Check Point Safe@Office

Internet Security Appliance

User Guide

Version 4.0.50

Part No:700797, October, 2003

COPYRIGHT & TRADEMARKS

Information in this document is subject to change without notice and does not represent a commitment on part of SofaWare Technologies Ltd.

SofaWare, Safe@Home and Safe@Office are trademarks, service marks, or registered trademarks of SofaWare Technologies Ltd.

Check Point, the Check Point logo, FireWall-1, FireWall-1 SecureServer, FireWall-1 SmallOffice, FloodGate-1, INSPECT, IQ Engine, Meta IP, MultiGate, Open Security Extension, OPSEC, Provider-1, SecureKnowledge, SecureUpdate, SiteManager-1, SVN, UAM, User-to-Address Mapping, UserAuthority, Visual Policy Editor, VPN-1, VPN-1 Accelerator Card, VPN-1 Gateway, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, and VPN-1 Edge are trademarks, service marks, or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

The products described in this document are protected by U.S. Patent No. 5,606,668 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, or pending applications.

SAFETY PRECAUTIONS

Carefully read the Safety Instructions the Installation and Operating Procedures provided in this User's Guide before attempting to install or operate the appliance. Failure to follow these instructions may result in damage to equipment and/or personal injuries.

- Before cleaning the appliance, unplug the power cord. Use only a soft cloth dampened with water for cleaning.
- Any changes or modifications to this product not explicitly approved by the manufacturer could void any assurances of Safety or Performance and could result in violation of Part 15 of the FCC Rules.
- When installing the appliance, ensure that the vents are not blocked.
- Do not use the appliance outdoors.
- Do not expose the appliance to liquid or moisture.
- Do not expose the appliance to extreme high or low temperatures.
- Do not drop, throw, or bend the appliance since rough treatment could damage it.
- Do not use any accessories other than those approved by Check Point. Failure to do so may result in loss of performance, damage to the product, fire, electric shock or injury, and will void the warranty.
- Do not disassemble or open the appliance. Failure to comply will void the warranty.
- Do not route the cables in a walkway or in a location that will crimp the cables.

POWER ADAPTER

- The appliance should only be used with the power adapter provided. The power adapter should be plugged into a surge protected power source. In addition, be careful not to overload the wall outlets, extension cords, etc. used to power this unit.
- Connect the power adapter only to power sources as marked on the product.
- To reduce risk of damage to the electric cord, remove it from the outlet by holding the power adapter rather than the cord.

SECURITY DISCLAIMER

The appliance provides your office network with the highest level of security. However, no product can provide you with absolute protection against a determined effort to break into your system. We recommend using additional security measures to secure highly valuable or sensitive information.

Contents

Chapter 1

Introduction

This chapter introduces the Check Point Safe@Office appliance and this guide.

This chapter includes the following topics:

About Your Check Point Safe@Office Appliance

The Check Point Safe@Office appliance is an advanced Internet security appliance that enables secure high-speed Internet access from the office. Developed and supported by SofaWare Technologies, an affiliate of Check Point Software Technologies, the worldwide leader in securing the Internet, the Safe@Office appliance incorporates the 100 and 200 product families. The 100 series and 200 series firewall, based on the world-leading Check Point Embedded NG Stateful Inspection technology, inspects and filters all incoming and outgoing traffic, blocking all unauthorized traffic.

The Safe@Office appliance also allows sharing your Internet connection among several PCs or other network devices, enabling advanced office networking and saving the cost of purchasing static IP addresses.

You can also connect Safe@Office appliances to security services available from select service providers, including firewall security updates, Web filtering, and dynamic DNS. Business users can use the Safe@Office appliance to securely connect to the office network.

Safe@Office Products

The Safe@Office appliance is available with the following hardware: Safe@Office 100 series or Safe@Office 200 series. Both provide a Web-based management interface, which enables you to manage and configure the Safe@Office appliance operation and options. However, the 200 series provides higher firewall and VPN throughput and has a dedicated DMZ port and a serial port.

The 100 series includes models Safe@Office 105 and Safe@Office 110. The 200 series includes model Safe@Office 225 and Safe@Office 225U.

Your Safe@Office appliance can be upgraded to a more advanced model within its hardware series, without replacing the hardware. Contact your reseller for more details.

Safe@Office 105

Safe@Office 105 protects your home or small business network from hostile Internet activity. It can also act as a VPN server which allows a single user to securely access resources protected by the Safe@Office appliance from home or while travelling. It is intended for home or small business users and can be used by up to five computers.

Safe@Office 110

In addition to all the benefits of Safe@Office 105, Safe@Office 110 provides expanded VPN functionality: it acts not only as a VPN server but as a VPN client, enabling employees working from home to securely connect to the office. Safe@Office 110 can also be configured as a VPN gateway, which allows permanent bi-directional connections between two gateways, such as two company offices.

Safe@Office 110 is intended for small and medium businesses with one or more branch offices, and for their employees working from home. It can be used by up to ten computers.

Safe@Office 225

Safe@Office 225 provides all the benefits of Safe@Office 110, along with support for High Availability. High Availability enables you to install a second Safe@Office appliance on your network and configure that appliance as a backup to the first Safe@Office appliance, thereby ensuring that your network is consistently protected and connected to the Internet.

Safe@Office 225 includes a hardware DMZ port and offers higher VPN and firewall performance than the 100 series.

Like Safe@Office 110, Safe@Office 225 is intended for companies with extended VPN networks. Safe@Office 225 supports 25 computers.

Safe@Office 225U

Safe@Office 225U provides the same functionality as Safe@Office 225 but does not have a license limitaion on the number of computers.

All references to Safe@Office 225 in this guide are also relevant to Safe@Office 225U.

Safe@Office Features and Compatibility

Connectivity

Feature	Safe@Office 105	Safe@Office 110	Safe@Office 225/225U
Concurrent firewall connections	2,000	2,000	8,000
LAN Ports	4-ports 10/100 Mbps Fast Ethernet switch	4-ports 10/100 Mbps Fast Ethernet switch	4-ports 10/100 Mbps Fast Ethernet switch

Feature	Safe@Office 105	Safe@Office 110	Safe@Office 225/225U
WAN Port	10/100 Mbps Fast Ethernet	10/100 Mbps Fast Ethernet	10/100 Mbps Fast Ethernet
DMZ/WAN2 Port			10/100 Mbps Fast Ethernet
Serial Console Port			✓
Ethernet cable type recognition			✓
Users (nodes)	5	10	25 or Unlimited
Supported Internet connection methods	Static IP, DHCP Client, Cable Modem, PPTP Client, PPPoE Client, Telstra BPA login		
DHCP Server	✓	✓	✓
MAC Cloning	✓	✓	✓
Backup Internet connection		✓	✓
High Availability			✓
Static NAT		✓	✓
Static Routes		✓	✓

Firewall

Feature	Safe@Office 105	Safe@Office 100	Safe@Office 225/225U
Firewall Type	Check Point Firewall-1 Embedded NG	Check Point Firewall-1 Embedded NG	Check Point Firewall-1 Embedded NG
Network Address Translation (NAT)	✓	✓	✓
INSPECT Policy Rules	Unlimited	Unlimited	Unlimited
User-defined rules	✓	✓	✓
Three levels preset security policies	✓	✓	✓
DoS Protection	✓	✓	✓
Anti-spoofing	✓	✓	✓
Attack Logging	✓	✓	✓
Voice over IP (H.323) Support	✓	✓	✓
Exposed Host	✓	✓	✓
DMZ Network		Logical	Physical

VPN

Feature	Safe@Office 105	Safe@Office 110	Safe@Office 225/225U
VPN Type	Check Point VPN-1 Embedded NG	Check Point VPN-1 Embedded NG	Check Point VPN-1 Embedded NG
IPSEC VPN mode	Remote Access Server	Remote Access Client RemoteAccess Server Site-to-Site	Remote Access Client Remote Access Server Site-to-Site
IPSEC VPN pass-through	✓	✓	✓
Encryption	AES/3DES/DES	AES/3DES/DES	AES/3DES/DES
Authentication	SHA1/MD5	SHA1/MD5	SHA1/MD5
X.509 Digital Certificates		✓	✓
RADIUS client		✓	✓
Hardware Acceleration			✓
Hardware Random Number Generator			✓

Management

Feature	Safe@Office 105	Safe@Office 110	Safe@Office 225/225U
Web Management	✓	✓	✓
HTTPS Access (local and remote)	✓	✓	✓
Multiple Administrators		✓	✓
CLI	✓	✓	✓
Management Systems	SofaWare SMP	SofaWare SMP	SofaWare SMP

Optional Security Services

Feature	Safe@Office 105	Safe@Office 110	Safe@Office 225/225U
Firewall security and software updates	✓	✓	✓
Web Filtering *	✓	✓	✓
Email Antivirus protection *	✓	✓	✓
Dynamic DNS Service *	✓	✓	✓
VPN Management	✓	✓	✓
Centralized Logging and Intrusion Detection	✓	✓	✓

* When managed by SofaWare Security Management Portal (SMP).

Package Contents

- Safe@Office Internet Security Appliance
- CAT5 Straight-through Ethernet Cable
- Power Adapter
- Getting Started Guide
- This Users Guide

Network Requirements

- A broadband Internet connection via cable or DSL modem with Ethernet interface (RJ-45)
- 10BaseT or 100BaseT Network Interface Card installed on each computer
- TCP/IP network protocol installed on each computer
- Internet Explorer 5.0 or higher, or Netscape Navigator 4.7 and higher
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device

Note: To cascade an additional hub or switch to the Safe@Office 100 appliance, you must use a crossed Ethernet cable instead. The Safe@Office 200 series automatically detects the cable type, so you can use either a straight-through or crossed cable.

Note: For optimal results, it is highly recommended to use either Microsoft Internet Explorer 5.5 or higher, or Netscape Navigator 6.2 or higher.

Getting to Know Your Safe@Office 100 Series

Safe@Office 105 | Safe@Office 110 | ~~Safe@Office 225~~

Rear Panel

The following figure shows the Safe@Office 100 series appliance's rear panel. All physical connections (network and power) to the Safe@Office appliance are made via the rear panel of your Safe@Office appliance.

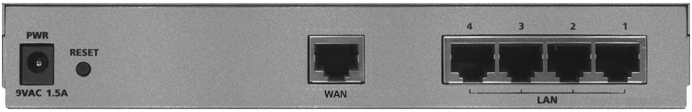


Figure 1: Safe@Office Appliance 100 Rear Panel Items

The following table lists the Safe@Office appliance's rear panel elements.

Table 1: Safe@Office Appliance 100 Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • **Short press**. Reboots the Safe@Office appliance • **Long press (7 seconds)**. Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
WAN	Wide Area Network: An Ethernet port (RJ-45) used for connecting your cable or xDSL modem
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices

Front Panel

The Safe@Office 100 appliance includes several status LEDs that enable you to monitor the appliance's operation.

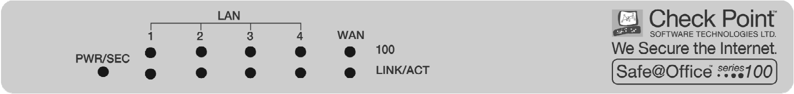


Figure 2: Safe@Office 100 Appliance Front Panel

For an explanation of the Safe@Office 100 appliance's status LEDs, see the table below.

Table 2: Safe@Office 100 Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up
	Flashing slowly (Green)	Establishing Internet connection
	On (Green)	Normal Operation
	Flashing (Red)	Hacker attack blocked
	On (Red)	Error
LAN 1-4/WAN	**LINK/ACT** Off, **100** Off	Link is down.
	LINK/ACT On, **100** Off	10 Mbps link established for the corresponding port.

LED	State	Explanation
	LINK/ACT On, **100** On	100 Mbps link established for the corresponding port.
	LINK/ACT Flashing	Data is being transmitted/received

Getting to Know Your Safe@Office 200 Series

~~Safe@Office 105~~ ~~Safe@Office 110~~ Safe@Office 225

Rear Panel

The following figure shows the Safe@Office 200 series appliance's rear panel. All physical connections (network and power) to the Safe@Office appliance are made via the rear panel of your Safe@Office appliance.

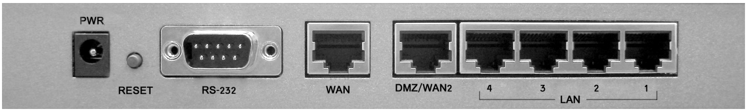


Figure 3: Safe@Office 200 Appliance Rear Panel Items

The following table lists the Safe@Office 200 appliance's rear panel elements.

Table 3: Safe@Office 200 Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • **Short press**. Reboots the Safe@Office appliance • **Long press (7 seconds)**. Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
RS-232	A serial port (reserved for future use)
WAN	Wide Area Network: An Ethernet port (RJ-45) used for connecting your cable or xDSL modem, or for connecting a hub when setting up more than one Internet connection
DMZ/WAN2	A dedicated Ethernet port (RJ-45) used for a DMZ computer, or for a hub when connecting a DMZ network
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices

Front Panel

The Safe@Office 200 appliances includes several status LEDs that enable you to monitor the appliance's operation.

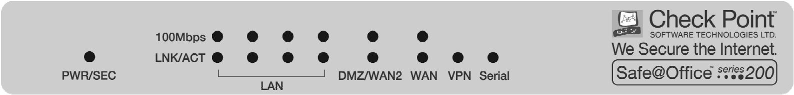


Figure 4: Safe@Office 200 Appliance Front Panel

For an explanation of the Safe@Office 200 appliance's status LEDs, see the table below.

Table 4: Safe@Office 200 Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up
	Flashing slowly (Green)	Establishing Internet connection
	On (Green)	Normal Operation
	Flashing (Red)	Hacker attack blocked
	On (Red)	Error
LAN 1-4/WAN/ DMZ/WAN2	**LINK/ACT** Off, **100** Off	Link is down.
	LINK/ACT On, **100** Off	10 Mbps link established for the corresponding port.

LED	State	Explanation
	LINK/ACT On, **100** On	100 Mbps link established for the corresponding port.
	LINK/ACT Flashing	Data is being transmitted/received.
VPN	Flashing (Green)	VPN tunnel in use
Serial	Flashing (Green)	Serial port in use

About This Guide

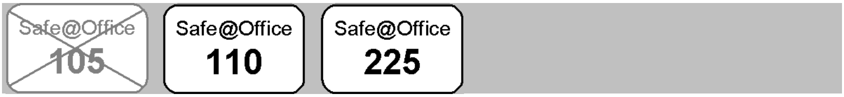
To make finding information in this manual easier, some types of information are marked with special symbols or formatting.

Boldface type is used for command and button names.

Note: Notes are denoted by indented text and preceded by the Note icon.

Warning: Warnings are denoted by indented text and preceded by the Warning icon.

Each task is marked with a product bar indicating the Safe@Office products required to perform the task. If you cannot perform the task using a particular product, that product is crossed out. For example, the product bar below indicates a task that requires Safe@Office 110, 225, or 225U. You cannot perform this task with Safe@Office 105.



Contacting Technical Support

If there is a problem with your Safe@Office appliance, surf to http://www.sofaware.com/support and fill out a technical support request form.

You can also download the latest version of this guide from the site.

Chapter 2

Installing and Setting up the Safe@Office Appliance

This chapter describes how to properly set up and install your Safe@Office appliance in your networking environment.

This chapter includes the following topics:

Before You Install the Safe@Office Appliance

Prior to connecting and setting up your Safe@Office appliance for operation, you must do the following:

- Check if TCP/IP Protocol is installed on your computer.
- Check your computer's TCP/IP settings to make sure it obtains its IP address automatically.

Refer to the relevant section in this guide in accordance with the operating system that runs on your computer. The following sections will guide you through the TCP/IP setup and installation process.

