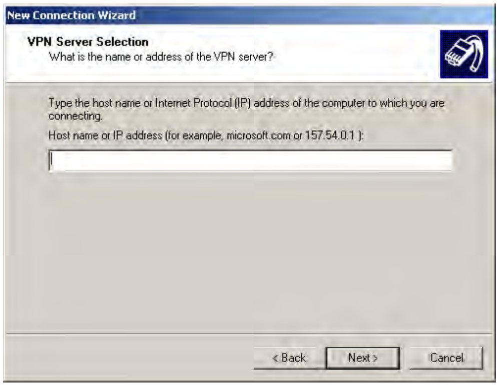
Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

● Do not dial the initial connection.

○ Automatically dial this initial connection:

12. Choose **Do not dial the initial connection.**
13. Click **Next.**

The **VPN Server Selection** dialog box appears.



New Connection Wizard

VPN Server Selection

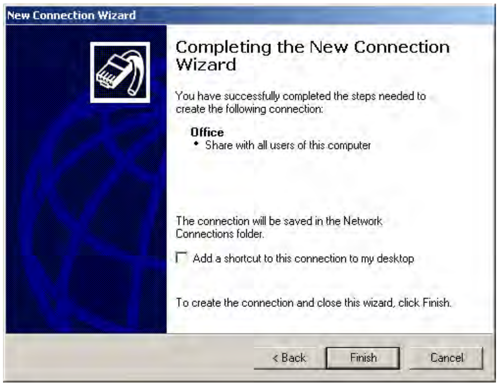
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

14. In the field, type the Safe@Office appliance's IP address.

The **Completing the New Connection Wizard** screen appears.



Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

Office
- Share with all users of this computer

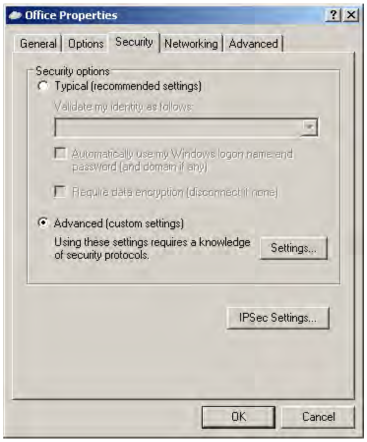
The connection will be saved in the Network Connections folder.

□ Add a shortcut to this connection to my desktop

To create the connection and close this wizard, click Finish.

15. Click **Finish**.
16. In the **Network and Dial-up Connections** window, right-click on the L2TP connection, and click **Properties** in the popup menu.

    The connection's **Properties** dialog box opens.
17. In the **Security** tab, choose **Advanced (custom settings)**.



Security options

○ Typical (recommended settings)

Validate my identity as follows:

□ Automatically use my Windows logon name and password (and domain if any)

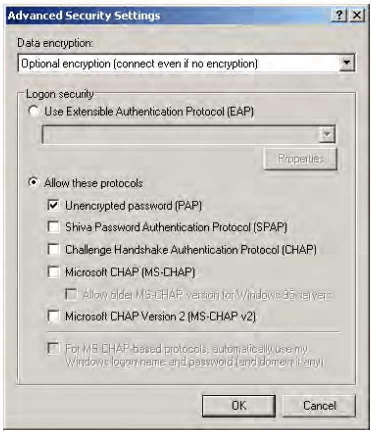
□ Require data encryption (disconnect if none)

● Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

18. Click **Settings**.

The **Advanced Security Settings** dialog box opens.



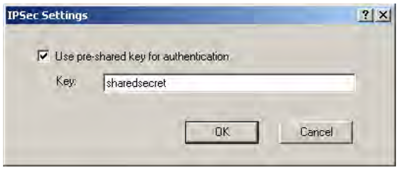
Data encryption:
Optional encryption (connect even if no encryption)

Logon security
○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols
☑ Unencrypted password (PAP)
□ Shiva Password Authentication Protocol (SPAP)
□ Challenge Handshake Authentication Protocol (CHAP)
□ Microsoft CHAP (MS-CHAP)
□ Allow older MS-CHAP version for Windows 95 servers
□ Microsoft CHAP Version 2 (MS-CHAP v2)
□ For MS-CHAP-based protocols, automatically use my Windows logon name and password (and domain if any)

19. In the **Data encryption** drop-down list, select **Optional encryption.**
20. Choose **Allow these protocols.**
21. Select the **Unencrypted password (PAP)** check box, and clear all other check boxes.
22. Click **OK.**
23. In **Properties** dialog box's **Security** tab, click **IPSec Settings.**

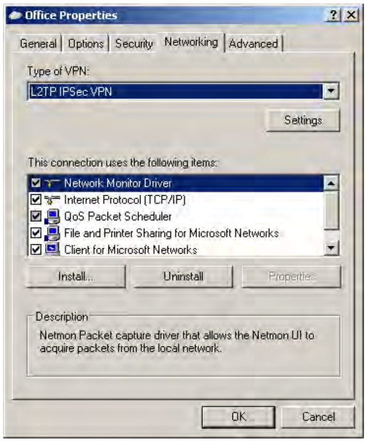
    The **IPSec Settings** dialog box opens.



☑ Use pre-shared key for authentication
Key: sharedsecret

24. Select the **Use pre-shared key for authentication** check box.
25. In the **Key** field, type the preshared secret you configured on the L2TP VPN Server.
26. Click **OK.**
27. In **Properties** dialog box, click the **Networking** tab.

28. In the **Type of VPN** drop-down list, select **L2TP IPSec VPN**.



Type of VPN: L2TP IPSec VPN

This connection uses the following items:

☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Client for Microsoft Networks

Description

Netmon Packet capture driver that allows the Netmon UI to acquire packets from the local network.

29. Click **OK**.

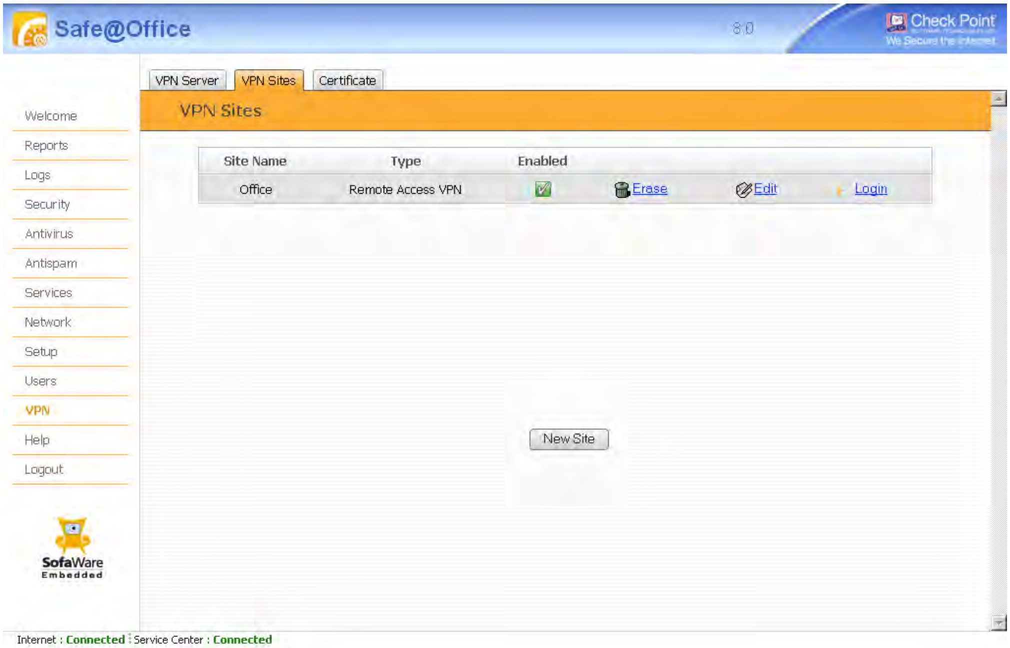
Adding and Editing VPN Sites

500

To add or edit VPN sites

1. Click **VPN** in the main menu, and click the **VPN Sites** tab.

   The **VPN Sites** page appears with a list of VPN sites.



VPN Sites

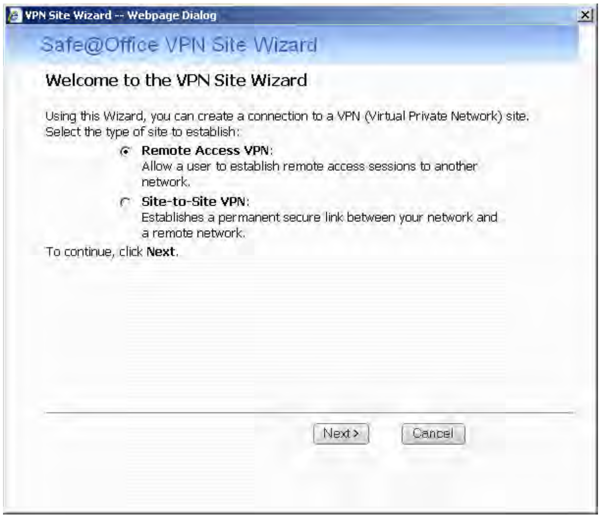
Site Name	Type	Enabled			
Office	Remote Access VPN	☑	Erase	Edit	Login

Internet : Connected | Service Center : Connected

2. Do one of the following:

   - To add a VPN site, click **New Site**.
   - To edit a VPN site, click **Edit** in the desired VPN site's row.

The **Safe@Office VPN Site Wizard** opens, with the **Welcome to the VPN Site Wizard** dialog box displayed.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard

Welcome to the VPN Site Wizard

Using this Wizard, you can create a connection to a VPN (Virtual Private Network) site. Select the type of site to establish:

● **Remote Access VPN**: Allow a user to establish remote access sessions to another network.

○ **Site-to-Site VPN**: Establishes a permanent secure link between your network and a remote network.

To continue, click **Next**.

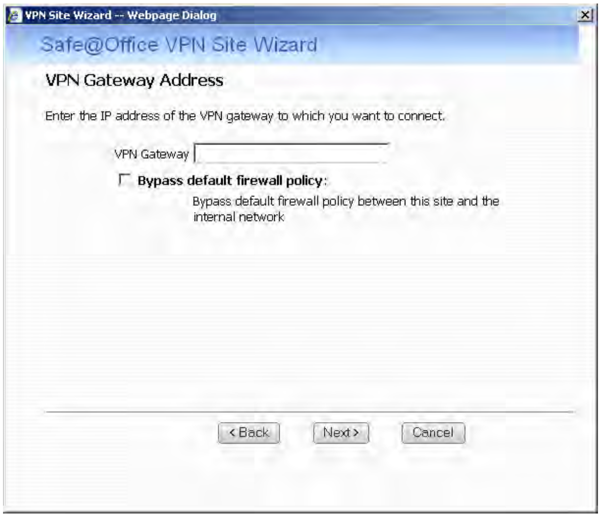
3. Do one of the following:

   - Select **Remote Access VPN** to establish remote access from your Remote Access VPN Client to a Remote Access VPN Server.
   - Select **Site-to-Site VPN** to create a permanent bi-directional connection to another Site-to-Site VPN Gateway.

4. Click **Next.**

Configuring a Remote Access VPN Site

If you selected Remote Access VPN, the VPN Gateway Address dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
< Back
Next >
Cancel

VPN Gateway Address

Enter the IP address of the VPN gateway to which you want to connect.

VPN Gateway

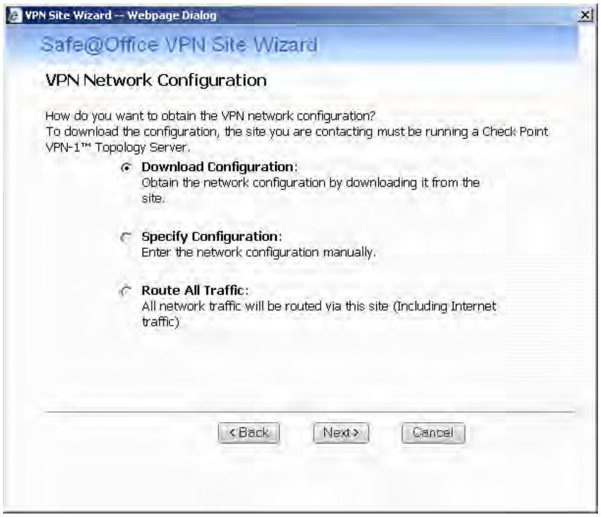
□ **Bypass default firewall policy:**

Bypass default firewall policy between this site and the internal network

1. Enter the IP address of the Remote Access VPN Server to which you want to connect, as given to you by the network administrator.
2. To allow the VPN site to bypass the default firewall policy and access your internal network without restriction, select the Bypass default firewall policy check box.

   User-defined rules will still apply to the VPN site.
3. Click Next.

The VPN Network Configuration dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

VPN Network Configuration

How do you want to obtain the VPN network configuration?
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.

● **Download Configuration**:
Obtain the network configuration by downloading it from the site.

○ **Specify Configuration**:
Enter the network configuration manually.

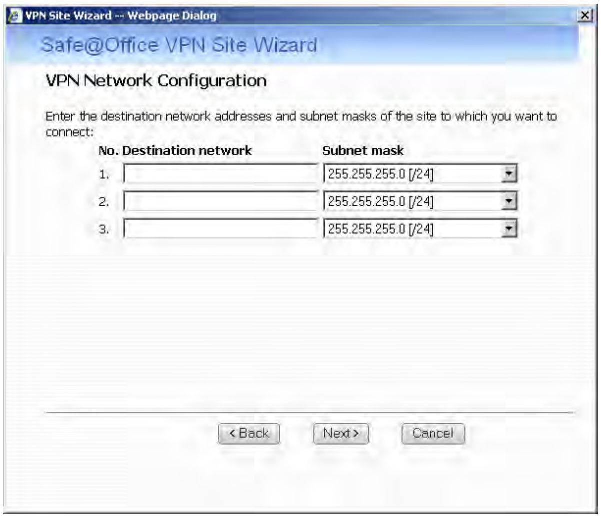
○ **Route All Traffic**:
All network traffic will be routed via this site (Including Internet traffic)

4. Specify how you want to obtain the VPN network configuration. Refer to ***VPN Network Configuration Fields*** on page 593.

5. Click Next.

   The following things happen in the order below:

- If you chose Specify Configuration, a second VPN Network Configuration dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

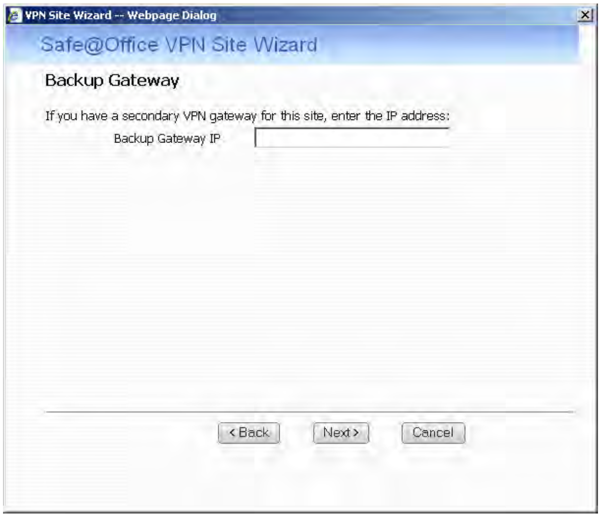
VPN Network Configuration

Enter the destination network addresses and subnet masks of the site to which you want to connect:

No.	Destination network	Subnet mask
1.		255.255.255.0 [/24]
2.		255.255.255.0 [/24]
3.		255.255.255.0 [/24]

Complete the fields using the information in ***VPN Network Configuration Fields*** on page 593 and click Next.

- If you chose Specify Configuration or Route All Traffic, the Backup Gateway dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

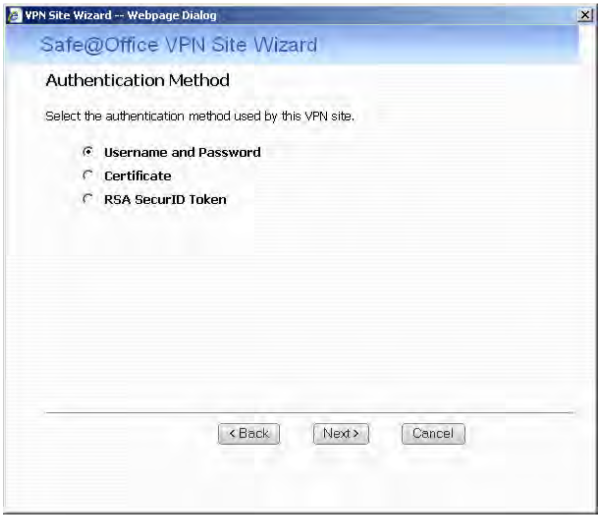
Backup Gateway

If you have a secondary VPN gateway for this site, enter the IP address:

Backup Gateway IP

In the **Backup Gateway IP** field, type the name of the VPN site to use if the primary VPN site fails, and then click **Next.**

- The **Authentication Method** dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

Authentication Method

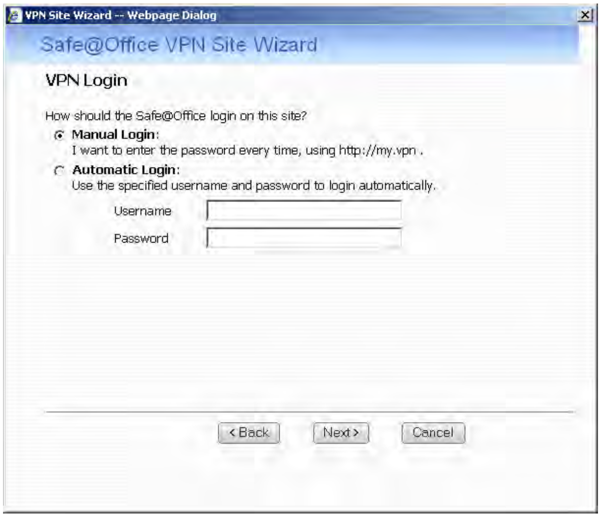
Select the authentication method used by this VPN site.

● Username and Password
○ Certificate
○ RSA SecurID Token

6. Complete the fields using the information in ***Authentication Methods Fields*** on page 595.
7. Click **Next.**

Username and Password Authentication Method

If you selected Username and Password, the VPN Login dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
< Back
Next >
Cancel

VPN Login

How should the Safe@Office login on this site?

● **Manual Login:**
I want to enter the password every time, using http://my.vpn .

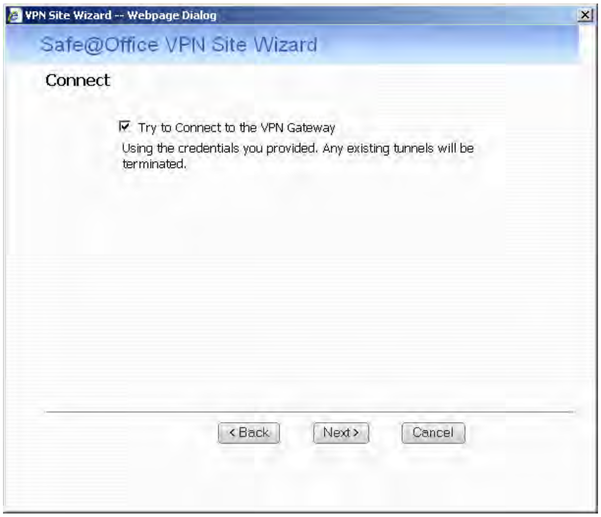
○ **Automatic Login:**
Use the specified username and password to login automatically.

Username

Password

1. Complete the fields using the information in ***VPN Login Fields*** on page 596.
2. Click Next.

- If you selected Automatic Login, the Connect dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
< Back
Next >
Cancel

Connect

☑ Try to Connect to the VPN Gateway

Using the credentials you provided. Any existing tunnels will be terminated.

Do the following:

1) To try to connect to the Remote Access VPN Server, select the **Try to Connect to the VPN Gateway** check box.

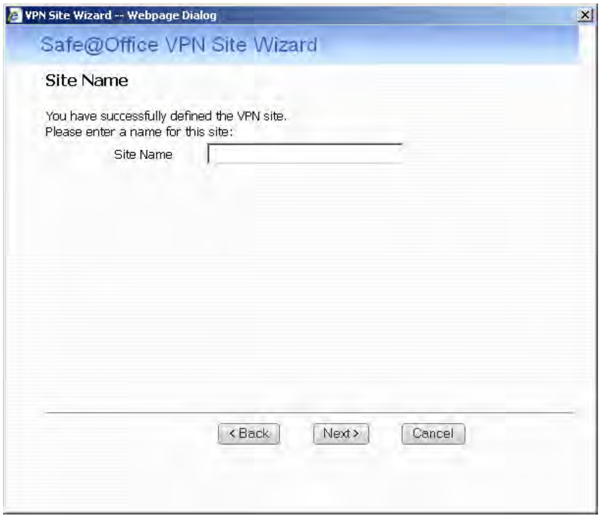
   This allows you to test the VPN connection.

⚠ **Warning:** If you try to connect to the VPN site before completing the wizard, all existing tunnels to this site will be terminated.

2) Click **Next.**

   If you selected **Try to Connect to the VPN Gateway**, the **Connecting**... screen appears, and then the **Contacting VPN Site** screen appears.

- The **Site Name** dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

Site Name

You have successfully defined the VPN site.
Please enter a name for this site:

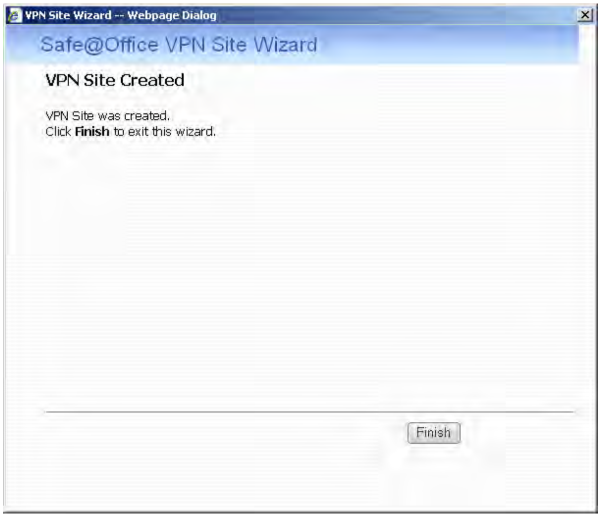
Site Name

3. Enter a name for the VPN site.

   You may choose any name.

4. Click **Next.**

The **VPN Site Created** screen appears.



VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard

VPN Site Created

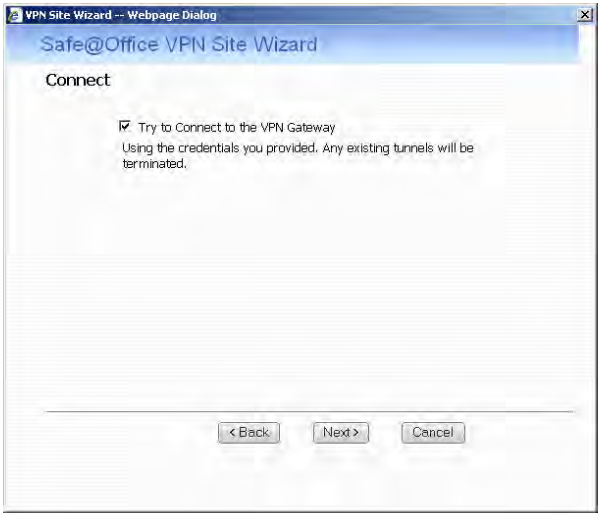
VPN Site was created.
Click **Finish** to exit this wizard.

5. Click **Finish.**

   The **VPN Sites** page reappears. If you added a VPN site, the new site appears in the **VPN Sites** list. If you edited a VPN site, the modifications are reflected in the **VPN Sites** list.

Certificate Authentication Method

If you selected **Certificate**, the **Connect** dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

Connect

☑ Try to Connect to the VPN Gateway

Using the credentials you provided. Any existing tunnels will be terminated.

1. To try to connect to the Remote Access VPN Server, select the **Try to Connect to the VPN Gateway** check box.

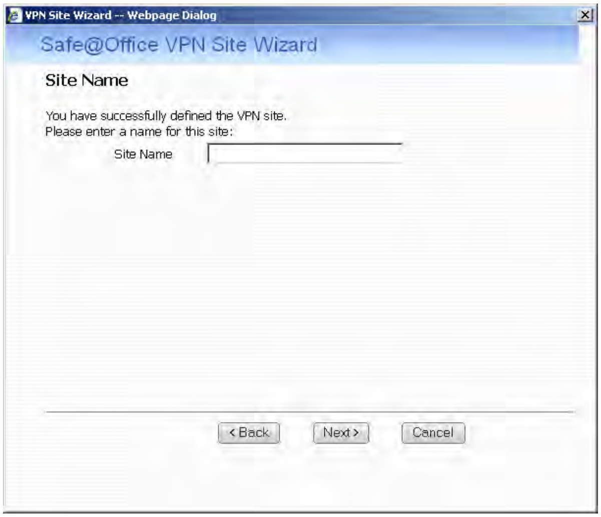
   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels to this site will be terminated.

2. Click **Next.**

   If you selected **Try to Connect to the VPN Gateway**, the **Connecting**... screen appears, and then the **Contacting VPN Site** screen appears.

The **Site Name** dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

Site Name

You have successfully defined the VPN site.
Please enter a name for this site:

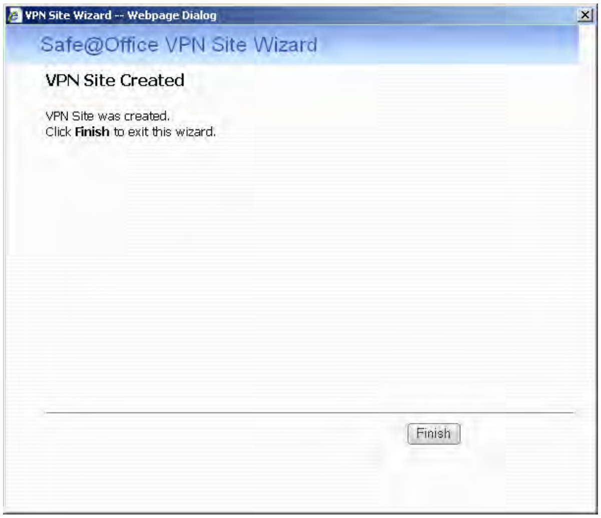
Site Name

3. Enter a name for the VPN site.

   You may choose any name.

4. Click **Next**.

   The **VPN Site Created** screen appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

VPN Site Created

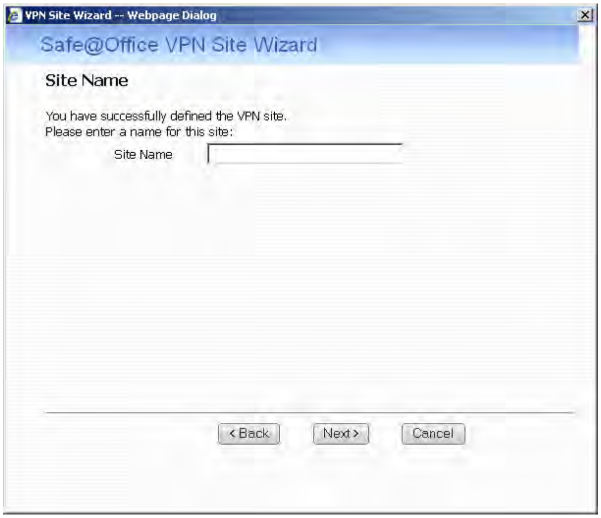
VPN Site was created.
Click **Finish** to exit this wizard.

5. Click **Finish.**

   The **VPN Sites** page reappears. If you added a VPN site, the new site appears in the **VPN Sites** list. If you edited a VPN site, the modifications are reflected in the **VPN Sites** list.

RSA SecurID Authentication Method

If you selected **RSA SecurID**, the **Site Name** dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard

Site Name

You have successfully defined the VPN site.
Please enter a name for this site:

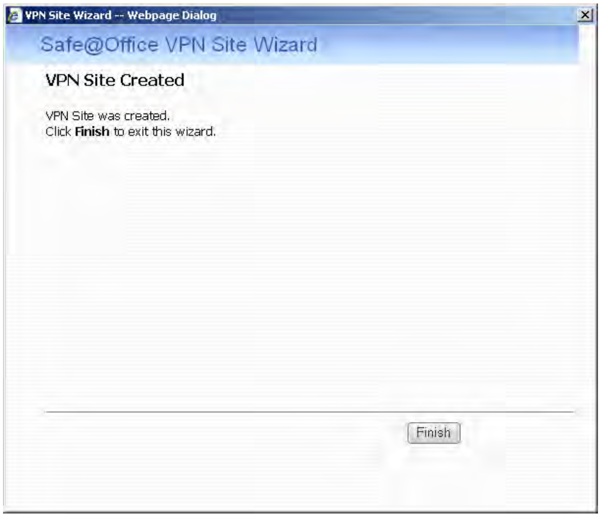
Site Name

1. Enter a name for the VPN site.

   You may choose any name.

2. Click **Next.**

The VPN Site Created screen appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard

VPN Site Created

VPN Site was created.
Click **Finish** to exit this wizard.

3. Click Finish.

   The VPN Sites page reappears. If you added a VPN site, the new site appears in the VPN Sites list. If you edited a VPN site, the modifications are reflected in the VPN Sites list.

Table 119: VPN Network Configuration Fields

In this field…	Do this…
Download Configuration	Click this option to obtain the network configuration by downloading it from the VPN site. This option will automatically configure your VPN settings, by downloading the network topology definition from the Remote Access VPN Server. Note: Downloading the network configuration is only possible if you are connecting to a Check Point VPN-1 or Safe@Office Site-to-Site VPN Gateway.

In this field…	Do this…
Specify Configuration	Click this option to provide the network configuration manually.
Route All Traffic	Click this option to route all network traffic through the VPN site. For example, if your VPN consists of a central office and a number of remote offices, and the remote offices are only allowed to access Internet resources through the central office, you can choose to route all traffic from the remote offices through the central office. Note: You can only configure one VPN site to route all traffic.
Route Based VPN	Click this option to create a virtual tunnel interface (VTI) for this site, so that it can participate in a route-based VPN. Route-based VPNs allow routing connections over VPN tunnels, so that remote VPN sites can participate in dynamic or static routing schemes. This improves network and VPN management efficiency for large networks. For constantly changing networks, it is recommended to use a route-based VPN combined with OSPF dynamic routing. This enables you to make frequent changes to the network topology, such as adding an internal network, without having to reconfigure static routes. OSPF is enabled using CLI. For information on using CLI, see ***Controlling the Appliance via the Command Line*** on page 673. For information on the relevant commands for OSPF, refer to the *Embedded NGX CLI Reference Guide*. This option is only available for when configuring a Site-to-Site VPN gateway.

In this field…	Do this…
Destination network	Type up to three destination network addresses at the VPN site to which you want to connect.
Subnet mask	Select the subnet masks for the destination network addresses. Note: Obtain the destination networks and subnet masks from the VPN site’s system administrator.

Table 120: Authentication Methods Fields

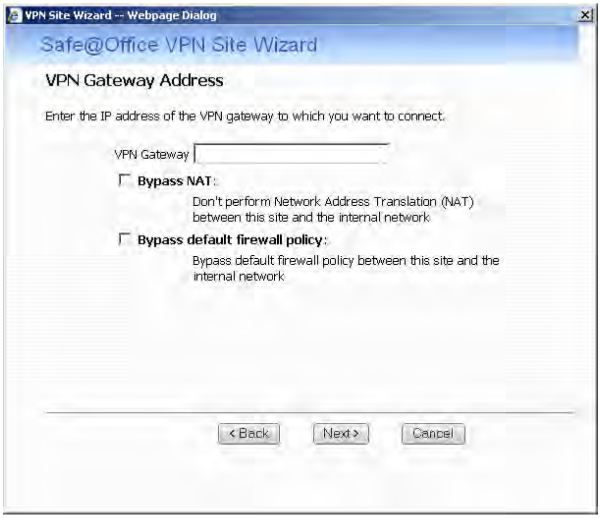
In this field…	Do this…
Username and Password	Select this option to use a user name and password for VPN authentication. In the next step, you can specify whether you want to log in to the VPN site automatically or manually.
Certificate	Select this option to use a certificate for VPN authentication. If you select this option, a certificate must have been installed. (Refer to ***Installing a Certificate*** on page 620 for more information about certificates and instructions on how to install a certificate.)
RSA SecurID Token	Select this option to use an RSA SecurID token for VPN authentication. When authenticating to the VPN site, you must enter a four-digit PIN code and the SecurID passcode shown in your SecurID token's display. The RSA SecurID token generates a new passcode every minute. SecurID is only supported in Remote Access manual login mode.

Table 121: VPN Login Fields

In this field...	Do this...
Manual Login	Click this option to configure the site for Manual Login. Manual Login connects only your computer to the VPN site, and only when the appropriate user name and password have been entered. For further information on Automatic and Manual Login, see, ***Logging in to a VPN Site*** on page 616.
Automatic Login	Click this option to enable the Safe@Office appliance to log in to the VPN site automatically. You must then fill in the Username and Password fields. Automatic Login provides all the computers on your internal network with constant access to the VPN site. For further information on Automatic and Manual Login, see ***Logging in to a VPN Site*** on page 616.
Username	Type the user name to be used for logging in to the VPN site.
Password	Type the password to be used for logging in to the VPN site.

Configuring a Site-to-Site VPN Gateway

If you selected **Site-to-Site VPN**, the **VPN Gateway Address** dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

VPN Gateway Address

Enter the IP address of the VPN gateway to which you want to connect.

VPN Gateway

□ **Bypass NAT**:

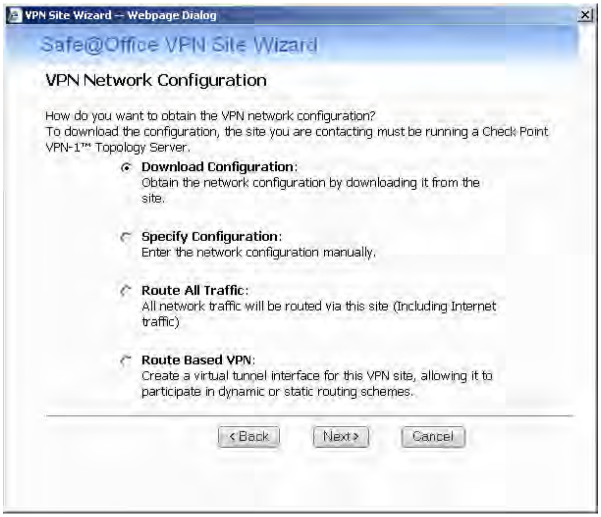
Don't perform Network Address Translation (NAT) between this site and the internal network

□ **Bypass default firewall policy**:

Bypass default firewall policy between this site and the internal network

1. Complete the fields using the information in ***VPN Gateway Address Fields*** on page 611.
2. Click **Next**.

The VPN Network Configuration dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard

VPN Network Configuration

How do you want to obtain the VPN network configuration?
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.

● **Download Configuration:** Obtain the network configuration by downloading it from the site.

○ **Specify Configuration:** Enter the network configuration manually.

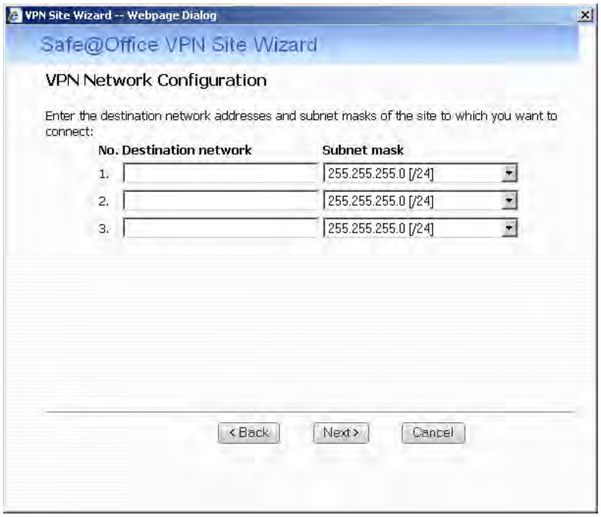
○ **Route All Traffic:** All network traffic will be routed via this site (Including Internet traffic)

○ **Route Based VPN:** Create a virtual tunnel interface for this VPN site, allowing it to participate in dynamic or static routing schemes.

3. Specify how you want to obtain the VPN network configuration. Refer to ***VPN Network Configuration Fields*** on page 593.