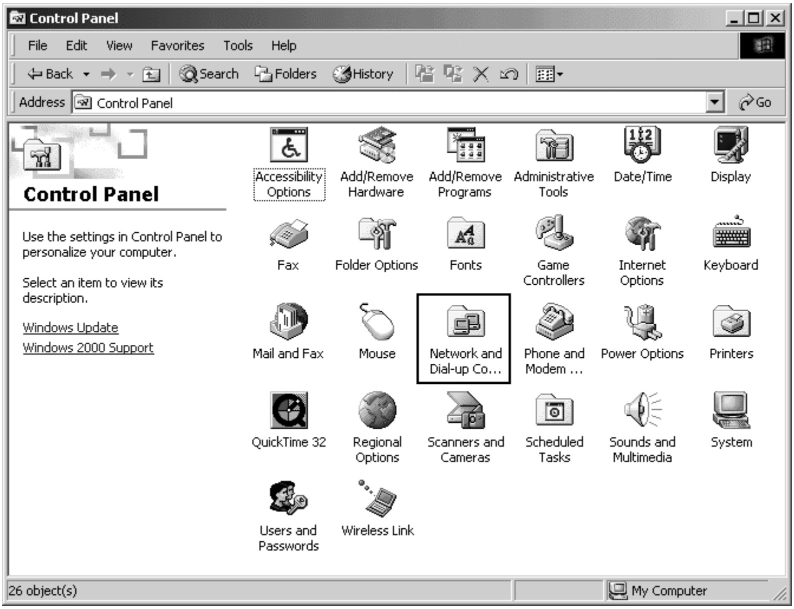
Windows 2000/XP

Note: While Windows XP has an "Internet Connection Firewall" option, it is recommended not to enable it if you are using a Safe@Office appliance, since the Safe@Office appliance offers better protection.

Checking the TCP/IP Installation

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

   The **Control Panel** window appears.

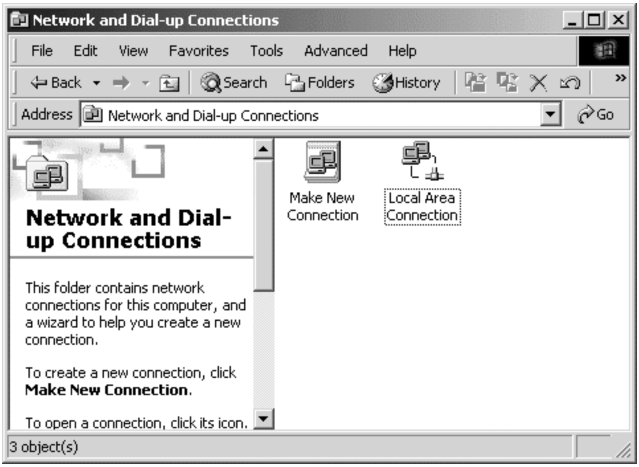


Use the settings in Control Panel to personalize your computer.

Select an item to view its description.

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

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


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections Go
Make New Connection
Local Area Connection
3 object(s)

Network and Dial-up Connections

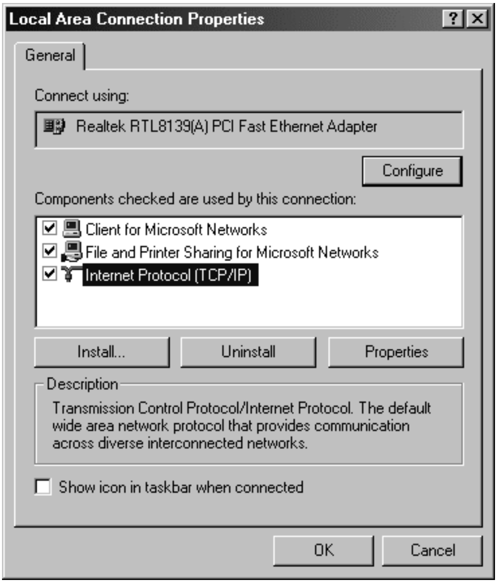
This folder contains network connections for this computer, and a wizard to help you create a new connection.

To create a new connection, click **Make New Connection.**

To open a connection, click its icon.

3. Right-click the Local Area Connection icon and select **Properties** from the pop-up menu that opens.

The **Local Area Connection Properties** window appears.



Local Area Connection Properties

General

Connect using:

Realtek RTL8139(A) PCI Fast Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

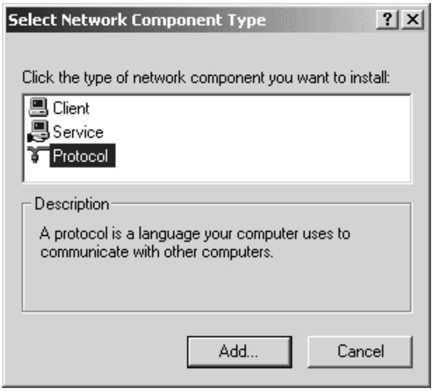
☐ Show icon in taskbar when connected

4. In the above window, check if **TCP/IP** appears in the components list and if it is properly configured with the Ethernet card, installed on your computer. If **TCP/IP** does not appear in the **Components** list, you must install it as described in the next section.

Installing TCP/IP Protocol

1. In the **Local Area Connection Properties** window click **Install...**.

   The **Select Network Component Type** window appears.



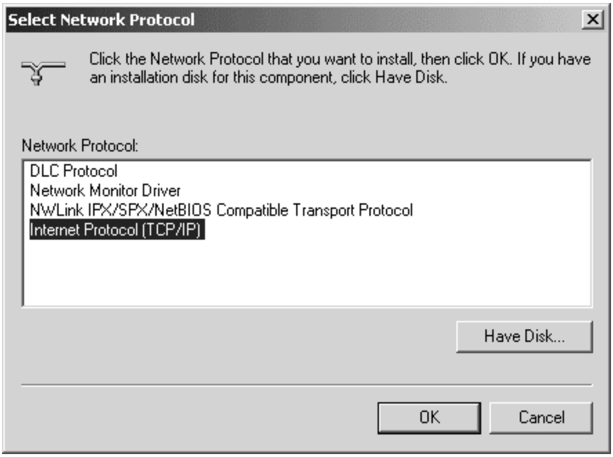
Select Network Component Type

Click the type of network component you want to install:

A protocol is a language your computer uses to communicate with other computers.

2. Choose **Protocol** and click **Add**.

   The **Select Network Protocol** window appears.



Select Network Protocol

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Network Protocol:

DLC Protocol
Network Monitor Driver
NWLink IPX/SPX/NetBIOS Compatible Transport Protocol
Internet Protocol (TCP/IP)
Have Disk...
OK
Cancel

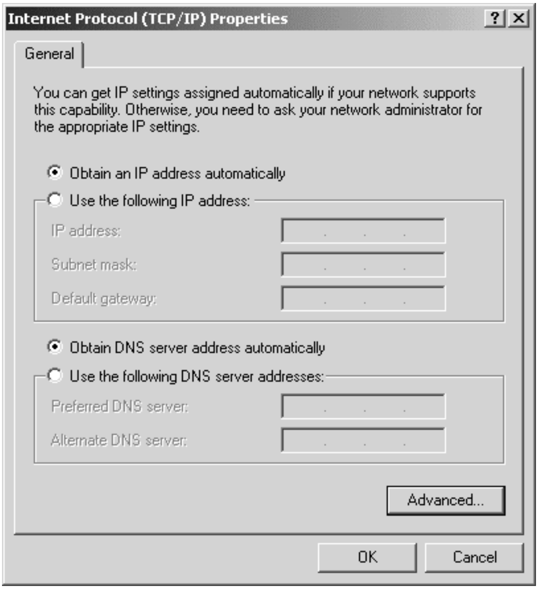
3. Choose **Internet Protocol (TCP/IP)** and click **OK**.

   TCP/IP protocol is installed on your computer.

TCP/IP Settings

1. In the **Local Area Connection Properties** window double-click the **Internet Protocol (TCP/IP)** component, or select it and click **Properties**.

   The **Internet Protocol (TCP/IP) Properties** window opens.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

2. Click the **Obtain an IP address automatically** radio button.

Note: Normally, it is not recommended to assign a static IP address to your PC but rather to obtain an IP address automatically. If for some reason you need to assign a static IP address, select Specify an IP address, type in an IP address in the range of 192.168.10.129-254, enter 255.255.255.0 in the Subnet Mask field, and click OK to save the new settings.

(Note that 192.168.10 is the default value, and it may vary if you changed it in the My Network page.)

3. Click the **Obtain DNS server address automatically** radio button.
4. Click **OK** to save the new settings.

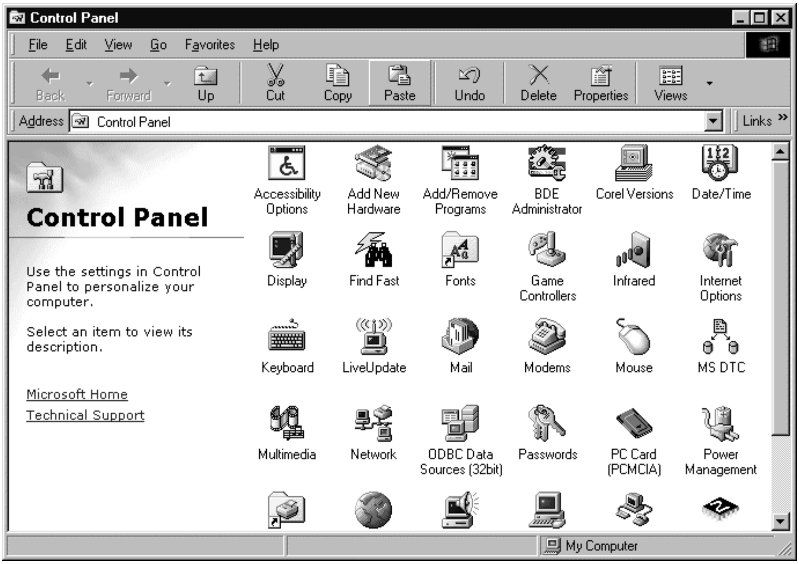
Your computer is now ready to access your Safe@Office appliance.

Windows 98/Millennium

Checking the TCP/IP Installation

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

   The **Control Panel** window appears.

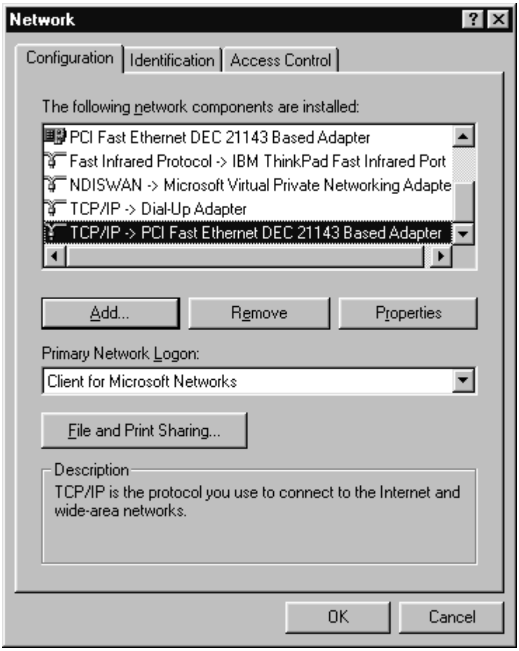


Use the settings in Control Panel to personalize your computer.

Select an item to view its description.

2. Double-click the Network icon.

The **Network** window appears.



Network

Configuration | Identification | Access Control

The following network components are installed:

PCI Fast Ethernet DEC 21143 Based Adapter
Fast Infrared Protocol -> IBM ThinkPad Fast Infrared Port
NDISWAN -> Microsoft Virtual Private Networking Adapte
TCP/IP -> Dial-Up Adapter
TCP/IP -> PCI Fast Ethernet DEC 21143 Based Adapter

Primary Network Logon:
Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

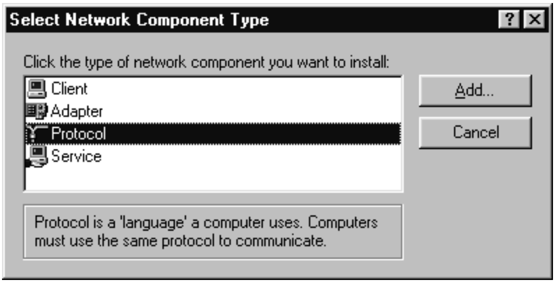
3. In the **Network** window, check if **TCP/IP** appears in the network components list and if it is already configured with the Ethernet card, installed on your computer.

Installing TCP/IP Protocol

Note: If TCP/IP is already installed and configured on your computer skip this section and move directly to TCP/IP Settings.

1. In the **Network** window, click **Add**.

   The **Select Network Component Type** window appears.



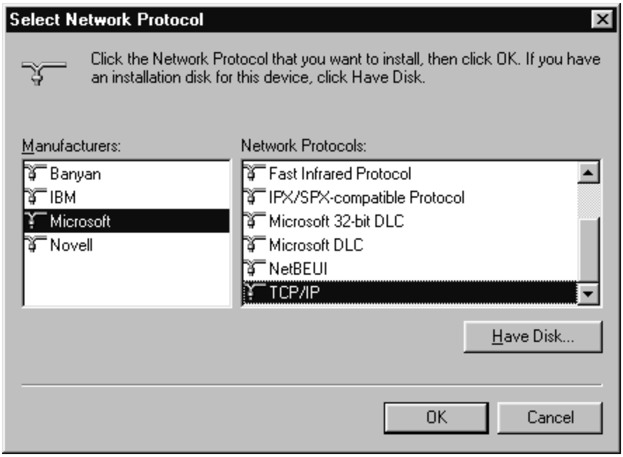
Select Network Component Type

Click the type of network component you want to install:

Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate.

2. Choose **Protocol** and click **Add**.

   The **Select Network Protocol** window appears.



Select Network Protocol

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

Manufacturers: Microsoft

Network Protocols: TCP/IP

3. In the **Manufacturers** list choose **Microsoft**, and in the **Network Protocols** list choose **TCP/IP**.

4. Click **OK**.

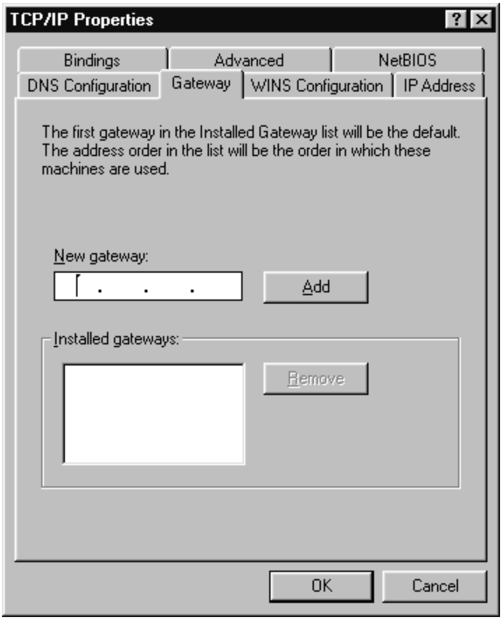
If Windows asks for original Windows installation files, provide the installation CD and relevant path when required (e.g. D:\win98)

5. Restart your computer if prompted.

TCP/IP Settings

Note: If you are connecting your Safe@Office appliance to an existing LAN, consult your network manager for the correct configurations.

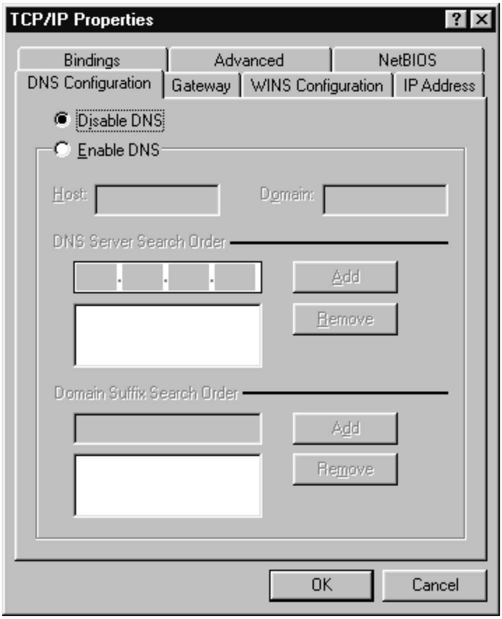
1. In the **Network** window, double-click the **TCP/IP** service for the Ethernet card, which has been installed on your computer (e.g. TCP/IP -> PCI Fast Ethernet DEC 21143 Based Adapter).
   The **TCP/IP Properties** window opens.



The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

2. Click the **Gateway** tab, and remove any installed gateways.

3. Click the **DNS Configuration** tab, and click the **Disable DNS** radio button.



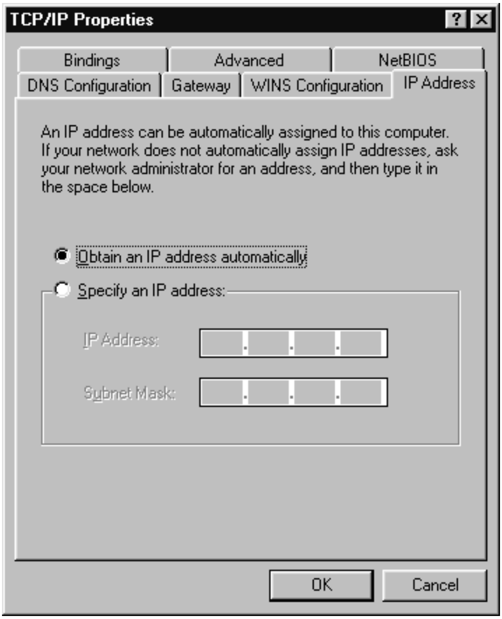
TCP/IP Properties

Tabs: Bindings, Advanced, NetBIOS, DNS Configuration, Gateway, WINS Configuration, IP Address

● Disable DNS

○ Enable DNS

4. Click the **IP Address** tab, and click the **Obtain an IP address automatically** radio button.



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

Note: Normally, it is not recommended to assign a static IP address to your PC but rather to obtain an IP address automatically. If for some reason you need to assign a static IP address, select Specify an IP address, type in an IP address in the range of 192.168.10.129-254, enter 255.255.255.0 in the Subnet Mask field, and click OK to save the new settings.

(Note that 192.168.10 is the default value, and it may vary if you changed it in the My Network page.)

5. Click **Yes** when prompted for "**Do you want to restart your computer?**".

Your computer restarts, and the new settings to take effect.

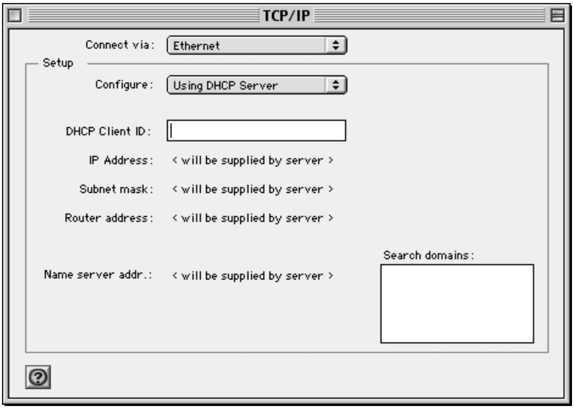
Your computer is now ready to access your Safe@Office appliance.

Mac OS

Use the following procedure for setting up the TCP/IP Protocol.

1. Choose **Apple Menus -> Control Panels -> TCP/IP**.

   The **TCP/IP window** appears.



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Search domains:

Name server addr.: < will be supplied by server >

2. Click the **Connect via** drop-down list and select **Ethernet**.
3. Click the **Configure** drop-down list and select **Using DHCP Server**.
4. Close the window and save the setup.

Network Installation

1. Verify that you have the correct cable type.

   For information, see ***Network Requirements*** on page 9.

2. Connect the LAN cable:

   - Connect one end of the Ethernet cable to one of the **LAN** ports at the back of the unit.
   - Connect the other end to PCs, hubs, or other network devices.

3. Connect the WAN cable:

- Connect one end of the Ethernet cable to the WAN port at the back of the unit.
- Connect the other end of the cable to a Cable Modem, xDSL modem or office network.

4. Connect the power adapter to the power socket, labeled **PWR**, at the back of the Safe@Office appliance. Plug in the AC power adapter to the wall electrical outlet.

Warning: The Safe@Office appliance AC adapter is compatible with either 100, 120 or 230 VAC input power. Please verify that the wall outlet voltage is compatible with the voltage specified on your power supply. Failure to observe this warning may result in injuries or damage to equipment.

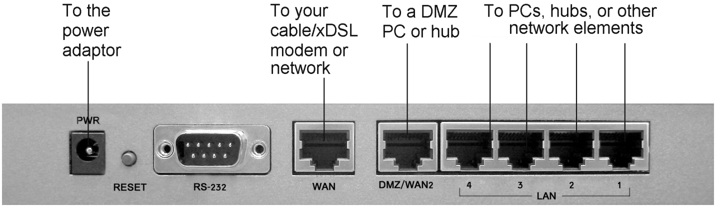
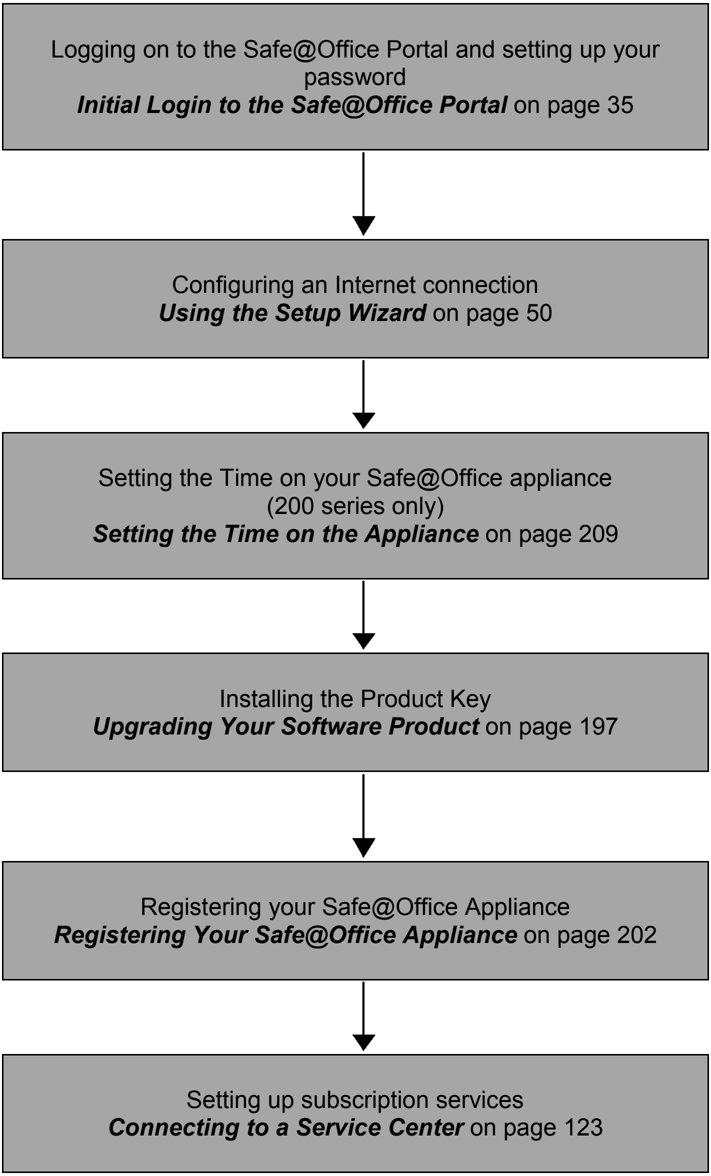

To the power adaptor
To your cable/xDSL modem or network
To a DMZ PC or hub
To PCs, hubs, or other network elements
PWR
RESET
RS-232
WAN
DMZ/WAN2
4
3
2
1
LAN

Figure 5: Typical Connection Diagram

Setting Up the Safe@Office Appliance

After you have installed the Safe@Office appliance, you must set it up using the steps shown below.

When setting up your Safe@Office appliance for the first time after installation, these steps follow each other automatically. After you have logged on and setup your password, the Setup Wizard automatically opens and displays the dialog boxes for configuring your Internet connection. After you have configured your Internet connection, the Setup Wizard automatically displays the dialog boxes for registering your Safe@Office appliance. If desired, you can exit the Setup Wizard and perform each of these steps separately.



Logging on to the Safe@Office Portal and setting up your password
Initial Login to the Safe@Office Portal on page 35

Configuring an Internet connection
Using the Setup Wizard on page 50

Setting the Time on your Safe@Office appliance (200 series only)
Setting the Time on the Appliance on page 209

Installing the Product Key
Upgrading Your Software Product on page 197

Registering your Safe@Office Appliance
Registering Your Safe@Office Appliance on page 202

Setting up subscription services
Connecting to a Service Center on page 123

Chapter 3

Getting Started

This chapter contains all the information you need in order to get started using your Safe@Office appliance.

This chapter includes the following topics:

Initial Login to the Safe@Office Portal

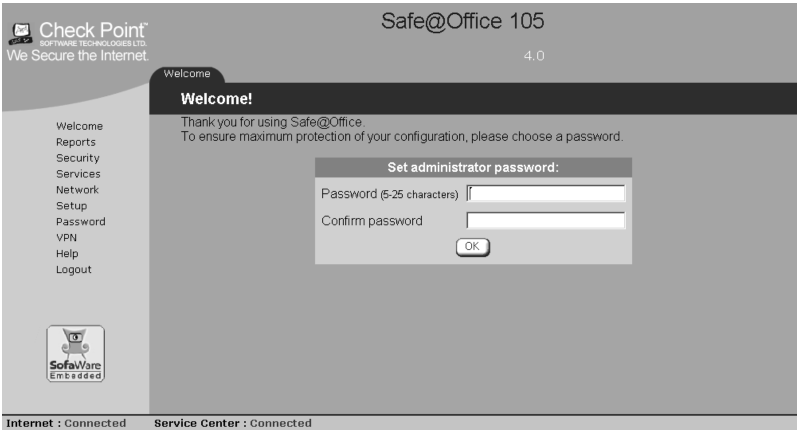
Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

The first time you log on to the Safe@Office Portal, you must set up your password.

To log on to the Safe@Office Portal for the first time

1. Browse to http://my.firewall.

The initial login page appears.



Safe@Office 105

4.0

Welcome!

Thank you for using Safe@Office.
To ensure maximum protection of your configuration, please choose a password.

Set administrator password:

Password (5-25 characters)

Confirm password

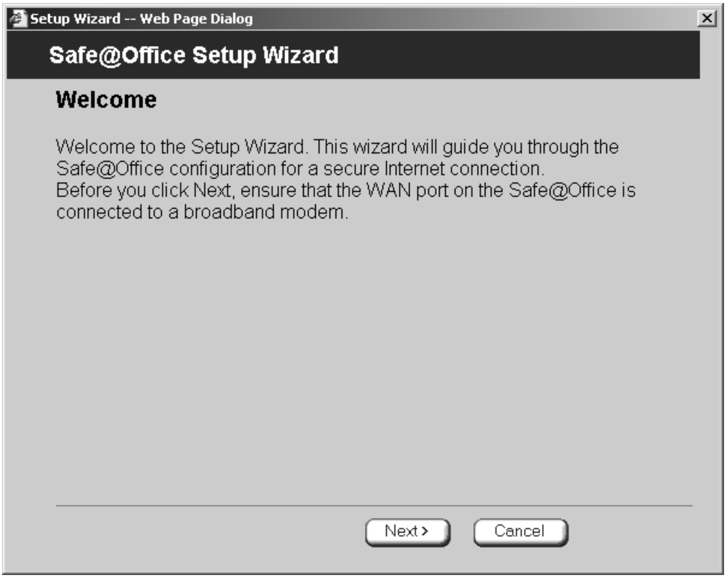
2. Type a password both in the **Password** and the **Confirm Password** fields.

Note: The password must be five to 25 characters (letters or numbers).

Note: You can change your password at any time. For further information, see ***Changing Your Password*** on page 181.

3. Click **OK**.

The Setup Wizard opens, with the **Welcome** screen displayed.



Safe@Office Setup Wizard

Welcome

Welcome to the Setup Wizard. This wizard will guide you through the Safe@Office configuration for a secure Internet connection.
Before you click Next, ensure that the WAN port on the Safe@Office is connected to a broadband modem.

4. Configure your Internet connection using either the Setup Wizard or Internet Setup.

   The Setup Wizard takes you through the configuration process step by step. For information on using the Setup Wizard, see ***Using the Setup Wizard*** on page 50.

   Internet Setup offers advanced setup options. For example, if you are using Safe@Office 110 or 225, you can configure two Internet connections using Internet Setup. To use Internet Setup, click **Cancel** and refer to ***Using Internet Setup*** on page 59.

Logging on to the Safe@Office Portal

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

To log on to the Safe@Office Portal

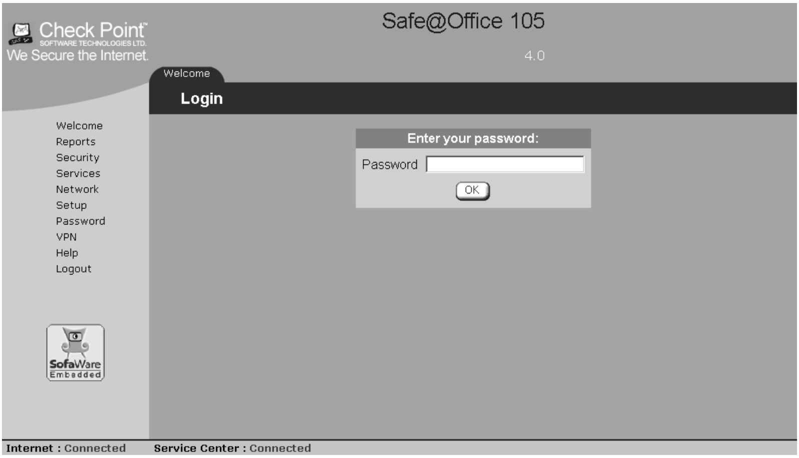
1. Do one of the following:

   - Browse to http://my.firewall.

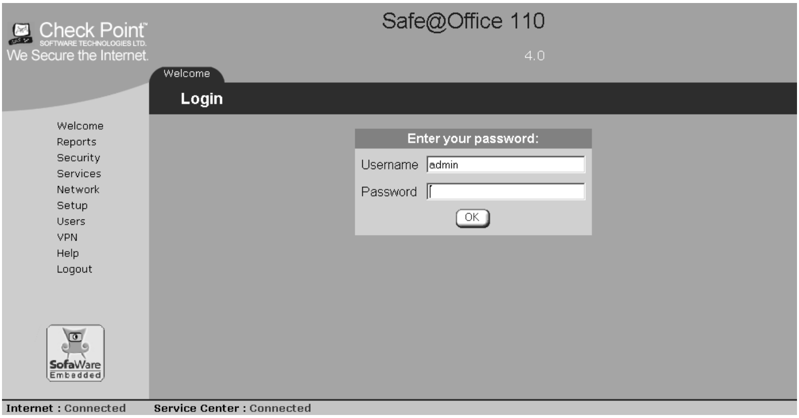
     Or

   - To log on through HTTPS (locally or remotely), follow the procedure ***Accessing the Safe@Office Portal Remotely*** on page 40.

   The login page appears.