4. Click Next.

   - If you chose Specify Configuration, a second VPN Network Configuration dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard

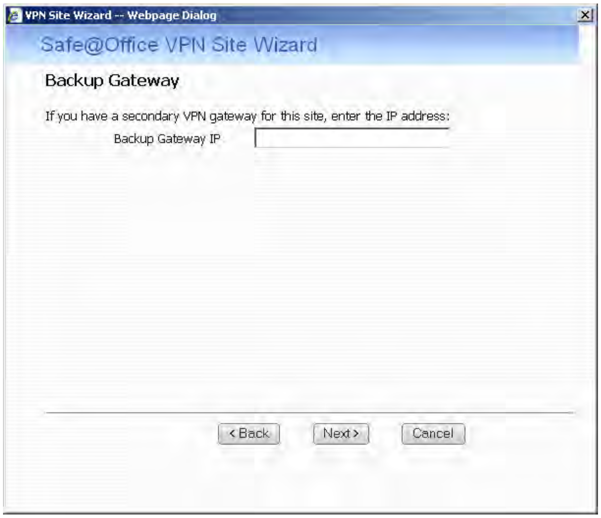
VPN Network Configuration

Enter the destination network addresses and subnet masks of the site to which you want to connect:

No.	Destination network	Subnet mask
1.		255.255.255.0 [/24]
2.		255.255.255.0 [/24]
3.		255.255.255.0 [/24]

Complete the fields using the information in ***VPN Network Configuration Fields*** on page 593, and then click Next.

- If you chose Specify Configuration or Route All Traffic, the Backup Gateway dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

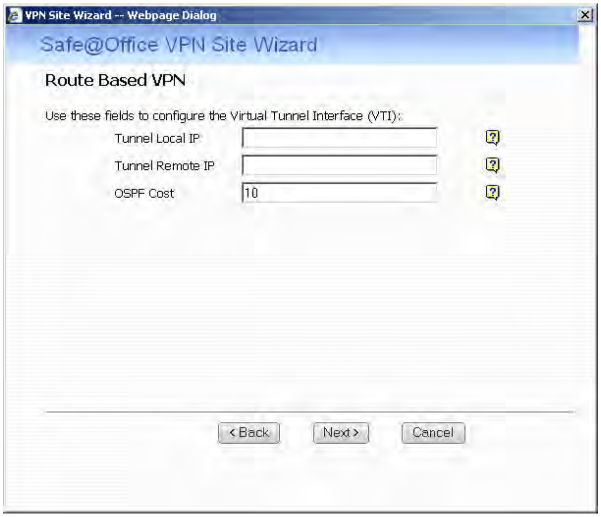
Backup Gateway

If you have a secondary VPN gateway for this site, enter the IP address:

Backup Gateway IP

In the Backup Gateway IP field, type the name of the VPN site to use if the primary VPN site fails, and then click Next.

- If you chose Route Based VPN, the Route Based VPN dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

Route Based VPN

Use these fields to configure the Virtual Tunnel Interface (VTI):

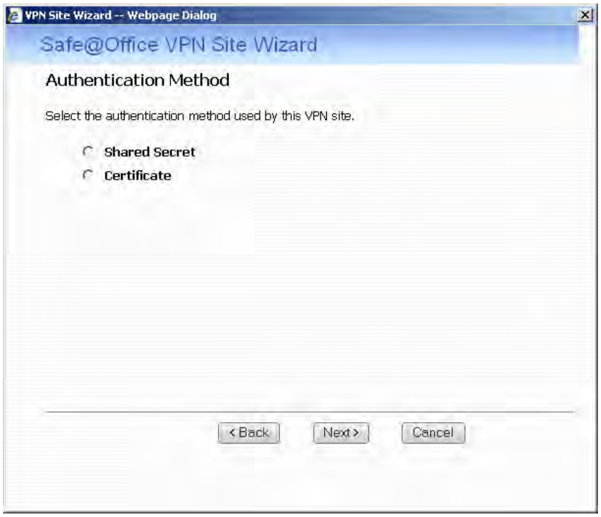
Tunnel Local IP

Tunnel Remote IP

OSPF Cost 10

Complete the fields using the information in ***Route Based VPN Fields*** on page 611, and then click Next.

- The Authentication Method dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

Authentication Method

Select the authentication method used by this VPN site.

○ Shared Secret

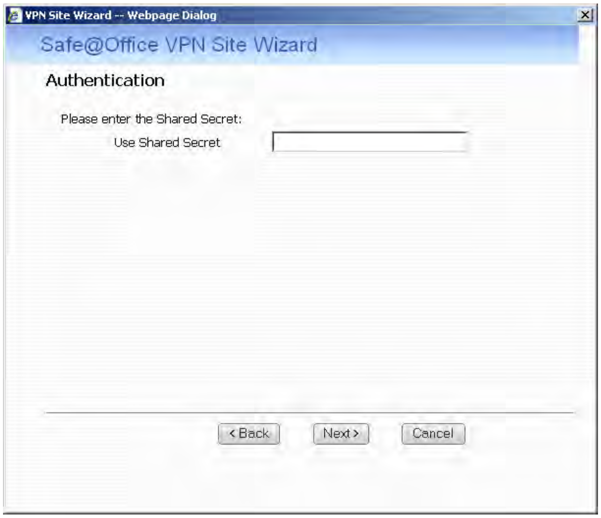
○ Certificate

5. Complete the fields using the information in ***Authentication Methods Fields*** on page 612.

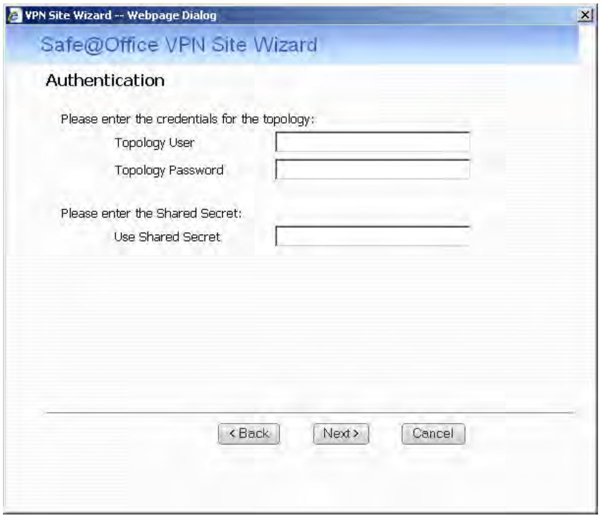
6. Click **Next**.

Shared Secret Authentication Method

If you selected **Shared Secret**, the **Authentication** dialog box appears.

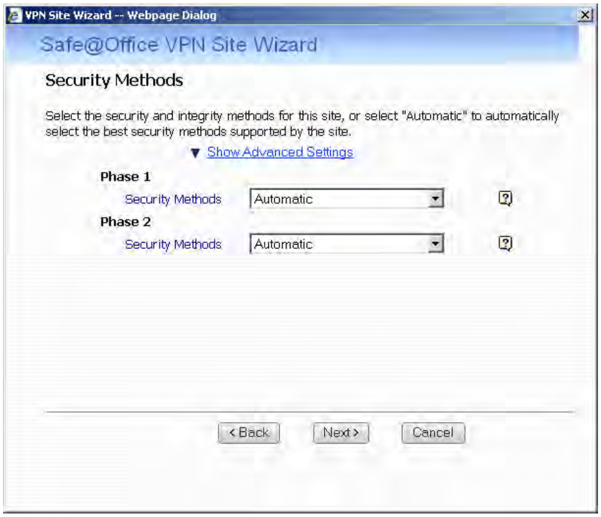

VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Authentication
Please enter the Shared Secret:
Use Shared Secret
< Back
Next >
Cancel

If you chose **Download Configuration**, the dialog box contains additional fields.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Authentication
Please enter the credentials for the topology:
Topology User
Topology Password
Please enter the Shared Secret:
Use Shared Secret
< Back
Next >
Cancel

1. Complete the fields using the information in ***VPN Authentication Fields*** on page 612 and click Next.

   The Security Methods dialog box appears.



VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
< Back
Next >
Cancel

Security Methods

Select the security and integrity methods for this site, or select "Automatic" to automatically select the best security methods supported by the site.

▼ Show Advanced Settings

Phase 1

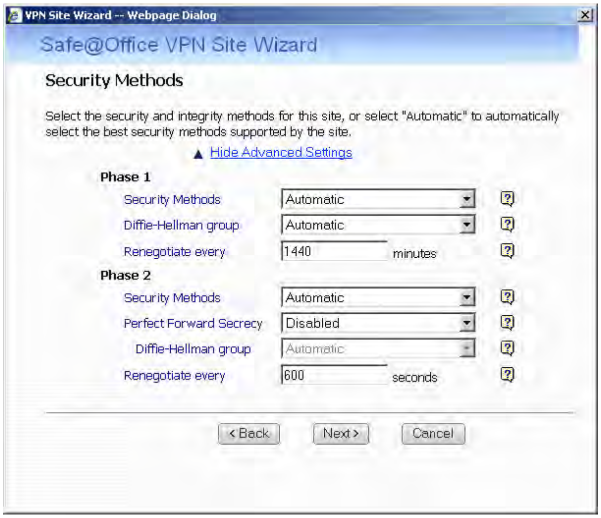
Security Methods: Automatic

Phase 2

Security Methods: Automatic

2. To configure advanced security settings, click Show Advanced Settings.

   New fields appear.



VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
< Back
Next >
Cancel

Security Methods

Select the security and integrity methods for this site, or select "Automatic" to automatically select the best security methods supported by the site.

▲ Hide Advanced Settings

Phase 1

Security Methods: Automatic

Diffie-Hellman group: Automatic

Renegotiate every: 1440 minutes

Phase 2

Security Methods: Automatic

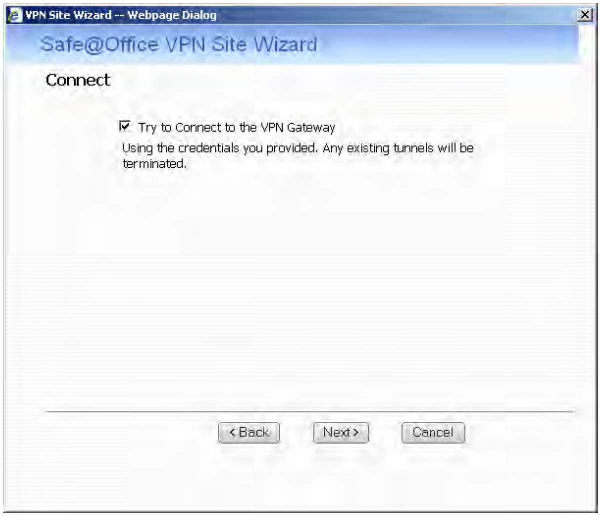
Perfect Forward Secrecy: Disabled

Diffie-Hellman group: Automatic

Renegotiate every: 600 seconds

3. Complete the fields using the information in ***Security Methods Fields*** on page 613 and click **Next.**

   The **Connect** dialog box appears.

   VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
< Back
Next >
Cancel

   Connect

   ☑ Try to Connect to the VPN Gateway

   Using the credentials you provided. Any existing tunnels will be terminated.

4. To try to connect to the Remote Access VPN Server, select the **Try to Connect to the VPN Gateway** check box.

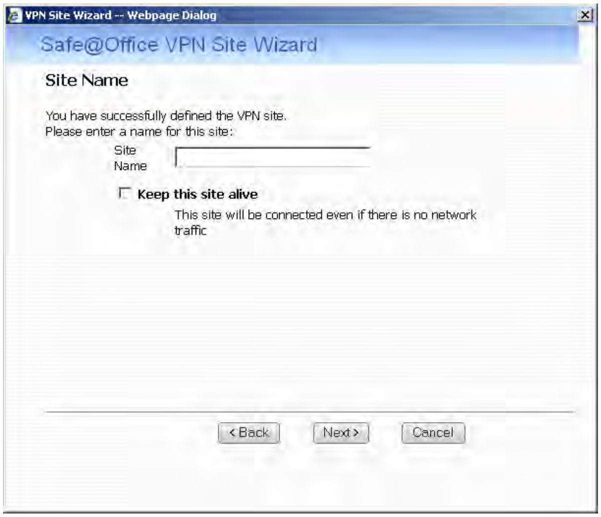
   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels to this site will be terminated.

5. Click **Next.**

   - If you selected **Try to Connect to the VPN Gateway**, the **Connecting**... screen appears, and then the **Contacting VPN Site** screen appears.

- The **Site Name** dialog box appears.



VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard

Site Name

You have successfully defined the VPN site.
Please enter a name for this site:

Site Name

□ Keep this site alive

This site will be connected even if there is no network traffic

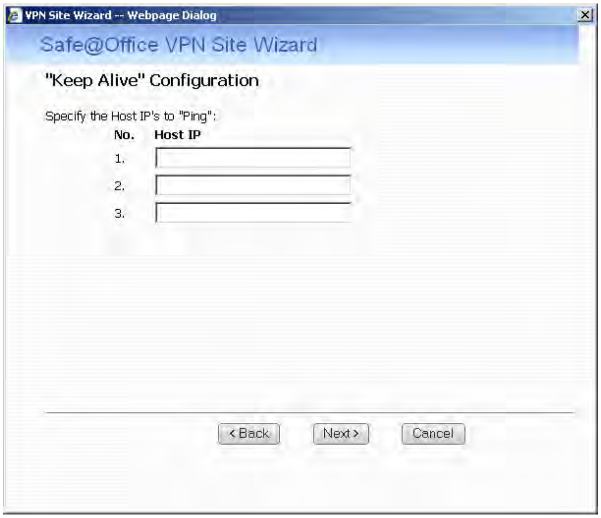
6. Type a name for the VPN site.

   You may choose any name.

7. To keep the tunnel to the VPN site alive even if there is no network traffic between the Safe@Office appliance and the VPN site, select **Keep this site alive**.

8. Click **Next**.

- If you selected **Keep this site alive**, and previously you chose **Download Configuration**, the **"Keep Alive" Configuration** dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

"Keep Alive" Configuration

Specify the Host IP's to "Ping":

No.	Host IP
1.	
2.	
3.	

Do the following:

1) Type up to three IP addresses which the Safe@Office appliance should ping in order to keep the tunnel to the VPN site alive.

2) Click **Next.**

- The **VPN Site Created** screen appears.

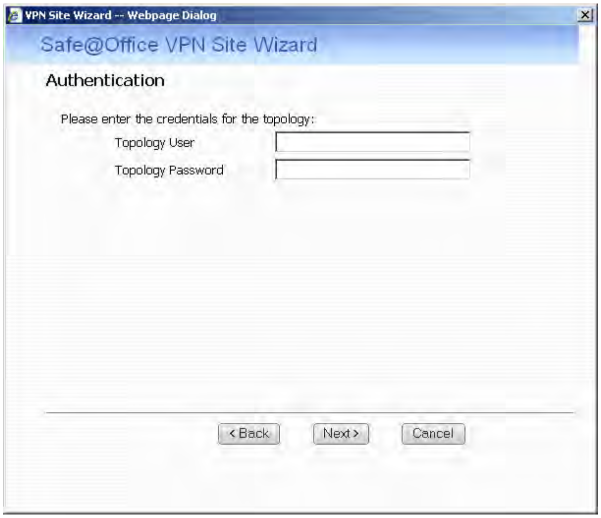
9. Click **Finish.**

The **VPN Sites** page reappears. If you added a VPN site, the new site appears in the **VPN Sites** list. If you edited a VPN site, the modifications are reflected in the **VPN Sites** list.

Certificate Authentication Method

If you selected **Certificate**, the following things happen:

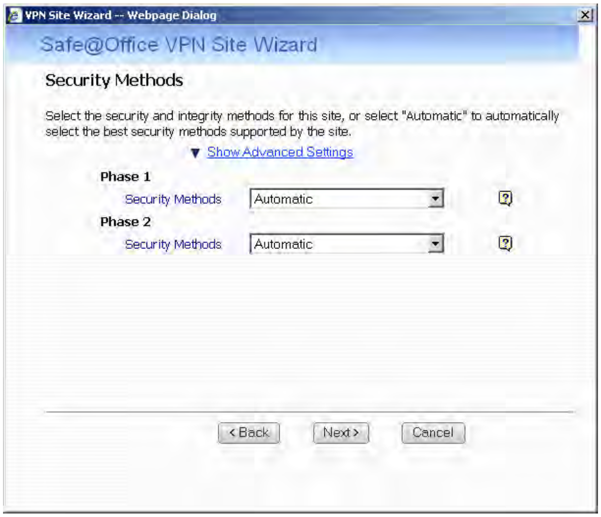
- If you chose **Download Configuration**, the **Authentication** dialog box appears.



VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Authentication
Please enter the credentials for the topology:
Topology User
Topology Password
< Back
Next >
Cancel

Complete the fields using the information in ***VPN Authentication Fields*** on page 612 and click **Next**.

- The **Security Methods** dialog box appears.



Safe@Office VPN Site Wizard

Security Methods

Select the security and integrity methods for this site, or select "Automatic" to automatically select the best security methods supported by the site.

▼ Show Advanced Settings

Phase 1

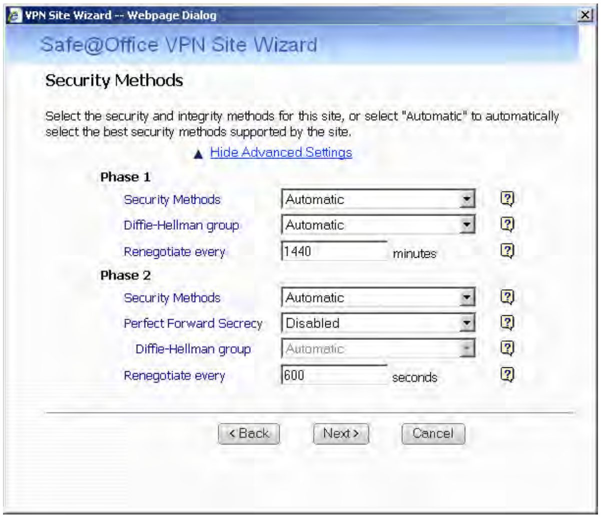
Security Methods: Automatic

Phase 2

Security Methods: Automatic

1. To configure advanced security settings, click **Show Advanced Settings**.

   New fields appear.



Safe@Office VPN Site Wizard

Security Methods

Select the security and integrity methods for this site, or select "Automatic" to automatically select the best security methods supported by the site.

▲ Hide Advanced Settings

Phase 1

Security Methods: Automatic

Diffie-Hellman group: Automatic

Renegotiate every: 1440 minutes

Phase 2

Security Methods: Automatic

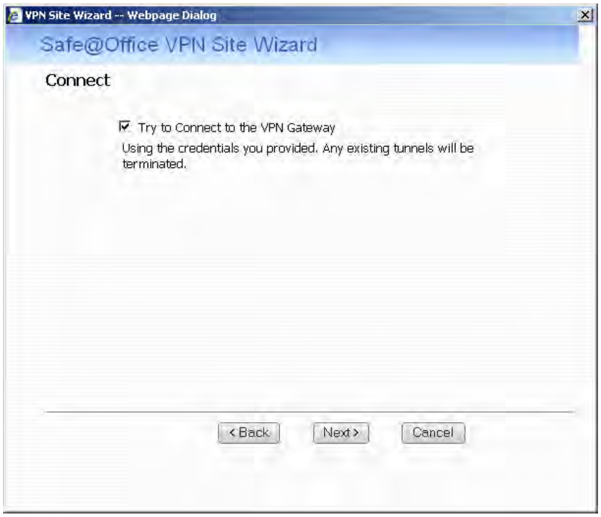
Perfect Forward Secrecy: Disabled

Diffie-Hellman group: Automatic

Renegotiate every: 600 seconds

2. Complete the fields using the information in ***Security Methods Fields*** on page 613 and click **Next**.

The **Connect** dialog box appears.


VPN Site Wizard -- Webpage Dialog
Safe@Office VPN Site Wizard
Connect

☑ Try to Connect to the VPN Gateway

Using the credentials you provided. Any existing tunnels will be terminated.

3. To try to connect to the Remote Access VPN Server, select the **Try to Connect to the VPN Gateway** check box.

   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels to this site will be terminated.

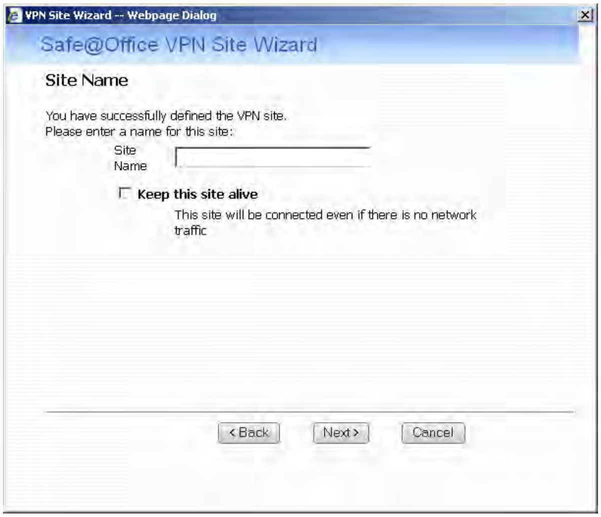
4. Click **Next.**

   - If you selected **Try to Connect to the VPN Gateway**, the following things happen:

     The **Connecting**... screen appears.

   - The **Contacting VPN Site** screen appears.

- The **Site Name** dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

Site Name

You have successfully defined the VPN site.
Please enter a name for this site:

Site Name

☐ **Keep this site alive**

This site will be connected even if there is no network traffic

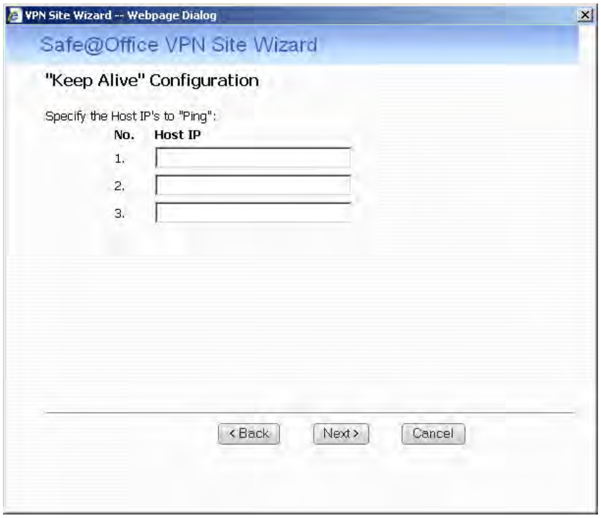
5. Enter a name for the VPN site.

   You may choose any name.

6. To keep the tunnel to the VPN site alive even if there is no network traffic between the Safe@Office appliance and the VPN site, select **Keep this site alive**.

7. Click **Next**.

- If you selected **Keep this site alive**, and previously you chose **Download Configuration**, the **"Keep Alive" Configuration** dialog box appears.



VPN Site Wizard -- Webpage Dialog

Safe@Office VPN Site Wizard

"Keep Alive" Configuration

Specify the Host IP's to "Ping":

No.	Host IP
1.	
2.	
3.	

Do the following:

1) Type up to three IP addresses which the Safe@Office appliance should ping in order to keep the tunnel to the VPN site alive.

2) Click **Next**.

- The **VPN Site Created** screen appears.

8. Click **Finish**.

The **VPN Sites** page reappears. If you added a VPN site, the new site appears in the **VPN Sites** list. If you edited a VPN site, the modifications are reflected in the **VPN Sites** list.

Table 122: VPN Gateway Address Fields

In this field...	Do this...
Gateway Address	Type the IP address of the Site-to-Site VPN Gateway to which you want to connect, as given to you by the network administrator.
Bypass NAT	Select this option to allow the VPN site to bypass NAT when connecting to your internal network. This option is selected by default.
Bypass default firewall policy	Select this option to allow the VPN site to bypass the default firewall policy and access your internal network without restriction. User-defined rules will still apply to the VPN site.

Table 123: Route Based VPN Fields

In this field...	Do this...
Tunnel Local IP	Type a local IP address for this end of the VPN tunnel.
Tunnel Remote IP	Type the IP address of the remote end of the VPN tunnel.
OSPF Cost	Type the cost of this link for dynamic routing purposes. The default value is 10. If OSPF is not enabled, this setting is not used. OSPF is enabled using the Safe@Office command line interface (CLI). For information on using CLI, see ***Controlling the Appliance via the Command Line*** on page 673. For information on the relevant commands for OSPF, refer to the *Embedded NGX CLI Reference Guide*.

Table 124: Authentication Methods Fields

In this field…	Do this…
Shared Secret	Select this option to use a shared secret for VPN authentication. A shared secret is a string used to identify VPN sites to each other.
Certificate	Select this option to use a certificate for VPN authentication. If you select this option, a certificate must have been installed. (Refer to ***Installing a Certificate*** on page 620 for more information about certificates and instructions on how to install a certificate.)

Table 125: VPN Authentication Fields

In this field…	Do this…
Topology User	Type the topology user's user name.
Topology Password	Type the topology user's password.
Use Shared Secret	Type the shared secret to use for secure communications with the VPN site. This shared secret is a string used to identify the VPN sites to each other. The secret can contain spaces and special characters.

Table 126: Security Methods Fields

In this field…	Do this…
Phase 1	
Security Methods	Select the encryption and integrity algorithm to use for IKE negotiations: • Automatic. The Safe@Office appliance automatically selects the best security methods supported by the site. This is the default. • A specific algorithm
Diffie-Hellman group	Select the Diffie-Hellman group to use: • Automatic. The Safe@Office appliance automatically selects a group. This is the default. • A specific group A group with more bits ensures a stronger key but lowers performance.
Renegotiate every	Type the interval in minutes between IKE Phase-1 key negotiations. This is the *IKE Phase-1 SA lifetime*. A shorter interval ensures higher security, but impacts heavily on performance. Therefore, it is recommended to keep the SA lifetime around its default value. The default value is 1440 minutes (one day).
Phase 2	
Security Methods	Select the encryption and integrity algorithm to use for VPN traffic: • Automatic. The Safe@Office appliance automatically selects the best security methods supported by the site. This is the default. • A specific algorithm

In this field…	Do this…
Perfect Forward Secrecy	Specify whether to enable Perfect Forward Secrecy (PFS), by selecting one of the following: • Enabled. PFS is enabled. The Diffie-Hellman group field is enabled. • Disabled. PFS is disabled. This is the default. Enabling PFS will generate a new Diffie-Hellman key during IKE Phase 2 and renew the key for each key exchange. PFS increases security but lowers performance. It is recommended to enable PFS only in situations where extreme security is required.
Diffie-Hellman group	Select the Diffie-Hellman group to use: • Automatic. The Safe@Office appliance automatically selects a group. This is the default. • A specific group A group with more bits ensures a stronger key but lowers performance.
Renegotiate every	Type the interval in seconds between IPSec SA key negotiations. This is the *IKE Phase-2 SA lifetime*. A shorter interval ensures higher security. The default value is 3600 seconds (one hour).

Viewing and Deleting VPN Sites

500

To view or delete a VPN site

1. Click **VPN** in the main menu, and click the **VPN Sites** tab.

   The **VPN Sites** page appears, with a list of all VPN sites.

2. To delete a VPN site, do the following.

   a. In the desired VPN site's row, click the Erase 🗑 icon.

      A confirmation message appears.

   b. Click **OK**.

      The VPN site is deleted.

Enabling/Disabling a VPN Site

500

You can only connect to VPN sites that are enabled.

To enable/disable a VPN site

1. Click **VPN** in the main menu, and click the **VPN Sites** tab.

   The **VPN Sites** page appears, with a list of VPN sites.

2. To enable a VPN site, do the following:

   a. Click the ☒ icon in the desired VPN site’s row.

      A confirmation message appears.

   b. Click **OK**.

      The icon changes to ☑, and the VPN site is enabled.

3. To disable a VPN site, do the following:

Note: Disabling a VPN site eliminates the tunnel and erases the network topology.

   a. Click the ☑ icon in the desired VPN site's row.

      A confirmation message appears.

   b. Click **OK**.

      The icon changes to ☒, and the VPN site is disabled.

Logging in to a Remote Access VPN Site

500

You need to manually log in to Remote Access VPN Servers configured for Manual Login. You do not need to manually log in to a Remote Access VPN Server configured for Automatic Login or a Site-to-Site VPN Gateway: all the computers on your network have constant access to it.

Manual Login can be done through either the Safe@Office Portal or the my.vpn page. When you log in and traffic is sent to the VPN site, a VPN tunnel is established. Only the computer from which you logged in can use the tunnel. To share the tunnel with other computers in your home network, you must log in to the VPN site from those computers, using the same user name and password.

Note: You must use a single user name and password for each VPN destination gateway.

Logging in through the Safe@Office Portal

500

Note: You can only log in to sites that are configured for Manual Login.

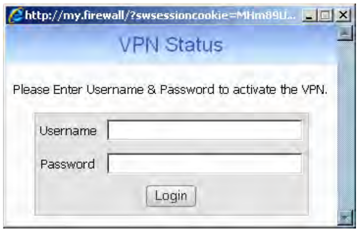
To manually log in to a VPN site through the Safe@Office Portal

1. Click VPN in the main menu, and click the VPN Sites tab.

   The VPN Sites page appears.

2. Next to the desired VPN site, click Login.

   The VPN Status dialog box appears.



VPN Status

Please Enter Username & Password to activate the VPN.

3. Type your user name and password in the appropriate fields.

4. Click Login.

   - If the Safe@Office appliance is configured to automatically download the network configuration, the Safe@Office appliance downloads the network configuration.
   - If when adding the VPN site you specified a network configuration, the Safe@Office appliance attempts to create a tunnel to the VPN site.

     Once the Safe@Office appliance has finished connecting, the dialog box displays “Connected”.
   - The VPN Status dialog box remains open until you manually log out of the VPN site.

Logging in through the my.vpn page

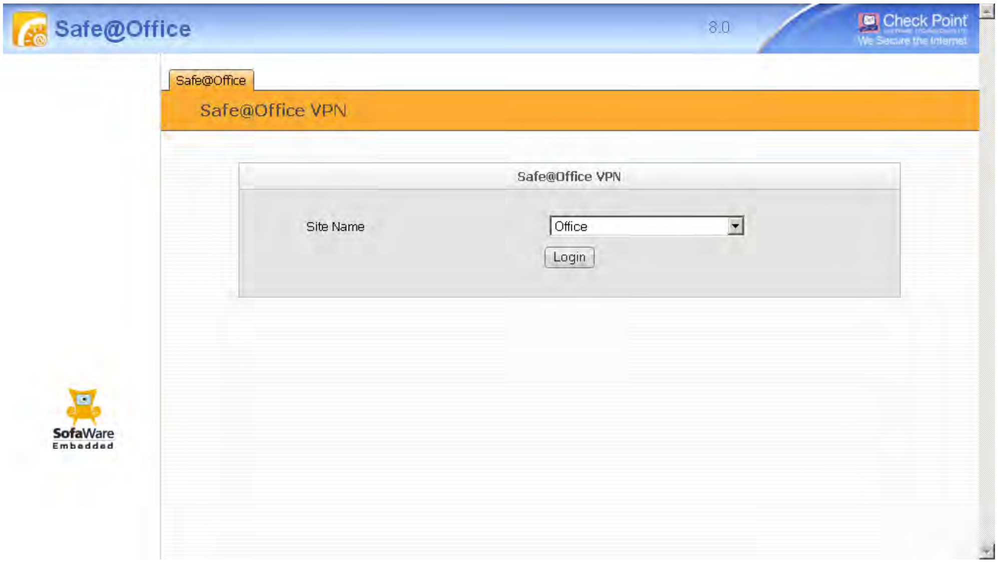
500

Note: You do not need to know the my.firewall page administrator's password in order to use the my.vpn page.

To manually log in to a VPN site through the my.vpn page

1. Direct your Web browser to http://my.vpn

   The VPN Login screen appears.



Safe@Office VPN

Site Name: Office

Login

2. In the Site Name list, select the site to which you want to log in.
3. Enter your user name and password in the appropriate fields.
4. Click Login.

   - If the Safe@Office appliance is configured to automatically download the network configuration, the Safe@Office appliance downloads the network configuration.

- If when adding the VPN site you specified a network configuration, the Safe@Office appliance attempts to create a tunnel to the VPN site.
- The **VPN Login Status** box appears. The **Status** field tracks the connection's progress.
- Once the Safe@Office appliance has finished connecting, the **Status** field changes to "Connected".
- The **VPN Login Status** box remains open until you manually log out of the VPN site.

Logging Out of a Remote Access VPN Site

500

You need to manually log out of a VPN site, if it is a Remote Access VPN site configured for Manual Login.

To log out of a VPN site

- In the **VPN Login Status** box, click **Logout**.

  All open tunnels from the Safe@Office appliance to the VPN site are closed, and the **VPN Login Status** box closes.

Note: Closing the browser or dismissing the **VPN Login Status** box will also terminate the VPN session within a short time.

Using Certificates

500

A digital certificate is a secure means of authenticating the Safe@Office appliance to other Site-to-Site VPN Gateways. The certificate is issued by the Certificate Authority (CA) to entities such as gateways, users, or computers. The entity then uses the certificate to identify itself and provide verifiable information.

For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself). After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

The certificate also includes a fingerprint, a unique text used to identify the certificate. You can email your certificate's fingerprint to the remote user. Upon connecting to the Safe@Office VPN Server for the first time, the entity should check that the VPN peer's fingerprint displayed in the SecuRemote/SecureClient VPN Client is identical to the fingerprint received.

The Safe@Office appliance supports certificates encoded in the PKCS#12 (Personal Information Exchange Syntax Standard) format.

Installing a Certificate

500

The Safe@Office appliance enables you to install PKCS#12 certificates in the following ways:

- By generating a self-signed certificate.

  See ***Generating a Self-Signed Certificate*** on page 621.

- By importing a certificate.

  The PKCS#12 file you import must have a ".p12" file extension. If you do not have such a PKCS#12 file, obtain one from your network security administrator.

  See ***Importing a Certificate*** on page 626.

Note: To use certificates authentication, each Safe@Office appliance should have a unique certificate. Do not use the same certificate for more than one gateway.

Note: If your Safe@Office appliance is centrally managed, a certificate is automatically generated and downloaded to your appliance. In this case, there is no need to generate a self-signed certificate.

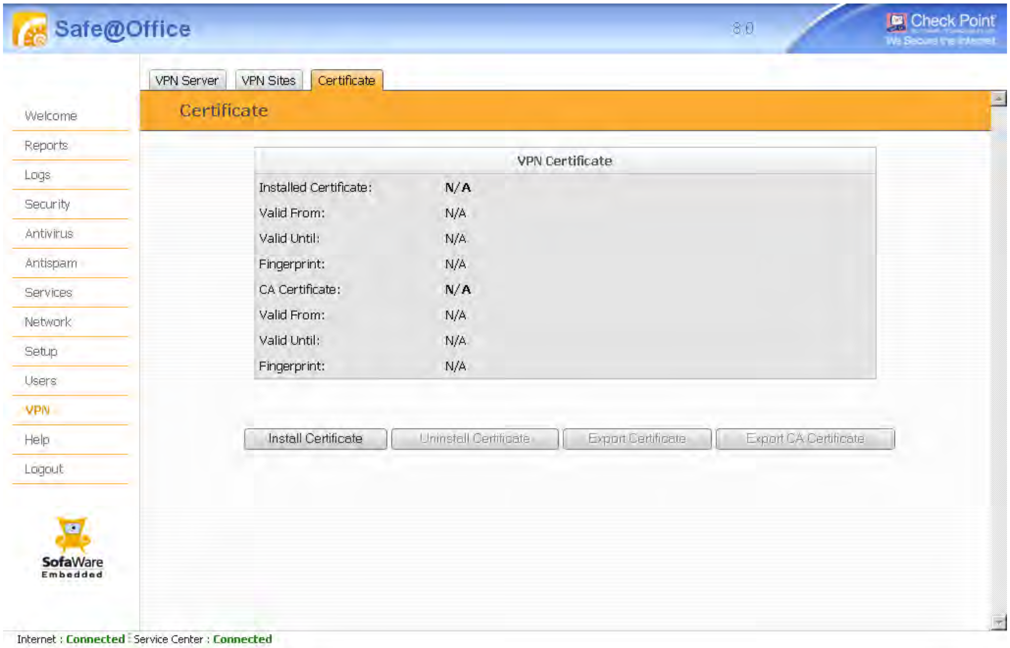
Generating a Self-Signed Certificate

500

To generate a self-signed certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears.