If you are using Safe@Office 110 or 225, the page appears as follows:



Login

Enter your password:

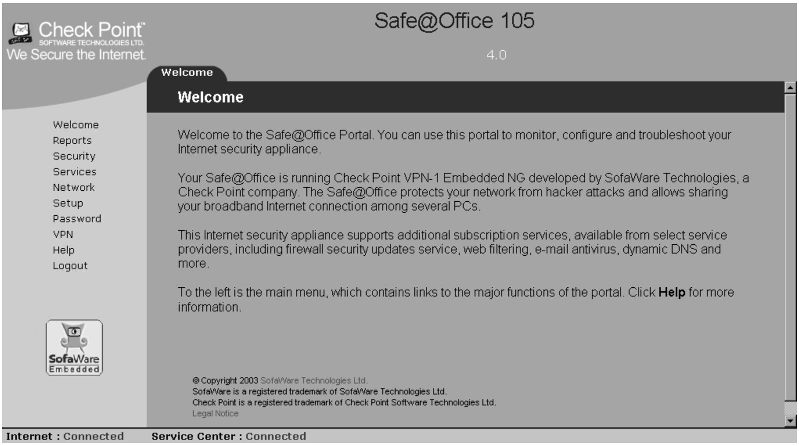
Username: admin

Password:

Internet : Connected Service Center : Connected

2. Type in your username and password.
3. Click **OK**.

The **Welcome** page appears.



Welcome

Welcome to the Safe@Office Portal. You can use this portal to monitor, configure and troubleshoot your Internet security appliance.

Your Safe@Office is running Check Point VPN-1 Embedded NG developed by SofaWare Technologies, a Check Point company. The Safe@Office protects your network from hacker attacks and allows sharing your broadband Internet connection among several PCs.

This Internet security appliance supports additional subscription services, available from select service providers, including firewall security updates service, web filtering, e-mail antivirus, dynamic DNS and more.

To the left is the main menu, which contains links to the major functions of the portal. Click **Help** for more information.

© Copyright 2003 SofaWare Technologies Ltd.
SofaWare is a registered trademark of SofaWare Technologies Ltd.
Check Point is a registered trademark of Check Point Software Technologies Ltd.
Legal Notice

Internet : Connected Service Center : Connected

Accessing the Safe@Office Portal Remotely

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

You can access the Safe@Office Portal remotely (from the Internet) through HTTPS. HTTPS is a protocol for accessing a secure Web server. It is used to transfer confidential user information, since it encrypts data and utilizes a secure port.

Note: You can also use HTTPS to access the Safe@Office Portal from your internal network.

Note: In order to access the Safe@Office Portal remotely, you must first do the following:

Configure your password, using HTTP. See ***Initial Login to the Safe@Office Portal*** on page 35.

Configure HTTPS. See ***Configuring HTTPS*** on page 206.

To access the Safe@Office Portal from your internal network

- Browse to https://my.firewall.

  (Note that the URL starts with "https", not "http".)

  The Safe@Office Portal appears.

To access the Safe@Office Portal from the Internet

- Browse to https://<firewall_IP_address>:981.

  (Note that the URL starts with "https", not "http".)

  The following things happen in the order below:

- If this is your first attempt to access the Safe@Office Portal through HTTPS, the certificate in the Safe@Office appliance is not yet known to the browser, so the **Security Alert** dialog box appears.

  To avoid seeing this dialog box again, install the certificate of the destination Safe@Office appliance. If you are using Internet Explorer 5, do the following:

  1) Click **View Certificate**.

     The **Certificate** dialog box appears, with the **General** tab displayed.

  2) Click **Install Certificate**.

     The **Certificate Import Wizard** opens.

  3) Click **Next**.

  4) Click **Next**.

  5) Click **Finish**.

  6) Click **Yes**.

  7) Click **OK**.

     The **Security Alert** dialog box reappears.

  8) Click **Yes**.

     The Safe@Office Portal appears.

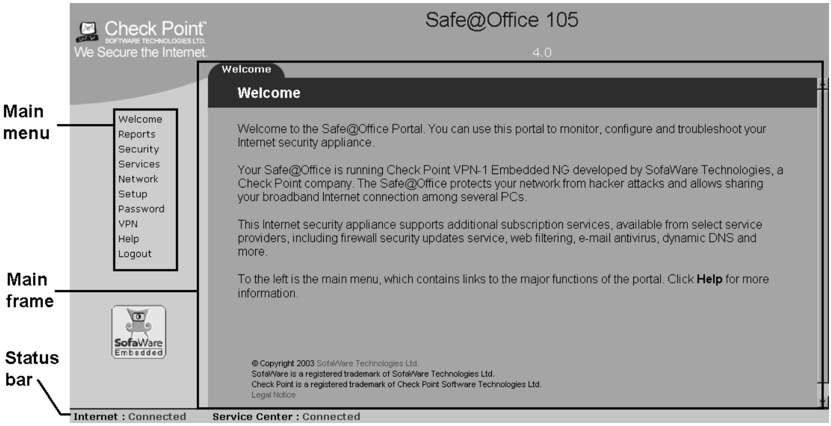
Using the Safe@Office Portal

The Safe@Office Portal is a web-based management interface, which enables you to manage and configure the Safe@Office appliance operation and options.

The Safe@Office Portal consists of three major elements.

Table 5: Safe@Office Portal Elements

Element	Description
Main menu	Used for navigating between the various topics (such as Reports, Security, and Setup).
Main frame	Displays information and controls related to the selected topic. The main frame may also contain tabs that allow you to view different pages related to the selected topic.
Status bar	Shows your Internet connection and managed services status.



Welcome

Welcome to the Safe@Office Portal. You can use this portal to monitor, configure and troubleshoot your Internet security appliance.

Your Safe@Office is running Check Point VPN-1 Embedded NG developed by SofaWare Technologies, a Check Point company. The Safe@Office protects your network from hacker attacks and allows sharing your broadband Internet connection among several PCs.

This Internet security appliance supports additional subscription services, available from select service providers, including firewall security updates service, web filtering, e-mail antivirus, dynamic DNS and more.

To the left is the main menu, which contains links to the major functions of the portal. Click **Help** for more information.

© Copyright 2003 SofaWare Technologies Ltd.
SofaWare is a registered trademark of SofaWare Technologies Ltd.
Check Point is a registered trademark of Check Point Software Technologies Ltd.
Legal Notice

Internet : Connected   Service Center : Connected

Figure 6: Safe@Office Portal

Main Menu

The main menu includes the following submenus.

Table 6: Main Menu Submenus

This submenu...	Does this...
Welcome	Displays the welcome information.
Reports	Provides reporting capabilities in terms of event logging, established connections, and active computers.
Security	Provides controls and options for setting the security of any computer in the network.
Services	Allows you to control your subscription to subscription services.
Network	Allows you to manage and configure your network settings and Internet connections.
Setup	Provides a set of tools for managing your Safe@Office appliance. Allows you to upgrade your product key and firmware and to configure HTTPS access to your Safe@Office appliance.
Password	Allows you to set your password. This submenu only appears in Safe@Office 105.

This submenu...	Does this...
Users	Allows you to manage Safe@Office appliance users. This submenu only appears in Safe@Office 110 and 225.
VPN	Allows you to manage, configure, and log on to VPN sites. This submenu only appears in Safe@Office 110 and 225.
Help	Provides context-sensitive help.
Logout	Allows you to log off of the Safe@Office Portal.

Main Frame

The main frame displays the relevant data and controls pertaining to the menu and tab you select. These elements sometimes differ depending on what model you are using. The differences are described throughout this guide.

Status Bar

The status bar, located at the bottom of each page, displays the fields below. In the Safe@Office 200 series, the status bar also displays the date and time.

Table 7: Status Bar Fields

This field...	Displays this...
Internet	Your Internet connection status. The connection status may be one of the following: • **Connected.** The Safe@Office appliance is connected to the Internet. • **Not Connected.** The Internet connection is down. • **Establishing Connection.** The Safe@Office appliance is connecting to the Internet. • **Contacting Gateway.** The Safe@Office appliance is trying to contact the Internet default gateway. • **Disabled.** The Internet connection has been manually disabled. Note: Using Safe@Office 110 and 225, you can configure both a primary and a secondary Internet connection. When both connections are configured, the Status bar displays both statuses. For example "Internet [Primary]: Connected". For information on configuring a secondary Internet connection, see ***Configuring the Internet Connection*** on page 49.

This field…	Displays this…
Service Center	Displays your subscription services status. Your Service Center may offer various subscription services. These include the firewall service and optional services such as Web Filtering and Email Antivirus. Your subscription services status may be one of the following: • **Not Subscribed.** You are not subscribed to security services. • **Connection Failed.** The Safe@Office appliance failed to connect to the Service Center. • **Connecting.** The Safe@Office appliance is connecting to the Service Center. • **Connected.** You are connected to the Service Center, and security services are active.

Logging off

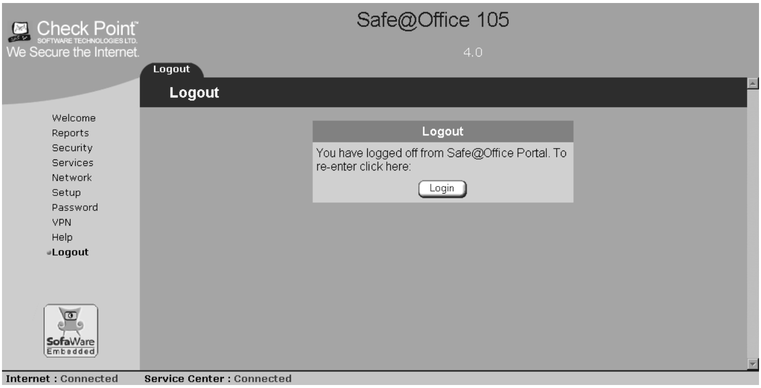
Safe@Office 105 | Safe@Office 110 | Safe@Office 225

Logging off terminates your administration session. Any subsequent attempt to connect to the Safe@Office Portal will require re-entering of the administration password.

To log off of the Safe@Office Portal

- Do one of the following:
  - If you are connected through HTTP, click **Logout** in the main menu.

    The **Logout** page appears.

    Logout

    You have logged off from Safe@Office Portal. To re-enter click here:

    Login

    Internet : Connected   Service Center : Connected

  - If you are connected through HTTPS, the **Logout** option does not appear in the main menu. Close the browser window.

Chapter 4

Configuring the Internet Connection

This chapter describes how to configure and work with an Safe@Office Internet connection.

This chapter includes the following topics:

Overview

You must configure your Internet connection before you can access the Internet through the Safe@Office appliance. You can configure your Internet connection using either of the following setup tools:

- **Setup Wizard**. Guides you through the configuration process step by step.
- **Internet Setup**. Offers advanced setup options. If you are using Safe@Office 110 or 225, you can configure two Internet connections using Internet Setup.

Using the Setup Wizard

Safe@Office **105** Safe@Office **110** Safe@Office **225**

The Setup Wizard allows you to configure your Safe@Office appliance for Internet connection quickly and easily through its user-friendly interface. It lets you to choose between the following three types of broadband connection methods:

- Direct LAN Connection
- Cable Modem
- PPTP or PPPoE dialer

Note: The first time you log on to the Safe@Office Portal, the Setup Wizard starts automatically. In this case, you should skip to step 2 in the procedure below.

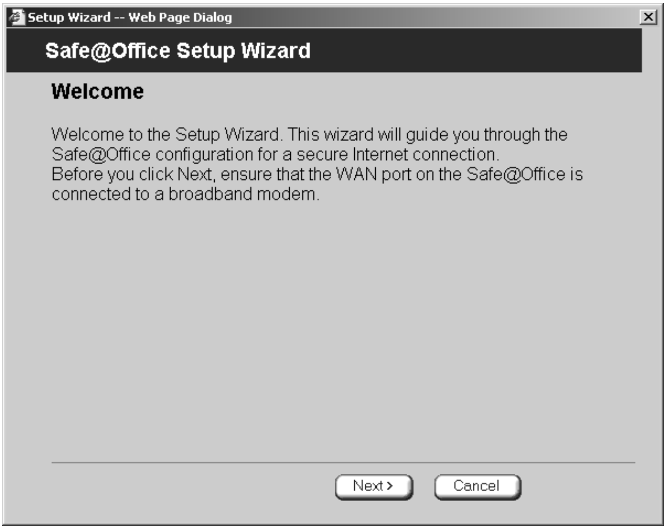
To set up the Internet connection using the Setup Wizard

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

   The **Internet** page appears

2. Click **Setup Wizard**.

The Setup Wizard opens with the **Welcome** page displayed.



Setup Wizard -- Web Page Dialog

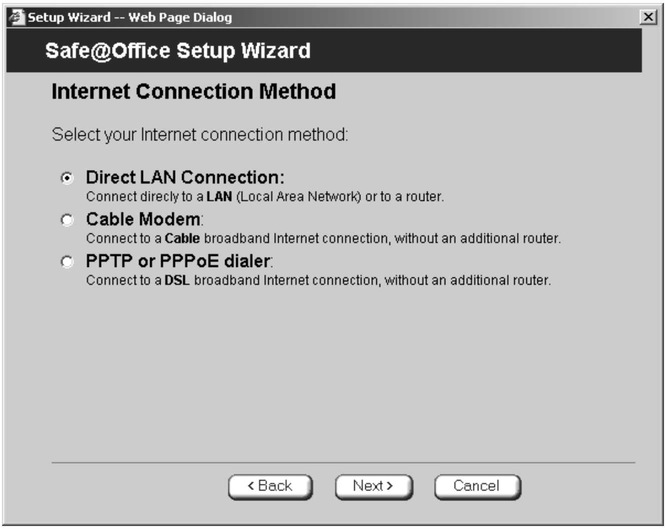
Safe@Office Setup Wizard

Welcome

Welcome to the Setup Wizard. This wizard will guide you through the Safe@Office configuration for a secure Internet connection.
Before you click Next, ensure that the WAN port on the Safe@Office is connected to a broadband modem.

3. Click **Next**.

The **Internet Connection Method** dialog box appears.



Setup Wizard -- Web Page Dialog

Safe@Office Setup Wizard

Internet Connection Method

Select your Internet connection method:

● **Direct LAN Connection:**
Connect direcly to a **LAN** (Local Area Network) or to a router.

○ **Cable Modem**:
Connect to a **Cable** broadband Internet connection, without an additional router.

○ **PPTP or PPPoE dialer**:
Connect to a **DSL** broadband Internet connection, without an additional router.

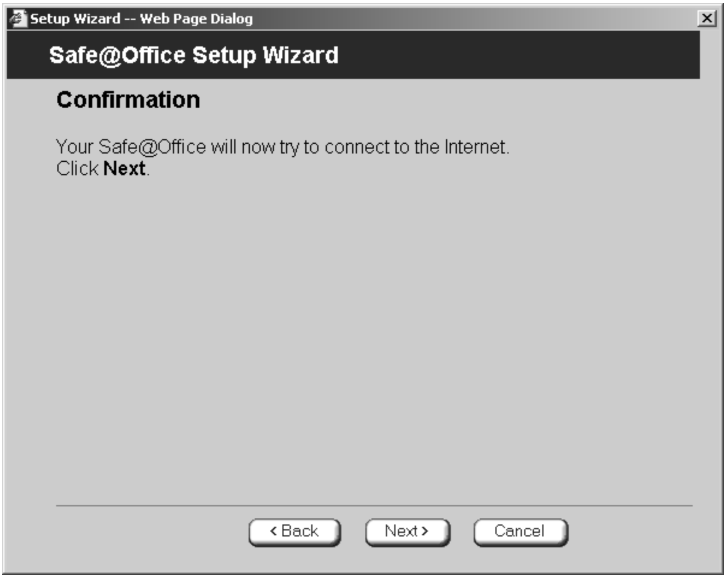
4. Select the Internet connection method you want to use for connecting to the Internet.

Note: If you selected PPTP or PPPoE dialer, do not use your dial-up software to connect to the Internet.