Certificate

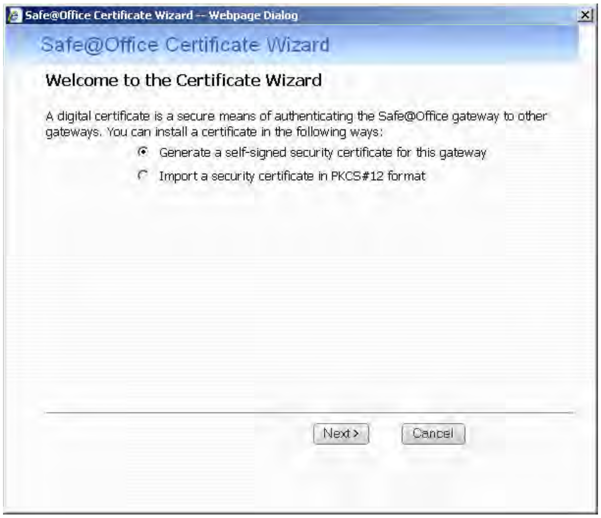
VPN Certificate

Installed Certificate:	N/A
Valid From:	N/A
Valid Until:	N/A
Fingerprint:	N/A
CA Certificate:	N/A
Valid From:	N/A
Valid Until:	N/A
Fingerprint:	N/A

Internet : Connected | Service Center : Connected

2. Click Install Certificate.

The **Safe@Office Certificate Wizard** opens, with the **Certificate Wizard** dialog box displayed.



Safe@Office Certificate Wizard -- Webpage Dialog

Safe@Office Certificate Wizard

Welcome to the Certificate Wizard

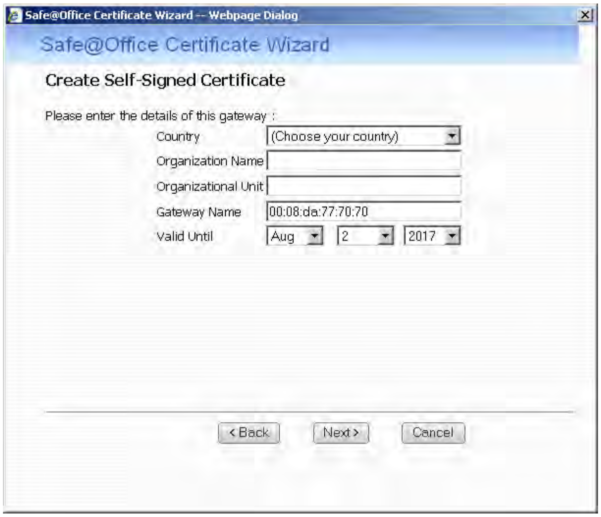
A digital certificate is a secure means of authenticating the Safe@Office gateway to other gateways. You can install a certificate in the following ways:

● Generate a self-signed security certificate for this gateway

○ Import a security certificate in PKCS#12 format

3. Click **Generate a self-signed security certificate for this gateway**.

   The **Create Self-Signed Certificate** dialog box appears.



Safe@Office Certificate Wizard -- Webpage Dialog

Safe@Office Certificate Wizard

Create Self-Signed Certificate

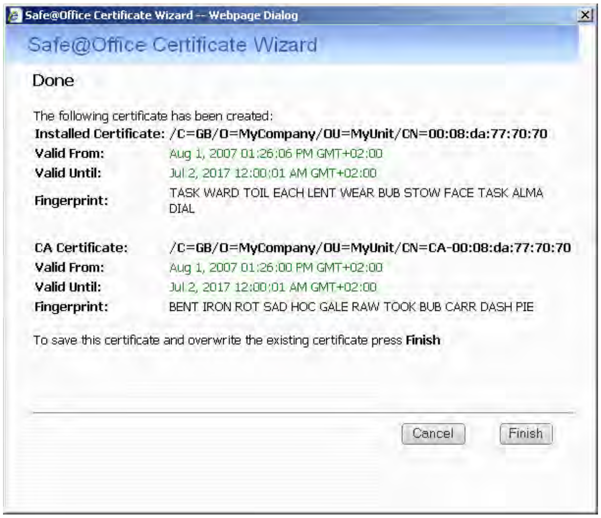
Please enter the details of this gateway :

Country	(Choose your country)
Organization Name	
Organizational Unit	
Gateway Name	00:08:da:77:70:70
Valid Until	Aug 2 2017

4. Complete the fields using the information in the following table.
5. Click **Next**.

The Safe@Office appliance generates the certificate. This may take a few seconds.

The **Done** dialog box appears, displaying the certificate's details.


Safe@Office Certificate Wizard -- Webpage Dialog
Safe@Office Certificate Wizard
Done
Cancel
Finish

The following certificate has been created:

Installed Certificate:	/C=GB/O=MyCompany/OU=MyUnit/CN=00:08:da:77:70:70
Valid From:	Aug 1, 2007 01:26:06 PM GMT+02:00
Valid Until:	Jul 2, 2017 12:00:01 AM GMT+02:00
Fingerprint:	TASK WARD TOIL EACH LENT WEAR BUB STOW FACE TASK ALMA DIAL
CA Certificate:	/C=GB/O=MyCompany/OU=MyUnit/CN=CA-00:08:da:77:70:70
Valid From:	Aug 1, 2007 01:26:00 PM GMT+02:00
Valid Until:	Jul 2, 2017 12:00:01 AM GMT+02:00
Fingerprint:	BENT IRON ROT SAD HOC GALE RAW TOOK BUB CARR DASH PIE

To save this certificate and overwrite the existing certificate press **Finish**

6. Click **Finish**.

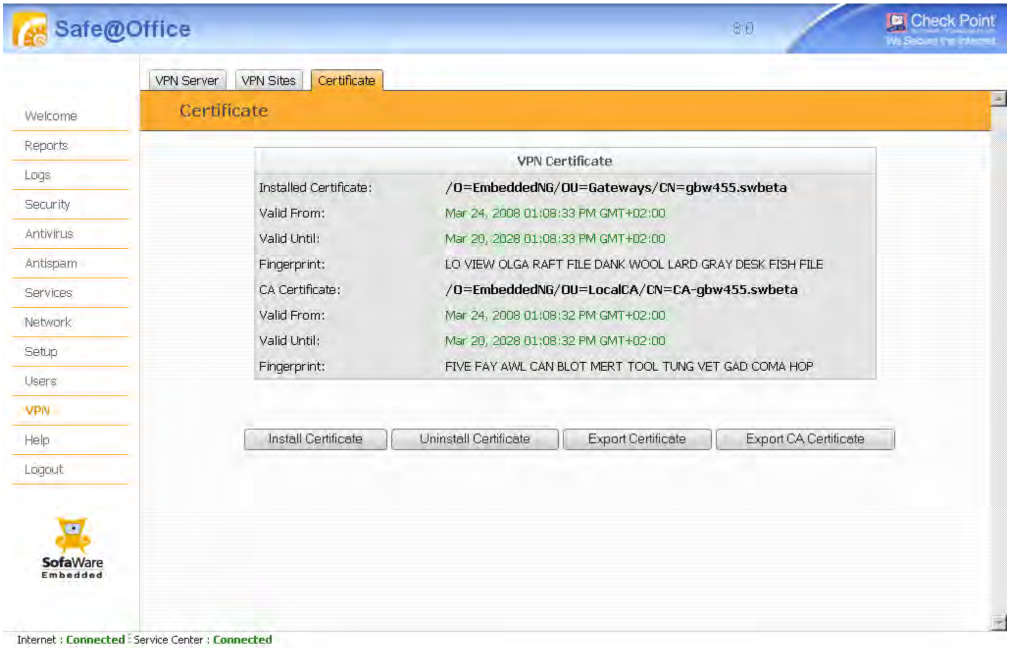
   The Safe@Office appliance installs the certificate. If a certificate is already installed, it is overwritten.

   The Certificate Wizard closes.

   The **Certificates** page displays the following information:

   - The gateway's certificate
   - The gateway's name
   - The gateway certificate's fingerprint
   - The CA's certificate
   - The name of the CA that issued the certificate (in this case, the Safe@Office gateway)
   - The CA certificate's fingerprint

- The starting and ending dates between which the gateway's certificate and the CA's certificate are valid



Certificate

VPN Certificate	
Installed Certificate:	/O=EmbeddedNG/OU=Gateways/CN=gbw455.swbeta
Valid From:	Mar 24, 2008 01:08:33 PM GMT+02:00
Valid Until:	Mar 20, 2028 01:08:33 PM GMT+02:00
Fingerprint:	LO VIEW OLGA RAFT FILE DANK WOOL LARD GRAY DESK FISH FILE
CA Certificate:	/O=EmbeddedNG/OU=LocalCA/CN=CA-gbw455.swbeta
Valid From:	Mar 24, 2008 01:08:32 PM GMT+02:00
Valid Until:	Mar 20, 2028 01:08:32 PM GMT+02:00
Fingerprint:	FIVE FAY AWL CAN BLOT MERT TOOL TUNG VET GAD COMA HOP

Internet : Connected Service Center : Connected

Table 127: Certificate Fields

In this field...	Do this...
Country	Select your country from the drop-down list.
Organization Name	Type the name of your organization.
Organizational Unit	Type the name of your division.
Gateway Name	Type the gateway's name. This name will appear on the certificate, and will be visible to remote users inspecting the certificate. This field is filled in automatically with the gateway's MAC address. If desired, you can change this to a more descriptive name.
Valid Until	Use the drop-down lists to specify the month, day, and year when this certificate should expire. Note: You must renew the certificate when it expires.

Importing a Certificate

500

To install a certificate

1. Click **VPN** in the main menu, and click the **Certificate** tab.

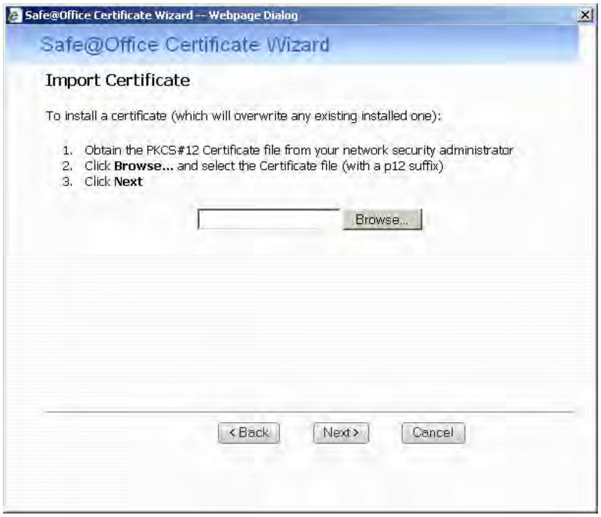
   The **Certificate** page appears.

2. Click **Install Certificate.**

   The **Safe@Office Certificate Wizard** opens, with the **Certificate Wizard** dialog box displayed.

3. Click **Import a security certificate in PKCS#12 format.**

   The **Import Certificate** dialog box appears.



Safe@Office Certificate Wizard -- Webpage Dialog
Safe@Office Certificate Wizard

Import Certificate

To install a certificate (which will overwrite any existing installed one):

1. Obtain the PKCS#12 Certificate file from your network security administrator
2. Click **Browse...** and select the Certificate file (with a p12 suffix)
3. Click **Next**

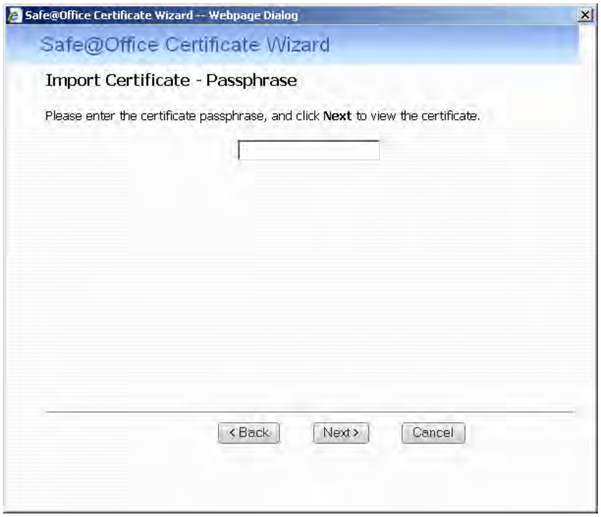
Browse...
< Back
Next >
Cancel

4. Click **Browse** to open a file browser from which to locate and select the file.

   The filename that you selected is displayed.

5. Click **Next.**

The **Import-Certificate Passphrase** dialog box appears. This may take a few moments.



Safe@Office Certificate Wizard -- Webpage Dialog

Safe@Office Certificate Wizard

Import Certificate - Passphrase

Please enter the certificate passphrase, and click **Next** to view the certificate.

6. Type the pass-phrase you received from the network security administrator.
7. Click **Next**.

   The **Done** dialog box appears, displaying the certificate's details.
8. Click **Finish**.

   The Safe@Office appliance installs the certificate. If a certificate is already installed, it is overwritten.

   The Certificate Wizard closes.

   The **Certificates** page displays the following information:

   - The gateway's certificate
   - The gateway's name
   - The gateway certificate's fingerprint
   - The CA's certificate
   - The name of the CA that issued the certificate
   - The CA certificate's fingerprint

- The starting and ending dates between which the gateway's certificate and the CA's certificate are valid

Uninstalling a Certificate

500

If you uninstall the certificate, no certificate will exist on the Safe@Office appliance, and you will not be able to connect to the VPN if a certificate is required.

You cannot uninstall the certificate if there is a VPN site currently defined to use certificate authentication.

Note: If you want to replace a currently-installed certificate, there is no need to uninstall the certificate first. When you install the new certificate, the old certificate will be overwritten.

To uninstall a certificate

1. Click **VPN** in the main menu, and click the **Certificate** tab.

   The **Certificate** page appears with the name of the currently installed certificate.

2. Click **Uninstall**.

   A confirmation message appears.

3. Click **OK**.

   The certificate is uninstalled.

   A success message appears.

4. Click **OK**.

Exporting Certificates

500

The Safe@Office appliance allows you to export the following certificates:

- The device certificate

  Exporting the device certificate is useful for backup purposes.

> Note: If your Safe@Office appliance is centrally managed, there is no need to back up the device certificate, as it can be downloaded from the Service Center as needed.

- The device Certificate Authority (CA) certificate

  When using the Safe@Office EAP authenticator with WPA-Enterprise or 802.1x security protocols, you must export the device CA certificate and send it to clients that need to connect to the Safe@Office appliance. For information on the EAP authenticator, see ***Using the EAP Authenticator*** on page 394.

The certificates are exported in PKCS#12 format (that is, as a *.p12 file).

Exporting the Safe@Office Appliance Certificate

500

To export the Safe@Office appliance certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears with the name of the currently installed certificate.

2. Click Export Certificate.

   A standard File Download dialog box appears.

3. Click Save.

   The Save As dialog box appears.

4. Browse to a destination directory of your choice.

5. Type a name for the certificate file and click Save.

The certificate is exported as a *.p12 file and saved to the specified directory.

Note: This file contains the gateway's private key, which is confidential and must not be passed to unauthorized users.

Exporting the CA Certificate

500

To export the CA certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears with the name of the currently installed certificate.

2. Click Export CA Certificate.

   A standard File Download dialog box appears.

3. Click Save.

   The Save As dialog box appears.

4. Browse to a destination directory of your choice.

5. Type a name for the CA certificate file and click Save.

   The CA certificate is exported as a *.p12 file and saved to the specified directory.

Viewing VPN Tunnels

500

You can view a list of currently established VPN tunnels. VPN tunnels are created and closed as follows:

- **Remote Access VPN sites configured for Automatic Login and Site-to-Site VPN Gateways**

  A tunnel is created whenever your computer attempts any kind of communication with a computer at the VPN site. The tunnel is closed when not in use for a period of time.

> Note: Although the VPN tunnel is automatically closed, the site remains open, and if you attempt to communicate with the site, the tunnel will be reestablished.

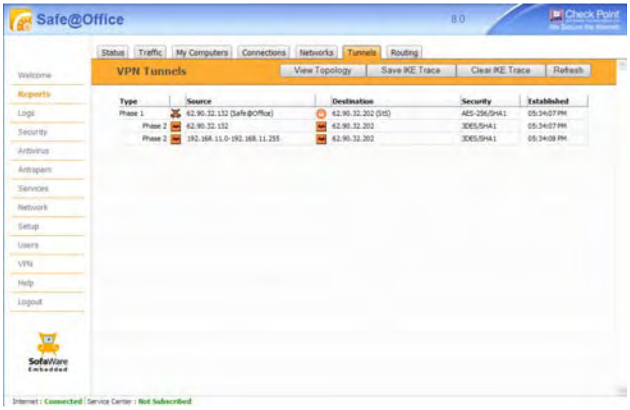
- **Remote Access VPN sites configured for Manual Login**

  A tunnel is created whenever your computer attempts any kind of communication with a computer at the VPN site, *after you have manually logged in to the site*. All open tunnels connecting to the site are closed when you manually log out.

To view VPN tunnels

1. Click **Reports** in the main menu, and click the **Tunnels** tab.

   The **VPN Tunnels** page appears with a table of open VPN tunnels.



Type	Source	Destination	Security	Established
Phase 1	62.90.32.132 (Safe@Office)	62.90.32.202 (StS)	AES-256/SHA1	05:34:07 PM
Phase 2	62.90.32.132	62.90.32.202	3DES/SHA1	05:34:07 PM
Phase 2	192.168.11.0-192.168.11.255	62.90.32.202	3DES/SHA1	05:34:08 PM

Internet : Connected | Service Center : Not Subscribed

The **VPN Tunnels** page includes the information described in the following table.

2. To resize a column, drag the relevant column divider right or left.
3. To refresh the table, click **Refresh**.

Table 128: VPN Tunnels Page Fields

This field...	Displays...
Type	The currently active security protocol (IPSEC).
Source	The IP address or address range of the entity from which the tunnel originates. The entity's type is indicated by an icon. See ***VPN Tunnel Icons*** on page 633.
Destination	The IP address or address range of the entity to which the tunnel is connected. The entity's type is indicated by an icon. See ***VPN Tunnel Icons*** on page 633.
Security	The type of encryption used to secure the connection, and the type of Message Authentication Code (MAC) used to verify the integrity of the message. This information is presented in the following format: Encryption type/Authentication type. In addition, if IPSec compression is enabled for the tunnel, this field displays the ⧉ icon. **Note**: All VPN settings are automatically negotiated between the two sites. The encryption and authentication schemes used for the connection are the strongest of those used at the two sites. Your Safe@Office appliance supports AES, 3DES, and DES encryption schemes, and MD5 and SHA authentication schemes.

This field...	Displays...

Established	The time at which the tunnel was established.
	This information is presented in the format hh:mm:ss, where:
	hh=hours
	mm=minutes
	ss=seconds

Table 129: VPN Tunnels Icons

This icon...	Represents...
	This gateway
	A network for which an IKE Phase-2 tunnel was negotiated
	A Remote Access VPN Server
	A Site-to-Site VPN Gateway
	A remote access VPN user
	An L2TP user

Viewing IKE Traces for VPN Connections

500

If you are experiencing VPN connection problems, you can save a trace of IKE (Internet Key Exchange) negotiations to a file, and then use the free IKE View tool to view the file.

The IKE View tool is available for the Windows platform.

Note: Before viewing IKE traces, it is recommended to do the following:

- The Safe@Office appliance stores traces for all recent IKE negotiations. If you want to view only new IKE trace data, clear all IKE trace data currently stored on the Safe@Office appliance.
- Close all existing VPN tunnels except for the problematic tunnel, so as to make it easier to locate the problematic tunnel's IKE negotiation trace in the exported file.

To clear all currently-stored IKE traces

1. Click Reports in the main menu, and click the Tunnels tab.

   The VPN Tunnels page appears with a table of open tunnels to VPN sites.

2. Click Clear IKE Trace.

   All IKE trace data currently stored on the Safe@Office appliance is cleared.

To view the IKE trace for a connection

1. Establish a VPN tunnel to the VPN site with which you are experiencing connection problems.

   For information on when and how VPN tunnels are established, see ***Viewing VPN Tunnels*** on page 631.

2. Click Reports in the main menu, and click the Tunnels tab.

   The VPN Tunnels page appears with a table of open tunnels to VPN sites.

3. Click Save IKE Trace.

   A standard File Download dialog box appears.

4. Click Save.

The **Save As** dialog box appears.

5. Browse to a destination directory of your choice.
6. Type a name for the *.elg file and click **Save**.

   The *.elg file is created and saved to the specified directory. This file contains the IKE traces of all currently-established VPN tunnels.
7. Use the IKE View tool to open and view the *.elg file, or send the file to technical support.

Viewing VPN Topology

500

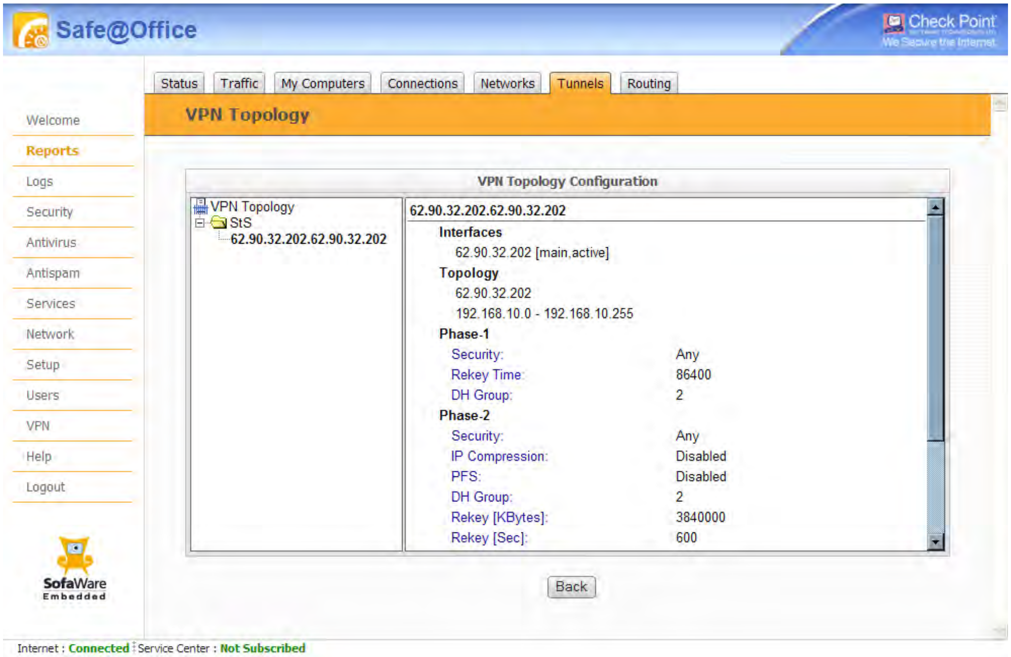
You can view the topology of VPN sites to which the Safe@Office appliance is currently connected.

To view VPN topology

1. Click **Reports** in the main menu, and click the **Tunnels** tab.

   The **VPN Tunnels** page appears with a table of open tunnels to VPN sites.
2. Click **View Topology**.

The VPN Topology page appears displaying a tree of VPN sites to which the appliance is connected.



VPN Topology
StS
62.90.32.202.62.90.32.202

62.90.32.202.62.90.32.202

Interfaces
62.90.32.202 [main,active]

Topology
62.90.32.202
192.168.10.0 - 192.168.10.255

Phase-1

Security:	Any
Rekey Time:	86400
DH Group:	2

Phase-2

Security:	Any
IP Compression:	Disabled
PFS:	Disabled
DH Group:	2
Rekey [KBytes]:	3840000
Rekey [Sec]:	600

3. To view topology information for a VPN site, in the tree, click the VPN site's name.

The right pane displays the information described in the following table.

Table 130: VPN Topology Page Fields

This field...	Displays...
Split DNS	The VPN site's split DNS mappings. When split DNS is configured for a VPN site, certain domain suffixes are mapped to corporate DNS servers. This means that requests for these domain suffixes are sent to the specific DNS servers to which they are mapped, while all other requests are sent to the ISP's DNS servers. For example, a VPN site's split DNS mappings might indicate that all requests for the domain suffix ".acme.com" should be sent to the Acme company's corporate DNS servers.
Trusted CAs	A list of root CAs at the VPN site, whose certificates are trusted by this gateway.
Sub-CAs	A list of second-level CAs at the VPN site, which are signed by a trusted root CA.

Chapter 20

Managing Users

This chapter describes how to manage Safe@Office appliance users. You can define multiple users, set their passwords, and assign them various permissions.

This chapter includes the following topics:

Changing Your Login Credentials

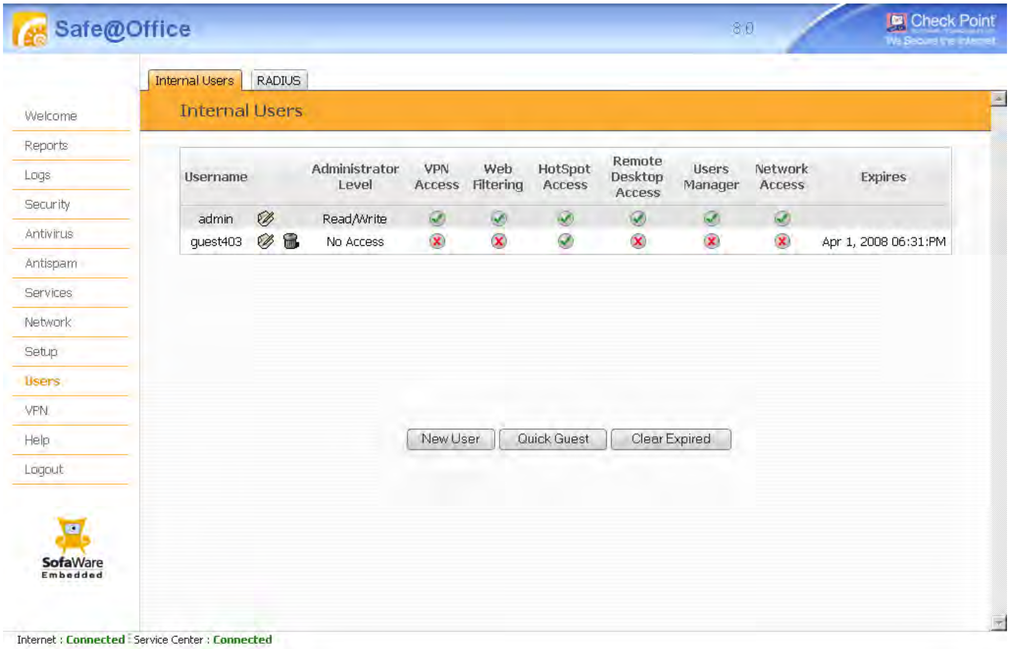
500

You can change your username and password at any time.

To change your login credentials

1. Click **Users** in the main menu, and click the **Internal Users** tab.

The **Internal Users** page appears.



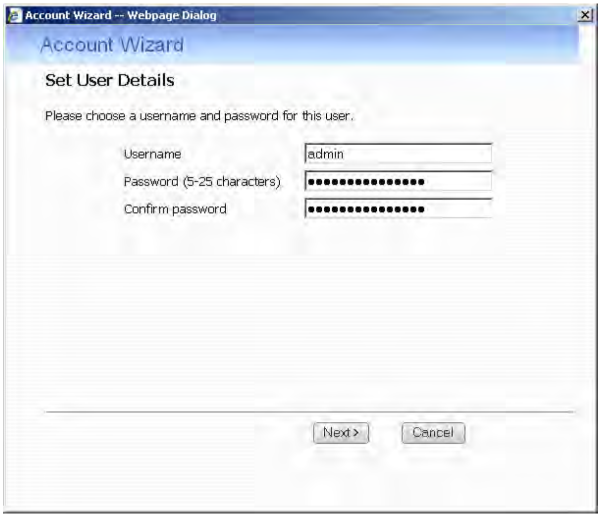
Internal Users

Username	Administrator Level	VPN Access	Web Filtering	HotSpot Access	Remote Desktop Access	Users Manager	Network Access	Expires
admin	Read/Write	✓	✓	✓	✓	✓	✓	
guest403	No Access	✗	✗	✓	✗	✗	✗	Apr 1, 2008 06:31:PM

Internet : Connected : Service Center : Connected

2. In the row of your username, click **Edit**.

The **Account Wizard** opens displaying the **Set User Details** dialog box.



Account Wizard -- Webpage Dialog

Account Wizard

Set User Details

Please choose a username and password for this user.

Username: admin

Password (5-25 characters): ●●●●●●●●●●●●●●●●

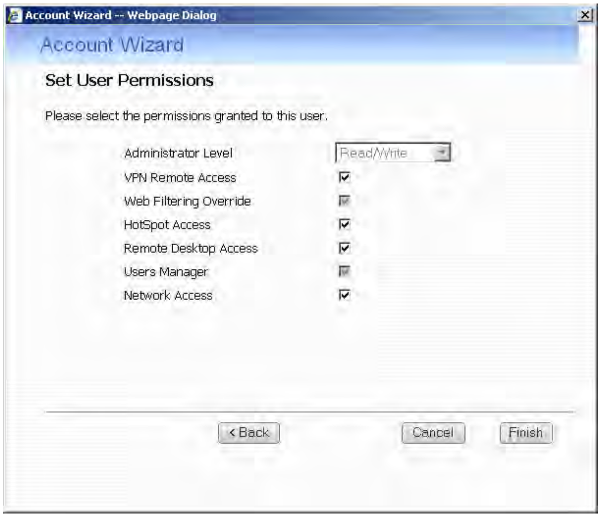
Confirm password: ●●●●●●●●●●●●●●●●

3. Edit the **Username** field.
4. Edit the **Password** and **Confirm password** fields.

Note: Use 5 to 25 characters (letters or numbers) for the new password.

5. Click **Next**.

The **Set User Permissions** dialog box appears.



Set User Permissions

Please select the permissions granted to this user.

Administrator Level	Read/Write
VPN Remote Access	☑
Web Filtering Override	☑
HotSpot Access	☑
Remote Desktop Access	☑
Users Manager	☑
Network Access	☑

6. Click **Finish**.

   Your changes are saved.

Adding and Editing Users

500

This procedure explains how to add and edit users.

For information on quickly adding guest HotSpot users via a shortcut that the Safe@Office appliance provides, see ***Adding Quick Guest HotSpot Users*** on page 647.

To add or edit a user

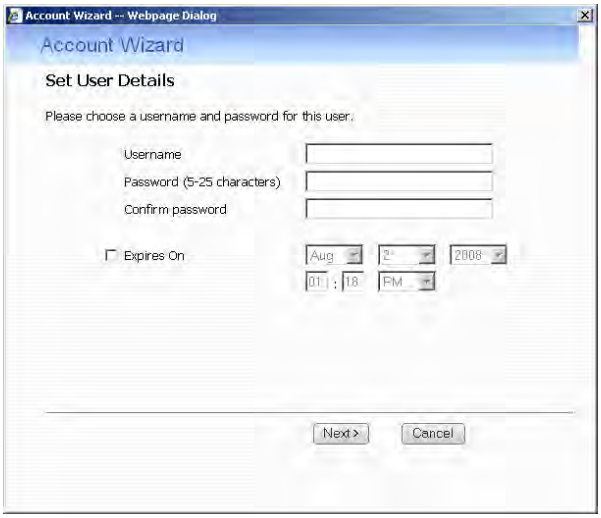
1. Click Users in the main menu, and click the Internal Users tab.

   The Internal Users page appears.

2. Do one of the following:

   - To create a new user, click New User.
   - To edit an existing user, click ✎ next to the desired user.

   The Account Wizard opens displaying the Set User Details dialog box.



Account Wizard -- Webpage Dialog

Account Wizard

Set User Details

Please choose a username and password for this user.

Username

Password (5-25 characters)

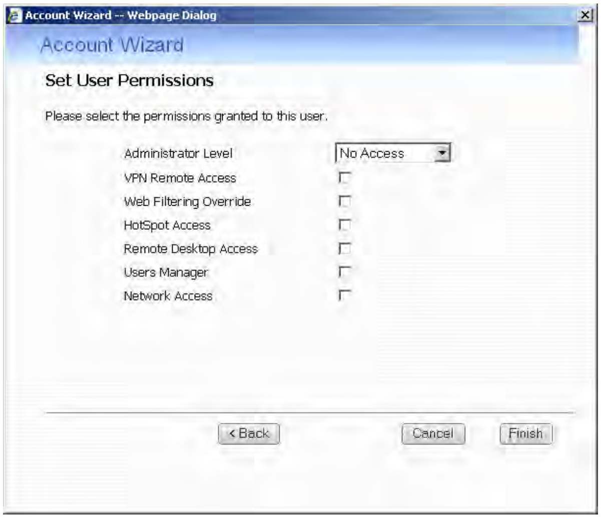
Confirm password

☐ Expires On Aug 2 2008 01 : 18 PM

3. Complete the fields using the information in ***Set User Details Fields*** on page 644.

4. Click **Next**.

   The **Set User Permissions** dialog box appears.



Account Wizard -- Webpage Dialog

Account Wizard

Set User Permissions

Please select the permissions granted to this user.

Administrator Level	No Access
VPN Remote Access	□
Web Filtering Override	□
HotSpot Access	□
Remote Desktop Access	□
Users Manager	□
Network Access	□

   The options that appear on the page are dependant on the software and services you are using.

5. Complete the fields using the information in ***Set User Permissions Fields*** on page 645.

6. Click **Finish**.

   The user is saved.

Table 131: Set User Details Fields

In this field…	Do this…
Username	Enter a username for the user.
Password	Enter a password for the user. Use five to 25 characters (letters or numbers) for the new password.
Confirm Password	Re-enter the user’s password.

In this field...	Do this...
Expires On	To specify an expiration time for the user, select this option and specify the expiration date and time in the fields provided. When the user account expires, it is locked, and the user can no longer log in to the Safe@Office appliance. If you do not select this option, the user will not expire.

Table 132: Set User Permissions Fields

In this field...	Do this...
Administrator Level	Select the user’s level of access to the Safe@Office Portal. The levels are: • No Access: The user cannot access the Safe@Office Portal. • Read Only: The user can log in to the Safe@Office Portal, but cannot modify system settings or export the appliance configuration via the Setup>Tools page. For example, you could assign this administrator level to technical support personnel who need to view the Event Log. • Read/Write: The user can log in to the Safe@Office Portal and modify system settings. The default level is No Access. The “admin” user’s Administrator Level (Read/Write) cannot be changed.
VPN Remote Access	Select this option to allow the user to connect to this Safe@Office appliance using their VPN client. For further information on setting up VPN remote access, see see ***Setting Up Remote VPN Access for Users*** on page 650

Web Filtering Override

Select this option to allow the user to override the Web Filtering service and Web rules.

This option cannot be changed for the “admin” user.

HotSpot Access

Select this option to allow the user to log in to the My HotSpot page.

For information on Secure HotSpot, see ***Configuring Secure HotSpot*** on page 380.

This option only appears in Safe@Office 500 with Power Pack.

Remote Desktop Access

Select this option to allow the user to log in to the my.firewall portal, view the Active Computers page, and remotely access computers' desktops, using the Remote Desktop feature.

Note: The user can perform these actions, even if their level of administrative access is "No Access".

For information on Remote Desktop, see ***Using Remote Desktop*** on page 661.

Users Manager

Select this option to allow the user to log in to the Safe@Office Portal and add, edit, or delete "No Access"-level users, but not modify other system settings.

For example, you could assign this administrator level to clerks who need to manage HotSpot users.

Network Access

Select this option to allow the user to connect to this Safe@Office appliance via a wireless client or by connecting to the appliance's ports, when the Safe@Office EAP authenticator is used.

For information on the Safe@Office EAP authenticator, see ***Using the Safe@Office EAP Authenticator*** on page 394.

Adding Quick Guest HotSpot Users

Power Pack

The Safe@Office appliance provides a shortcut for quickly adding a guest HotSpot user. This is useful in situations where you want to grant temporary network access to guests, for example in an Internet café. The shortcut also enables printing the guest user's details in one click.

By default, the quick guest user has the following characteristics:

- Username in the format `guest<number>`, where `<number>` is a unique three-digit number.

  For example: guest123
- Randomly generated password
- Expires in 24 hours
- Administration Level: No Access
- Permissions: HotSpot Access only

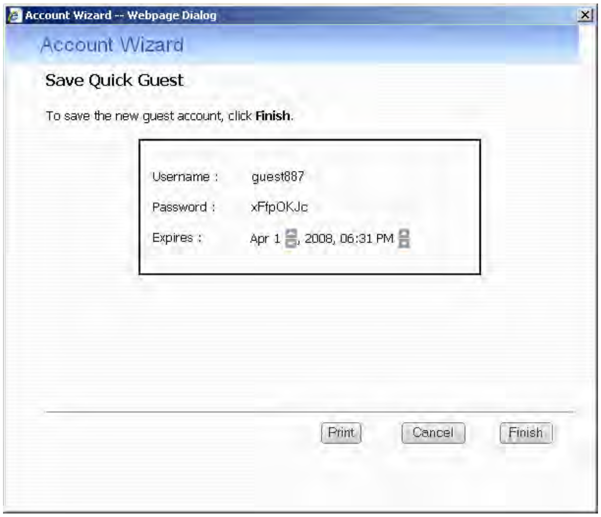
For information on configuring Secure HotSpot, see ***Using Secure HotSpot*** on page 380. For information on changing the default expiration period, refer to the *Embedded NGX CLI Reference Guide*.