5. Click **Next**.

Using a Direct LAN Connection

No further settings are required for a direct LAN (Local Area Network) connection. The **Confirmation** screen appears.



Confirmation

Your Safe@Office will now try to connect to the Internet.
Click **Next**.

1. Click **Next**.

   The system attempts to connect to the Internet via the selected connection.

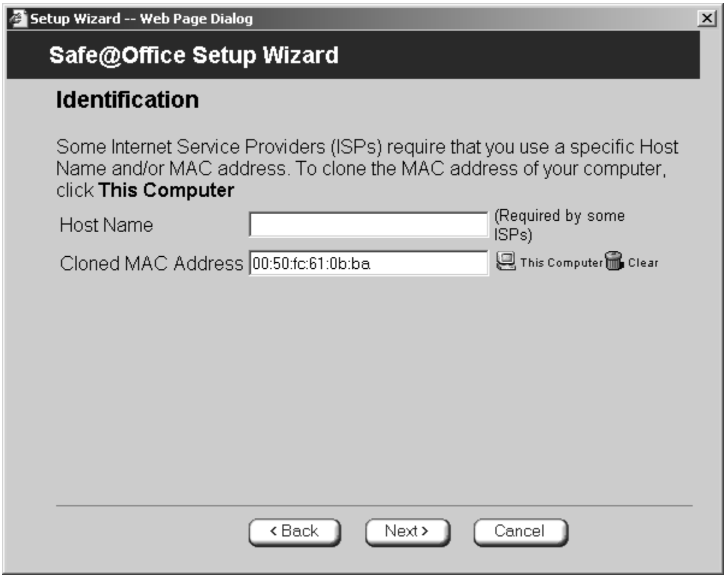
   The **Connecting...** screen appears.

   At the end of the connection process the **Connected** screen appears.

2. Click **Finish**.

Using a Cable Modem Connection

If you selected the Cable Modem connection method, the **Identification** dialog box appears.



Setup Wizard -- Web Page Dialog

Safe@Office Setup Wizard

Identification

Some Internet Service Providers (ISPs) require that you use a specific Host Name and/or MAC address. To clone the MAC address of your computer, click **This Computer**

Host Name: (Required by some ISPs)

Cloned MAC Address: 00:50:fc:61:0b:ba

1. If your ISP requires a specific hostname for authentication, enter it in the **Host Name** field. The ISP will supply you with the proper hostname, if required.

   Most ISPs do not require a specific hostname.

2. A MAC address is a 12-digit identifier assigned to every network device. If your ISP restricts connections to specific, recognized MAC addresses, they will instruct you to enter the MAC address. Otherwise, you may leave this field blank.

   If your ISP requires the MAC address, do either of the following:

   - Click **This Computer** to automatically "clone" the MAC address of your computer to the Safe@Office appliance.

     Or

- If the ISP requires authentication using the MAC address of a different computer, enter the MAC address in the **MAC cloning** field.

3. Click **Next**.

   The **Confirmation** screen appears.

4. Click **Next**.

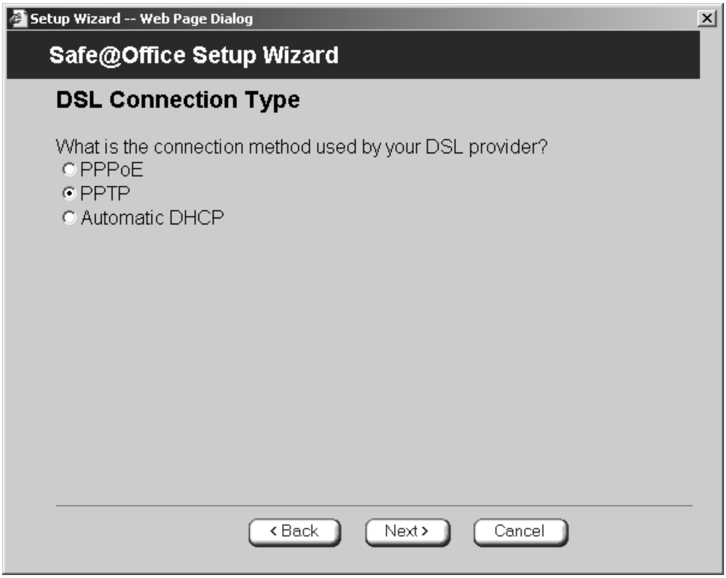
   The system attempts to connect to the Internet.

   The **Connecting…** screen appears. At the end of the connection process the **Connected** screen appears.

5. Click **Finish**.

Using a PPTP or PPPoE Dialer Connection

If you selected the PPTP or PPPoE dialer connection method, the **DSL Connection Type** dialog box appears.



Setup Wizard -- Web Page Dialog

Safe@Office Setup Wizard

DSL Connection Type

What is the connection method used by your DSL provider?

○ PPPoE
● PPTP
○ Automatic DHCP

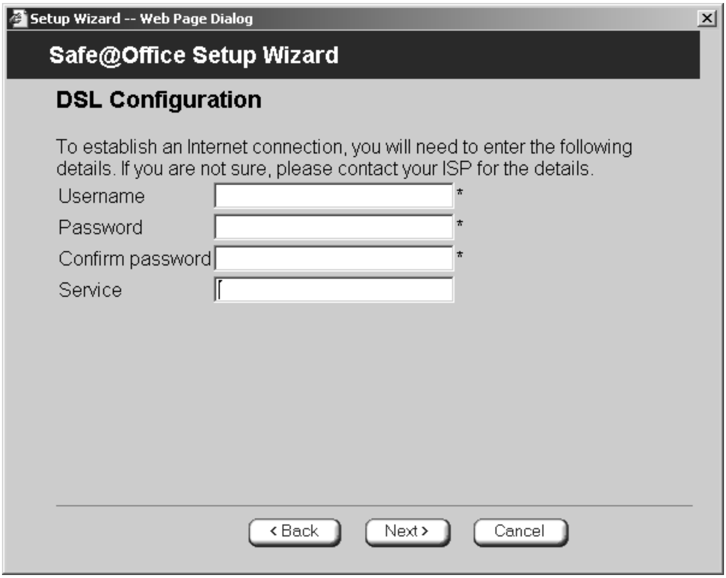
1. Select the connection method used by your DSL provider.

Note: Most xDSL providers use PPPoE. If you are uncertain regarding which connection method to use contact your xDSL provider.

2. Click **Next**.

Using PPPoE

If you selected the PPPoE connection method, the **DSL Configuration** dialog box appears.



DSL Configuration

To establish an Internet connection, you will need to enter the following details. If you are not sure, please contact your ISP for the details.

Username *
Password *
Confirm password *
Service

1. Complete the fields using the information in the table below.
2. Click **Next**.

   The **Confirmation** screen appears.

3. Click **Next**.

   The system attempts to connect to the Internet via the DSL connection.

   The **Connecting...** screen appears.

   At the end of the connection process the **Connected** screen appears.

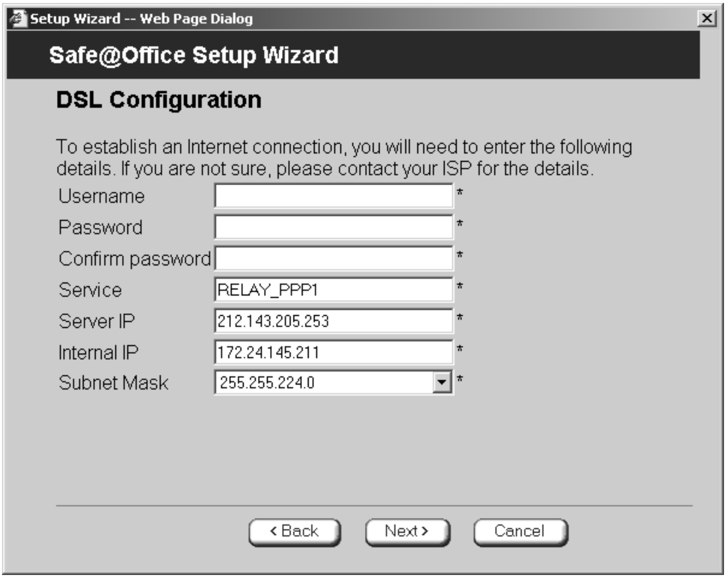
4. Click **Finish**.

Table 8: PPPoE Connection Fields

In this field...	Do this...
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password.
Service	Type your service name. This field can be left blank.

Using PPTP

If you selected the PPTP connection method, the **DSL Configuration** dialog box appears.



Setup Wizard -- Web Page Dialog

Safe@Office Setup Wizard

DSL Configuration

To establish an Internet connection, you will need to enter the following details. If you are not sure, please contact your ISP for the details.

Username	*
Password	*
Confirm password	*
Service	RELAY_PPP1 *
Server IP	212.143.205.253 *
Internal IP	172.24.145.211 *
Subnet Mask	255.255.224.0 *

1. Complete the fields using the information in the table below.
2. Click **Next**.

   The **Confirmation** screen appears.
3. Click **Next**.

   The system attempts to connect to the Internet via the DSL connection.

   The **Connecting...** screen appears.

   At the end of the connection process the **Connected** screen appears.
4. Click **Finish**.

Table 9: PPTP Connection Fields

In this field...	Do this...
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password.
Service	Type your service name.
Server IP	Type the IP address of the PPTP modem.
Internal IP	Type the local IP address required for accessing the PPTP modem.
Subnet Mask	Type the subnet mask of the PPTP modem.

Using Automatic DHCP

If you selected the Automatic DHCP connection method, no further configuration is required. The **Confirmation** screen appears.

1. Click **Next**.

   The system attempts to connect to the Internet via the selected connection.

   The **Connecting...** screen appears.

   At the end of the connection process the **Connected** screen appears.

2. Click **Finish**.

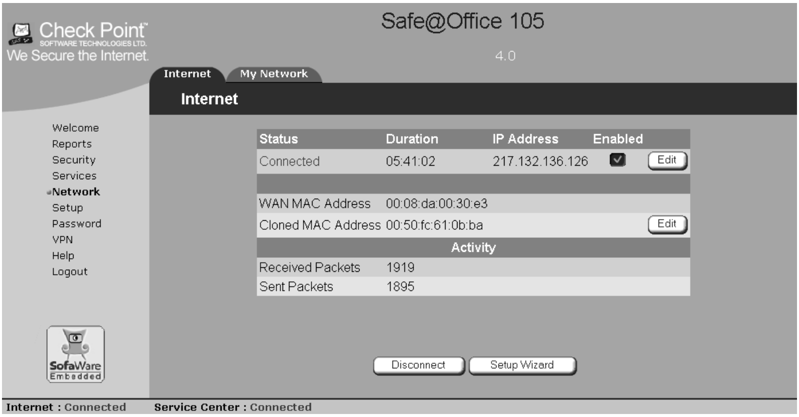
Using Internet Setup

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

Internet Setup allows you to manually configure your Internet connection.

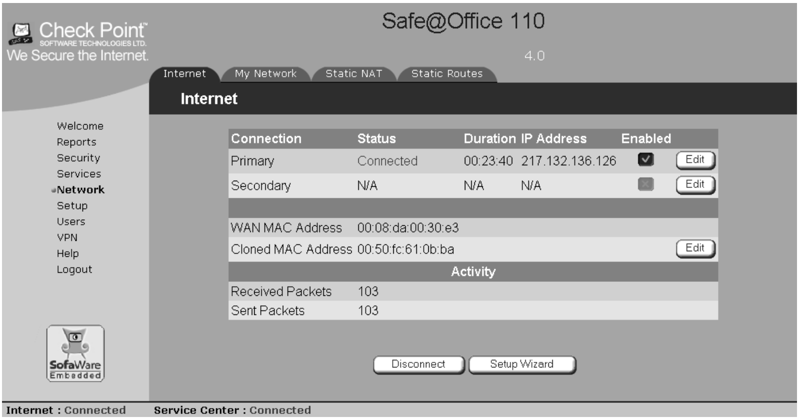
To configure the Internet connection using Internet Setup

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



Status	Duration	IP Address	Enabled	
Connected	05:41:02	217.132.136.126	☑	Edit
WAN MAC Address	00:08:da:00:30:e3			
Cloned MAC Address	00:50:fc:61:0b:ba			Edit
Activity				
Received Packets	1919			
Sent Packets	1895			

When using Safe@Office 110 or 225, the **Internet** page appears as follows:



Internet

Connection	Status	Duration	IP Address	Enabled	
Primary	Connected	00:23:40	217.132.136.126	☑	Edit
Secondary	N/A	N/A	N/A	☒	Edit

WAN MAC Address 00:08:da:00:30:e3

Cloned MAC Address 00:50:fc:61:0b:ba

Activity

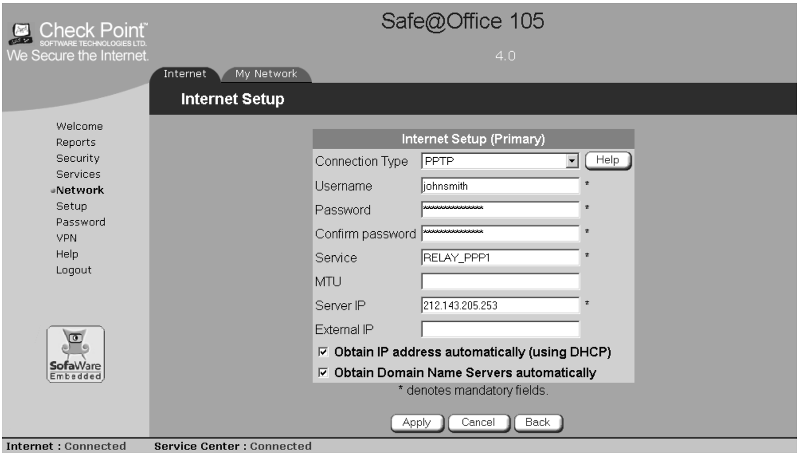
Received Packets	103
Sent Packets	103

Internet : Connected Service Center : Connected

2. If your ISP restricts connections to specific, recognized MAC addresses, clone a MAC address using the procedure ***Cloning a MAC Address*** on page 72.

3. Next to the Internet connection, click **Edit**.

The **Internet Setup** page appears.



Internet Setup

Internet Setup (Primary)

Connection Type	PPTP
Username	johnsmith *
Password	************** *
Confirm password	************** *
Service	RELAY_PPP1 *
MTU	
Server IP	212.143.205.253 *
External IP	

☑ Obtain IP address automatically (using DHCP)

☑ Obtain Domain Name Servers automatically

* denotes mandatory fields.

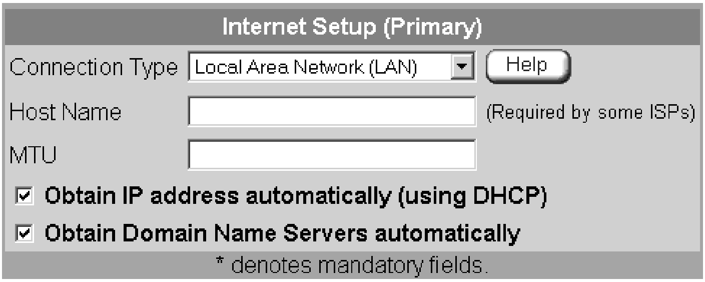
Internet : Connected Service Center : Connected

4. From the **Connection Type** drop-down list, select the Internet connection type you are using/intend to use.

   The display changes according to the connection type you selected.

The following steps should be performed in accordance with the connection type you have chosen.