To quickly create a guest user

1. Click Users in the main menu, and click the Internal Users tab.

   The Internal Users page appears.
2. Click Quick Guest.

The Account Wizard opens displaying the Save Quick Guest dialog box.



Account Wizard -- Webpage Dialog

Account Wizard

Save Quick Guest

To save the new guest account, click **Finish**.

Username : guest887

Password : xFfpOKJc

Expires : Apr 1, 2008, 06:31 PM

3. In the Expires field, click on the arrows to specify the expiration date and time.
4. To print the user details, click Print.
5. Click Finish.

   The guest user is saved.

   You can edit the guest user's details and permissions using the procedure ***Adding and Editing Users*** on page 643.

Viewing and Deleting Users

500

Note: The “admin” user cannot be deleted.

To view or delete users

1. Click **Users** in the main menu, and click the **Internal Users** tab.

   The **Internal Users** page appears with a list of all users and their permissions.

   The expiration time of expired users appears in red.

2. To delete a user, do the following:

   a) In the desired user’s row, click 🗑.

      A confirmation message appears.

   b) Click **OK**.

      The user is deleted.

3. To delete all expired users, do the following:

   a) Click **Clear Expired**.

      A confirmation message appears.

   b) Click **OK**.

      The expired users are deleted.

Setting Up Remote VPN Access for Users

500

If you are using your Safe@Office appliance as a SecuRemote Remote Access VPN Server, as an internal VPN Server, or as an L2TP VPN Server, you can allow users to access it remotely through their Remote Access VPN Clients (a Check Point SecureClient, Check Point SecuRemote, an L2TP VPN Client, or another Embedded NGX appliance).

To set up remote VPN access for a user

1. Enable your VPN Server, using the procedure ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 567.
2. Add or edit the user, using the procedure ***Adding and Editing Users*** on page 643.

   You must select the VPN Remote Access option.

Using RADIUS Authentication

500

You can use Remote Authentication Dial-In User Service (RADIUS) to authenticate both Safe@Office appliance users and Remote Access VPN Clients trying to connect to the Safe@Office appliance.

Note: When RADIUS authentication is in use, Remote Access VPN Clients must have a certificate.

When a user tries to log in to the Safe@Office Portal, the Safe@Office appliance sends the entered user name and password to the RADIUS server. The server then checks whether the RADIUS database contains a matching user name and password pair. If so, then the user is logged in.

By default, all RADIUS-authenticated users are assigned the set of permissions specified in the Safe@Office Portal's RADIUS page. However, you can configure the RADIUS server to pass the Safe@Office appliance a specific set of permissions to grant the authenticated user, instead of these default permissions. This is done by configuring the RADIUS

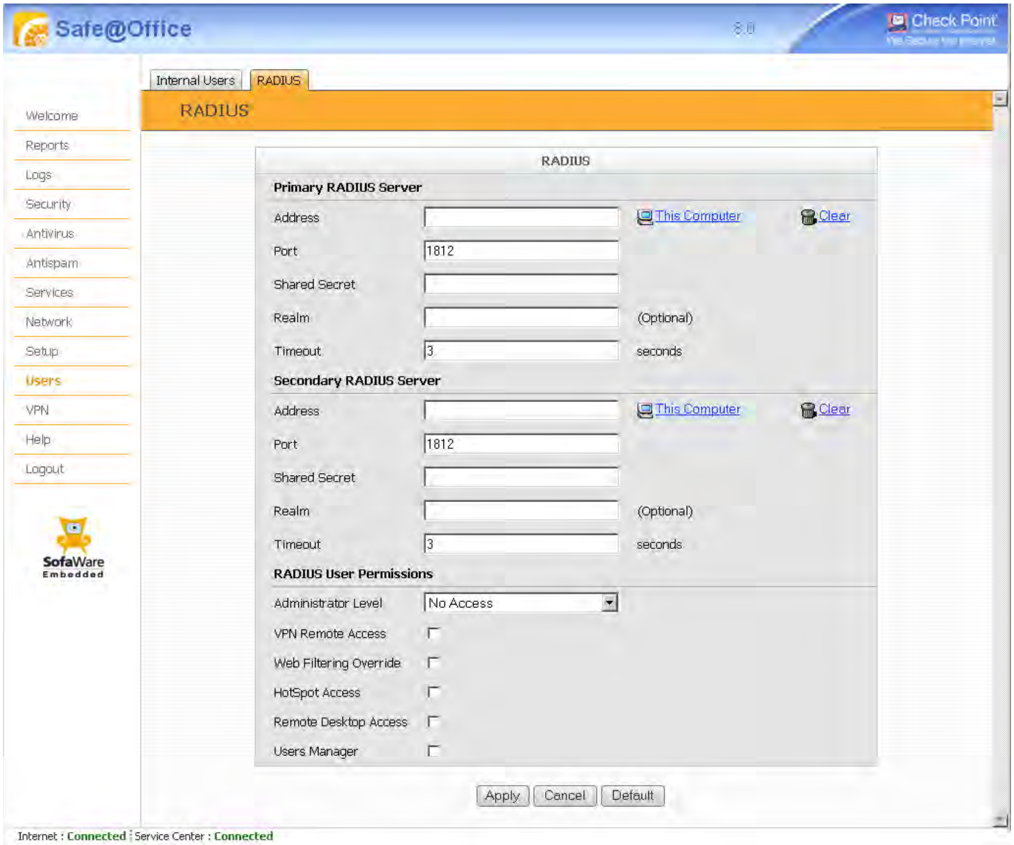
Vendor-Specific Attribute (VSA) with a set of attributes containing permission information for specific users. If the VSA is configured for a user, then the RADIUS server passes the VSA to the Safe@Office appliance as part of the response to the authentication request, and the gateway assigns the user permissions as specified in the VSA. If the VSA is not returned by the RADIUS server for a specific user, the gateway will use the default permission set for this user.

In addition, you can configure the RADIUS server to pass the Safe@Office appliance a Secure HotSpot session timeout value. When the RADIUS server's Session-Timeout Attribute is configured, HotSpot users will be logged out after the specified session timeout has elapsed.

To use RADIUS authentication

1. Click Users in the main menu, and click the RADIUS tab.

The **RADIUS** page appears.



RADIUS

Primary RADIUS Server

Address		This Computer	Clear
Port	1812		
Shared Secret			
Realm		(Optional)	
Timeout	3	seconds	

Secondary RADIUS Server

Address		This Computer	Clear
Port	1812		
Shared Secret			
Realm		(Optional)	
Timeout	3	seconds	

RADIUS User Permissions

Administrator Level	No Access
VPN Remote Access	□
Web Filtering Override	□
HotSpot Access	□
Remote Desktop Access	□
Users Manager	□

2. Complete the fields using the following table.
3. Click **Apply**.
4. To restore the default RADIUS settings, do the following:

    a) Click **Default**.

    A confirmation message appears.

    b) Click **OK**.

    The RADIUS settings are reset to their defaults. For information on the default values, refer to the following table.

5. If desired, configure user permissions and/or the HotSpot session timeout on the RADIUS server.

   See ***Configuring RADIUS Attributes*** on page 657.

Table 133: RADIUS Page Fields

In this field…	Do this…
Primary/Secondary RADIUS Server	Configure the primary and secondary RADIUS servers. By default, the Safe@Office appliance sends a request to the primary RADIUS server first. If the primary RADIUS server does not respond after three attempts, the Safe@Office appliance will send the request to the secondary RADIUS server.
Address	Type the IP address of the computer that will run the RADIUS service (one of your network computers) or click the corresponding This Computer button to allow your computer to host the service. To clear the text box, click Clear.
Port	Type the port number on the RADIUS server's host computer. The default port number is 1812.
Shared Secret	Type the shared secret to use for secure communication with the RADIUS server.

In this field…	Do this…
Realm	If your organization uses RADIUS realms, type the realm to append to RADIUS requests. The realm will be appended to the username as follows: <username>@<realm> For example, if you set the realm to “myrealm”, and the user "JohnS" attempts to log in to the Safe@Office Portal, the Safe@Office appliance will send the RADIUS server an authentication request with the username “JohnS@myrealm”. This field is optional.
Timeout	Type the interval of time in seconds between attempts to communicate with the RADIUS server. The default value is 3 seconds.
RADIUS User Permissions	If the RADIUS VSA (Vendor-Specific Attribute) is configured for a user, the fields in this area will have no effect, and the user will be granted the permissions specified in the VSA. If the VSA is not configured for the user, the permissions configured in this area will be used.

In this field…	Do this…
Administrator Level	Select the level of access to the Safe@Office Portal to assign to all users authenticated by the RADIUS server. The levels are: • No Access: The user cannot access the Safe@Office Portal. • Read Only: The user can log in to the Safe@Office Portal, but cannot modify system settings or export the appliance configuration via the Setup>Tools page. For example, you could assign this administrator level to technical support personnel who need to view the Event Log. • Read/Write: The user can log in to the Safe@Office Portal and modify system settings. The default level is No Access.
VPN Remote Access	Select this option to allow all users authenticated by the RADIUS server to connect to this Safe@Office appliance using their VPN client. For further information on setting up VPN remote access, see ***Setting Up Remote VPN Access for Users*** on page 650.
Web Filtering Override	Select this option to allow all users authenticated by the RADIUS server to override Web Filtering. This option only appears if the Web Filtering service is defined.
HotSpot Access	Select this option to allow all users authenticated by the RADIUS server to access the My HotSpot page. For information on Secure HotSpot, see ***Configuring Secure HotSpot*** on page 380. This option only appears in Safe@Office 500 with Power Pack.

In this field...	Do this...
Remote Desktop Access	Select this option to allow all users authenticated by the RADIUS server to log in to the my.firewall portal, view the Active Computers page, and remotely access computers' desktops, using the Remote Desktop feature. Note: Authenticated users can perform these actions, even if their level of administrative access is "No Access". For information on Remote Desktop, see ***Using Remote Desktop*** on page 661.
Users Manager	Select this option to allow all users authenticated by the RADIUS server to log in to the Safe@Office Portal and add, edit, or delete "No Access"-level users, but not modify other system settings. For example, you could assign this administrator level to clerks who need to manage HotSpot users.

Configuring RADIUS Attributes

500

To define a timeout for Secure HotSpot sessions

- Set the Session-Timeout Attribute (attribute 27) to the number of seconds after which users should be automatically logged out from the hotspot.

To assign permissions to specific RADIUS-authenticated users

1. Create a remote access policy as follows:

   a) Assign the policy's VSA (attribute 26) the SofaWare vendor code (6983).

   b) For each permission you want to grant, configure the relevant attribute of the VSA with the desired value, as described in the following table.

   For example, to assign the user VPN access permissions, set attribute number 2 to "true".

2. Assign the policy to the desired user or user group.

For detailed instructions and examples, refer to the "Configuring the RADIUS Vendor-Specific Attribute" white paper.

Table 134: VSA Syntax

Permission	Description	Attribute Number	Attribute Format	Attribute Values	Notes
Admin	Indicates the administrator's level of access to the Safe@Office Portal	1	String	none. The user cannot access the Safe@Office Portal. readonly. The user can log in to the Safe@Office Portal, but cannot modify system settings. users-manager. The user can log in to the Safe@Office Portal and add, edit, or delete "No Access"-level users. However, the user cannot modify other system settings. readwrite. The user can log in to the Safe@Office Portal and modify system settings.	

Permission	Description	Attribute Number	Attribute Format	Attribute Values	Notes
VPN	Indicates whether the user can access the network from a Remote Access VPN Client.	2	String	true. The user can remotely access the network via VPN. false. The user cannot remotely access the network via VPN.	This permission is only relevant if the Safe@Office Remote Access VPN Server is enabled. The gateway must have a certificate.
Hotspot	Indicates whether the user can log in via the My HotSpot page.	3	String	true. The user can access the Internet via My HotSpot. false. The user cannot access the Internet via My HotSpot.	This permission is only relevant if the Secure HotSpot feature is enabled.
UFP	Indicates whether the user can override Web Filtering.	4	String	true. The user can override Web Filtering. false. The user cannot override Web Filtering.	This permission is only relevant if the Web Filtering service is enabled.

Permission	Description	Attribute Number	Attribute Format	Attribute Values	Notes
RemoteDesktop	Indicates whether the user can remotely access computers' desktops, using the Remote Desktop feature.	5	String	true. The user can log in to the my.firewall portal, view the Active Computers page, and remotely access computers' desktops (irrespective of their level of administrative access). false. The user cannot remotely access computers' desktops.	This permission is only relevant if the Remote Desktop feature is enabled.

Chapter 21

Using Remote Desktop

This chapter describes how to remotely access the desktop of each of your computers, using the Safe@Office appliance's Remote Desktop feature.

This chapter includes the following topics:

Overview

500

Your Safe@Office appliance includes an integrated client for Microsoft Terminal Services, allowing you to remotely access the desktop of each of your computers from anywhere, via the Safe@Office Portal. You can even redirect your printers or ports to a remote computer, so that you can print and transfer files with ease.

Remote Desktop sessions use the Microsoft Remote Desktop Protocol (RDP) on TCP port 3389. This port is opened dynamically between the Remote Desktop client and the Remote Desktop server as needed, meaning that the port is not exposed to the Internet, and your constant security is ensured.

Note: By default, the Microsoft RDP protocol is secured with 128-bit RC4 encryption. For the strongest possible security, it is recommended to use Remote Desktop over an IPSec VPN connection. For information on VPNs, see ***Working With VPNs*** on page 561.

Workflow

500

To use Remote Desktop

1. Configure Remote Desktop.

   See ***Configuring Remote Desktop*** on page 663.

2. Enable the Remote Desktop server on computers that authorized users should be allowed to remotely access.

   See ***Configuring the Host Computer*** on page 666.

3. Grant Remote Desktop Access permissions to users who should be allowed to remotely access desktops.

   See ***Adding and Editing Users*** on page 643.

4. The authorized users can access remote computers' desktops as desired.

   See ***Accessing a Remote Computer's Desktop*** on page 669.

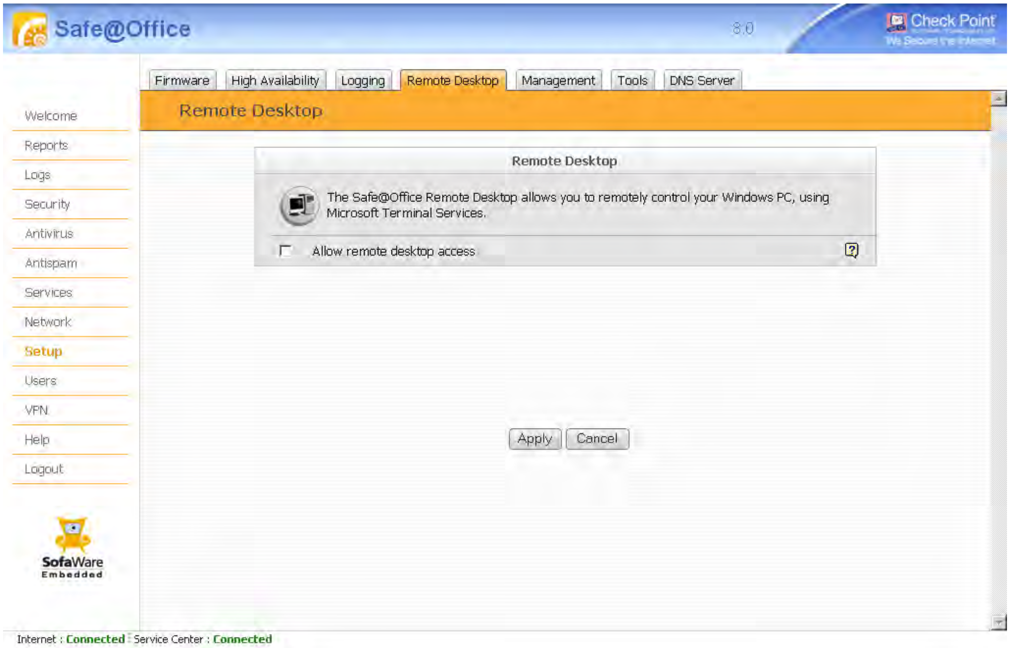
Configuring Remote Desktop

500

To configure Remote Desktop

1. Click **Setup** in the main menu, and click the **Remote Desktop** tab.

   The **Remote Desktop** page appears.



Remote Desktop

The Safe@Office Remote Desktop allows you to remotely control your Windows PC, using Microsoft Terminal Services.

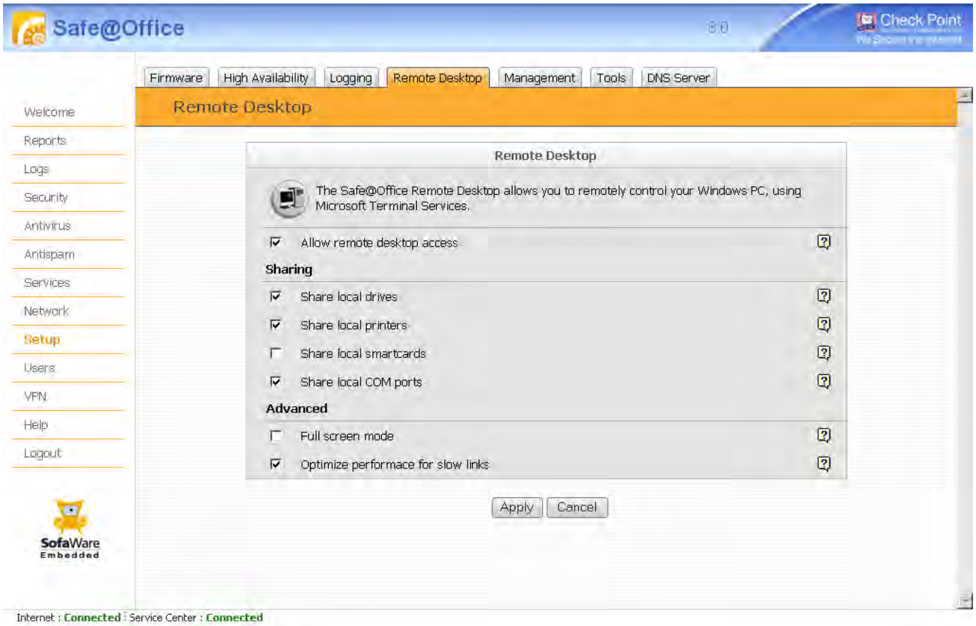
☐ Allow remote desktop access

Internet : Connected Service Center : Connected

2. Do one of the following:

   - To enable Remote Desktop, select the **Allow remote desktop access** check box.

New fields appear.



Remote Desktop

Remote Desktop

The Safe@Office Remote Desktop allows you to remotely control your Windows PC, using Microsoft Terminal Services.

☑ Allow remote desktop access

Sharing

☑ Share local drives

☑ Share local printers

□ Share local smartcards

☑ Share local COM ports

Advanced

□ Full screen mode

☑ Optimize performace for slow links

Internet : Connected Service Center : Connected

- To disable Remote Desktop, clear the **Allow remote desktop access** check box.

  Fields disappear.

3. Complete the fields using the information in the following table.
4. Click **Apply**.

Table 135: Remote Desktop Options

In this field...	Do this...
Sharing	
Share local drives	Select this option to allow the host computer to access hard drives on the client computer. This enables remote users to access their local hard drives when logged in to the host computer.
Share local printers	Select this option to allow the host computer to access printers on the client computer. This enables remote users to access their local printer when logged in to the host computer.
Share local smartcards	Select this option to allow the host computer to access smartcards on the client computer. This enables remote users to access their local smartcards when logged in to the host computer.
Share local COM ports	Select this option to allow the host computer to access COM ports on the client computer. This enables remote users to access their local COM ports when logged in to the host computer.
Advanced	
Full screen mode	Select this option to open Remote Desktop sessions on the whole screen.
Optimize performance for slow links	Select this option to optimize Remote Desktop sessions for slow links. Bandwidth-consuming options, such as wallpaper and menu animations, will be disabled.

Configuring the Host Computer

To enable remote users to connect to a computer, you must enable the Remote Desktop server on that computer.

Note: The host computer must have one of the following operating systems installed:

- Microsoft Windows Server 2003
- Microsoft Windows XP Professional
- Microsoft Windows XP Media Center
- Microsoft Windows XP Tablet PC 2005

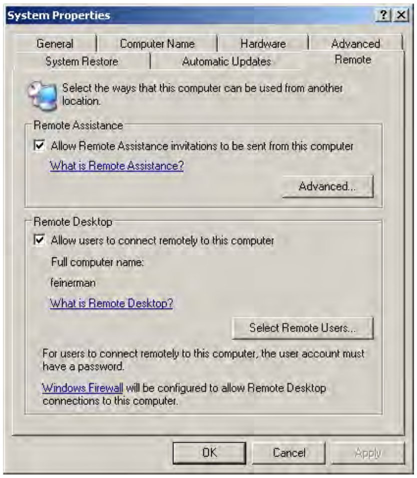
To enable users to remotely connect to a computer

1. Log on to the desired computer as an administrator.
2. For each remote user who should be allowed to access this computer, create a user account with a password.

   For information, refer to Microsoft documentation.
3. On the desktop, right-click on **My Computer**, and select **Properties** in the pop-up menu that appears.

   The **System Properties** dialog box appears displaying the **General** tab.
4. Click the **Remote** tab.

The **Remote** tab appears.



Select the ways that this computer can be used from another location.

Remote Assistance

☑ Allow Remote Assistance invitations to be sent from this computer

What is Remote Assistance?

Remote Desktop

☑ Allow users to connect remotely to this computer

Full computer name:

feinerman

What is Remote Desktop?

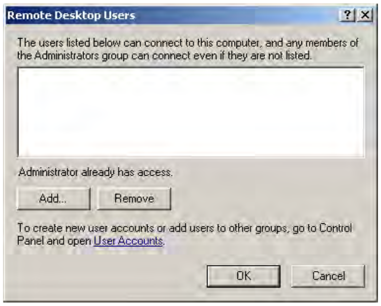
For users to connect remotely to this computer, the user account must have a password.

Windows Firewall will be configured to allow Remote Desktop connections to this computer.

5. Select the **Allow users to connect remotely to this computer** check box.

6. Click **Select Remote Users.**

   The **Remote Desktop Users** dialog box appears.



The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

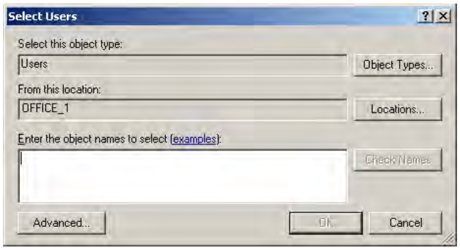
Administrator already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

7. Do the following for each remote user who should be allowed to access this computer:

   a. Click **Add.**

The **Select Users** dialog box appears.



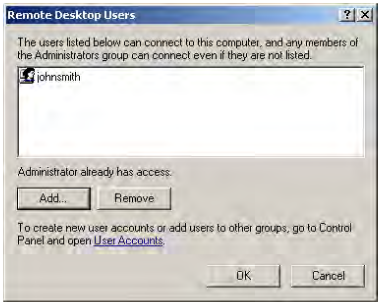
b. Type the desired user's username in the text box.

The **Check Names** button is enabled.

c. Click **Check Names**.

d. Click **OK**.

The **Remote Desktop Users** dialog box reappears with the desired user's username.



The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

johnsmith

Administrator already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

8. Click **OK**.
9. Click **OK**.

Accessing a Remote Computer's Desktop

500

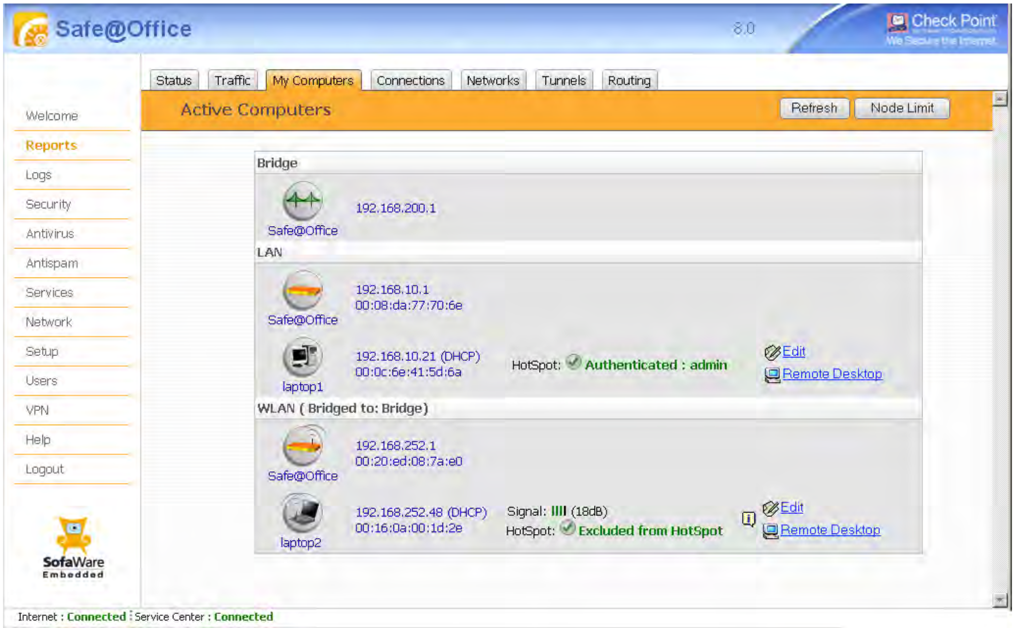
Note: The client computer must meet the following requirements:

- Microsoft Internet Explorer 6.0 or later
- A working Internet connection

To access a remote computer's desktop

1. Click **Reports** in the main menu, and click the **My Computers** tab.

   The **My Computers** page appears.



Bridge

Safe@Office 192.168.200.1

LAN

Safe@Office 192.168.10.1 00:08:da:77:70:6e

laptop1 192.168.10.21 (DHCP) 00:0c:6e:41:5d:6a HotSpot: ✓ Authenticated : admin Edit Remote Desktop

WLAN (Bridged to: Bridge)

Safe@Office 192.168.252.1 00:20:ed:08:7a:e0

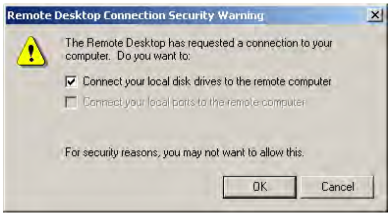
laptop2 192.168.252.48 (DHCP) 00:16:0a:00:1d:2e Signal: IIII (18dB) HotSpot: ✓ Excluded from HotSpot Edit Remote Desktop

Internet : Connected | Service Center : Connected

2. Next to the desired computer, click **Remote Desktop**.

   The following things happen:

- If you are prompted to install the Remote Desktop Active X Control, then install it.
- The Remote Desktop Connection Security Warning dialog box appears.



Remote Desktop Connection Security Warning

The Remote Desktop has requested a connection to your computer. Do you want to:

☑ Connect your local disk drives to the remote computer

☐ Connect your local ports to the remote computer

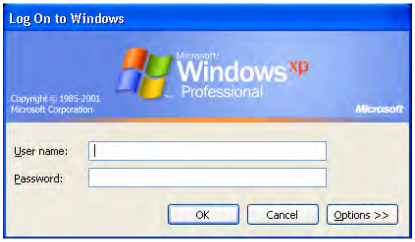
For security reasons, you may not want to allow this.

3. Select the desired connection options.

   The available options depend on your Remote Desktop configuration. See ***Configuring Remote Desktop*** on page 663.

4. Click OK.

   The Log On to Windows dialog box appears.



Log On to Windows

5. Type your username and password for the remote computer.

   These are the credentials configured for your user account in ***Enabling the Remote Desktop Server*** on page 666.

6. Click OK.

   The remote computer's desktop appears onscreen.

You can use the following keyboard shortcuts during the Remote Desktop session:

Table 136: Remote Desktop Keyboard Shortcuts

This shortcut…	Does this…
ALT+INSERT	Cycles through running programs in the order that they were started
ALT+HOME	Displays the Start menu
CTRL+ALT+BREAK	Toggles between displaying the session in a window and on the full screen
CTRL+ALT+END	Opens the Windows Security dialog box

Chapter 22

Controlling the Appliance via the Command Line

This chapter describes various ways of controlling your Safe@Office appliance through the command line.

This chapter includes the following topics:

Overview

500

Depending on your Safe@Office model, you can control your appliance via the command line in the following ways:

- Using the Safe@Office Portal's command line interface.

  See ***Using the Safe@Office Portal*** on page 674.

- Using a console connected to the Safe@Office appliance.

  For information, see ***Using the Serial Console*** on page 676.

- Using an SSH client.

  See ***Configuring SSH*** on page 679.

Using the Safe@Office Portal

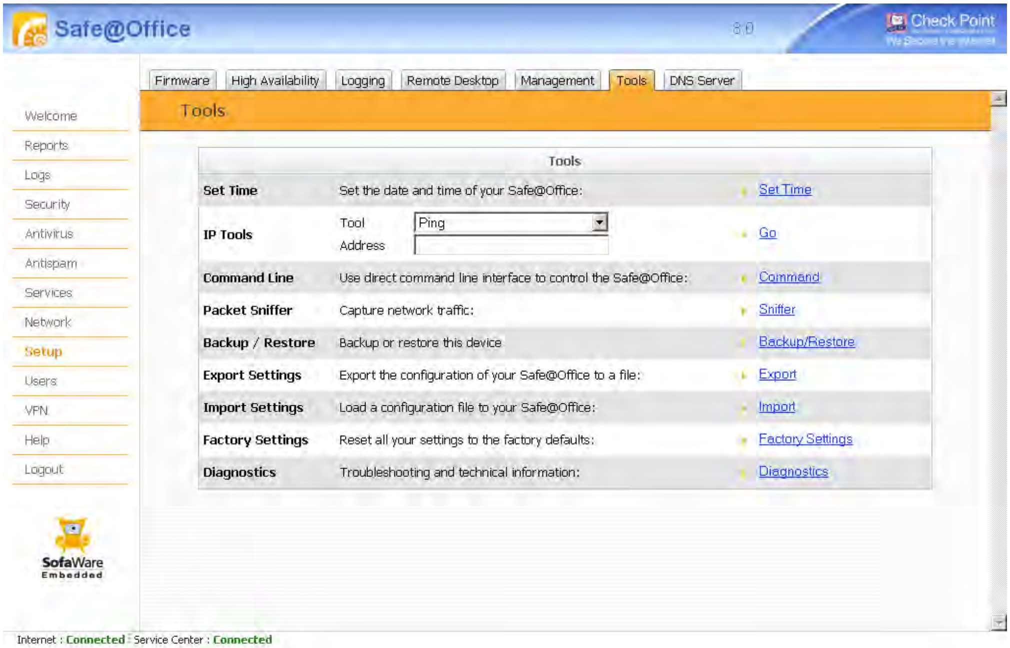
500

You can control your appliance via the Safe@Office Portal's command line interface.

To control the appliance via the Safe@Office Portal

1. Click **Setup** in the main menu, and click the **Tools** tab.

   The **Tools** page appears.



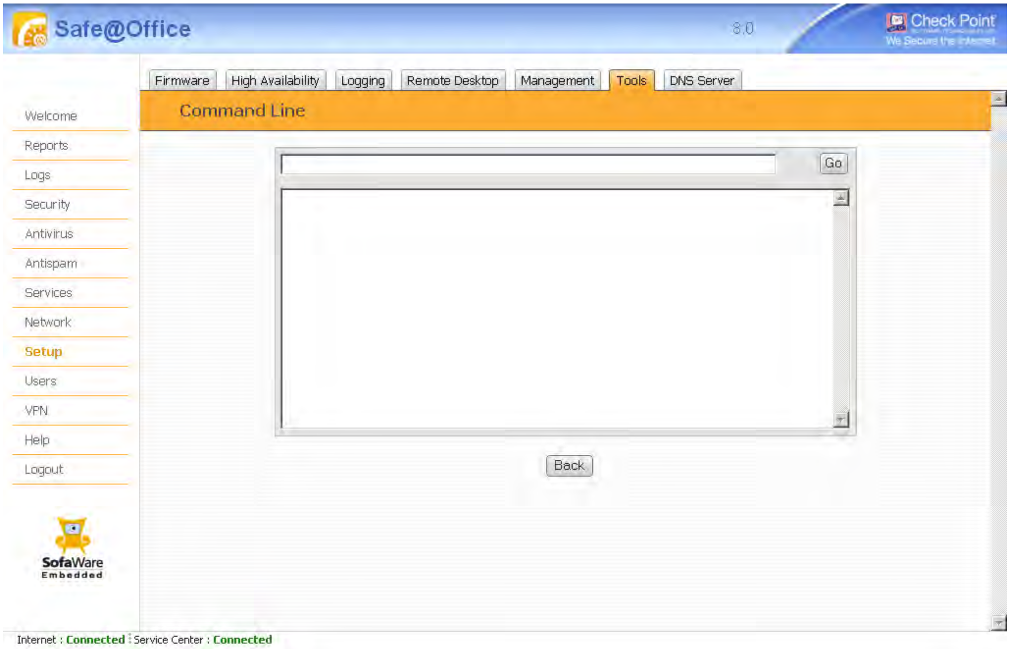
Tools

Tools		
Set Time	Set the date and time of your Safe@Office:	Set Time
IP Tools	Tool: Ping Address:	Go
Command Line	Use direct command line interface to control the Safe@Office:	Command
Packet Sniffer	Capture network traffic:	Sniffer
Backup / Restore	Backup or restore this device	Backup/Restore
Export Settings	Export the configuration of your Safe@Office to a file:	Export
Import Settings	Load a configuration file to your Safe@Office:	Import
Factory Settings	Reset all your settings to the factory defaults:	Factory Settings
Diagnostics	Troubleshooting and technical information:	Diagnostics

Internet : Connected | Service Center : Connected

2. Click **Command**.

The **Command Line** page appears.



3. In the upper field, type a command.

   You can view a list of supported commands using the command **help**.

   For information on all commands, refer to the *Embedded NGX CLI Reference Guide*.

4. Click **Go**.

   The command is implemented.

Using the Serial Console

500

You can connect a console to the Safe@Office appliance, and use the console to control the appliance via the command line.

Note: Your terminal emulation software and your Safe@Office appliance's Serial port must be configured for the same speed.

By default, the appliance's Serial port's speed is 57600 bps. For information on changing the Serial port's speed, refer to the *Embedded NGX CLI Reference Guide*.

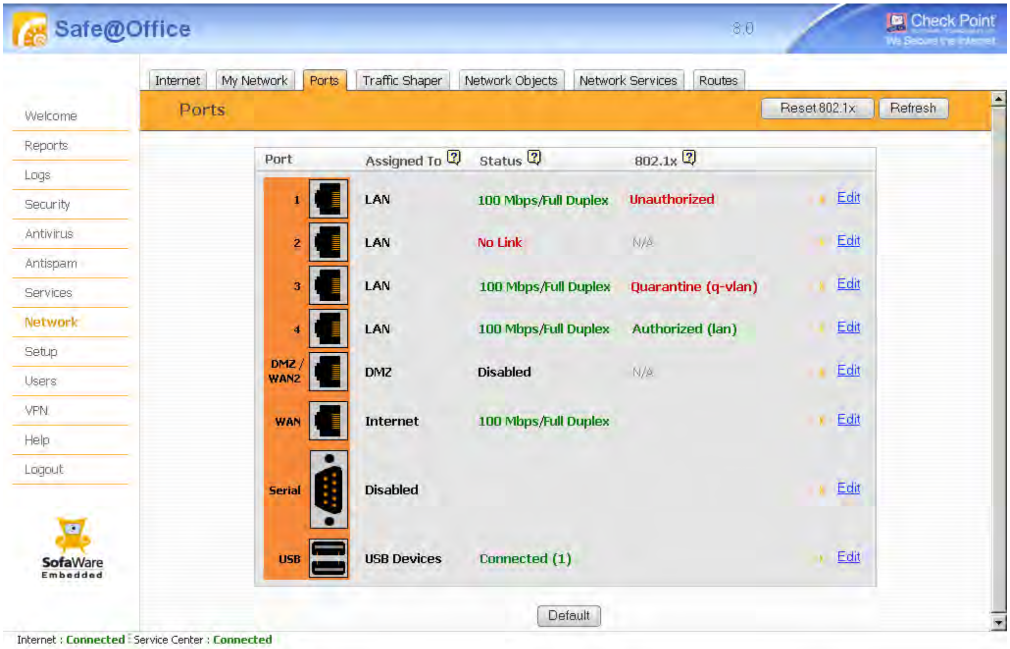
To control the appliance via a console

1. Connect the serial console to your Safe@Office appliance's Serial port, using an RS-232 Null modem cable.

   For information on locating the Serial port, see Rear Panel.