Using a LAN Connection



Internet Setup (Primary)

Connection Type: Local Area Network (LAN)

Host Name: (Required by some ISPs)

MTU:

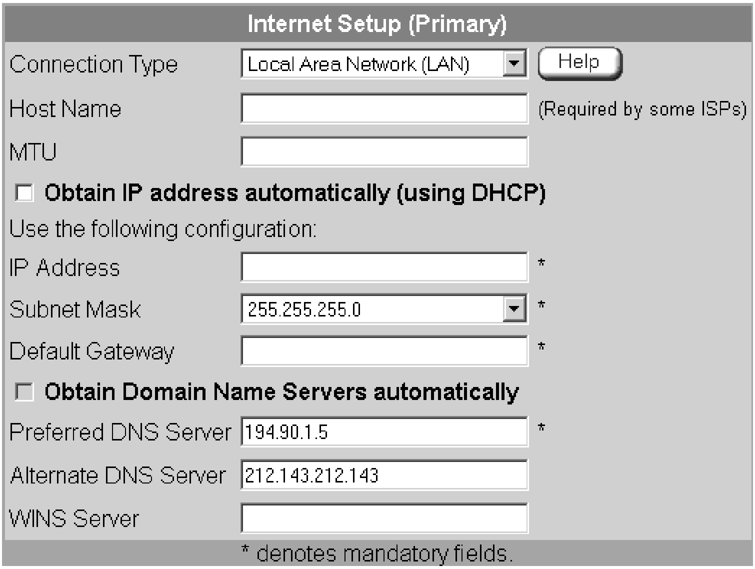
☑ Obtain IP address automatically (using DHCP)

☑ Obtain Domain Name Servers automatically

* denotes mandatory fields.

1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 69.

If you cleared the **Obtain IP address automatically (using DHCP)** check box, the page appears as follows:

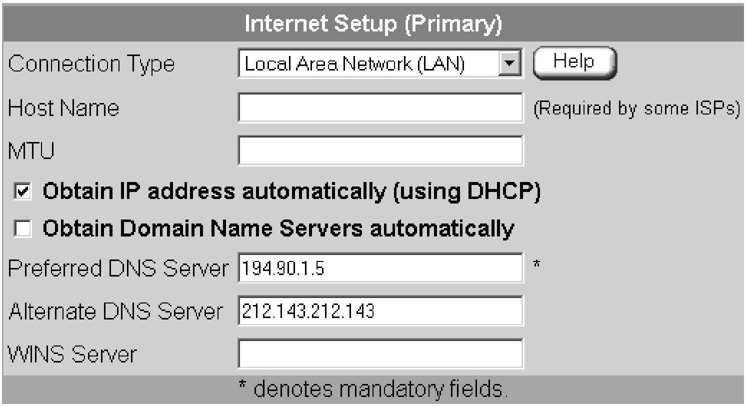


Internet Setup (Primary)

Connection Type	Local Area Network (LAN)	Help
Host Name		(Required by some ISPs)
MTU		
□ Obtain IP address automatically (using DHCP)		
Use the following configuration:		
IP Address		*
Subnet Mask	255.255.255.0	*
Default Gateway		*
□ Obtain Domain Name Servers automatically		
Preferred DNS Server	194.90.1.5	*
Alternate DNS Server	212.143.212.143	
WINS Server		

* denotes mandatory fields.

If you cleared the **Obtain Domain Name Servers automatically** check box, the page appears as follows:



Internet Setup (Primary)

Connection Type	Local Area Network (LAN)	Help
Host Name		(Required by some ISPs)
MTU		
☑ Obtain IP address automatically (using DHCP)		
□ Obtain Domain Name Servers automatically		
Preferred DNS Server	194.90.1.5	*
Alternate DNS Server	212.143.212.143	
WINS Server		

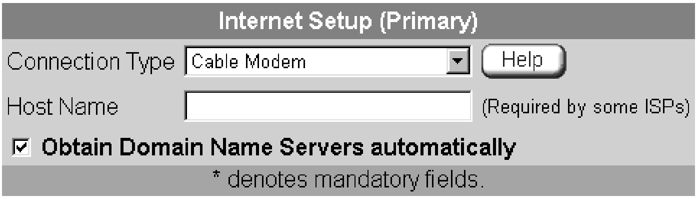
* denotes mandatory fields.

2. Click **Apply**.

The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a Cable Modem Connection



Internet Setup (Primary)

Connection Type: Cable Modem

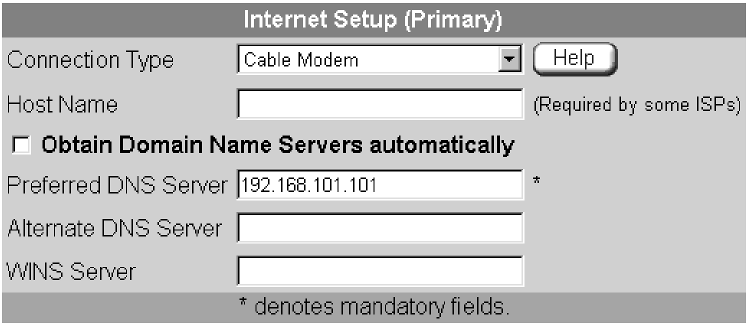
Host Name: (Required by some ISPs)

☑ Obtain Domain Name Servers automatically

* denotes mandatory fields.

1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 69.

   If you cleared the **Obtain Domain Name Servers automatically** check box, the page appears as follows:



Internet Setup (Primary)

Connection Type: Cable Modem

Host Name: (Required by some ISPs)

☐ Obtain Domain Name Servers automatically

Preferred DNS Server: 192.168.101.101 *

Alternate DNS Server:

WINS Server:

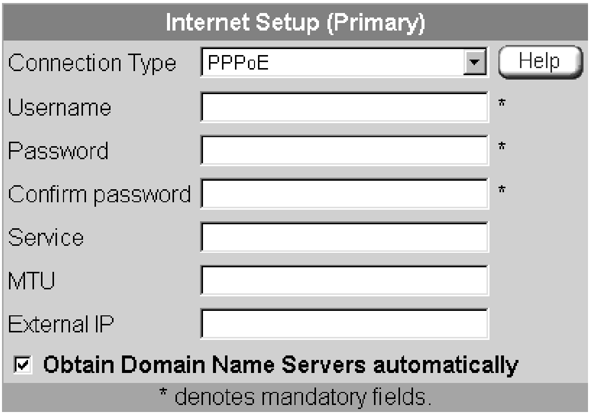
* denotes mandatory fields.

2. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPPoE Connection



Internet Setup (Primary)

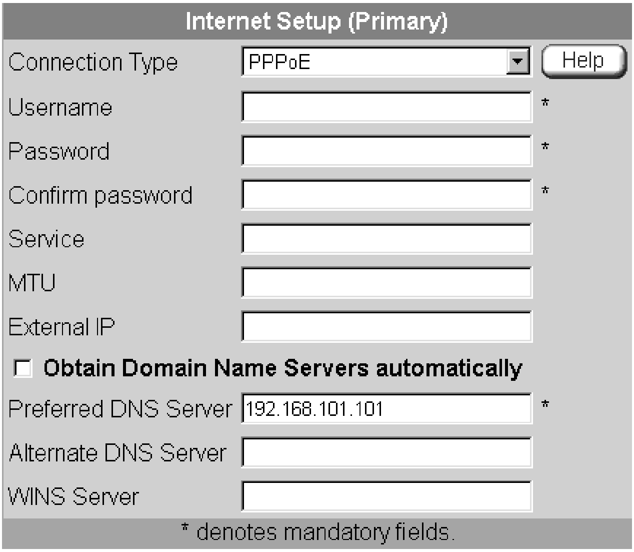
Connection Type	PPPoE	Help
Username		*
Password		*
Confirm password		*
Service		
MTU		
External IP		

☑ **Obtain Domain Name Servers automatically**

* denotes mandatory fields.

1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 69.

   If you cleared the **Obtain Domain Name Servers automatically** check box, the page appears as follows:



Internet Setup (Primary)

Connection Type	PPPoE	Help
Username		*
Password		*
Confirm password		*
Service		
MTU		
External IP		

□ **Obtain Domain Name Servers automatically**

Preferred DNS Server	192.168.101.101	*
Alternate DNS Server		
WINS Server		

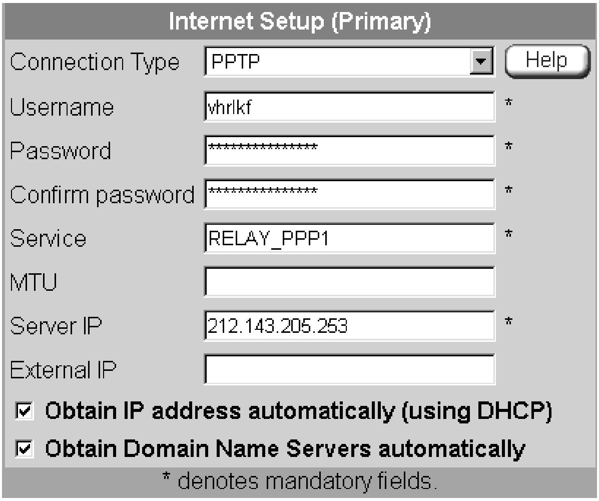
* denotes mandatory fields.

2. Click **Apply**.

The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPTP Connection



Internet Setup (Primary)

Connection Type	PPTP	Help
Username	vhrlkf	*
Password	****************	*
Confirm password	****************	*
Service	RELAY_PPP1	*
MTU		
Server IP	212.143.205.253	*
External IP		

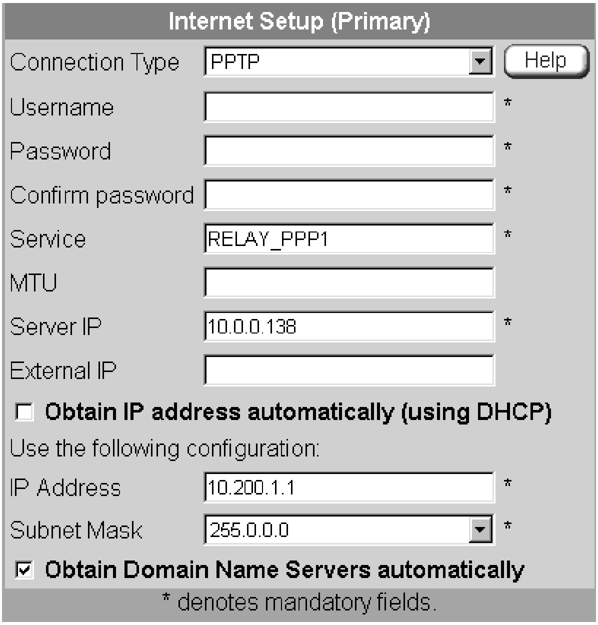
☑ Obtain IP address automatically (using DHCP)

☑ Obtain Domain Name Servers automatically

* denotes mandatory fields.

1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 69.

If you cleared the **Obtain IP address automatically (using DHCP)** check box, the page appears as follows:



Internet Setup (Primary)

Connection Type	PPTP	Help
Username		*
Password		*
Confirm password		*
Service	RELAY_PPP1	*
MTU		
Server IP	10.0.0.138	*
External IP		

□ **Obtain IP address automatically (using DHCP)**

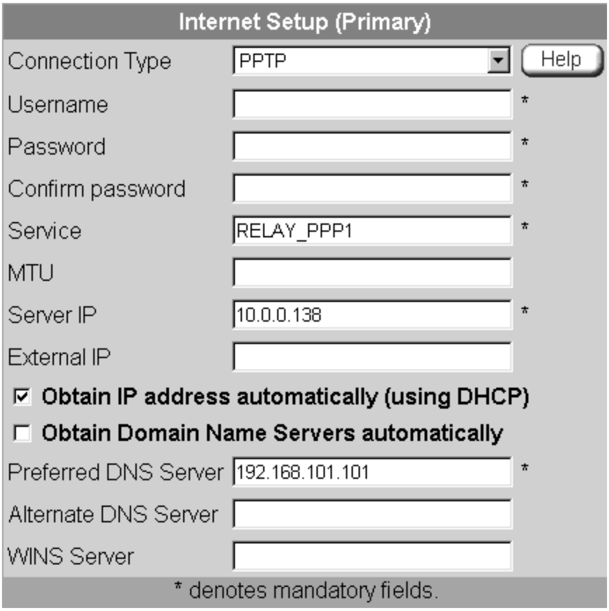
Use the following configuration:

IP Address	10.200.1.1	*
Subnet Mask	255.0.0.0	*

☑ **Obtain Domain Name Servers automatically**

* denotes mandatory fields.

If you cleared the **Obtain Domain Name Servers automatically** check box, the page appears as follows:



Internet Setup (Primary)

Connection Type	PPTP	Help
Username		*
Password		*
Confirm password		*
Service	RELAY_PPP1	*
MTU		
Server IP	10.0.0.138	*
External IP		

☑ Obtain IP address automatically (using DHCP)

□ Obtain Domain Name Servers automatically

Preferred DNS Server	192.168.101.101	*
Alternate DNS Server		
WINS Server		

* denotes mandatory fields.

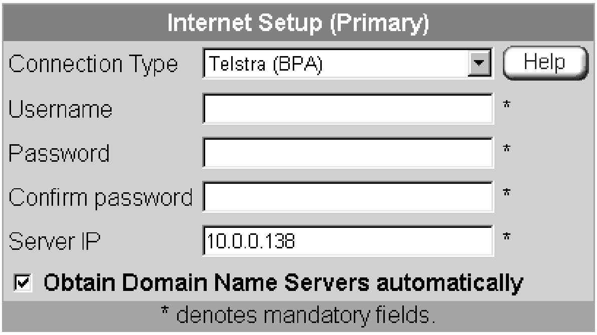
2. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a Telstra (BPA) Connection

Use this Internet connection type only if you are subscribed to Telstra® BigPond™ Internet. Telstra BigPond is a trademark of Telstra Corporation Limited.



Internet Setup (Primary)

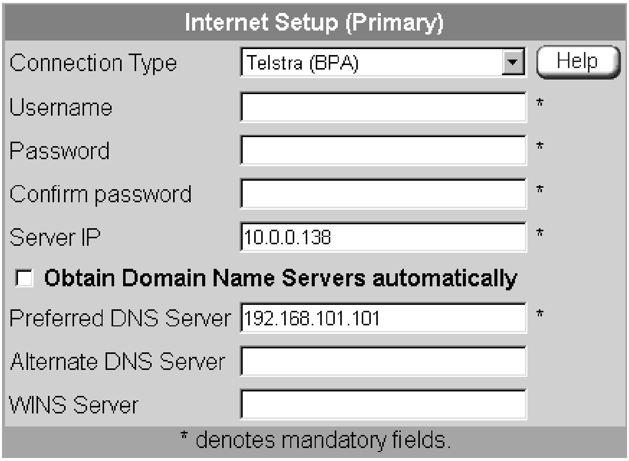
Connection Type	Telstra (BPA)	Help
Username		*
Password		*
Confirm password		*
Server IP	10.0.0.138	*

☑ Obtain Domain Name Servers automatically

* denotes mandatory fields.

1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 69.

   If you cleared the **Obtain Domain Name Servers automatically** check box, the page appears as follows:



Internet Setup (Primary)

Connection Type	Telstra (BPA)	Help
Username		*
Password		*
Confirm password		*
Server IP	10.0.0.138	*

□ Obtain Domain Name Servers automatically

Preferred DNS Server	192.168.101.101	*
Alternate DNS Server		
WINS Server		

* denotes mandatory fields.

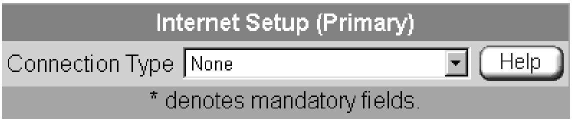
2. Click **Apply**.

The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status "Connecting". This may take several seconds.

Once the connection is made, the Status Bar displays the Internet status "Connected".

Using No Connection

If you are using Safe@Office 110 or 225, and you do not have a secondary Internet connection, set the connection type to None.



Internet Setup (Primary)

Connection Type: None

* denotes mandatory fields.

- Click **Apply**.