2. Click **Network** in the main menu, and click the **Ports** tab.

The **Ports** page appears.

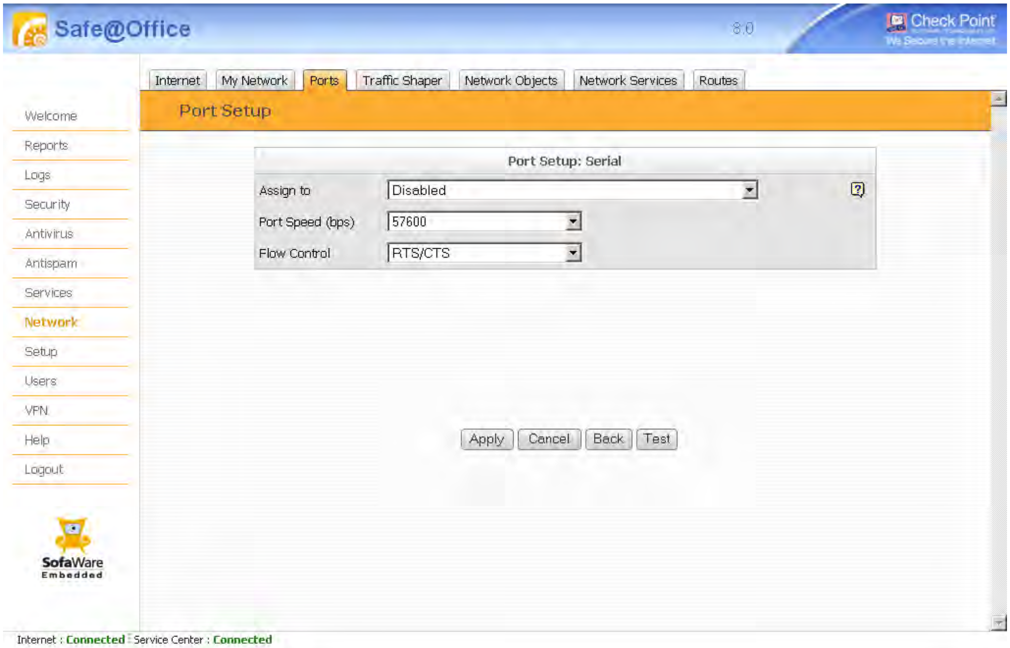


Port	Assigned To	Status	802.1x	
1	LAN	100 Mbps/Full Duplex	Unauthorized	Edit
2	LAN	No Link	N/A	Edit
3	LAN	100 Mbps/Full Duplex	Quarantine (q-vlan)	Edit
4	LAN	100 Mbps/Full Duplex	Authorized (lan)	Edit
DMZ / WAN2	DMZ	Disabled	N/A	Edit
WAN	Internet	100 Mbps/Full Duplex		Edit
Serial	Disabled			Edit
USB	USB Devices	Connected (1)		Edit

Internet : Connected : Service Center : Connected

3. Next to the **Serial** port, click **Edit**.

The **Port Setup** page appears.



Port Setup

Port Setup: Serial

Assign to: Disabled

Port Speed (bps): 57600

Flow Control: RTS/CTS

Internet : Connected Service Center : Connected

4. In the **Assign to** drop-down list, select **Console**.
5. In the **Port Speed** drop-down list, select the Serial port's speed (in bits per second).

   The Serial port's speed must match that of the attached serial console. The default value is 57600.
6. In the **Flow Control** drop-down list, select the method of flow control supported by the attached device:

   - **RTS/CTS**. Hardware-based flow control, using the Serial port's RTS/CTS lines.
   - **XON/XOFF**. Software-based flow control, using XON/XOFF characters.
7. Click **Apply**.

   You can now control the Safe@Office appliance from the serial console.

   For information on all supported commands, refer to the *Embedded NGX CLI Reference Guide*.

Configuring SSH

500

Safe@Office appliance users can control the appliance via the command line, using the SSH (Secure Shell) management protocol. You can enable users to do so via the Internet, by configuring remote SSH access. You can also integrate the Safe@Office appliance with SSH-based management systems.

Note: The Safe@Office appliance supports SSHv2 clients only. The SSHv1 protocol contains security vulnerabilities and is not supported.

Note: Configuring SSH is equivalent to creating a simple Allow rule, where the destination is This Gateway. To create more complex rules for SSH, such as allowing SSH connections from multiple IP address ranges, define Allow rules for TCP port 22, with the destination This Gateway. For information, see ***Using Rules*** on page 360.

To configure SSH

1. Click Setup in the main menu, and click the Management tab.

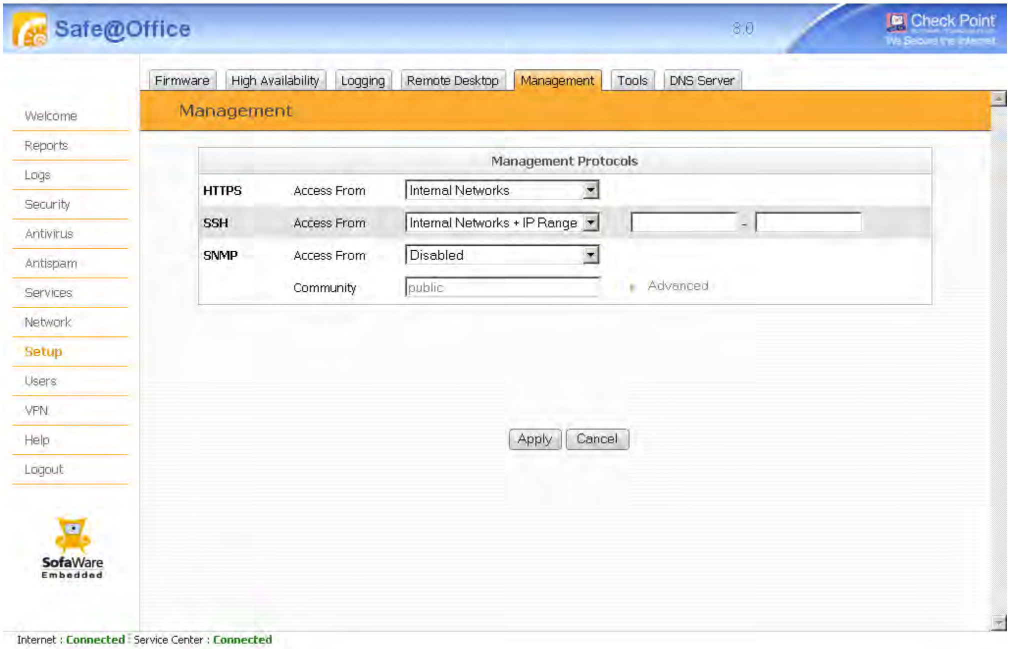
   The Management page appears.

2. Specify from where SSH access should be granted.

   Refer to the following table.

Warning: If remote SSH is enabled, your Safe@Office appliance settings can be changed remotely, so it is especially important to make sure all Safe@Office appliance users' passwords are difficult to guess.

If you selected **Internal Networks + IP Range**, additional fields appear.



Management

Management Protocols

HTTPS	Access From	Internal Networks	
SSH	Access From	Internal Networks + IP Range	-
SNMP	Access From	Disabled	
	Community	public	Advanced

3. If you selected **Internal Networks + IP Range**, enter the desired IP address range in the fields provided.

4. Click **Apply**.

   The SSH configuration is saved. If you configured remote SSH access, you can now control the Safe@Office appliance from the Internet, using an SSHv2 client.

   For information on all supported commands, refer to the *Embedded NGX CLI Reference Guide*.

Table 137: SSH Access Options

Select this option…	To allow access from…
Internal Networks	The internal network only. This disables remote access capability. This is the default.
Internal Networks + VPN	The internal network and your VPN.
Internal Networks + IP Range	A particular range of IP addresses. Additional fields appear, in which you can enter the desired IP address range.
ANY	Any IP address.
Disabled	Nowhere. This disables both local and remote access capability. This option is relevant to the SNMP protocol only.

Chapter 23

Maintenance

This chapter describes the tasks required for maintenance and diagnosis of your Safe@Office appliance.

This chapter includes the following topics:

Viewing Firmware Status

500

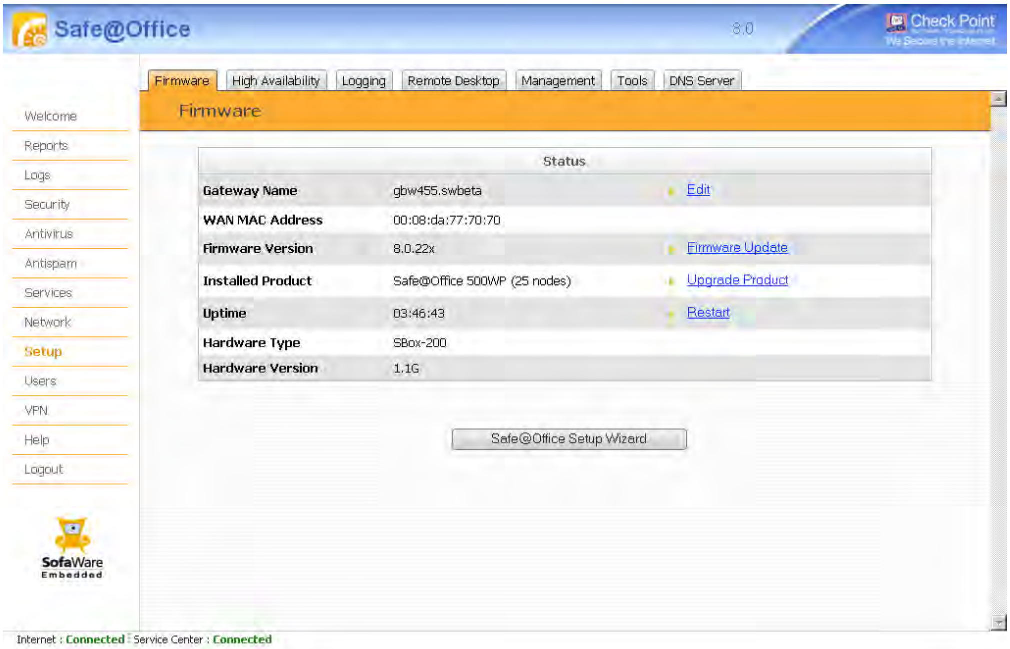
The firmware is the software program embedded in the Safe@Office appliance.

You can view your current firmware version and additional details.

To view the firmware status

- Click Setup in the main menu, and click the Firmware tab.

The **Firmware** page appears.



Status		
Gateway Name	gbw455.swbeta	Edit
WAN MAC Address	00:08:da:77:70:70	
Firmware Version	8.0.22x	Firmware Update
Installed Product	Safe@Office 500WP (25 nodes)	Upgrade Product
Uptime	03:46:43	Restart
Hardware Type	SBox-200	
Hardware Version	1.1G	

Internet : Connected | Service Center : Connected

The **Firmware** page displays the following information:

Table 138: Firmware Status Fields

This field…	Displays…	For example…
WAN MAC Address	The MAC address used for the Internet connection	00:80:11:22:33:44
Firmware Version	The current version of the firmware	7.5
Installed Product	The licensed software and the number of allowed nodes	Safe@Office 500 (unlimited nodes)

This field...	Displays...	For example...
Uptime	The time that elapsed from the moment the unit was turned on	01:21:15
Hardware Type	The type of the current Safe@Office appliance hardware	SBox-200
Hardware Version	The current hardware version of the Safe@Office appliance	1.0

Upgrading Your Software Product

500

You can upgrade your Safe@Office 500 appliance by adding the Safe@Office 500 Power Pack. After purchasing the Power Pack, you will receive a new Product Key that enables you to use the Power Pack on the same Safe@Office appliance you have today. There is no need to replace your hardware. You can also purchase node upgrades, as needed.

Note: To purchase the Power Pack or node upgrades, contact your Safe@Office appliance provider. Alternatively, you can click Upgrades & Services in the Welcome page to view and purchase available upgrades.

To upgrade your product, you must install the new Product Key.

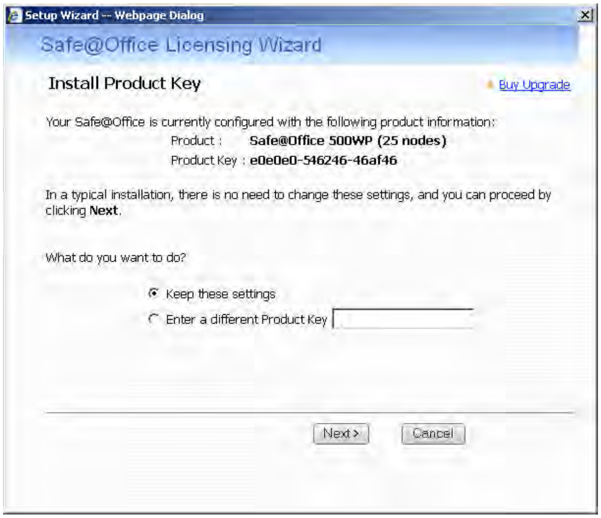
To install a Product Key

1. Click Setup in the main menu, and click the Firmware tab.

   The Firmware page appears.

2. Click Upgrade Product.

The **Safe@Office Licensing Wizard** opens, with the **Install Product Key** dialog box displayed.



Setup Wizard -- Webpage Dialog

Safe@Office Licensing Wizard

Install Product Key

Your Safe@Office is currently configured with the following product information:
Product : **Safe@Office 500WP (25 nodes)**
Product Key : **e0e0e0-546246-46af46**

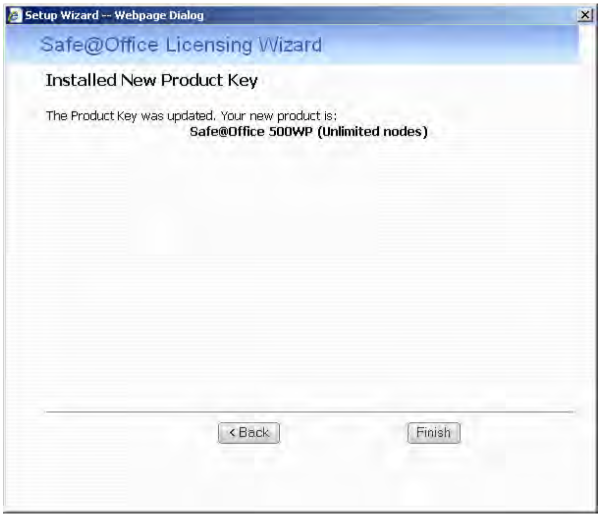
In a typical installation, there is no need to change these settings, and you can proceed by clicking **Next**.

What do you want to do?

● Keep these settings
○ Enter a different Product Key

3. Click **Enter a different Product Key**.
4. In the **Product Key** field, enter the new Product Key.
5. Click **Next**.

The **Installed New Product Key** dialog box appears.



Setup Wizard -- Webpage Dialog

Safe@Office Licensing Wizard

Installed New Product Key

The Product Key was updated. Your new product is:
Safe@Office 500WP (Unlimited nodes)

6. Click **Finish**.

Configuring a Gateway Hostname

500

You can define a gateway hostname for the Safe@Office appliance. The gateway hostname is used to identify the Safe@Office appliance and appears in the following places:

- The Safe@Office Portal’s title bar
- The Safe@Office appliance's SNMP hostname
- Syslog messages sent by the Safe@Office appliance
- The command line prompt

By default, the Safe@Office appliance's MAC address is used as the gateway hostname.

Note: Configuring the gateway hostname is only available if the Safe@Office is not subscribed to the Remote Management service. When remotely managed, the gateway hostname is set by the Service Center.

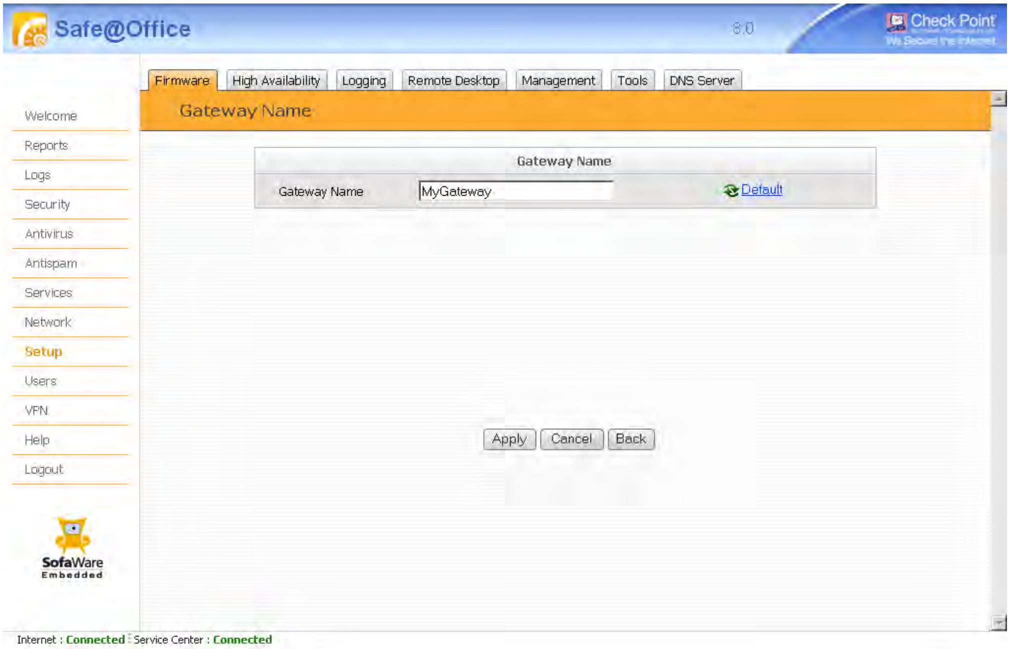
To configure the gateway hostname

1. Click **Setup** in the main menu, and click the **Firmware** tab.

   The **Firmware** page appears.

2. In the **Gateway Name** row, click **Edit**.

The **Gateway Name** page appears.



Gateway Name

Gateway Name

Gateway Name: MyGateway

Internet : Connected | Service Center : Connected

3. In the **Gateway Name** field, type the desired hostname.
4. To reset the gateway hostname to the default value (the appliance's MAC address), click **Default**.
5. Click **Apply**.

Configuring Syslog Logging

500

You can configure the Safe@Office appliance to send event logs to a Syslog server residing in your internal network or on the Internet. The logs detail the date and the time each event occurred. If the event is a communication attempt that was rejected by the firewall, the event details include the source and destination IP address, the destination port, and the protocol used for the communication attempt (for example, TCP or UDP).

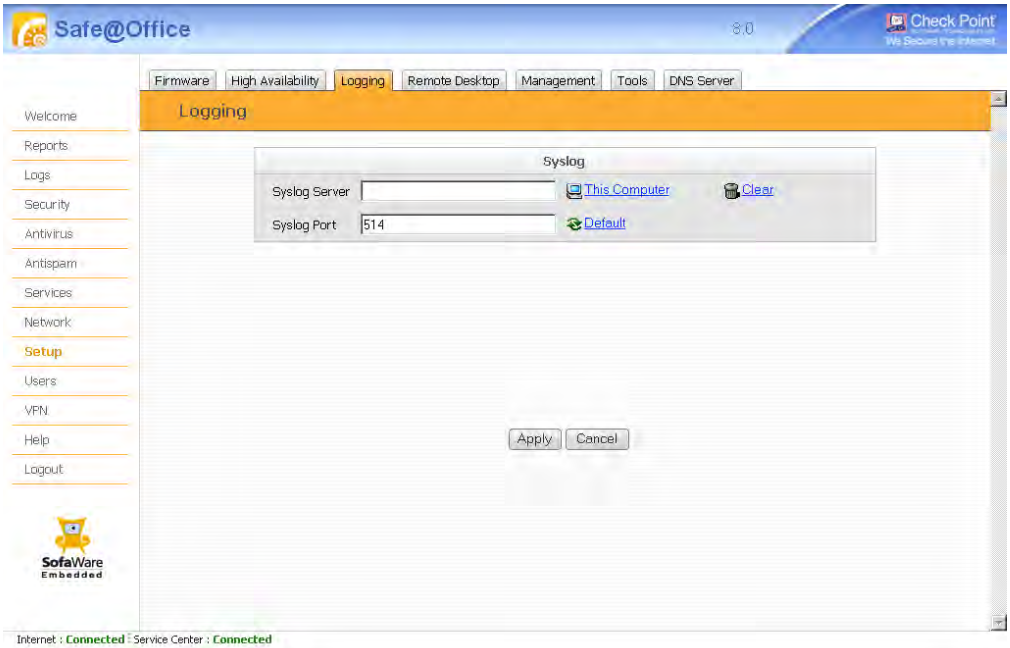
This same information is also available in the Event Log page (see ***Viewing the Event Log*** on page 339). However, while the Event Log can display hundreds of logs, a Syslog server can store an unlimited number of logs. Furthermore, Syslog servers can provide useful tools for managing your logs.

Note: Kiwi Syslog Daemon is freeware and can be downloaded from http://www.kiwisyslog.com. For technical support, contact Kiwi Enterprises.

To configure Syslog logging

1. Click Setup in the main menu, and click the Logging tab.

The **Logging** page appears.



Logging

Syslog

Syslog Server:

Syslog Port: 514

Internet : Connected Service Center : Connected

2. Complete the fields using the information in the following table.
3. Click **Apply**.

Table 139: Logging Page Fields

In this field…	Do this…
Syslog Server	Type the IP address of the computer that will run the Syslog service (one of your network computers), or click **This Computer** to allow your computer to host the service.
Clear	Click to clear the **Syslog Server** field.
Syslog Port	Type the port number of the Syslog server.
Default	Click to reset the **Syslog Port** field to the default (port 514 UDP).

Configuring HTTPS

500

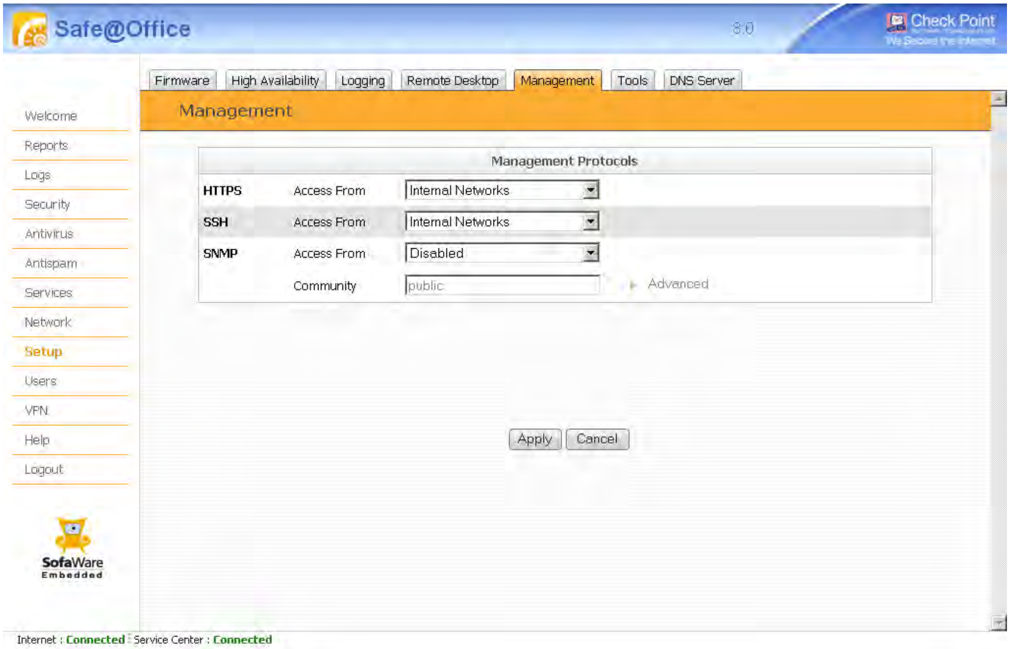
You can enable Safe@Office appliance users to access the Safe@Office Portal from the Internet. To do so, you must first configure HTTPS.

Note: Configuring HTTPS is equivalent to creating a simple Allow rule, where the destination is This Gateway. To create more complex rules for HTTPS, such as allowing HTTPS connections from multiple IP address ranges, define Allow rules for TCP port 443, with the destination This Gateway. For information, see ***Using Rules*** on page 360.

To configure HTTPS

1. Click Setup in the main menu, and click the Management tab.

   The Management page appears.



Management

Management Protocols		
HTTPS	Access From	Internal Networks
SSH	Access From	Internal Networks
SNMP	Access From	Disabled
	Community	public

Advanced

Internet : Connected : Service Center : Connected

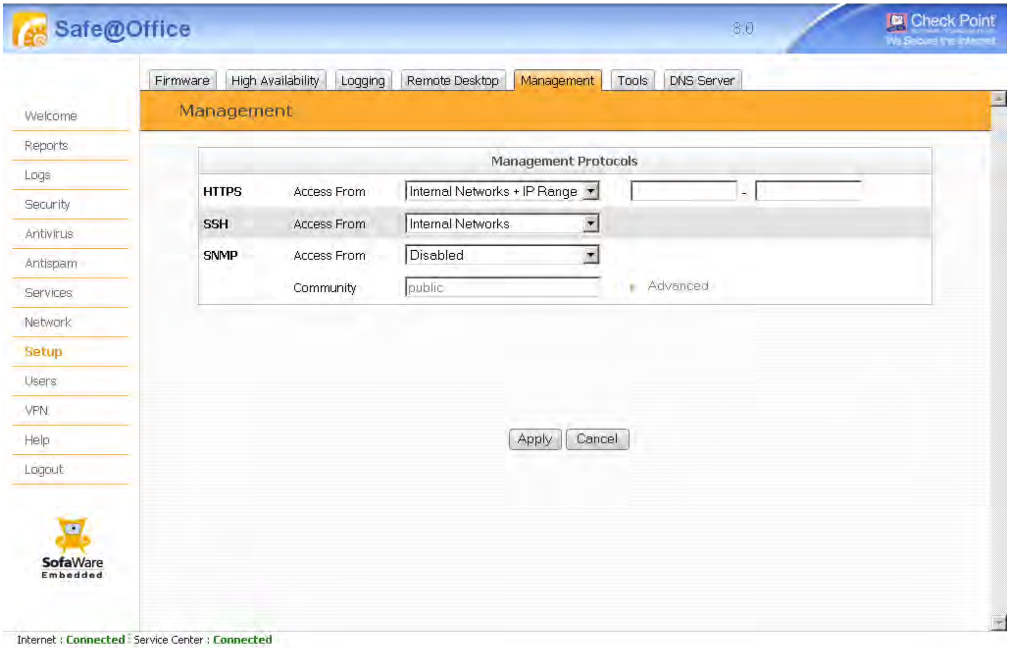
2. Specify from where HTTPS access to the Safe@Office Portal should be granted.

   See ***Access Options*** on page 693 for information.

Warning: If remote HTTPS is enabled, your Safe@Office appliance settings can be changed remotely, so it is especially important to make sure all Safe@Office appliance users' passwords are difficult to guess.

Note: You can use HTTPS to access the Safe@Office Portal from your internal network, by surfing to https://my.firewall.

If you selected Internal Networks + IP Range, additional fields appear.



Management

Management Protocols

HTTPS	Access From	Internal Networks + IP Range	-
SSH	Access From	Internal Networks	
SNMP	Access From	Disabled	
	Community	public	Advanced

Internet : Connected Service Center : Connected

3. If you selected Internal Networks + IP Range, enter the desired IP address range in the fields provided.

4. Click Apply.

   The HTTPS configuration is saved. If you configured remote HTTPS, you can now access the Safe@Office Portal through the Internet, using the procedure ***Accessing the Safe@Office Portal Remotely*** on page 77.

Table 140: Access Options

Select this option…	To allow access from…
Internal Networks	The internal network only. This disables remote access capability. This is the default.
Internal Networks + VPN	The internal network and your VPN.
Internal Networks + IP Range	A particular range of IP addresses. Additional fields appear, in which you can enter the desired IP address range.
ANY	Any IP address.
Disabled	Nowhere. This disables both local and remote access capability. This option is relevant to the SNMP protocol only.

Configuring SNMP

500

The Safe@Office appliance users can monitor the Safe@Office appliance, using tools that support SNMP (Simple Network Management Protocol). You can enable users to do so via the Internet, by configuring remote SNMP access.

The Safe@Office appliance supports the following SNMP MIBs:

- SNMPv2-MIB
- RFC1213-MIB
- IF-MIB
- IP-MIB

All SNMP access is read-only.

Note: Configuring SNMP is equivalent to creating a simple Allow rule, where the destination is This Gateway. To create more complex rules for SNMP, such as allowing SNMP connections from multiple IP address ranges, define Allow rules for the relevant port (by default, TCP port 161), with the destination This Gateway. For information, see ***Using Rules*** on page 360.

To configure SNMP

1. Click Setup in the main menu, and click the Management tab.

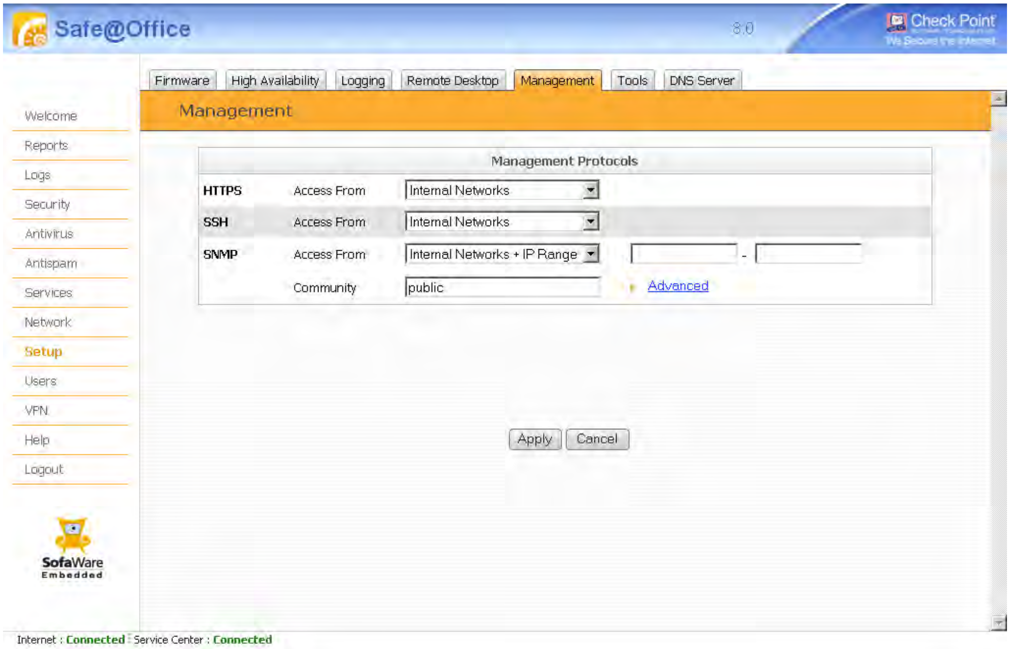
   The Management page appears.

2. Specify from where SNMP access should be granted.

   See ***Access Options*** on page 693 for information.

   If you selected Internal Networks + IP Range, additional fields appear.

The **Community** field and the **Advanced** link are enabled.



Management

Management Protocols

HTTPS	Access From	Internal Networks
SSH	Access From	Internal Networks
SNMP	Access From	Internal Networks + IP Range
	Community	public

Internet : Connected Service Center : Connected

3. If you selected **Internal Networks + IP Range**, enter the desired IP address range in the fields provided.

4. In the **Community** field, type the name of the SNMP community string.

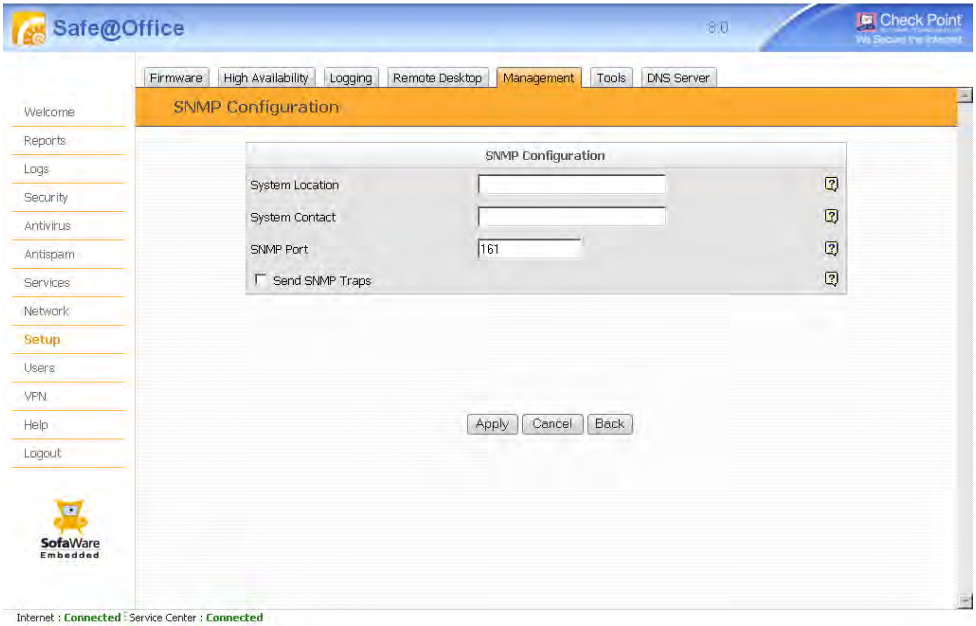
   SNMP clients uses the SNMP community string as a password, when connecting to the Safe@Office appliance.

   The default value is "public". It is recommended to change this string.

5. To configure advanced SNMP settings, do the following:

   a. Click **Advanced**.

The **SNMP Configuration** page appears.



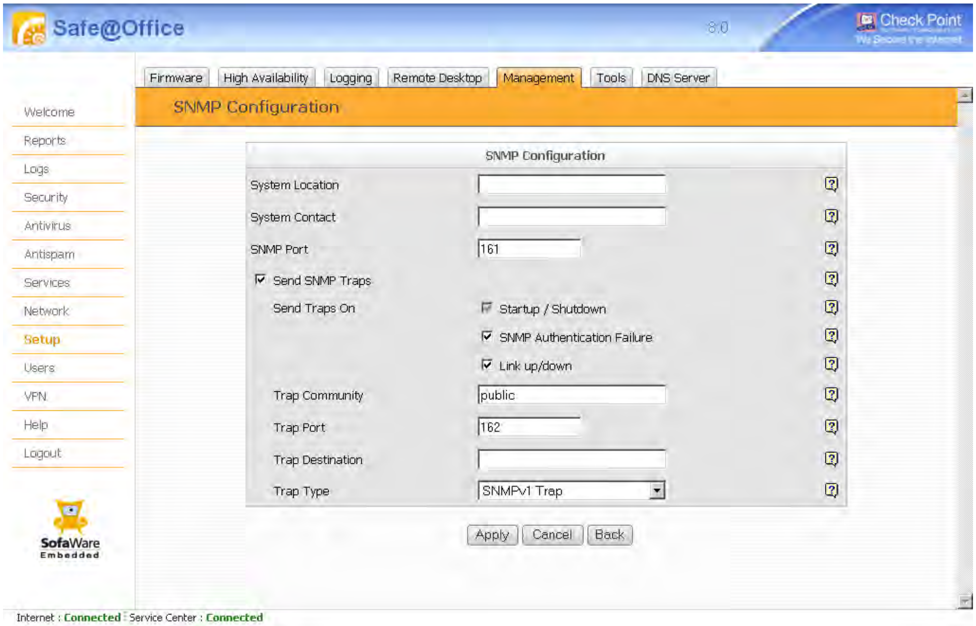
SNMP Configuration

SNMP Configuration	
System Location	
System Contact	
SNMP Port	161
□ Send SNMP Traps	

Internet : Connected : Service Center : Connected

b. Complete the fields using the following table.

If you selected the **Send SNMP Traps** check box, additional fields appear.



SNMP Configuration

SNMP Configuration	
System Location	
System Contact	
SNMP Port	161
☑ Send SNMP Traps	
Send Traps On	☑ Startup / Shutdown
	☑ SNMP Authentication Failure
	☑ Link up/down
Trap Community	public
Trap Port	162
Trap Destination	
Trap Type	SNMPv1 Trap

6. Click **Apply**.

   The SNMP configuration is saved.

7. Configure the SNMP clients with the SNMP community string.

Table 141: Advanced SNMP Settings

In this field...	Do this...
System Location	Type a description of the appliance's location. This information will be visible to SNMP clients, and is useful for administrative purposes.
System Contact	Type the name of the contact person. This information will be visible to SNMP clients, and is useful for administrative purposes.

In this field...	Do this...
SNMP Port	Type the port to use for SNMP. The default port is 161.
Send SNMP Traps	Select this option to enable sending SNMP traps. An SNMP trap is a notification sent from one application to another.
Send Traps On: Startup / Shutdown	Indicates that SNMP traps will automatically be sent upon startup/shutdown events. This option is always selected.
Send Traps On: SNMP Authentication Failure	Select this option to to send an SNMP trap on each SNMP authentication failure event.
Send Traps On: Link up/down	Select this option to send an SNMP trap on each link up/down event.
Trap Community	Type the SNMP community string of the trap receiver. The default value is `public`.
Trap Port	Type The UDP port of the trap receiver. The default value is 162.
Trap Destination	Type the IP address or DNS name of the SNMP trap receiver agent.
Trap Type	Select the type of SNMP traps to use.

Setting the Time on the Appliance

500

You set the time displayed in the Safe@Office Portal during initial appliance setup. If desired, you can change the date and time using the procedure below.

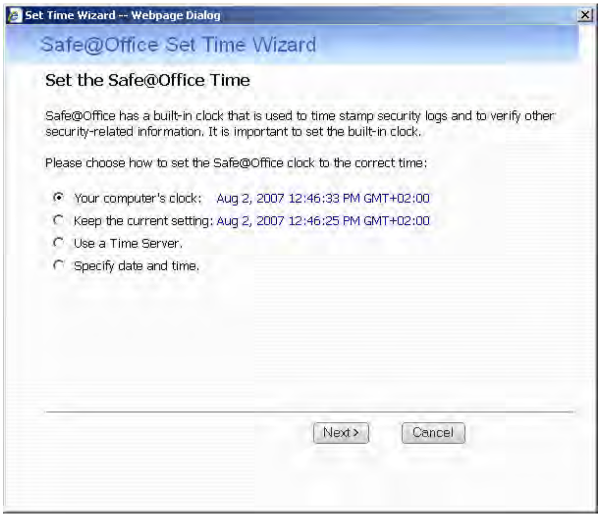
To set the time

1. Click **Setup** in the main menu, and click the **Tools** tab.

   The **Tools** page appears.

2. Click **Set Time.**

   The **Safe@Office Set Time Wizard** opens displaying the **Set the Safe@Office Time** dialog box.



Set Time Wizard -- Webpage Dialog

Safe@Office Set Time Wizard

Set the Safe@Office Time

Safe@Office has a built-in clock that is used to time stamp security logs and to verify other security-related information. It is important to set the built-in clock.

Please choose how to set the Safe@Office clock to the correct time:

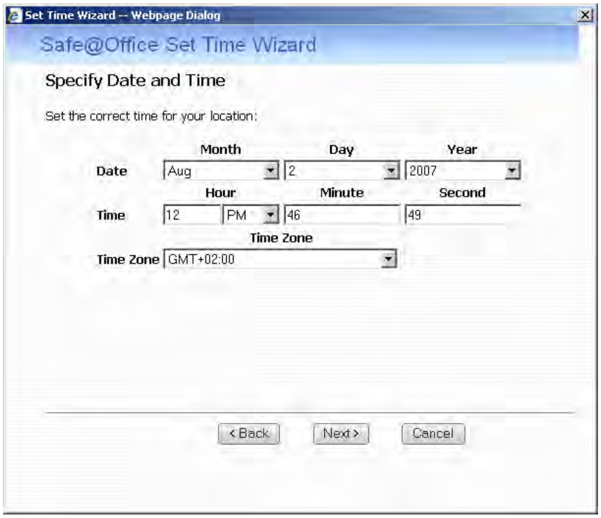
● Your computer's clock: Aug 2, 2007 12:46:33 PM GMT+02:00
○ Keep the current setting: Aug 2, 2007 12:46:25 PM GMT+02:00
○ Use a Time Server.
○ Specify date and time.

3. Complete the fields using the information in ***Set Time Wizard Fields*** on page 701.

4. Click **Next.**

   The following things happen in the order below:

- If you selected **Specify date and time**, the **Specify Date and Time** dialog box appears.



Set Time Wizard -- Webpage Dialog

Safe@Office Set Time Wizard

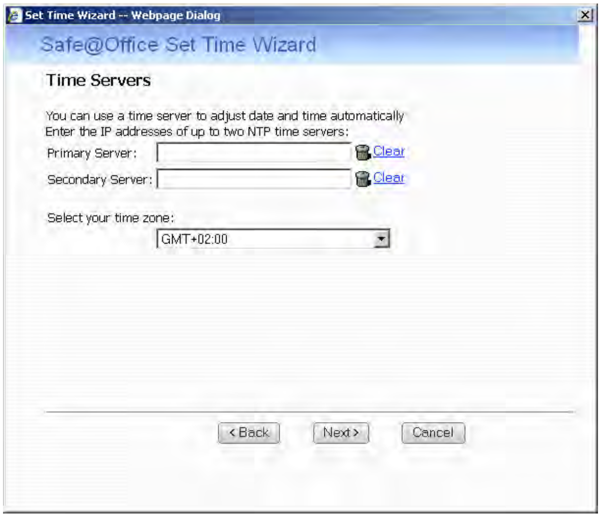
Specify Date and Time

Set the correct time for your location:

	Month	Day	Year
Date	Aug	2	2007
	Hour	Minute	Second
Time	12 PM	46	49
	Time Zone		
Time Zone	GMT+02:00		

Set the date, time, and time zone in the fields provided, then click **Next**.

- If you selected **Use a Time Server**, the **Time Servers** dialog box appears.



Set Time Wizard -- Webpage Dialog

Safe@Office Set Time Wizard

Time Servers

You can use a time server to adjust date and time automatically
Enter the IP addresses of up to two NTP time servers:

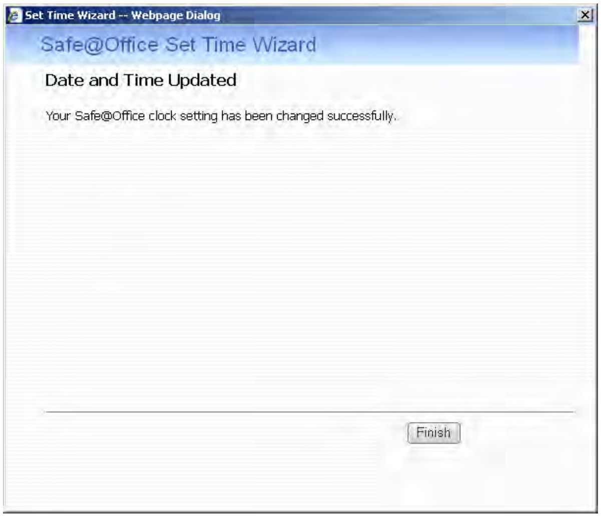
Primary Server: Clear

Secondary Server: Clear

Select your time zone: GMT+02:00

Complete the fields using the information in ***Time Servers Fields*** on page 702, then click **Next**.

- The **Date and Time Updated** screen appears.


Set Time Wizard -- Webpage Dialog

Safe@Office Set Time Wizard

Date and Time Updated

Your Safe@Office clock setting has been changed successfully.

5. Click **Finish**.

Table 142: Set Time Wizard Fields

Select this option...	To do the following...
Your computer's clock	Set the appliance time to your computer's system time. Your computer's system time is displayed to the right of this option.
Keep the current setting	Do not change the appliance's time. The current appliance time is displayed to the right of this option.
Use a Time Server	Synchronize the appliance time with a Network Time Protocol (NTP) server.
Specify date and time	Set the appliance to a specific date and time.

Table 143: Time Servers Fields

In this field…	Do this…
Primary Server	Type the IP address of the Primary NTP server.
Secondary Server	Type the IP address of the Secondary NTP server. This field is optional.
Clear	Clear the field.
Select your time zone	Select the time zone in which you are located.

Using Diagnostic Tools

500

The Safe@Office appliance is equipped with a set of diagnostic tools that are useful for troubleshooting Internet connectivity.

Table 144: Diagnostic Tools

Use this tool…	To do this…	For information, see...
Ping	Check that a specific IP address or DNS name can be reached via the Internet.	***Using IP Tools*** on page 703
Traceroute	Display a list of all routers used to connect from the Safe@Office appliance to a specific IP address or DNS name.	***Using IP Tools*** on page 703

Use this tool…	To do this…	For information, see...
WHOIS	Display the name and contact information of the entity to which a specific IP address or DNS name is registered. This information is useful in tracking down hackers.	***Using IP Tools*** on page 703
Packet Sniffer	Capture network traffic. This information is useful troubleshooting network problems.	***Using Packet Sniffer*** on page 706

Using IP Tools

To use an IP tool

1. Click Setup in the main menu, and click the Tools tab.

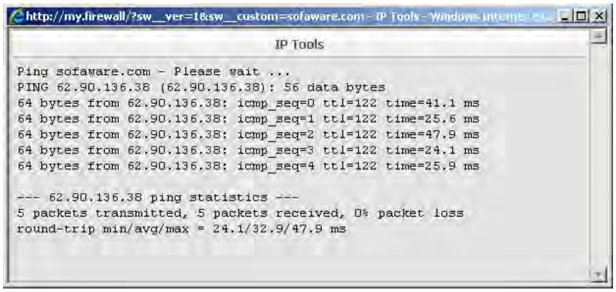
   The Tools page appears.

2. In the Tool drop-down list, select the desired tool.
3. In the Address field, type the IP address or DNS name for which to run the tool.
4. Click Go.

   - If you selected Ping, the following things happen:

     The Safe@Office appliance sends packets to the specified the IP address or DNS name.

The IP Tools window opens and displays the percentage of packet loss and the amount of time it took each packet to reach the specified host and return (round-trip) in milliseconds.



http://my.firewall/?sw__ver=1&sw__custom=sofaware.com - IP Tools - Windows Interne
IP Tools

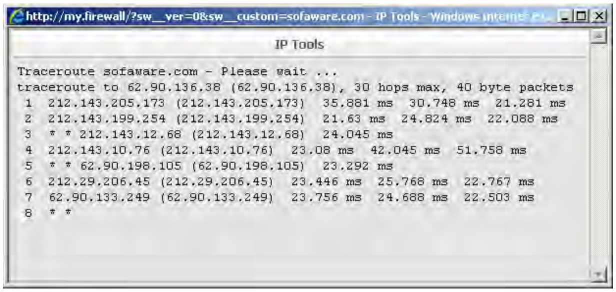
```
Ping sofaware.com - Please wait ...
PING 62.90.136.38 (62.90.136.38): 56 data bytes
64 bytes from 62.90.136.38: icmp_seq=0 ttl=122 time=41.1 ms
64 bytes from 62.90.136.38: icmp_seq=1 ttl=122 time=25.6 ms
64 bytes from 62.90.136.38: icmp_seq=2 ttl=122 time=47.9 ms
64 bytes from 62.90.136.38: icmp_seq=3 ttl=122 time=24.1 ms
64 bytes from 62.90.136.38: icmp_seq=4 ttl=122 time=25.9 ms

--- 62.90.136.38 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 24.1/32.9/47.9 ms
```

- If you selected **Traceroute**, the following things happen:

  The Safe@Office appliance connects to the specified IP address or DNS name.

  The **IP Tools** window opens and displays a list of routers used to make the connection.



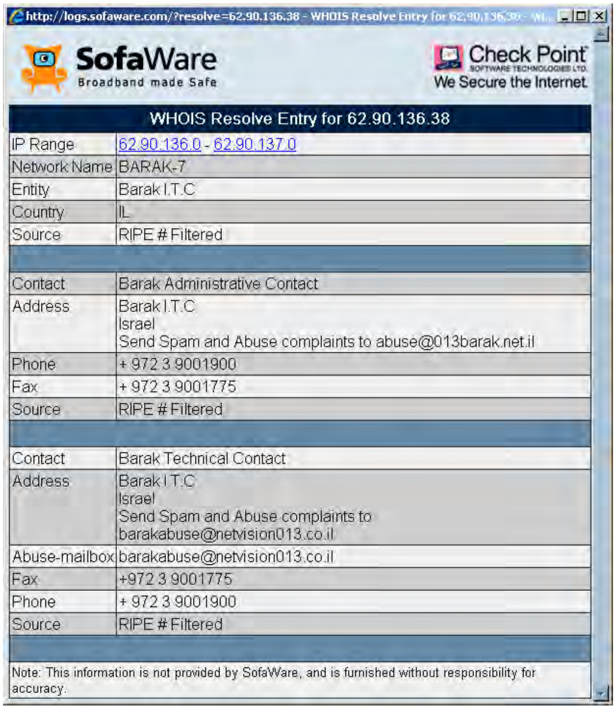
http://my.firewall/?sw__ver=0&sw__custom=sofaware.com - IP Tools - Windows Interne
IP Tools

```
Traceroute sofaware.com - Please wait ...
traceroute to 62.90.136.38 (62.90.136.38), 30 hops max, 40 byte packets
 1  212.143.205.173 (212.143.205.173)  35.881 ms  30.748 ms  21.281 ms
 2  212.143.199.254 (212.143.199.254)  21.63 ms  24.824 ms  22.088 ms
 3  * * 212.143.12.68 (212.143.12.68)  24.045 ms
 4  212.143.10.76 (212.143.10.76)  23.08 ms  42.045 ms  51.758 ms
 5  * * 62.90.198.105 (62.90.198.105)  23.292 ms
 6  212.29.206.45 (212.29.206.45)  23.446 ms  25.768 ms  22.767 ms
 7  62.90.133.249 (62.90.133.249)  23.756 ms  24.688 ms  22.503 ms
 8  * *
```

- If you selected WHOIS, the following things happen:

  The Safe@Office appliance queries the Internet WHOIS server.

  A window displays the name of the entity to which the IP address or DNS name is registered and their contact information.



http://logs.sofaware.com/?resolve=62.90.136.38 - WHOIS Resolve Entry for 62.90.136.38 - Wi...

WHOIS Resolve Entry for 62.90.136.38	
IP Range	62.90.136.0 - 62.90.137.0
Network Name	BARAK-7
Entity	Barak I.T.C
Country	IL
Source	RIPE # Filtered
Contact	Barak Administrative Contact
Address	Barak I.T.C Israel Send Spam and Abuse complaints to abuse@013barak.net.il
Phone	+ 972 3 9001900
Fax	+ 972 3 9001775
Source	RIPE # Filtered
Contact	Barak Technical Contact
Address	Barak I.T.C Israel Send Spam and Abuse complaints to barakabuse@netvision013.co.il
Abuse-mailbox	barakabuse@netvision013.co.il
Fax	+972 3 9001775
Phone	+ 972 3 9001900
Source	RIPE # Filtered

Note: This information is not provided by SofaWare, and is furnished without responsibility for accuracy.

Using Packet Sniffer

500

The Safe@Office appliance includes the Packet Sniffer tool, which enables you to capture packets from any internal network or Safe@Office port. This is useful for troubleshooting network problems and for collecting data about network behavior.

If desired, you can configure Packet Sniffer to capture each packet twice: once before firewall processing and once after firewall processing. This allows you to observe exactly what the Safe@Office firewall does to your packets.

The Safe@Office appliance saves the captured packets to a file on your computer. You can use a free protocol analyzer, such as Ethereal or Wireshark, to analyze the file, or you can send it to technical support. Wireshark runs on all popular computing platforms and can be downloaded from http://www.wireshark.org. Ethereal can be downloaded from http://www.ethereal.com.

Note: If you enabled the Packet Sniffer's Firewall Monitor option, and you would like to view the results in Ethereal/Wireshark, you must do the following: open the capture file, click Edit > Preferences, in the left pane click Protocols > Ethernet, and select the Attempt to interpret as Firewall-1 monitor file check box. The capture file will display the interface name on which the packet was captured, and the packet's processing direction will be indicated by i (input) or o (output).

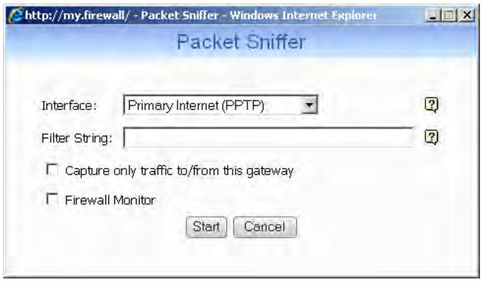
To use Packet Sniffer

1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

2. Click Sniffer.

The **Packet Sniffer** window opens.



http://my.firewall/ - Packet Sniffer - Windows Internet Explorer

Packet Sniffer

Interface: Primary Internet (PPTP)

Filter String:

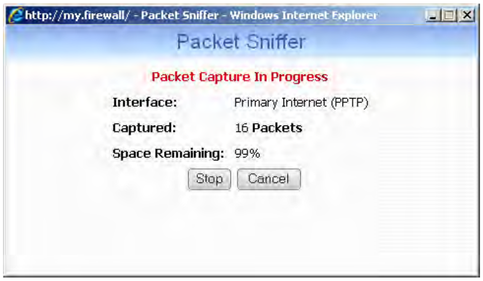
☐ Capture only traffic to/from this gateway

☐ Firewall Monitor

3. Complete the fields using the information in the following table.

4. Click **Start**.

   The **Packet Sniffer** window displays the name of the interface, the number of packets collected, and the percentage of storage space remaining on the appliance for storing the packets.



http://my.firewall/ - Packet Sniffer - Windows Internet Explorer

Packet Sniffer

Packet Capture In Progress

Interface: Primary Internet (PPTP)

Captured: 16 **Packets**

Space Remaining: 99%

5. Click **Stop** to stop collecting packets.

   A standard **File Download** dialog box appears.

6. Click **Save**.

   The **Save As** dialog box appears.

7. Browse to a destination directory of your choice.

8. Type a name for the configuration file and click **Save**.

   The *.cap file is created and saved to the specified directory.

9. Click **Cancel** to close the **Packet Sniffer** window.

Table 145: Packet Sniffer Fields

In this field…	Do this…
Interface	Select the interface from which to collect packets. The list includes the primary Internet connection, the Safe@Office appliance ports, and all defined networks.
Filter String	Type the filter string to use for filtering the captured packets. Only packets that match the filter condition will be saved. For a list of basic filter strings elements, see ***Filter String Syntax*** on page 709. For detailed information on filter syntax, go to http://www.tcpdump.org/tcpdump_man.html. Note: Do not enclose the filter string in quotation marks. If you do not specify a filter string, Packet Sniffer will save all packets on the selected interface.
Capture only traffic to/from this gateway	Select this option to capture incoming and outgoing packets for this gateway only. If this option is not selected, Packet Sniffer will collect packets for all traffic on the interface.
Firewall Monitor	Select this option to capture each packet both before and after firewall processing, and to record the name of the interface on which the packet was captured.

Filter String Syntax

The following represents a list of basic filter string elements:

- ***and*** on page 709
- ***dst*** on page 710
- ***dst port*** on page 710
- ***ether proto*** on page 711
- ***host*** on page 712
- ***not*** on page 712
- ***or*** on page 713
- ***port*** on page 713
- ***src*** on page 714
- ***src port*** on page 714
- ***tcp*** on page 715
- ***udp*** on page 716

For detailed information on filter syntax, refer to http://www.tcpdump.org.

and

PURPOSE

The `and` element is used to concatenate filter string elements. The filtered packets must match *all* concatenated filter string elements.

SYNTAX

element and element [and element...]

element && element [&& element...]

PARAMETERS

`element`	String. A filter string element.

EXAMPLE

The following filter string saves packets that both originate from IP address is 192.168.10.1 and are destined for port 80:

```
src 192.168.10.1 and dst port 80
```

dst

PURPOSE

The `dst` element captures all packets with a specific destination.

SYNTAX

dst *destination*

PARAMETERS

`destination`	IP Address or String. The computer to which the packet is sent. This can be the following: • An IP address • A host name

EXAMPLE

The following filter string saves packets that are destined for the IP address 192.168.10.1:

```
dst 192.168.10.1
```

dst port

PURPOSE

The `dst port` element captures all packets destined for a specific port.

SYNTAX

dst port *port*

Note: This element can be prepended by tcp or udp. For information, see ***tcp*** on page 715 and ***udp*** on page 716.

PARAMETERS

`port` Integer. The port to which the packet is sent.

EXAMPLE

The following filter string saves packets that are destined for port 80:

```
dst port 80
```

ether proto

PURPOSE

The `ether proto` element is used to capture packets of a specific ether protocol type.

SYNTAX

ether proto \protocol

PARAMETERS

`protocol` String. The protocol type of the packet.

This can be the following: `ip, ip6, arp, rarp, atalk, aarp, dec net, sca, lat, mopdl, moprc, iso, stp, ipx,` or `netbeui`.

EXAMPLE

The following filter string saves ARP packets:

```
ether proto arp
```

host

PURPOSE

The `host` element captures all incoming and outgoing packets for a specific computer.

SYNTAX

host *host*

PARAMETERS

`host` IP Address or String. The computer to/from which the packet is sent. This can be the following:

- An IP address
- A host name

EXAMPLE

The following filter string saves all packets that either originated from IP address 192.168.10.1, or are destined for that same IP address:

host 192.168.10.1

not

PURPOSE

The `not` element is used to negate filter string elements.

SYNTAX

not element

! element

PARAMETERS

`element` String. A filter string element.

EXAMPLE

The following filter string saves packets that are *not* destined for port 80:

```
not dst port 80
```

or

PURPOSE

The `or` element is used to alternate between string elements. The filtered packets must match at least one of the filter string elements.

SYNTAX

element **or** element [**or** element...]

element **||** element [**||** element...]

PARAMETERS

`element`	String. A filter string element.

EXAMPLE

The following filter string saves packets that either originate from IP address 192.168.10.1 or IP address 192.168.10.10:

```
src 192.168.10.1 or src 192.168.10.10
```

port

PURPOSE

The `port` element captures all packets originating from or destined for a specific port.

SYNTAX

port *port*

Note: This element can be prepended by tcp or udp. For information, see ***tcp*** on page 715 and ***udp*** on page 716.

PARAMETERS

`port`	Integer. The port from/to which the packet is sent.

EXAMPLE

The following filter string saves all packets that either originated from port 80, or are destined for port 80:

```
port 80
```

src

PURPOSE

The `src` element captures all packets with a specific source.

SYNTAX

src *source*

PARAMETERS

`source`	IP Address or String. The computer from which the packet is sent. This can be the following: • An IP address • A host name

EXAMPLE

The following filter string saves packets that originated from IP address 192.168.10.1:

```
src 192.168.10.1
```

src port

PURPOSE

The `src port` element captures all packets originating from a specific port.

SYNTAX

src port *port*

Note: This element can be prepended by tcp or udp. For information, see ***tcp*** on page 715 and ***udp*** on page 716.

PARAMETERS

`port`	Integer. The port from which the packet is sent.

EXAMPLE

The following filter string saves packets that originated from port 80:

```
src port 80
```

tcp

PURPOSE

The `tcp` element captures all TCP packets. This element can be prepended to port-related elements.

Note: When not prepended to other elements, the `tcp` element is the equivalent of `ip proto tcp`.

SYNTAX

tcp

tcp *element*

PARAMETERS

`element`	String. A port-related filter string element that should be restricted to saving only TCP packets. This can be the following: • `dst port` - Capture all TCP packets destined for a specific port. • `port` - Capture all TCP packets originating from or destined for a specific port. • `src port` - Capture all TCP packets originating from a specific port.

EXAMPLE 1

The following filter string captures all TCP packets:

```
tcp
```

EXAMPLE 2

The following filter string captures all TCP packets destined for port 80:

```
tcp dst port 80
```

udp

PURPOSE

The `udp` element captures all UDP packets. This element can be prepended to port-related elements.

Note: When not prepended to other elements, the `udp` element is the equivalent of `ip proto udp`.

SYNTAX

udp

udp *element*

PARAMETERS

`element`	String. A port-related filter string element that should be restricted to saving only UDP packets. This can be the following: • `dst port` - Capture all UDP packets destined for a specific port. • `port` - Captures all UDP packets originating from or destined for a specific port. • `src port` - Capture all UDP packets originating from a specific port.

EXAMPLE 1

The following filter string captures all UDP packets:

```
udp
```

EXAMPLE 2

The following filter string captures all UDP packets destined for port 80:

```
udp dst port 80
```

Backing Up and Restoring the Safe@Office Appliance Configuration

500

The Safe@Office appliance provides the following ways of backing up and restoring its configuration:

- Backup and restore on your computer

  You can export the Safe@Office appliance configuration to a *.cfg file on your computer, and use this file to backup and restore Safe@Office appliance settings, as needed.

  The file includes all of your settings, except for the security policy and certificate.

- Backup and restore on a USB flash drive

  You can back up the appliance configuration and device certificate to a USB flash drive. You can then restore the Safe@Office appliance settings from the USB flash drive as needed.

  This method requires a USB port on your appliance.

Note: If both cases, the configuration file is saved as a textual CLI script. If desired, you can edit the file. For a full explanation of the CLI script format and the supported CLI commands, see the Embedded NGX CLI Reference Guide.

Backing Up the Appliance Configuration

Exporting the Appliance Configuration to Your Computer

500

To export the Safe@Office appliance configuration to your computer

1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

2. Click Export.

   A standard File Download dialog box appears.

3. Click Save.

   The Save As dialog box appears.

4. Browse to a destination directory of your choice.

5. Type a name for the configuration file and click Save.

   The *.cfg configuration file is created and saved to the specified directory.

   You can now import the configuration file as needed. See ***Importing the Appliance Configuration from Your Computer*** on page 721.

Backing Up the Appliance Configuration to a USB Flash Drive

USB

The USB flash drive must have at least 64MB of free space.

Note: Some USB flash drives may not be supported by the appliance.

To backup the appliance configuration to a USB flash drive

1. Connect a USB flash drive to one of your Safe@Office appliance's USB ports.

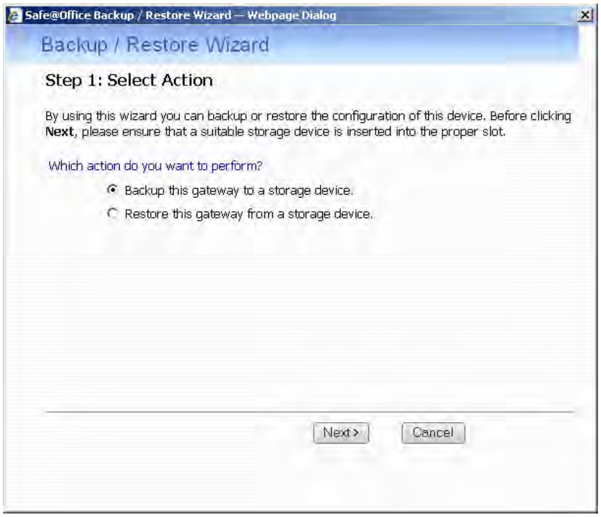
   For information on locating the USB ports, see ***Introduction*** on page 1.

2. Click **Setup** in the main menu, and click the **Tools** tab.

   The **Tools** page appears.

3. Click **Backup/Restore.**

   The **Backup/Restore Wizard** opens displaying the **Step 1: Select Action** dialog box.



Safe@Office Backup / Restore Wizard -- Webpage Dialog

Backup / Restore Wizard

Step 1: Select Action

By using this wizard you can backup or restore the configuration of this device. Before clicking **Next**, please ensure that a suitable storage device is inserted into the proper slot.

Which action do you want to perform?

● Backup this gateway to a storage device.

○ Restore this gateway from a storage device.

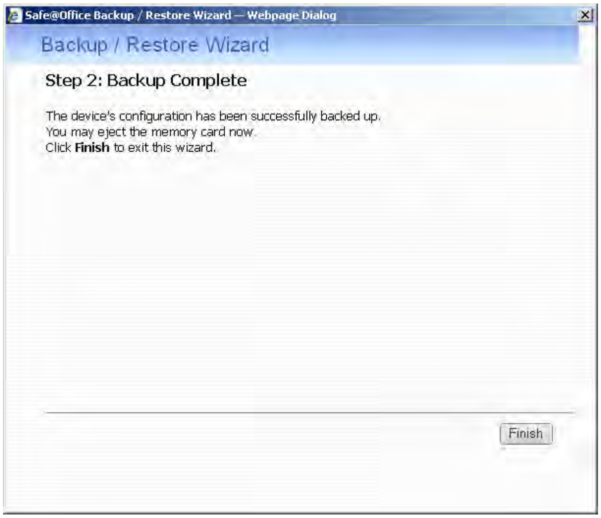
4. Click **Backup this gateway to a storage device.**

5. Click **Next.**

The Safe@Office appliance creates the folder `<MACAddress>` on the USB flash drive, where `<MACAddress>` is the appliance's MAC address, and writes the following files to this folder:

- `embeddedngx.cfg`
- `embeddedngx.p12`

The **Step 2: Backup Complete** screen appears.



Step 2: Backup Complete

The device's configuration has been successfully backed up.
You may eject the memory card now.
Click **Finish** to exit this wizard.

6. Click **Finish**.

   You can now restore the configuration from the USB flash drive as needed. See ***Restoring the Appliance Configuration from a USB Flash Drive*** on page 723.

Restoring the Appliance Configuration

Importing the Appliance Configuration from Your Computer

500

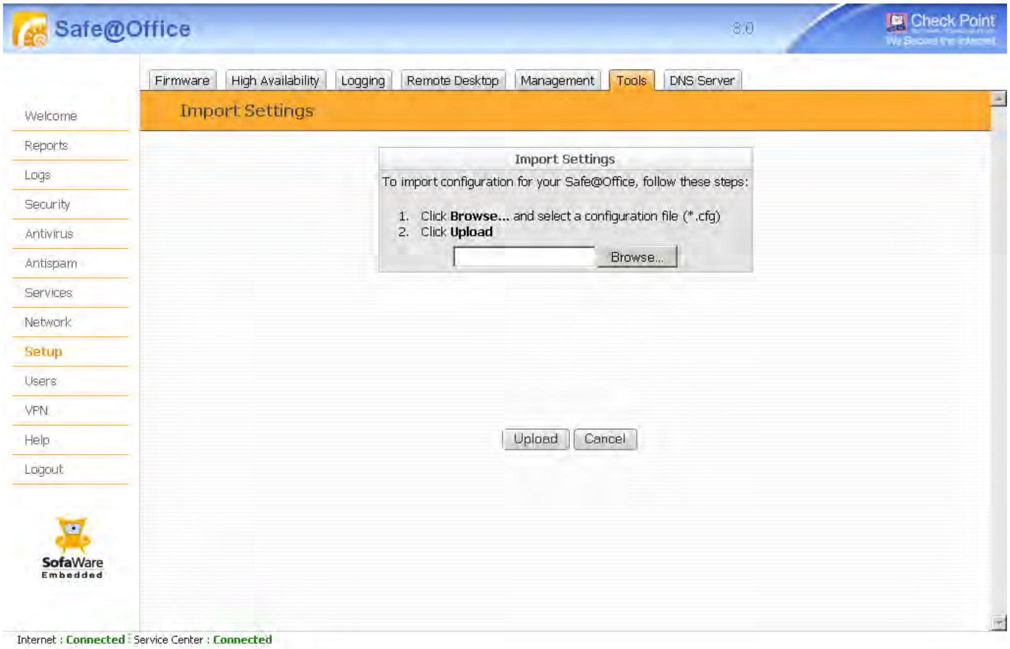
To import the appliance configuration from your computer

1. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

2. Click Import.

   The Import Settings page appears.



Import Settings

To import configuration for your Safe@Office, follow these steps:

1. Click **Browse...** and select a configuration file (*.cfg)
2. Click **Upload**

3. Do one of the following:

   - In the Import Settings field, type the full path to the configuration file.

   Or

- Click **Browse**, and browse to the configuration file.

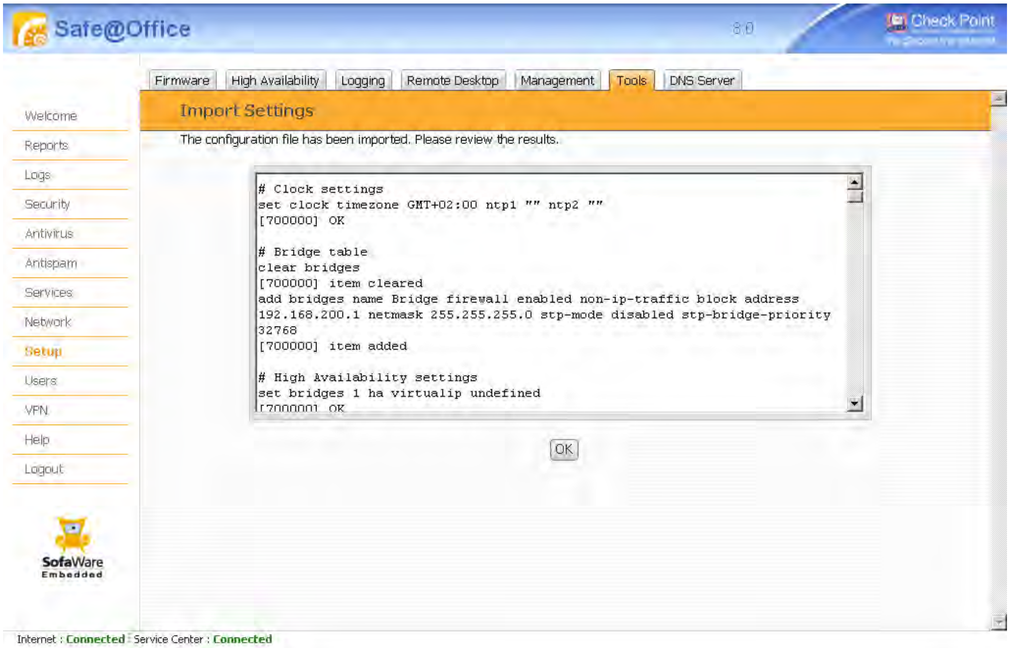
4. Click **Upload**.

   A confirmation message appears.

5. Click **OK**.

   The Safe@Office appliance settings are imported.

   The **Import Settings** page displays the configuration file's content and the result of implementing each configuration command.



Import Settings

The configuration file has been imported. Please review the results.

```
# Clock settings
set clock timezone GMT+02:00 ntp1 "" ntp2 ""
[700000] OK

# Bridge table
clear bridges
[700000] item cleared
add bridges name Bridge firewall enabled non-ip-traffic block address
192.168.200.1 netmask 255.255.255.0 stp-mode disabled stp-bridge-priority
32768
[700000] item added

# High Availability settings
set bridges 1 ha virtualip undefined
[700000] OK
```

Note: If the appliance's IP address changed as a result of the configuration import, your computer may be disconnected from the network; therefore you may not be able to see the results.

Restoring the Appliance Configuration from a USB Flash Drive

To restore the appliance configuration from a USB flash drive

1. Connect a USB flash drive to one of your Safe@Office appliance's USB ports.

   For information on locating the USB ports, see ***Introduction*** on page 1.

2. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

3. Click Backup/Restore.

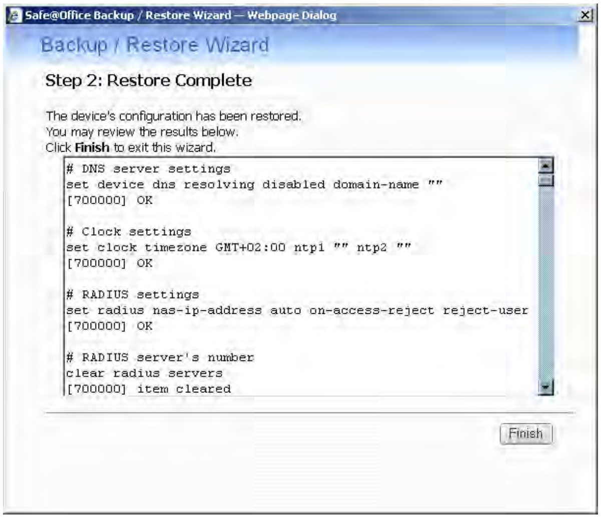
   The Backup/Restore Wizard opens displaying the Step 1: Select Action dialog box.

4. Click Restore this gateway from a storage device.

5. Click Next.

   The Safe@Office appliance is restored from the `<MACAddress>` folder on the USB flash drive, where `<MACAddress>` is the appliance's MAC address. This may take some time.

The **Step 2: Restore Complete** screen appears displaying the configuration file's content and the result of implementing each configuration command.



Step 2: Restore Complete

The device's configuration has been restored.
You may review the results below.
Click **Finish** to exit this wizard.

```
# DNS server settings
set device dns resolving disabled domain-name ""
[700000] OK

# Clock settings
set clock timezone GMT+02:00 ntp1 "" ntp2 ""
[700000] OK

# RADIUS settings
set radius nas-ip-address auto on-access-reject reject-user
[700000] OK

# RADIUS server's number
clear radius servers
[700000] item cleared
```

Note: If the appliance's IP address changed as a result of the configuration import, your computer may be disconnected from the network; therefore you may not be able to see the results.