Table 10: Internet Setup Fields

In this field...	Do this...
Host Name	Type the hostname for authentication. If your ISP has not provided you with a host name, leave this field blank. Most ISPs do not require a specific hostname.
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password.

In this field...	Do this...
Service	Type your service name. If your ISP has not provided you with a service name, leave this field empty.
MTU	The MTU field allows you to control the maximum transmission unit size. As a general recommendation you should leave this field empty. If however you wish to modify the default MTU, it is recommended that you consult with your ISP first and use MTU values between 1300 and 1500.
Server IP	If you selected PPTP, type the IP address of the PPTP server as given by your ISP. If you selected Telstra (BPA), type the IP address of the Telstra authentication server as given by Telstra.
External IP	If you selected PPTP, type the IP address of the PPTP client as given by your ISP. If you selected PPPoE, this field is optional, and you do not have to fill it in unless your ISP has instructed you to do so.
Obtain IP address automatically (using DHCP)	Clear this option if you do not want the Safe@Office appliance to obtain an IP address automatically using DHCP.

In this field…	Do this…
Obtain Domain Name Servers automatically	Clear this option if you want the Safe@Office appliance to obtain an IP address automatically using DHCP, but not to automatically configure DNS and WINS servers
IP Address	Type the static IP address of your Safe@Office appliance.
Subnet Mask	Select the subnet mask that applies to the static IP address of your Safe@Office appliance.
Default Gateway	Type the IP address of your ISP's default gateway.
Preferred DNS Server	Type the Primary DNS server IP address.
Alternate DNS Server	Type the Secondary DNS server IP address.
WINS Server	Type the WINS server IP address.

Cloning a MAC Address

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

A MAC address is a 12-digit identifier assigned to every network device. If your ISP restricts connections to specific, recognized MAC addresses, you must clone a MAC address.

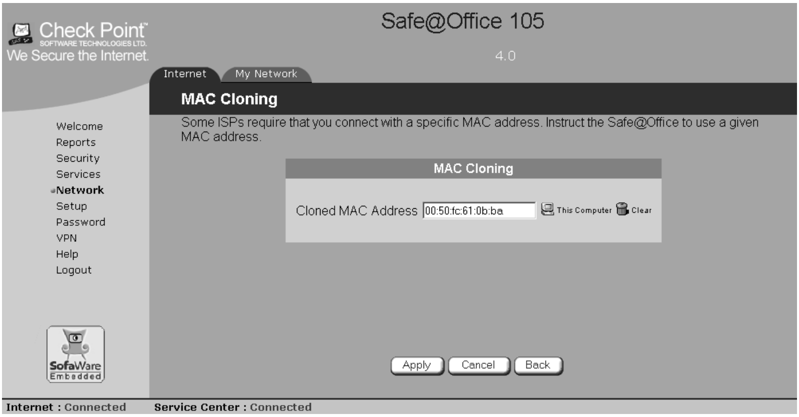
To clone a MAC address

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

   The **Internet** page appears.

2. In the **Cloned MAC address** field, click **Edit**.

   The **MAC Cloning** page appears.



MAC Cloning

Some ISPs require that you connect with a specific MAC address. Instruct the Safe@Office to use a given MAC address.

Cloned MAC Address: 00:50:fc:61:0b:ba

3. Do one of the following:
   - Click **This Computer** to automatically "clone" the MAC address of your computer to the Safe@Office appliance.

     Or

   - If the ISP requires authentication using the MAC address of a different computer, enter the MAC address in the **MAC cloning** field.
4. Click **Apply**.
5. Click **Back**.

   The Internet page reappears with your computer's MAC address displayed.

Viewing Internet Connection Information

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

You can view information on your Internet connection(s) in terms of status, duration, and activity.

To view Internet connection information

- Click **Network** in the main menu, and click the **Internet** tab.

  The **Internet** page appears.

  The following information is displayed:

Table 11: Internet Page Fields

Field	Description
Status	Indicates the connection's status.

Duration	Indicates the connection duration, if active. The duration is given in the format hh:mm:ss, where:
	hh=hours
	mm=minutes
	ss=seconds

IP Address	Your IP address.
Enabled	Indicates whether or not the connection is enabled. For further information, see ***Enabling/Disabling the Internet Connection*** on page 75
WAN MAC Address	The Safe@Office appliance's MAC address.
Cloned MAC Address	The cloned MAC address. For further information, see ***Cloning a MAC Address*** on page 72.
Received Packets	The number of data packets received in the active connection.
Sent Packets	The number of data packets sent in the active connection.

Enabling/Disabling the Internet Connection

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

You can temporarily disable an Internet connection. This is useful if, for example, you are going on vacation and do not want to leave your computer connected to the Internet. If you are using Safe@Office 110 or 225 and have two Internet connections, you can force the Safe@Office appliance to use a particular connection, by disabling the other connection.

The Internet connection's Enabled/Disabled status is persistent through Safe@Office appliance reboots.

To enable/disable an Internet connection

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

   The **Internet** page appears.

2. Next to the Internet connection, do one of the following:

   - To enable the connection, click ☒.

     The button changes to ☑ and the connection is enabled.

   - To disable the connection, click ☑.

     The button changes to ☒ and the connection is disabled.

Using Quick Internet Connection/Disconnection

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

By clicking the **Connect** or **Disconnect** button (depending on the connection status) on the **Internet** page, you can establish a quick Internet connection using the currently-selected connection type. In the same manner, you can terminate the active connection.

The Internet connection retains its Connected/Not Connected status until the Safe@Office appliance is rebooted. The Safe@Office appliance then connects to the Internet if the connection is enabled. For information on enabling an Internet connection, see ***Enabling/Disabling the Internet Connection*** on page 75.

Configuring a Backup Internet Connection

~~Safe@Office 105~~ | Safe@Office 110 | Safe@Office 225

You can configure both a primary and a secondary Internet connection. The secondary connection acts as a backup, so that if the primary connection fails, the Safe@Office appliance remains connected to the Internet.

To set up a backup Internet connection

1. Connect a hub or switch to the WAN port on your appliance's rear panel.

Note: Do not connect to the DMZ port.

2. Connect your two modems or routers to the hub/switch.
3. Configure two Internet connections.

For instructions, see ***Using Internet Setup*** on page 59.

Note: You can configure different DNS servers for the two connections. The Safe@Office appliance acts as a DNS relay and routes requests from computers within the network to the appropriate DNS server for the active Internet connection.

Important: The two connections can be of different types. However, they cannot both be LAN DHCP connections.

Chapter 5

Managing Your Network

This chapter describes how to manage and configure your network connection and settings.

This chapter includes the following topics:

Configuring Network Settings

Warning: These are advanced settings. Do not change them unless it is necessary and you are qualified to do so.

Note: If you change the network settings to incorrect values and are unable to correct the error, you can reset the Safe@Office appliance to its default settings. See ***Resetting the Safe@Office appliance to Defaults*** on page 222.

Enabling/Disabling the DHCP Server

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

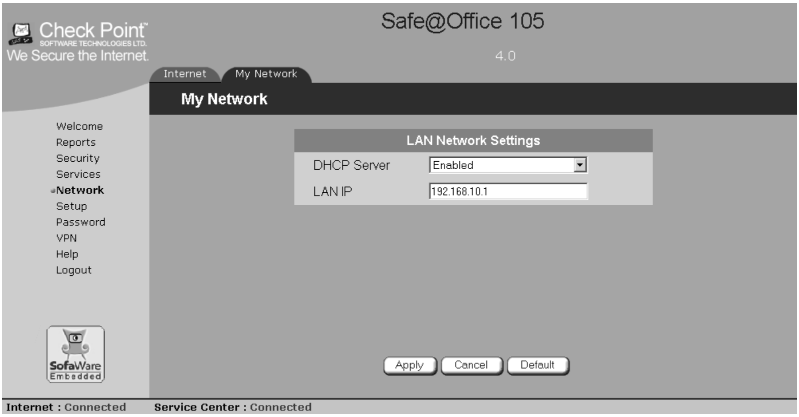
By default, the Safe@Office appliance operates as a DHCP (Dynamic Host Configuration Protocol) server. This allows the Safe@Office appliance to automatically configure all the devices on your network with their network configuration details. If you have another DHCP server configured in your network, you must disable the Safe@Office DHCP server. Otherwise, it is highly recommended to leave this setting enabled.

Note: When using a Safe@Office 200 series appliance, you can enable the DHCP server for a DMZ network.

To enable/disable the DHCP server

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

   The **My Network** page appears.



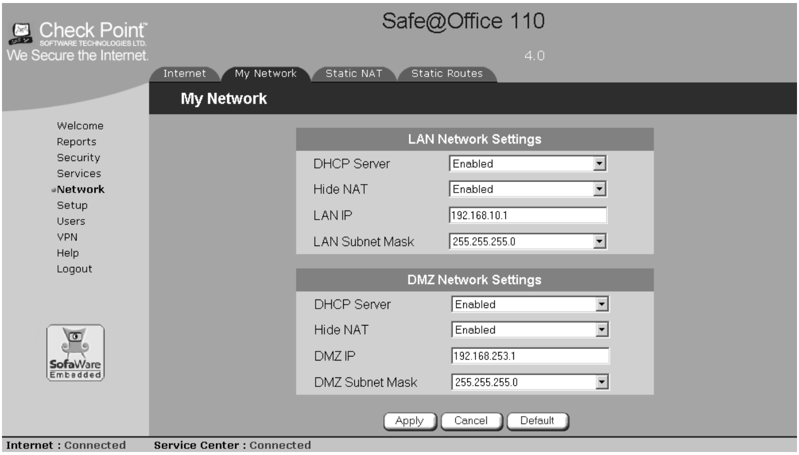
LAN Network Settings

DHCP Server: Enabled

LAN IP: 192.168.10.1

Internet : Connected   Service Center : Connected

When using Safe@Office 110 and 225, the **My Network** page appears as follows:



My Network

LAN Network Settings

DHCP Server	Enabled
Hide NAT	Enabled
LAN IP	192.168.10.1
LAN Subnet Mask	255.255.255.0

DMZ Network Settings

DHCP Server	Enabled
Hide NAT	Enabled
DMZ IP	192.168.253.1
DMZ Subnet Mask	255.255.255.0

Internet : Connected   Service Center : Connected

2. In the **DHCP Server** list, select **Enabled** or **Disabled**.
3. Click **Apply**.

   A warning message appears.
4. Click **OK**.

   - If you chose to disable the DHCP server, the DHCP server is disabled.
   - If you chose to enable the DHCP server, it is enabled.
   - A success message appears
5. Do **one** of the following:

   - If your computer is configured to obtain its IP address automatically
     (using DHCP), and the Safe@Office DHCP server is enabled, restart your computer.
   - Otherwise, manually reconfigure your computer to use the new address range using the TCP/IP settings. For information on configuring TCP/IP, see ***TCP/IP Settings*** on page 28, on page 24.

Changing IP Addresses

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

If desired, you can change your Safe@Office appliance's internal IP address. Using Safe@Office 110 or 225, you can also change the entire range of IP addresses in your internal network. You may want to perform these tasks if, for example, you are adding the Safe@Office appliance to a large existing network and don't want to change that network's IP address range, or if you are using a DHCP server other than the Safe@Office appliance, that assigns addresses within a different range.

To change IP addresses

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

   The **My Network** page appears.

2. To change the Safe@Office appliance's internal IP address, enter the new IP address in the **Safe@Office LAN IP** field.

3. To change the internal network range, enter a new value in the **LAN Subnet Mask** field.

Note: The internal network range is defined both by the Safe@Office appliance's internal IP address and by the subnet mask.

For example, if the Safe@Office appliance's internal IP address is 192.168.100.7, and you set the subnet mask to 255.255.255.0, the network's IP address range will be 192.168.100.1 – 192.168.100.254.

4. To reset the network to its default settings, do the following:

   a. Click **Default**.

      A confirmation message appears.

   b. Click **OK**.

      The internal network range is set to 192.168.10.*, and DHCP and Hide NAT are enabled.

5. Click **Apply**.

   A warning message appears.

6. Click **OK**.

   - The Safe@Office appliance's internal IP address and/or the internal network range are changed.
   - A success message appears.

7. Do **one** of the following:

   - If your computer is configured to obtain its IP address automatically
     (using DHCP), and the Safe@Office DHCP server is enabled, restart your computer.

     Your computer obtains an IP address in the new range.

   - Otherwise, manually reconfigure your computer to use the new address range using the TCP/IP settings. For information on configuring TCP/IP, see ***TCP/IP Settings*** on page 28, on page 24.

Enabling/Disabling Hide NAT

~~Safe@Office 105~~ | Safe@Office 110 | Safe@Office 225

Hide Network Address Translation (NAT) enables you to share a single public Internet IP address among several computers, by "hiding" the private IP addresses of the internal computers behind the Safe@Office appliance's single Internet IP address.

Note: If Hide NAT is disabled, you must obtain a range of Internet IP addresses from your ISP. Hide NAT is enabled by default.

Note: Static NAT and Hide NAT can be used together.

To enable/disable Hide NAT

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

   The **My Network** page appears.

2. From the **Hide NAT** list, select **Enabled** or **Disabled**.

3. Click **Apply**.

   A warning message appears.

4. Click **OK**.

   - If you chose to disable Hide NAT, it is disabled.
   - If you chose to enable Hide NAT, it is enabled.

Configuring a DMZ Network

~~Safe@Office 105~~ | Safe@Office 110 | Safe@Office 225

In addition to the LAN network, you can define a second internal network called a DMZ (demilitarized zone) network, when using Safe@Office 110 and 225. Safe@Office 110 does not have a dedicated DMZ port, so the DMZ is a logical second network behind the Safe@Office appliance, and you must connect DMZ computers to LAN ports. Safe@Office 225 has a dedicated DMZ port to which you must connect all DMZ computers.

By default, all traffic is allowed from the LAN network to the DMZ network, and no traffic is allowed from the DMZ network to the LAN network. You can easily customize this behavior by creating firewall user rules. For further information, see ***Creating Rules*** on page 112.

For example, you could assign your company's accounting department to the LAN network and the rest of the company to the DMZ network. The accounting department would be able to connect to all company computers, while the rest of the employees would not be able to access any sensitive information on the accounting department computers. You could then create firewall rules that allow specific DMZ computers (such a manager's computer) to connect to the LAN network and the accounting department.

Configuring a DMZ Network using Safe@Office 110

~~Safe@Office 105~~ Safe@Office 110 ~~Safe@Office 225~~

Note: Computers in the DMZ network cannot obtain IP addresses using DHCP, and therefore must be assigned static IP address. For instructions, see ***TCP/IP Settings*** on page 28, on page 24.

The default gateway for the DMZ computers should be specified as the Safe@Office DMZ IP address.

To configure a DMZ network

1. Connect the DMZ computers to any of the appliance's LAN ports.
2. Click **Network** in the main menu, and click the **My Network** tab.

   The **My Network** page appears.
3. In the **Logical DMZ Settings** area, in the **DMZ Mode** drop-down list, select **Enabled**.

   The **Logical DMZ Settings** fields are enabled.
4. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 83.
5. In the **Safe@Office DMZ IP** text box, the IP address of the DMZ network's default gateway.

Note: The DMZ network must not overlap the LAN network.

6. In the **DMZ Subnet Mask** text box, type the DMZ's internal network range.
7. To reset the network to its default settings, do the following:

   a. Click **Default**.

      A confirmation message appears.

b. Click **OK**.

The default settings are restored.

8. Click **Apply**.

   A warning message appears.

9. Click **OK**.

   A success message appears.

Configuring a DMZ Network using Safe@Office 225

~~Safe@Office 105~~ ~~Safe@Office 110~~ Safe@Office 225

Note: If desired, you can enable the DHCP server for the DMZ network.

The default gateway for the DMZ computers should be specified as the Safe@Office DMZ IP address.