6. Click **Finish.**

Using Rapid Deployment

USB

Safe@Office appliances are shipped with a specific firmware and group of settings that represent the appliance's default state. When installing a new appliance, you can configure different settings and install new firmware versions as needed; however, this can be time-consuming. Rapid deployment avoids this hassle, by allowing you to load the following settings from a USB flash drive during product initialization:

- The primary firmware
- The backup firmware
- The configuration file
- The default configuration file

  The default configuration file contains settings that represent the desired appliance default state. The settings in the default configuration file become the appliance's new default settings and are retained even after a reset to defaults operation.

Important: The default configuration file cannot be cleared by performing a Reset to Defaults operation. It can only be cleared by loading an empty default configuration file.

- The certificate

Rapid deployment can be used to configure several appliances in succession. If multiple appliances share a group of settings, you can use rapid deployment to configure each appliance with both the shared settings and the appliance-specific settings, all in one action. For example, before shipping appliances to your company’s branch offices, you can quickly configure all of the appliances with the corporate security policy and VPN settings, as well as with branch-specific settings.

Preparing the USB Flash Drive for Rapid Deployment

USB

Before performing a rapid deployment, you must load the USB flash drive with the files you want to install on the appliance(s).

To prepare the USB flash drive

1. For each appliance you want to deploy, create a folder named `<MACAddress>`, where `<MACAddress>` is the appliance's MAC address, and the colons are replaced by underscores.

   For example, if the appliance's MAC address is 00:11:22:33:44:55, the folder name should be `00_11_22_33_44_55`.

2. If you would like to deploy multiple appliances that share settings, create a folder named `deploy`.

3. Prepare the files that you want to install on the appliances.

   The files must be named according to the following table.

4. Add files containing settings that should be shared by all of the appliances to the `deploy` folder.

5. For each appliance, add files containing settings that are specific to the appliance to the folder named after the appliance's MAC address.

For example, if you want two Safe@Office appliances to share the same primary firmware but to have different configuration files, you must prepare a single `primary.firm` file and add it to the `deploy` folder. Then you must prepare two different `embeddedngx.cfg` configuration files, and add one to each appliance's folder.

Table 146: Rapid Deployment File Names

This file...	Should be named...
The primary firmware	`primary.firm / primary.img`
The backup firmware	`secondary.firm / secondary.img`

This file...	Should be named...
The configuration file	`embeddedngx.cfg`
The default configuration file	`preset.cfg`
The certificate	`embeddedngx.p12`

Performing a Rapid Deployment

USB

You must perform the following procedure on each Safe@Office appliance you want to deploy.

To perform a rapid deployment

1. Reset the Safe@Office appliance to its default settings.

   See ***Resetting the Safe@Office Appliance to Defaults*** on page 728.

2. While the appliance is powering up, insert the USB flash drive into the appliance’s USB port.

   For information on locating the USB ports, see ***Introduction*** on page 1.

   The following things happen:

   - The PWR/SEC LED flashes quickly in green, signaling that rapid deployment is in progress.
   - The file `results-<MACAddress>.log` is created in the USB flash drive's root folder, where `<MACAddress>` is the appliance's MAC address.
   - If the `deploy` folder exists, the appliance loads shared settings from it. The appliance then loads its private settings from the folder named after its MAC address.

     Note: If the appliance loads an updated firmware file, the appliance restarts and then continues the rapid deployment process. Do not disconnect the USB flash drive until the process is complete.

- If an error occurs during the rapid deployment process, the PWR/SEC LED blinks quickly in red, the errors are logged to the Event Log, and rapid deployment continues.
- When rapid deployment is complete, the PWR/SEC LED is a constant green.

3. To check the results of rapid deployment, in the USB flash drive's root folder, open the file `results-<MACAddress>.log`.

   Settings that loaded successfully are marked as "ok", and settings that failed to load are marked as "failed".

Resetting the Safe@Office Appliance to Defaults

500

You can reset the Safe@Office appliance to its default settings. When you reset your Safe@Office appliance, it reverts to the state it was originally in when you purchased it.

Warning: This operation erases all your settings and password information. You will have to set a new password and reconfigure your Safe@Office appliance for Internet connection. For information on performing these tasks, see ***Setting Up the Safe@Office Appliance*** on page 67.

This operation also resets your appliance to its default Product Key. Therefore, if you upgraded your license, you should save your Product Key before resetting to defaults. You can view the installed Product Key by in the Safe@Office Licensing Wizard. For information on accessing this wizard, see ***Upgrading Your License*** on page 685.

You can reset the Safe@Office appliance to defaults via the Web management interface (software) or by manually pressing the Reset button (hardware) located at the back of the Safe@Office appliance.

When resetting the appliance via the Safe@Office Portal, you can choose to keep the current firmware or to revert to the firmware version that shipped with the Safe@Office appliance. In contrast, using the Reset button automatically reverts the firmware version.

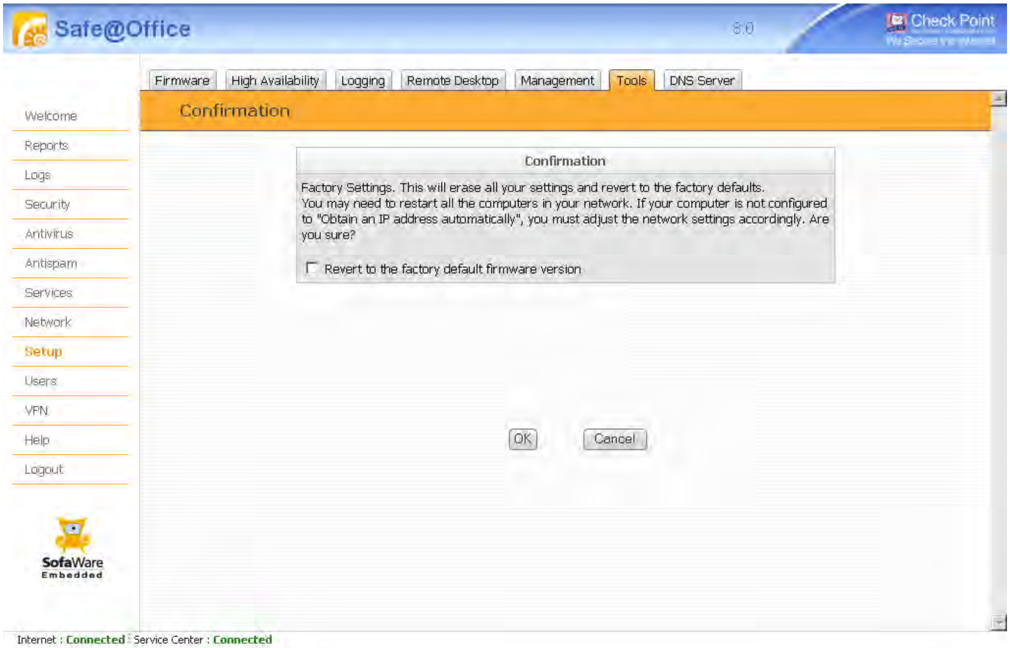
To reset the Safe@Office appliance to factory defaults via the Web interface

1. Click **Setup** in the main menu, and click the **Tools** tab.

   The **Tools** page appears.

2. Click **Factory Settings**.

   A confirmation message appears.



Confirmation

Confirmation

Factory Settings. This will erase all your settings and revert to the factory defaults. You may need to restart all the computers in your network. If your computer is not configured to "Obtain an IP address automatically", you must adjust the network settings accordingly. Are you sure?

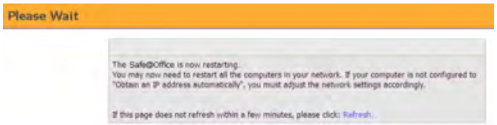
□ Revert to the factory default firmware version

Internet : Connected Service Center : Connected

3. To revert to the firmware version that shipped with the appliance, select the check box.

4. Click **OK**.

   - The **Please Wait** screen appears.



Please Wait

The Safe@Office is now restarting.
You may now need to restart all the computers in your network. If your computer is not configured to "Obtain an IP address automatically", you must adjust the network settings accordingly.

If this page does not refresh within a few minutes, please click: Refresh.

   - The Safe@Office appliance returns to its factory defaults.

- The Safe@Office appliance is restarted.

  This may take a few minutes.

- The **Login** page appears.

To reset the Safe@Office appliance to factory defaults using the Reset button

1. Make sure the Safe@Office appliance is powered on.
2. Using a pointed object, press the RESET button on the back of the Safe@Office appliance steadily for seven seconds and then release it.
3. Allow the Safe@Office appliance to boot-up until the system is ready.

   For information on the appliance's front and rear panels, see the *Getting to Know Your Appliance* section in ***Introduction*** on page 1.

⚠ Warning: If you choose to reset the Safe@Office appliance by disconnecting the power cable and then reconnecting it, be sure to leave the Safe@Office appliance disconnected for at least three seconds. Disconnecting and reconnecting the power without waiting might cause permanent damage.

Running Diagnostics

500

You can view technical information about your Safe@Office appliance's hardware, firmware, license, network status, and Service Center.

This information is useful for troubleshooting. You can export it to an *.html file and send it to technical support.

To view diagnostic information

1. Click **Setup** in the main menu, and click the **Tools** tab.

   The **Tools** page appears.

2. Click **Diagnostics.**

   Technical information about your Safe@Office appliance appears in a new window.

3. To save the displayed information to an *.html file:

   a. Click **Save**.

      A standard **File Download** dialog box appears.

   b. Click **Save**.

      The **Save As** dialog box appears.

   c. Browse to a destination directory of your choice.

   d. Type a name for the configuration file and click **Save**.

      The *.html file is created and saved to the specified directory.

4. To refresh the contents of the window, click **Refresh.**

   The contents are refreshed.

5. To close the window, click **Close**.

Rebooting the Safe@Office Appliance

500

If your Safe@Office appliance is not functioning properly, rebooting it may solve the problem.

To reboot the Safe@Office appliance

1. Click **Setup** in the main menu, and click the **Firmware** tab.

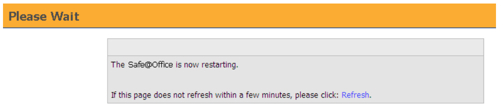
   The **Firmware** page appears.

2. Click **Restart**.

   A confirmation message appears.

3. Click **OK**.

   - The **Please Wait** screen appears.

     Please Wait

     The Safe@Office is now restarting.

     If this page does not refresh within a few minutes, please click: Refresh.

   - The Safe@Office appliance is restarted.

     This may take a few minutes.

   - The **Login** page appears.

Chapter 24

Using Network Printers

This chapter describes how to set up and use network printers.

This chapter includes the following topics:

Overview

Some Safe@Office models include a built-in print server, enabling you to connect USB-based printers to the appliance and share them across the network.

Note: When using computers with a Windows 2000/XP/Vista operating system, the Safe@Office appliance supports connecting up to four USB-based printers to the appliance. When using computers with a MAC OS-X operating system, the Safe@Office appliance supports connecting one printer.

The appliance automatically detects printers as they are plugged in, and they immediately become available for printing. Usually, no special configuration is required on the Safe@Office appliance.

Note: The Safe@Office print server supports printing via "all-in-one" printers. Copying and scanning functions are not supported.

Setting Up Network Printers

USB

To set up a network printer

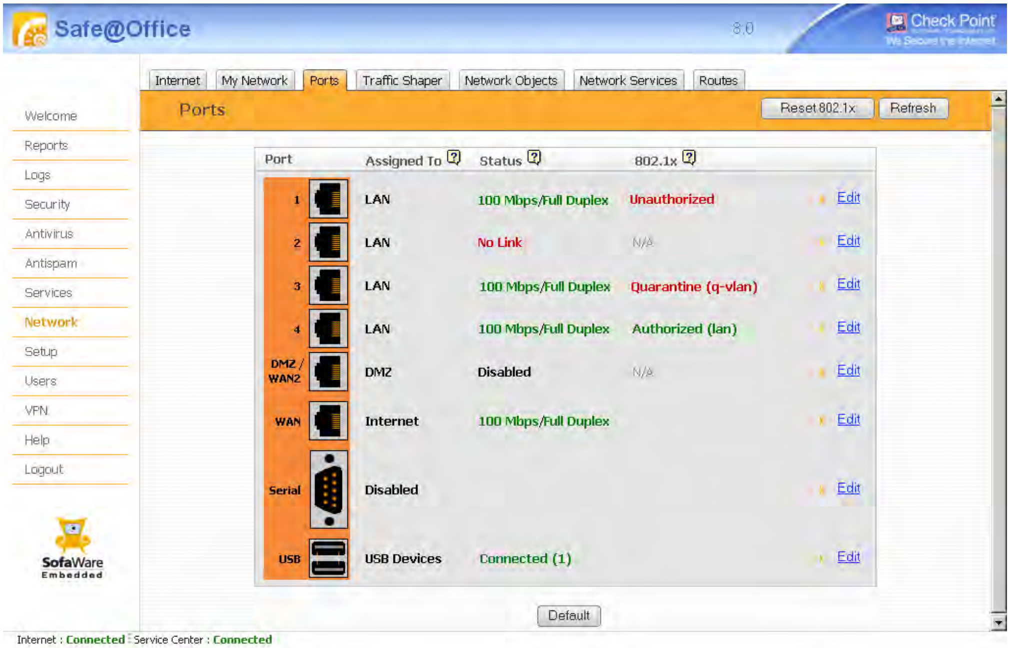
1. Connect the network printer to the Safe@Office appliance.

   See ***Connecting the Appliance to Network Printers*** on page 63.

2. Turn the printer on.

3. In the Safe@Office Portal, click Network in the main menu, and click the Ports tab.

   The Ports page appears.

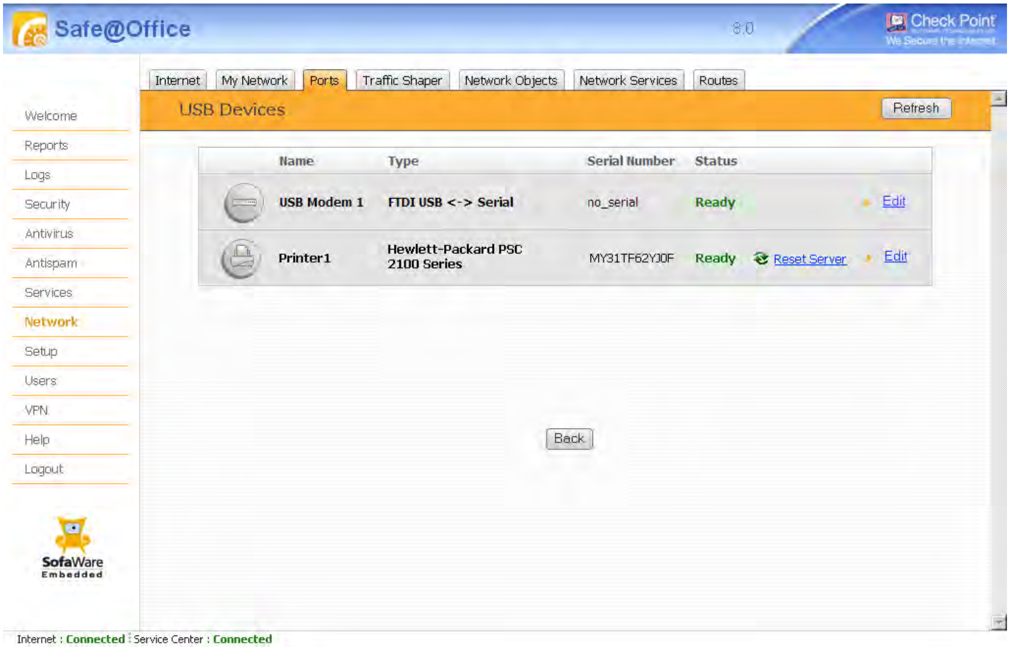


Port	Assigned To	Status	802.1x	
1	LAN	100 Mbps/Full Duplex	Unauthorized	Edit
2	LAN	No Link	N/A	Edit
3	LAN	100 Mbps/Full Duplex	Quarantine (q-vlan)	Edit
4	LAN	100 Mbps/Full Duplex	Authorized (lan)	Edit
DMZ / WAN2	DMZ	Disabled	N/A	Edit
WAN	Internet	100 Mbps/Full Duplex		Edit
Serial	Disabled			Edit
USB	USB Devices	Connected (1)		Edit

Internet : Connected : Service Center : Connected

4. Next to USB, click Edit.

The **USB Devices** page appears. If the Safe@Office appliance detected the printer, the printer is listed on the page.



USB Devices

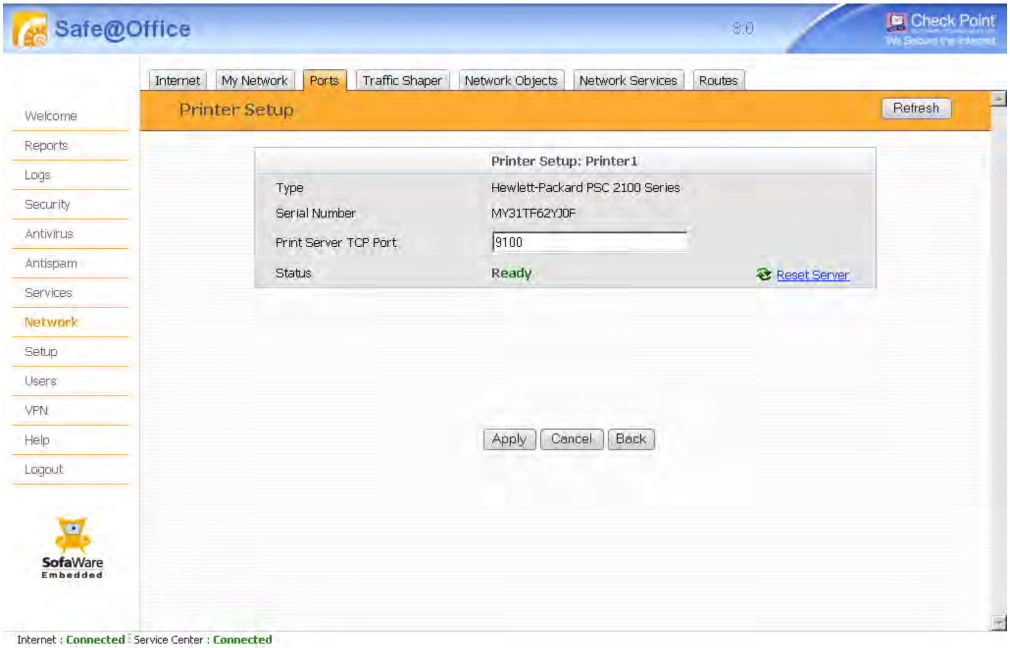
Name	Type	Serial Number	Status		
USB Modem 1	FTDI USB <-> Serial	no_serial	Ready		Edit
Printer1	Hewlett-Packard PSC 2100 Series	MY31TF62YJ0F	Ready	Reset Server	Edit

Internet : Connected ⋮ Service Center : Connected

If the printer is not listed, check that you connected the printer correctly, then click **Refresh** to refresh the page.

5. Next to the printer, click **Edit**.

The **Printer Setup** page appears.



Printer Setup: Printer1

Type	Hewlett-Packard PSC 2100 Series
Serial Number	MY31TF62YJ0F
Print Server TCP Port	9100
Status	Ready

Internet : Connected | Service Center : Connected

6. Write down the port number allocated to the printer.

   The port number appears in the **Printer Server TCP Port** field. You will need this number later, when configuring computers to use the network printer.

7. To change the port number, do the following:

   a. Type the desired port number in the **Printer Server TCP Port** field.

   Note: Printer port numbers may not overlap, and must be high ports.

   b. Click **Apply**.

   You may want to change the port number if, for example, the printer you are setting up is intended to replace another printer. In this case, you should change the replacement printer's port number to the old printer's port number, and you can skip the next step.

8. Configure each computer from which you want to enable printing to the network printer.

See ***Configuring Computers to Use Network Printers*** on page 737.

Configuring Computers to Use Network Printers

USB

Perform the relevant procedure on each computer from which you want to enable printing via the Safe@Office print server to a network printer.

Windows Vista

This procedure is relevant for computers with a Windows Vista operating system.

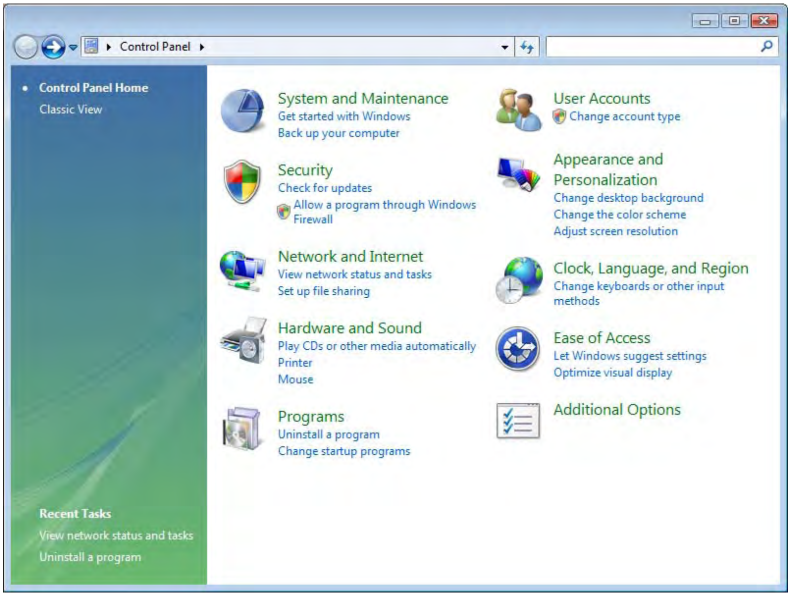
To configure a computer to use a network printer

1. If the computer for which you want to enable printing is located on the WAN, create an Allow rule for connections from the computer to This Gateway.

   See ***Adding and Editing Rules*** on page 364.

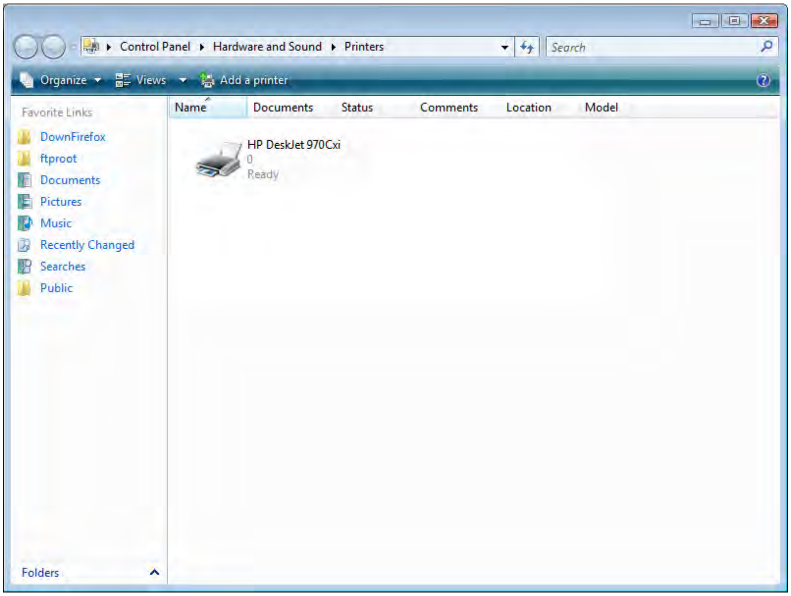
2. Click Start > Control Panel.

The **Control Panel** window opens.



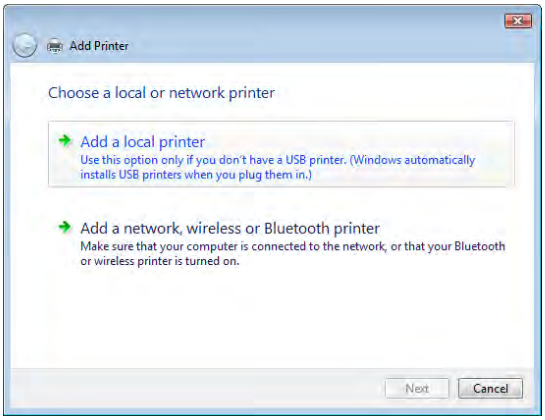
3. Under **Hardware and Sound,** click **Printer.**

The **Printers** screen appears.



4. Click **Add a printer.**

   The **Add Printer** wizard opens displaying the **Choose a local or network printer** screen.



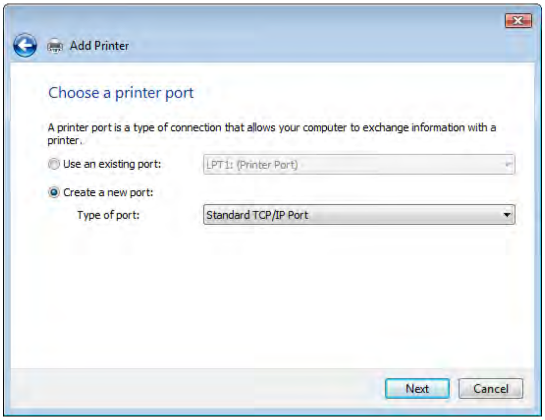
Choose a local or network printer

→ Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

→ Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

5. Click **Add a local printer.**
6. Click **Next.**

The **Choose a printer port** dialog box appears.



Add Printer

Choose a printer port

A printer port is a type of connection that allows your computer to exchange information with a printer.

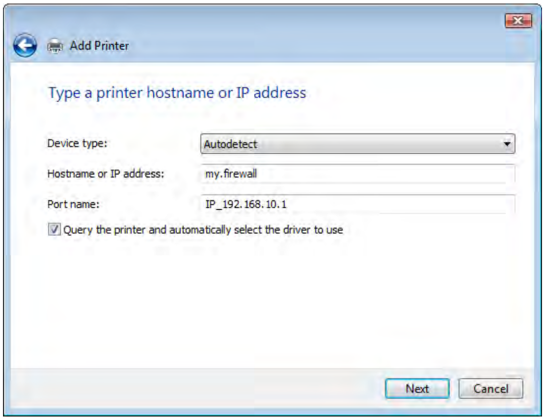
○ Use an existing port: LPT1: (Printer Port)

● Create a new port:

Type of port: Standard TCP/IP Port

7. Click **Create a new port**.
8. In the **Type of port** drop-down list, select **Standard TCP/IP Port**.
9. Click **Next**.

The **Type a printer hostname or IP address** dialog box appears.



Add Printer

Type a printer hostname or IP address

Device type: Autodetect

Hostname or IP address: my.firewall

Port name: IP_192.168.10.1

☑ Query the printer and automatically select the driver to use

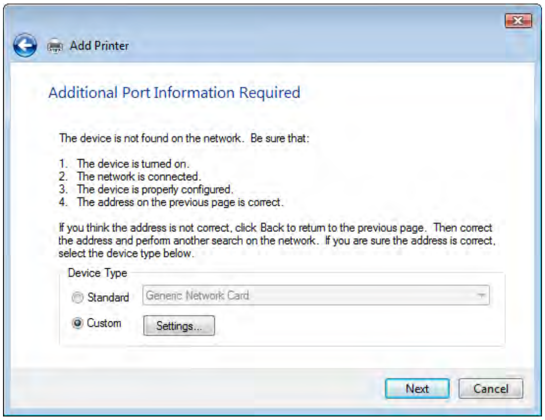
10. In the **Device type** drop-down list, select **Autodetect**.
11. In the **Hostname or IP address** field, type the Safe@Office appliance's LAN IP address, or "my.firewall".

You can find the LAN IP address in the Safe@Office Portal, under **Network > My Network**.

12. In the **Port name** field, type the port name.
13. Select the **Query the printer and automatically select the driver to use** check box.
14. Click **Next.**

    The following things happen:

    - If Windows cannot identify your printer, the **Additional Port Information Required** dialog box appears.



Additional Port Information Required

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

○ Standard Generic Network Card

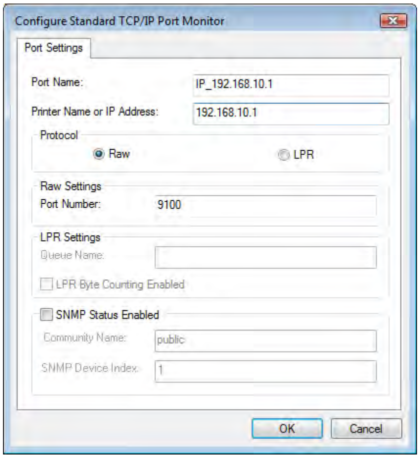
● Custom Settings...

Do the following:

1) Click **Custom.**

2) Click **Settings.**

The **Configure Standard TCP/IP Port Monitor** dialog box opens.



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.10.1

Printer Name or IP Address: 192.168.10.1

Protocol

● Raw ○ LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name:

□ LPR Byte Counting Enabled

□ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

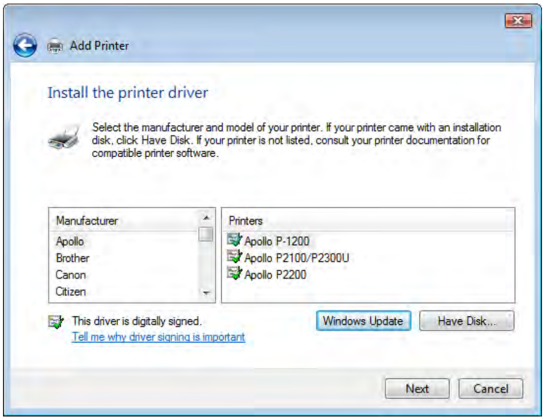
3) In the **Protocol** area, make sure that **Raw** is selected.

4) In the **Port Number** field, type the printer's port number, as shown in the **Printers** page.

5) Click **OK**.

6) Click **Next**.

- The **Install the printer driver** dialog box displayed.



Add Printer

Install the printer driver

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

Manufacturer	Printers
Apollo	Apollo P-1200
Brother	Apollo P2100/P2300U
Canon	Apollo P2200
Citizen	

This driver is digitally signed.

Tell me why driver signing is important

15. Do one of the following:

- Use the lists to select the printer's manufacturer and model.

- If your printer does not appear in the lists, insert the CD that came with your printer in the computer's CD-ROM drive, and click **Have Disk.**

16. Click **Next.**

17. Complete the remaining dialog boxes in the wizard as desired, and click **Finish.**

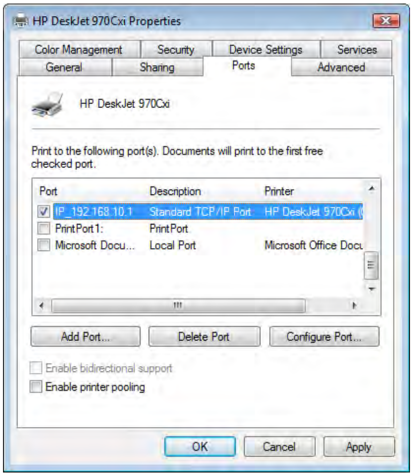
    The printer appears in the **Printers and Faxes** window.

18. Right-click the printer and click **Properties** in the popup menu.

    The printer's **Properties** dialog box opens.

19. In the **Ports** tab, in the list box, select the port you added.

    The port's name is IP_<LAN IP address>.



Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
☑ IP_192.168.10.1	Standard TCP/IP Port	HP DeskJet 970Cxi (
□ PrintPort1:	PrintPort	
□ Microsoft Docu...	Local Port	Microsoft Office Docu

□ Enable bidirectional support

□ Enable printer pooling

20. Click **OK.**

Windows 2000/XP

This procedure is relevant for computers with a Windows 2000/XP operating system.

To configure a computer to use a network printer

1. If the computer for which you want to enable printing is located on the WAN, create an Allow rule for connections from the computer to This Gateway.

   See ***Adding and Editing Rules*** on page 364.

2. Click Start > Settings > Control Panel.

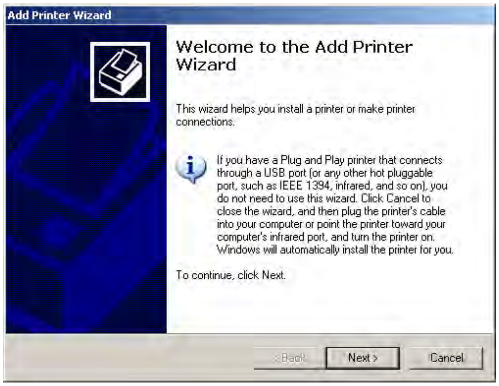
   The Control Panel window opens.

3. Click Printers and Faxes.

   The Printers and Faxes window opens.

4. Right-click in the window, and click Add Printer in the popup menu.

   The Add Printer Wizard opens with the Welcome dialog box displayed.



Add Printer Wizard

Welcome to the Add Printer Wizard

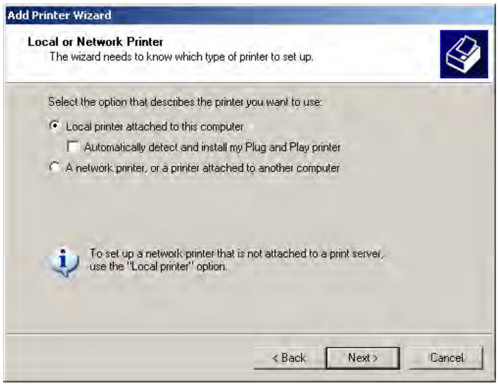
This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

5. Click Next.

The **Local or Network Printer** dialog box appears.



Add Printer Wizard

Local or Network Printer
The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

● Local printer attached to this computer

□ Automatically detect and install my Plug and Play printer

○ A network printer, or a printer attached to another computer

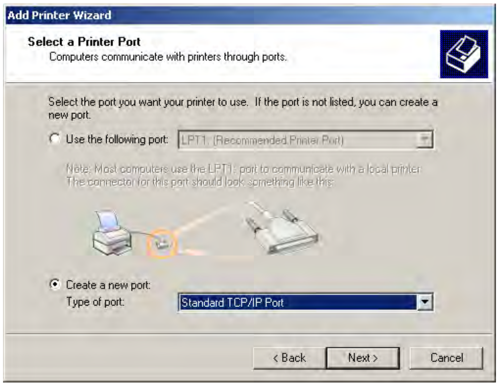
To set up a network printer that is not attached to a print server, use the "Local printer" option.

6. Click **Local printer attached to this computer.**

Note: Do not select the **Automatically detect and install my Plug and Play printer** check box.

7. Click **Next.**

The **Select a Printer Port** dialog box appears.



Add Printer Wizard

Select a Printer Port
Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

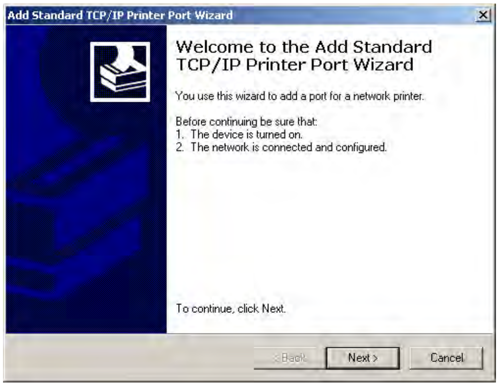
○ Use the following port: LPT1: (Recommended Printer Port)

Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:

● Create a new port:
Type of port: Standard TCP/IP Port

8. Click **Create a new port.**
9. In the **Type of port** drop-down list, select **Standard TCP/IP Port.**
10. Click **Next.**

The **Add Standard TCP/IP Port Wizard** opens with the **Welcome** dialog box displayed.



Welcome to the Add Standard TCP/IP Printer Port Wizard

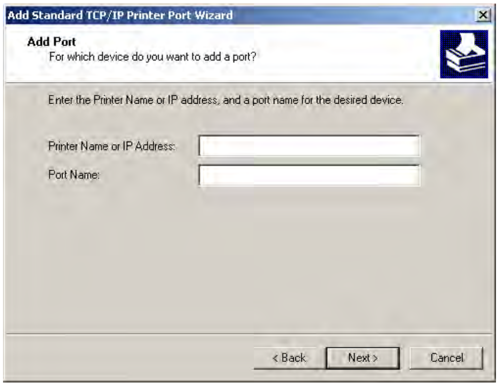
You use this wizard to add a port for a network printer.

Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.

To continue, click Next.

11. Click **Next.**

    The **Add Port** dialog box appears.



Add Port
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address:

Port Name:

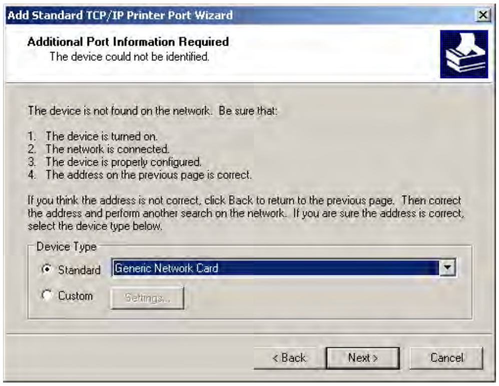
12. In the **Printer Name or IP Address** field, type the Safe@Office appliance's LAN IP address, or "my.firewall".

    You can find the LAN IP address in the Safe@Office Portal, under **Network > My Network.**

    The **Port Name** field is filled in automatically.

13. Click **Next.**

The **Add Standard TCP/IP Printer Port Wizard** opens, with the **Additional Port Information Required** dialog box displayed.



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required
The device could not be identified.

The device is not found on the network. Be sure that:

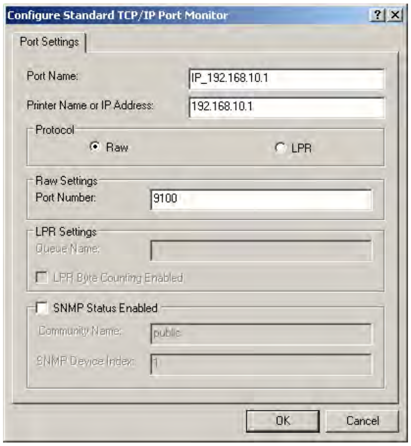
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type
● Standard: Generic Network Card
○ Custom

14. Click **Custom**.
15. Click **Settings**.

The **Configure Standard TCP/IP Port Monitor** dialog box opens.



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.10.1
Printer Name or IP Address: 192.168.10.1

Protocol
● Raw ○ LPR

Raw Settings
Port Number: 9100

LPR Settings
Queue Name:
□ LPR Byte Counting Enabled

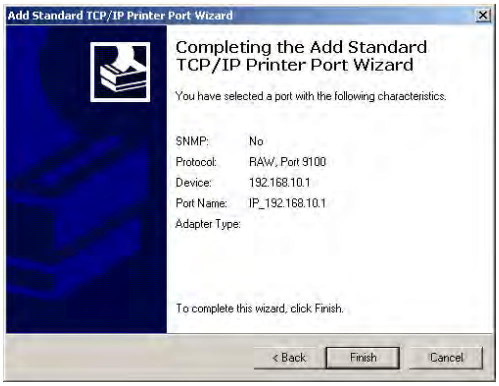
□ SNMP Status Enabled
Community Name: public
SNMP Device Index: 1

16. In the **Port Number** field, type the printer's port number, as shown in the **Printers** page.
17. In the **Protocol** area, make sure that **Raw** is selected.
18. Click **OK**.

The **Add Standard TCP/IP Printer Port Wizard** reappears.

19. Click **Next**.

    The **Completing the Add Standard TCP/IP Printer Port Wizard** dialog box appears.



Completing the Add Standard TCP/IP Printer Port Wizard

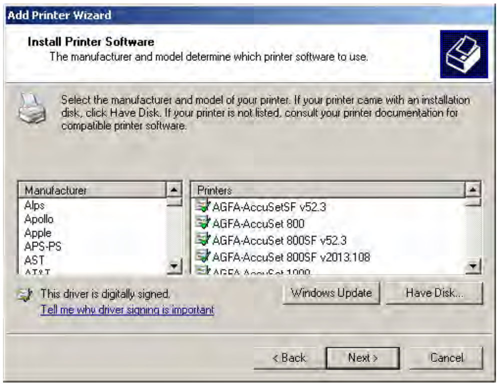
You have selected a port with the following characteristics.

SNMP: No
Protocol: RAW, Port 9100
Device: 192.168.10.1
Port Name: IP_192.168.10.1
Adapter Type:

To complete this wizard, click Finish.

20. Click **Finish**.

    The **Add Printer Wizard** reappears, with the **Install Printer Software** dialog box displayed.



Install Printer Software
The manufacturer and model determine which printer software to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

This driver is digitally signed.
Tell me why driver signing is important

21. Do one of the following:

    - Use the lists to select the printer's manufacturer and model.
    - If your printer does not appear in the lists, insert the CD that came with your printer in the computer's CD-ROM drive, and click **Have Disk**.

22. Click **Next**.

23. Complete the remaining dialog boxes in the wizard as desired, and click **Finish**.

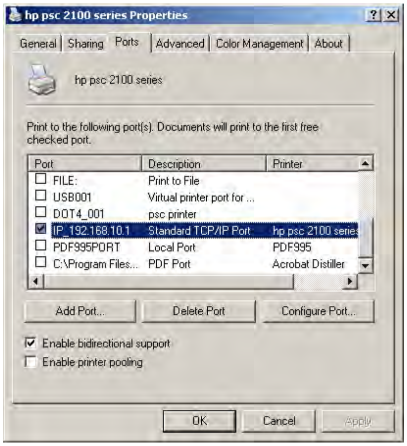
    The printer appears in the **Printers and Faxes** window.

24. Right-click the printer and click **Properties** in the popup menu.

    The printer's **Properties** dialog box opens.

25. In the **Ports** tab, in the list box, select the port you added.

    The port's name is IP_<LAN IP address>.



hp psc 2100 series Properties

? ×
General | Sharing | Ports | Advanced | Color Management | About

hp psc 2100 series

Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
□ FILE:	Print to File	
□ USB001	Virtual printer port for ...	
□ DOT4_001	psc printer	
☑ IP_192.168.10.1	Standard TCP/IP Port	hp psc 2100 series
□ PDF995PORT	Local Port	PDF995
□ C:\Program Files...	PDF Port	Acrobat Distiller

Add Port...
Delete Port
Configure Port...

☑ Enable bidirectional support
□ Enable printer pooling

26. Click **OK**.

MAC OS-X

This procedure is relevant for computers with the latest version of the MAC OS-X operating system.

Note: This procedure may not apply to earlier MAC OS-X versions.

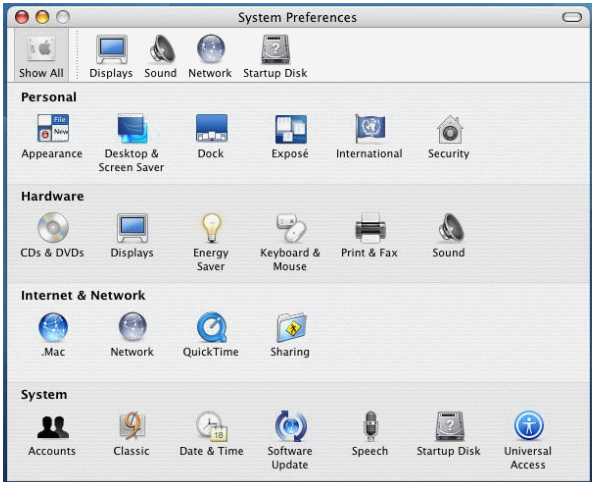
To configure a computer to use a network printer

1. If the computer for which you want to enable printing is located on the WAN, create an Allow rule for connections from the computer to This Gateway.

   See ***Adding and Editing Rules*** on page 364.

2. Choose Apple -> System Preferences.

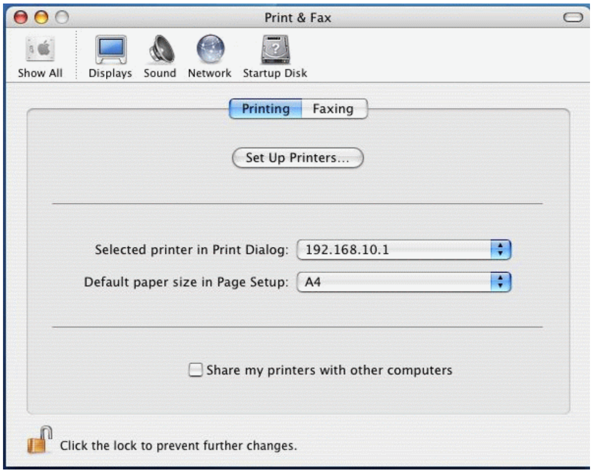
   The System Preferences window appears.



3. Click Show All to display all categories.

4. In the Hardware area, click Print & Fax.

The **Print & Fax** window appears.



Selected printer in Print Dialog: 192.168.10.1

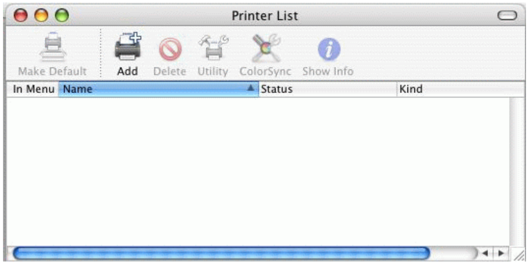
Default paper size in Page Setup: A4

□ Share my printers with other computers

Click the lock to prevent further changes.

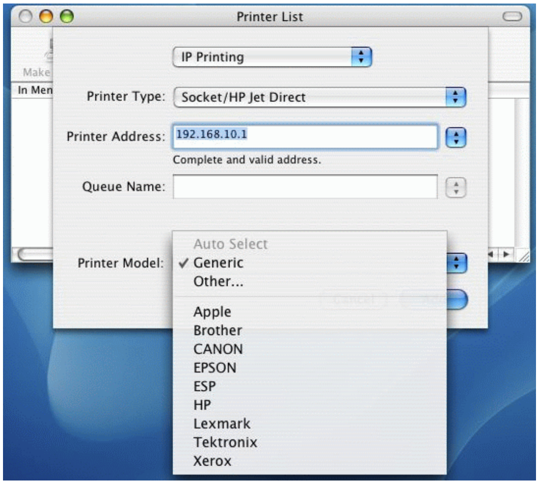
5. In the **Printing** tab, click **Set Up Printers.**

   The **Printer List** window appears.



6. Click **Add.**

New fields appear.



Printer List

IP Printing

Printer Type: Socket/HP Jet Direct

Printer Address: 192.168.10.1

Complete and valid address.

Queue Name:

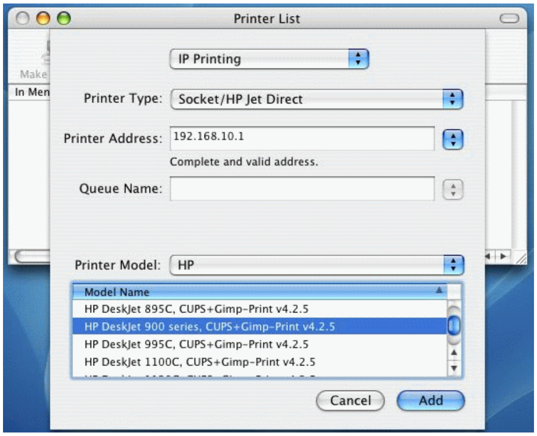
Printer Model: ✓ Generic

7. In the first drop-down list, select **IP Printing**.
8. In the **Printer Type** drop-down list, select **Socket/HP Jet Direct**.
9. In the **Printer Address** field, type the Safe@Office appliance's LAN IP address, or "my.firewall".

   You can find the LAN IP address in the Safe@Office Portal, under **Network > My Network**.
10. In the **Queue Name** field, type the name of the required printer queue.

    For example, the printer queue name for HP printers is RAW.
11. In the **Printer Model** list, select the desired printer type.

A list of models appears.



IP Printing

Printer Type: Socket/HP Jet Direct

Printer Address: 192.168.10.1

Complete and valid address.

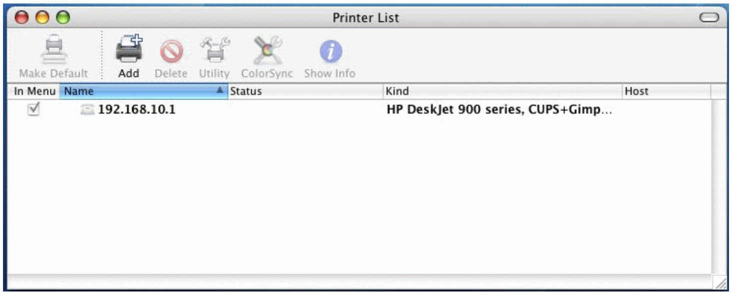
Queue Name:

Printer Model: HP

Model Name
- HP DeskJet 895C, CUPS+Gimp-Print v4.2.5
- HP DeskJet 900 series, CUPS+Gimp-Print v4.2.5
- HP DeskJet 995C, CUPS+Gimp-Print v4.2.5
- HP DeskJet 1100C, CUPS+Gimp-Print v4.2.5

12. In the **Model Name** list, select the desired model.
13. Click **Add**.

The new printer appears in the **Printer List** window.



In Menu	Name	Status	Kind	Host
☑	192.168.10.1		HP DeskJet 900 series, CUPS+Gimp...	

14. In the **Printer List** window, select the newly added printer, and click **Make Default**.

Viewing Network Printers

USB

To view network printers

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Next to USB, click Edit.

   The USB Devices page appears, displaying a list of connected printers.

   For each printer, the model, serial number, and status is displayed.

   A printer can have the following statuses:

   - Initialize. The printer is initializing.
   - Ready. The printer is ready.
   - Not Ready. The printer is not ready. For example, it may be out of paper.
   - Printing. The printer is processing a print job.
   - Restarting. The printer server is restarting.
   - Fail. An error occurred. See the Event Log for details (***Viewing the Event Log*** on page 339).

3. To refresh the display, click Refresh.

Changing Network Printer Ports

USB

When you set up a new network printer, the Safe@Office appliance automatically assigns a port number to the printer. If you want to use a different port number, you can easily change it, as described in ***Setting Up Network Printers*** on page 734.

However, you may sometimes need to change the port number after completing printer setup. For example, you may want to replace a malfunctioning network printer, with another existing network printer, without reconfiguring the client computers. To do this, you must change the replacement printer's port number to the malfunctioning printer's port number, as described below.

Note: Each printer port number must be different, and must be a high port.

To change a printer's port

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Next to USB, click Edit.

   The USB Devices page appears, displaying a list of connected printers.

3. Next to the desired printer, click Edit.

   The Printer Setup page appears.

4. In the printer's Printer Server TCP Port field, type the desired port number.

5. Click Apply.

Resetting Network Printers

USB

You can cause a network printer to restart the current print job, by resetting the network printer. You may want to do this if the print job has stalled.

To reset a network printer

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Next to USB, click Edit.

   The USB Devices page appears, displaying a list of connected printers.

3. Next to the desired printer, click Reset Server.

   The network printer's current print job is restarted.

Chapter 25

Troubleshooting

This chapter provides solutions to common problems you may encounter while using the Safe@Office appliance.

Note: For information on troubleshooting wireless connectivity, see ***Troubleshooting Wireless Connectivity*** on page 302.

This chapter includes the following topics:

Connectivity

I cannot access the Internet. What should I do?

- Verify that the Safe@Office appliance is operating. If not, check the power connection to the Safe@Office appliance.
- Check if the LED for the WAN port is green. If not, check the network cable to the modem and make sure the modem is turned on.
- Check if the LED for the LAN port used by your computer is green. If not, check if the network cable linking your computer to the Safe@Office appliance is connected properly. Try replacing the cable or connecting it to a different LAN port.
- Using your Web browser, go to http://my.firewall and see whether "Connected" appears on the Status Bar. Make sure that your Safe@Office appliance network settings are configured as per your ISP directions.
- Check your TCP/IP configuration according to ***Installing and Setting up the Safe@Office Appliance*** on page 45.
- If Web Filtering or Email Filtering are on, try turning them off.

- Check if you have defined firewall rules which block your Internet connectivity.
- Check with your ISP for possible service outage.
- Check whether you are exceeding the maximum number of computers allowed by your license, by viewing the My Computers page.

I cannot access my DSL broadband connection. What should I do?

DSL equipment comes in two flavors: bridges (commonly known as DSL modems) and routers. Some DSL equipment can be configured to work both ways.

- If you connect to your ISP using a PPPoE or PPTP dialer defined in your operating system, your equipment is most likely configured as a DSL bridge. Configure a PPPoE or PPTP type DSL connection.
- If you were not instructed to configure a dialer in your operating system, your equipment is most likely configured as a DSL router. Configure a LAN connection, even if you are using a DSL connection.

For instructions, see ***Configuring the Internet Connection*** on page 85.

I cannot access my Cable broadband connection. What should I do?

- Some cable ISPs require you to register the MAC address of the device behind the cable modem. You may need to clone your Ethernet adapter MAC address onto the Safe@Office appliance. For instructions, see ***Configuring the Internet Connection*** on page 85.
- Some cable ISPs require using a hostname for the connection. Try reconfiguring your Internet connection and specifying a hostname. For further information, see ***Configuring the Internet Connection*** on page 85.

I cannot access my ADSL connection from an ADSL appliance. What should I do?

- Check that a micro-filter is used on all the phone sockets on the line (required in most locations).
- Check that the DSL Standard setting configured for your appliance is compatible with your service provider. You can view this setting in the Network > Internet Setup page.
- Advanced ADSL configuration fine tuning options are available via the CLI. For information, refer to the *Embedded NGX CLI Reference Guide*.

I cannot access http://my.firewall or http://my.vpn. What should I do?

- Verify that the Safe@Office appliance is operating.
- Check if the LED for the LAN port used by your computer is green. If not, check if the network cable linking your computer to the Safe@Office appliance is connected properly.
- By default, unencrypted HTTP access is not allowed from the wireless LAN to http://my.firewall or http://my.vpn. Therefore, if you are connecting from the wireless LAN, try connecting to https://my.firewall instead.
- Try surfing to 192.168.10.1 instead of to my.firewall.

Note: 192.168.10 is the default value, and it may vary if you changed it in the My Network page.

- Check your TCP/IP configuration according to ***Installing and Setting up the Safe@Office Appliance*** on page 45.
- Restart your Safe@Office appliance and your broadband modem by disconnecting the power and reconnecting after 5 seconds.
- If your Web browser is configured to use an HTTP proxy to access the Internet, add my.firewall or my.vpn to your proxy exceptions list.

My network seems extremely slow. What should I do?

- The Ethernet cables may be faulty. For proper operation, the Safe@Office appliance requires STP CAT5 (Shielded Twisted Pair Category 5) Ethernet cables. Make sure that this specification is printed on your cables.
- Your Ethernet card may be faulty or incorrectly configured. Try replacing your Ethernet card.
- There may be an IP address conflict in your network. Check that the TCP/IP settings of all your computers are configured to obtain an IP address automatically.

I changed the network settings to incorrect values and am unable to correct my error. What should I do?

Reset the network to its default settings using the button on the back of the Safe@Office appliance unit. See ***Resetting the Safe@Office Appliance to Defaults*** on page 728.

I am using the Safe@Office appliance behind another NAT device, and I am having problems with some applications. What should I do?

By default, the Safe@Office appliance performs Network Address Translation (NAT). It is possible to use the Safe@Office appliance behind another device that performs NAT, such as a DSL router or Wireless router, but the device will block all incoming connections from reaching your Safe@Office appliance.

To fix this problem, do ONE of the following. (The solutions are listed in order of preference.)

- Consider whether you really need the router. The Safe@Office appliance can be used as a replacement for your router, unless you need it for some additional functionality that it provides.
- If possible, disable NAT in the router. Refer to the router's documentation for instructions on how to do this.
- If the router has a "DMZ Computer" or "Exposed Host" option, set it to the Safe@Office appliance's external IP address.
- Open the following ports in the NAT device:
  - UDP 9281/9282
  - UDP 500
  - UDP 2746
  - TCP 256
  - TCP 264
  - ESP IP protocol 50
  - TCP 981

I cannot receive audio or video calls through the Safe@Office appliance. What should I do?

To enable audio/video, you must configure an IP Telephony (H.323) virtual server. For instructions, see ***Configuring Servers*** on page 357.

I run a public Web server at home but it cannot be accessed from the Internet. What should I do?

Configure a virtual Web Server. For instructions, see ***Configuring Servers*** on page 357.

I cannot connect to the LAN network from the DMZ or primary WLAN network. What should I do?

By default, connections from the DMZ or primary WLAN network to the LAN network are blocked. To allow traffic from the DMZ or primary WLAN to the LAN, configure appropriate firewall rules. For instructions, see ***Using Rules*** on page 360.

Service Center and Upgrades

I have exceeded my node limit. What does this mean? What should I do?

Your Product Key specifies a maximum number of nodes that you may connect to the Safe@Office appliance.

The Safe@Office appliance tracks the cumulative number of nodes on the internal network that have communicated through the firewall. When the Safe@Office appliance encounters an IP address that exceeds the licensed node limit, the My Computers page displays a warning message and marks nodes over the node limit in red. These nodes will not be able to access the Internet through the Safe@Office appliance, but will be protected. The Event Log page also warns you that you have exceeded the node limit.

To upgrade your Safe@Office appliance to support more nodes, purchase a new Product Key. Contact your reseller for upgrade information.

While trying to connect to a Service Center, I received the message “The Service Center did not respond”. What should I do?

- If you are using a Service Center other than the Check Point Service Center, check that the Service Center IP address is typed correctly.
- The Safe@Office appliance connects to the Service Center using UDP ports 9281/9282. If the Safe@Office appliance is installed behind another firewall, make sure that these ports are open.

I purchased an advanced Safe@Office model, but I only have the functionality of a simpler Safe@Office model. What should I do?

Your have not installed your product key. For further information, see ***Upgrading Your Software Product*** on page 685.

Other Problems

I have forgotten my password. What should I do?

Reset your Safe@Office appliance to factory defaults using the Reset button as detailed in ***Resetting the Safe@Office Appliance to Defaults*** on page 728.

Why are the date and time displayed incorrectly?

You can adjust the time on the Setup page's Tools tab. For information, see ***Setting the Time on the Appliance*** on page 699.

I cannot use a certain network application. What should I do?

Look at the Event Log page. If it lists blocked attacks, do the following:

- Set the Safe@Office appliance's firewall level to Low and try again.
- If the application still does not work, set the computer on which you want to use the application to be the exposed host.

  For instructions, see Defining an Exposed Host.

When you have finished using the application, make sure to clear the exposed host setting, otherwise your security might be compromised.

In the Safe@Office Portal, I do not see the pop-up windows that the guide describes. What should I do?

Disable any pop-up blockers for http://my.firewall.

Chapter 26

Specifications

This chapter includes the following topics:

Technical Specifications

Check Point is committed to protecting the environment. Safe@Office unified threat management appliances are compliant with the RoHS Directive, meeting the European Union's strict restrictions on hazardous substances.

RoHS & WEEE Declaration and Certification

The Safe@Office appliance has been verified to comply with the following directives, throughout the design, development, and supply chain stages:

- Directive of the European Parliament and of the Council, of 27 January 2003, on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS – 2002/95/EC)
- Directive of the European Parliament and of the Council, of 27 January 2003, on Waste Electrical and Electronic Equipment (WEEE – 2002/96/CE)

For a copy of the original signed declaration (in full conformance with EN45014), contact SofaWare technical support at www.sofaware.com/support.

Table 147: Safe@Office ADSL Models Attributes

Attribute	Safe@Office 500 ADSL SBXD-166LHGE-5	Safe@Office 500W ADSL SBXWD-166LHGE-5
Physical Attributes		
Dimensions (width x height x depth)	200 x 33 x 122 mm (7.87 x 1.3 x 4.8 inches)	200 x 33 x 130 mm (7.87 x 1.3 x 5.12 inches) (incl. antenna connectors)
Weight	660 g (1.46 lbs)	694 g (1.53 lbs)
Retail Box Dimensions (width x height x depth)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)
5V Power Supply Unit		
Power Supply Nominal Input	In: 100~240VAC @ 0.5A	In: 100~240VAC @ 0.5A
Power Supply Nominal Output	5V DC @ 3.3A	5V DC @ 3.3A
Max. Power Consumption	8.5W 13.5W (including USB devices)	10.5W 15.5W (including USB devices)
Environmental Conditions		
Temperature: Storage/Transport	-5ºC ~ 80º C	-5ºC ~ 80ºC
Temperature: Operation	0ºC ~ 40ºC	0ºC ~ 40ºC

Humidity: Storage/Operation	10 ~ 95% / 10 ~ 90% (non-condensed)	10 ~ 95% / 10 ~ 90% (non-condensed)
Applicable Standards		
Safety	cULus, CB, LVD	cULus, CB, LVD
Quality	ISO9001, ISO 14001, TL9000	ISO9001, ISO 14001, TL9000
EMC	CE . FCC 15B.VCCI	CE . FCC 15B.VCCI
Reliability	EN 300 019 - 1, 2, 3	EN 300 019 - 1, 2, 3
Environment	RoHS & WEEE	RoHS & WEEE
ADSL	Part 68.CS03	Part 68.CS03
RF	N/A	R&TTE .FCC15C, TELCO

Table 148: Safe@Office Non-ADSL Models Attributes

Attribute	Safe@Office 500 SBX-166LHGE-5	Safe@Office 500W SBXW-166LHGE-5
Physical Attributes		
Dimensions (width x height x depth)	200 x 33 x 122 mm (7.87 x 1.3 x 4.8 inches)	200 x 33 x 130 mm (7.87 x 1.3 x 5.12 inches) (incl. antenna connectors)
Weight	580 g (1.28 lbs)	635 g (1.40 lbs)
Retail Box Dimensions (width x height x depth)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)

5V Power Supply Unit		
Power Supply Nominal Input	In: 100~240VAC @ 0.5A	In: 100~240VAC @ 0.5A
Power Supply Nominal Output	9VAC @ 1.5 A OR: 12VDC @ 1.5 A	12VDC @ 1.5 A
Max. Power Consumption	4.5W	6.5W 11.5W (including USB devices)
Environmental Conditions		
Temperature: Storage/Transport	-5ºC ~ 80ºC	-5ºC ~ 80ºC
Temperature: Operation	0ºC ~ 40ºC	0ºC ~ 40ºC
Humidity: Storage/Operation	10 ~ 95% / 10 ~ 90% (non-condensed)	10 ~ 95% / 10 ~ 90% (non-condensed)
Applicable Standards		
Safety	cULus, CB, LVD	cULus, CB, LVD
Quality	ISO9001, ISO 14001, TL9000	ISO9001, ISO 14001, TL9000
EMC	CE . FCC 15B.VCCI	CE . FCC 15B.VCCI
Reliability	EN 300 019 - 1, 2, 3	EN 300 019 - 1, 2, 3
Environment	RoHS & WEEE	RoHS & WEEE

MTBF (hours)	68,000 hours at 30ºC	68,000 hours at 30ºC
RF	N/A	R&TTE .FCC15C,TELCO

Table 149: Safe@Office Non-ADSL Models Attributes

Attribute	Safe@Office 500 SBX-166LHGE-6	Safe@Office 500W SBXW-166LHGE-6
Physical Attributes		
Dimensions (width x height x depth)	200 x 32 x 128 mm (7.87 x 1.26 x 5.04 inches)	200 x 32 x 128 mm (7.87 x 1.26 x 5.04 inches)
Weight	675 g (1.49 lbs)	685 g (1.51 lbs)
Retail Box Dimensions (width x height x depth)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)
Retail box weight	1.36 kg (3 lbs)	1.38 kg (3.04 lbs)
5V Power Supply Unit		
Power Supply Nominal Input	100 to 240 Vac 50 to 60 Hz	100 to 240 Vac 50 to 60 Hz
Power Supply Nominal Output	12VDC @ 1.5 A	12VDC @ 1.5 A
Max. Power Consumption	15W	15W 20W (including USB devices)

Environmental Conditions		
Temperature: Storage/Transport	-20ºC ~ 65ºC	-20ºC ~ 65ºC
Temperature: Operation	0ºC ~ 40ºC	0ºC ~ 40ºC
Humidity: Storage/Operation	10% ~ 85% (non-condensed)	10% ~ 85% (non-condensed)
Applicable Standards		
Safety	EN 60950	EN 60950
Quality	ISO 9001, 9002, 14001	ISO 9001, 9002, 14001
EMC	FCC part 15B	FCC Part 15 B & C
	VCCI V-3/V-4	AS/NZS 4268: 2003 A1
		DGT
Reliability	EN 300 019 - 1, 2, 3	EN 300 019 - 1, 2, 3
Environment	RoHS & WEEE	RoHS & WEEE
MTBF (hours)	68,000	68,000
RF	N/A	R&TTE .FCC15C, TELCO

Wireless Attributes

Table 150: Safe@Office Wireless Attributes

Attribute	All Wireless Models
Operation Frequency	2.412-2.484 MHz
Transmission Power	79.4 mW
Modulation	OFDM, DSSS, 64QAM, 16QAM, QPSK, BPSK, CCK, DQPSK, DBPSK
WPA Authentication Modes	EAP-TLS, EAP-TTLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2)

CE Declaration of Conformity

SofaWare Technologies Ltd., 3 Hilazon St., Ramat-Gan Israel, hereby declares that this equipment is in conformity with the essential requirements specified in Article 3.1 (a) and 3.1 (b) of:

- Directive 89/336/EEC (EMC Directive)
- Directive 73/23/EEC (Low Voltage Directive – LVD)
- Directive 99/05/EEC (Radio Equipment and Telecommunications Terminal Equipment Directive)

In accordance with the following standards:

Table 151: Safe@Office Appliance Standards

Attribute	Safe@Office 500 SBX-166LHGE-5	Safe@Office 500 SBX-166LHGE-6 / Safe@Office 500W SBXW-166LHGE-6
EMC	EN 55022	EN 50081-1
	EN 61000-3-2	EN 50082-1
	EN 61000-3-3	EN 61000-6-1
	EN 61000-4-2	EN 61000-6-3
	EN 61000-4-3	EN 55022
	EN 61000-4-4	EN 55024
	EN 61000-4-5	EN 61000-3-2
	EN 61000-4-6	EN 61000-3-3

Attribute	Safe@Office 500 SBX-166LHGE-5	Safe@Office 500 SBX-166LHGE-6 / Safe@Office 500W SBXW-166LHGE-6
	EN 61000-4-8	EN 61000-4-2
	EN 61000-4-11	EN 61000-4-3
	ENV50204	EN 61000-4-4
		EN 61000-4-5
		EN 61000-4-6
		EN 61000-4-7
		EN 61000-4-8
		EN 61000-4-9
		EN 61000-4-10
		EN 61000-4-11
		EN 61000-4-12
Safety	EN 60950	EN 60950
	IEC 60950	IEC 60950

The "CE" mark is affixed to this product to demonstrate conformance to the R&TTE Directive 99/05/EEC (Radio Equipment and Telecommunications Terminal Equipment Directive) and FCC Part 15 Class B.

The product has been tested in a typical configuration. For a copy of the Original Signed Declaration (in full conformance with EN45014), please contact SofaWare at the above address.

Federal Communications Commission Radio Frequency Interference Statement

This equipment complies with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Shielded cables must be used with this equipment to maintain compliance with FCC regulations.

Any changes or modifications to this product not explicitly approved by the manufacturer could void the user’s authority to operate the equipment and any assurances of Safety or Performance, and could result in violation of Part 15 of the FCC Rules.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

FCC Radiation Exposure Statement for Wireless Models

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this equipment must be installed to provide a separation distance of at least eight inches (20 cm) from all persons. This equipment must not be operated in conjunction with any other antenna.

Glossary of Terms

A

ADSL Modem

A device connecting a computer to the Internet via an existing phone line. ADSL (Asymmetric Digital Subscriber Line) modems offer a high-speed 'always-on' connection.

C

CA

The Certificate Authority (CA) issues certificates to entities such as gateways, users, or computers. The entity later uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself), and possibly the IP address.

After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

Cable Modem

A device connecting a computer to the Internet via the cable television network. Cable modems offer a high-speed 'always-on' connection.

Certificate Authority

The Certificate Authority (CA) issues certificates to entities such as gateways, users, or computers. The entity later uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself), and possibly the IP address.

After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

Cracking

An activity in which someone breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is that whatever resides on the computer can be viewed and sensitive data can be stolen without anyone knowing about it. Sometimes, tiny programs are 'planted' on the computer that are designed to watch out for, seize and then transmit to another computer, specific types of data.

D

DHCP

Any machine requires a unique IP address to connect to the Internet using Internet Protocol. Dynamic Host Configuration Protocol (DHCP) is a communications protocol that assigns Internet Protocol (IP) addresses to computers on the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer.

DMZ

A DMZ (demilitarized zone) is an internal network defined in addition to the LAN network and protected by the Safe@Office appliance.

DNS

The Domain Name System (DNS) refers to the Internet domain names, or easy-to-remember "handles", that are translated into IP addresses.

An example of a Domain Name is 'www.sofaware.com'.

Domain Name System

Domain Name System. The Domain Name System (DNS) refers to the Internet domain names, or easy-to-remember "handles", that are translated into IP addresses.

An example of a Domain Name is 'www.sofaware.com'.

E

Exposed Host

An exposed host allows one computer to be exposed to the Internet. An example of using an exposed host would be exposing a public server, while preventing outside users from getting direct access form this server back to the private network.

F

Firmware

Software embedded in a device.

G

Gateway

A network point that acts as an entrance to another network.

H

Hacking

An activity in which someone breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is that whatever resides on the computer can be viewed and sensitive data can be stolen without anyone knowing about it. Sometimes, tiny programs are 'planted' on the computer that are designed to watch out for, seize and then transmit to another computer, specific types of data.

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL.

A protocol for accessing a secure Web server. It uses SSL as a sublayer under the regular HTTP application. This directs messages to a secure port number rather than the default Web port number, and uses a public key to encrypt data

HTTPS is used to transfer confidential user information.

Hub

A device with multiple ports, connecting several PCs or network devices on a network.

I

IP Address

An IP address is a 32-bit number that identifies each computer sending or receiving data packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IP Spoofing

A technique where an attacker attempts to gain unauthorized access through a false source address to make it appear as though communications have originated in a part of the network with higher access privileges. For example, a packet originating on the Internet may be masquerading as a local packet with the source IP address of an internal host. The firewall can protect against IP spoofing attacks by limiting network access based on the gateway interface from which data is being received.

IPSEC

IPSEC is the leading Virtual Private Networking (VPN) standard. IPSEC enables individuals or offices to establish secure communication channels ('tunnels') over the Internet.

ISP

An ISP (Internet service provider) is a company that provides access to the Internet and other related services.

L

LAN

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single server within a small geographic area.

M

MAC Address

The MAC (Media Access Control) address is a computer's unique hardware number. When connected to the Internet from your computer, a mapping relates your IP address to your computer's physical (MAC) address on the LAN.

Mbps

Megabits per second. Measurement unit for the rate of data transmission.

MTU

The Maximum Transmission Unit (MTU) is a parameter that determines the largest datagram than can be transmitted by an IP interface (without it needing to be broken down into smaller units). The MTU should be larger than the largest datagram you wish to transmit un-fragmented. Note: This only prevents fragmentation locally. Some other link in the path may have a smaller MTU - the datagram will be fragmented at that point. Typical values are 1500 bytes for an Ethernet interface or 1452 for a PPP interface.

N

NAT

Network Address Translation (NAT) is the translation or mapping of an IP address to a different IP address. NAT can be used to map several internal IP addresses to a single IP address, thereby sharing a single IP address assigned by the ISP among several PCs.

Check Point FireWall-1's Stateful Inspection Network Address Translation (NAT) implementation supports hundreds of pre-defined applications, services, and protocols, more than any other firewall vendor.

NetBIOS

NetBIOS is the networking protocol used by DOS and Windows machines.

P

Packet

A packet is the basic unit of data that flows from one source on the Internet to another destination on the Internet. When any file (e-mail message, HTML file, GIF file etc.) is sent from one place to another on the Internet, the file is divided into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file at the receiving end.

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) enables connecting multiple computer users on an Ethernet local area network to a remote site or ISP, through common customer premises equipment (e.g. modem).

PPTP

The Point-to-Point Tunneling Protocol (PPTP) allows extending a local network by establishing private “tunnels” over the Internet. This protocol it is also used by some DSL providers as an alternative for PPPoE.

R

RJ-45

The RJ-45 is a connector for digital transmission over ordinary phone wire.

Router

A router is a device that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks.

S

Server

A server is a program (or host) that awaits and requests from client programs across the network. For example, a Web server is the computer program, running on a specific host, that serves requested HTML pages or files. Your browser is the client program, in this case.

Stateful Inspection

Stateful Inspection was invented by Check Point to provide the highest level of security by examining every layer within a packet, unlike other systems of inspection. Stateful Inspection extracts information required for security decisions from all application layers and retains this information in dynamic state tables for evaluating subsequent connection attempts. In other words, it learns!

Subnet Mask

A 32-bit identifier indicating how the network is split into subnets. The subnet mask indicates which part of the IP address is the host ID and which indicates the subnet.

T

TCP

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

For example, when an HTML file is sent to you from a Web server, the Transmission Control Protocol (TCP) program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network.

At the other end (the client program in your computer), TCP reassembles the individual packets and waits until they have arrived to forward them to you as a single file.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the underlying communication protocol of the Internet.

U

UDP

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end.

UDP is often used for applications such as streaming data.

URL

A URL (Uniform Resource Locator) is the address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol. On the Web (which uses the Hypertext Transfer Protocol), an example of a URL is 'http://www.sofaware.com'.

V

VPN

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

VPN tunnel

A secure connection between a Remote Access VPN Client and a Remote Access VPN Server.

W

WLAN

A WLAN is a wireless local area network protected by the Safe@Office appliance.

Index