To configure a DMZ network

1. Connect the DMZ computer to the DMZ port.

   If you have more than one computer in the DMZ network, connect a hub or switch to the DMZ port, and connect the DMZ computers to the hub.

2. Click **Network** in the main menu, and click the **My Network** tab.

   The **My Network** page appears.

3. In the **Logical DMZ Settings** area, in the **DMZ Mode** drop-down list, select **Enabled**.

   The **Logical DMZ Settings** fields are enabled.

4. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 83.

5. In the **Safe@Office DMZ IP** text box, the IP address of the DMZ network's default gateway.

Note: The DMZ network must not overlap the LAN network.

6. In the **DMZ Subnet Mask** text box, type the DMZ's internal network range.
7. To reset the network to its default settings, do the following:

   a. Click **Default**.

      A confirmation message appears.

   b. Click **OK**.

      The default settings are restored.
8. Click **Apply**.

   A warning message appears.
9. Click **OK**.

   A success message appears.

Configuring High Availability

~~Safe@Office 105~~ ~~Safe@Office 110~~ Safe@Office 225

You can install two Safe@Office 225 appliances on your network, one acting as the "Master", the default gateway through which all network traffic is routed, and one acting as the "Backup". If the Master fails, the Backup automatically and transparently takes over all the roles of the Master. This ensures that your network is consistently protected by a Safe@Office appliance and connected to the Internet.

The Master and Backup each have separate IP addresses within the local network. In addition, the Master and Backup share a single virtual IP address, which is the default gateway address for the local network. The virtual IP address is used by the Master gateway, which sends periodic signals, or "heartbeats", to the network. If the Backup gateway detects that the heartbeat has stopped (indicating that the Master gateway has failed), it takes over of the virtual IP address and all of the Master gateway's roles. When the Master gateway is running once again, it reclaims the virtual IP address and resumes its roles.

Before configuring High Availability, the following requirements must be met:

- You must have two identical Safe@Office 225 appliances.
- The Safe@Office appliances must have identical firmware versions and firewall rules.
- The Safe@Office appliances must have different LAN and DMZ IP addresses, and they must be located on the same subnet. For information on configuring LAN and DMZ addresses, see ***Configuring Network Settings*** on page 79.
- The LAN ports of the two Safe@Office appliances must be connected via a hub or a switch.

You can configure both the LAN network and the DMZ network for High Availability.

The procedure below explains how to configure High Availability for the LAN network, but can be used to configure High Availability for the DMZ network as well.

Note: You can enable the DHCP server in both Safe@Office appliances. The Backup gateway's DHCP server will start answering DHCP requests only if the Master gateway fails.

Note: You can force a fail-over to the Backup Safe@Office appliance. You may want to do this in order to verify that High Availability is working properly, or if the Master Safe@Office appliance needs repairs. To force a fail-over, switch off the primary box or disconnect it from the LAN network.

To configure High Availability

1. In the Master Safe@Office appliance, do the following:

   a. Set the appliance's internal IP address.

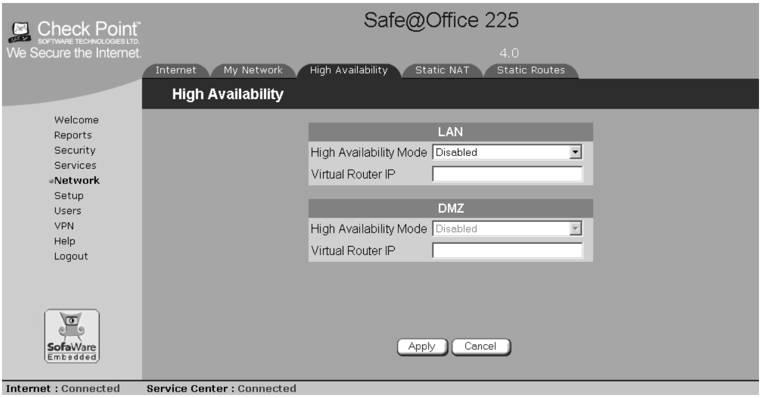
   For further information, see ***Changing IP Addresses*** on page 82.

   b. Configure the LAN network range.

   For further information, see ***Changing IP Addresses*** on page 82.

   c. Click **Network** in the main menu, and click the **High Availability** tab.

   The **High Availability page** appears.



High Availability

LAN

High Availability Mode: Disabled

Virtual Router IP:

DMZ

High Availability Mode: Disabled

Virtual Router IP:

Internet : Connected   Service Center : Connected

   d. In the **LAN** area, in the **High Availability Mode** drop-down list, select **Master.**

   e. In the **Virtual Router IP** text box, type the default gateway IP address.

   This can be any unused IP address in the LAN network, and must be the same for both gateways.

   f. Click **Apply**.

   A success message appears.

2. In the Backup appliance, do the following:

   a. Set the appliance's internal IP address.

      For further information, see ***Changing IP Addresses*** on page 82.

      The internal IP address must differ from the Master appliance's internal IP address.

   b. Configure the LAN network range to the same range you configured in the Master appliance.

      For further information, see ***Changing IP Addresses*** on page 82.

   c. Click **Network** in the main menu, and click the **High Availability** tab.

      The **High Availability** page appears.

   d. In the **LAN** area, in the **High Availability Mode** drop-down list, select **Backup**.

   e. In the **Virtual Router IP** text box, type the default gateway IP address.

      This address must be identical to the Virtual Router IP address you specified when configuring the Master gateway.

   f. Click **Apply**.

      A success message appears.

Using Static NAT

~~Safe@Office 105~~ | Safe@Office 110 | Safe@Office 225

Static NAT (or One-to-One NAT) allows the mapping of Internet IP addresses or address ranges to hosts inside the internal network.

This is useful if you want a computer in your private network to have its own Internet IP address. For example, if you have both a mail server and a Web server in your network, you can map each one to a separate Internet IP address.

Static NAT rules do not imply any security rules. To allow incoming traffic to a host for which you defined Static NAT, you must create an Allow rule. When specifying firewall rules for such hosts, use the host's internal IP address, and not the Internet IP address to which the internal IP address is mapped. For further information, see ***Creating Rules*** on page 112.

Note: Static NAT and Hide NAT can be used together.

Note: Safe@Office appliance supports Proxy ARP (Address Resolution Protocol). When an external source attempts to communicate with such a computer, the Safe@Office appliance automatically replies to ARP queries with its own MAC address, thereby enabling communication. As a result, the Static NAT Internet IP addresses appear to external sources to be real computers connected to the WAN interface.

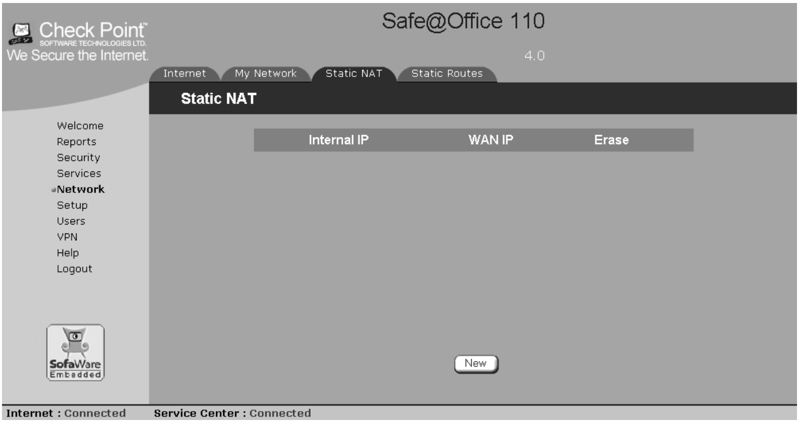
Adding and Editing Static NAT Mappings

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

To add or edit a static NAT mapping

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

   The **Static NAT** page appears.



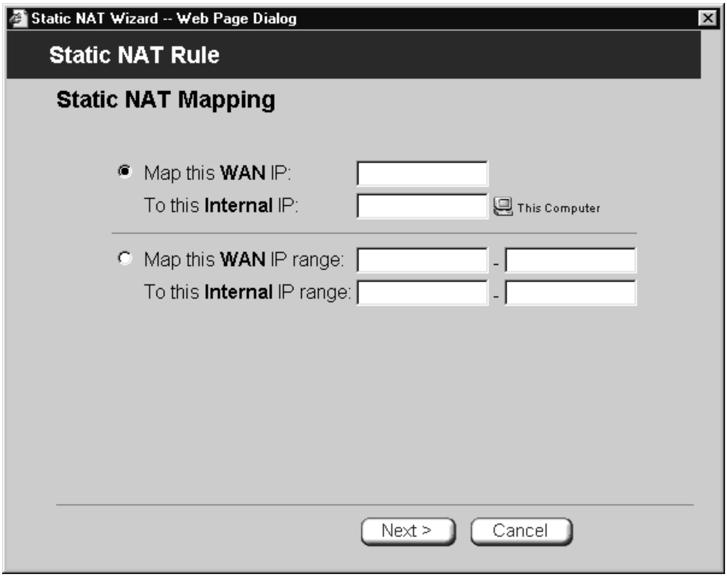
Internal IP	WAN IP	Erase

Internet : Connected   Service Center : Connected

2. Do one of the following:

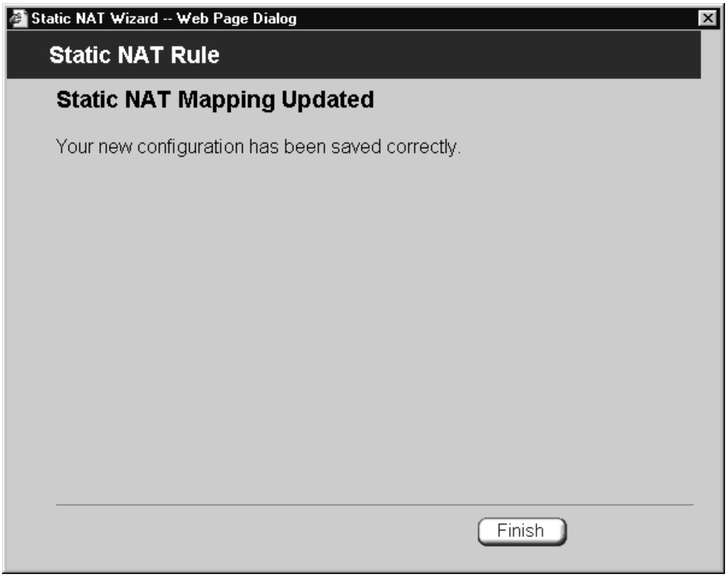
   - To add a new Static NAT mapping, click **New**.
   - To edit an existing Static NAT mapping, click **Edit**.

The Static NAT wizard opens, with the **Static NAT Mapping** dialog box displayed.



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

The **Static NAT Mapping Updated** dialog box is displayed.



Static NAT Mapping Updated

Your new configuration has been saved correctly.

5. Click **Finish**.

   If you added a new mapping, it appears in the **Static NAT** page.

Table 12: Static NAT Fields

In this field...	Do this...
Map this WAN IP	Click this option to map an Internet IP address to a local computer. You must then fill in the **MAP this WAN IP** and **To this Internal IP** fields.
Map this WAN IP	Type the desired Internet IP address.
To this Internal IP	Type the IP address of the local computer, or click **This Computer** to specify your computer.
Map this WAN IP range	Click this option to map a range of Internet IP addresses to a range of local computer IP addresses of the same size. You must then fill in the **MAP this WAN IP range** and **To this Internal IP range** fields.
Map this WAN IP range	Type the desired Internet IP address range.
To this Internal IP range	Type the range of local computer IP addresses.

Viewing and Deleting Static NAT Mappings

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

To view static NAT mappings

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

   The **Static NAT** page appears with a list of existing static NAT mappings.

2. To delete a static NAT mapping, do the following:

   a. In the desired static NAT mapping row, click the Delete 🗑 icon.

      A confirmation message appears.

   b. Click **OK**.

      The mapping is deleted.

Using Static Routes

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

A static route is a setting that explicitly specifies the route for packets destined for a certain subnet. Packets with a destination that does not match any defined static route will be routed to the default gateway.

To modify the default gateway, see ***Using a LAN Connection*** on page 61.

The **Static Routes** page lists all existing routes, including the default, and indicates whether each route is currently "Up", or reachable, or not.

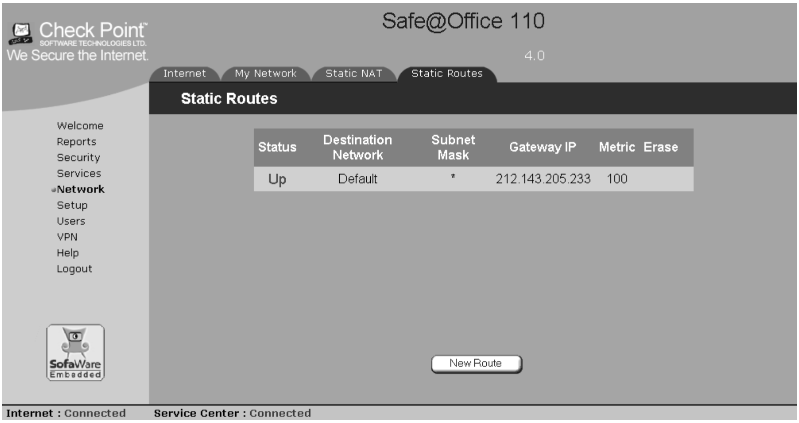
Adding a Static Route

~~Safe@Office 105~~ | Safe@Office 110 | Safe@Office 225

To add a static route

1. Click **Network** in the main menu, and click the **Static Routes** tab.

   The **Static Routes** page appears, with a listing of existing static routes.



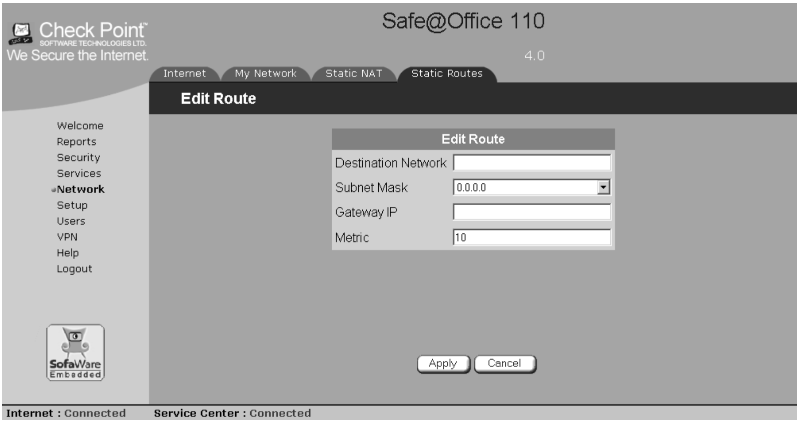
Static Routes

Status	Destination Network	Subnet Mask	Gateway IP	Metric	Erase
Up	Default	*	212.143.205.233	100	

Internet : Connected   Service Center : Connected

2. Click **New Route**.

The **Edit Route** page appears.



Edit Route	
Destination Network	
Subnet Mask	0.0.0.0
Gateway IP	
Metric	10

3. Complete the fields using the information in ***Edit Route Page Fields*** on page 98.
4. Click **Apply**.

   The new static route is saved.

Table 13: Edit Route Page Fields

In this field…	Do this…
Destination Network	Type the network address of the destination network.
Subnet Mask	Select the subnet mask.
Gateway IP	Type the IP address of the gateway (next hop router) to which to route the packets destined for this network.

In this field...	Do this...
Metric	Type the static route's metric. The gateway sends a packet to the route that matches the packet's destination and has the lowest metric.

Viewing and Editing Static Routes

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

To edit a static route

1. Click **Network** in the main menu, and click the **Static Routes** tab.

   The **Static Routes** page appears, with a listing of existing static routes.

2. To edit the route details, do the following:

   a. In the desired route row, click **Edit**.

      The **Edit Route** page appears displaying the destination network, subnet mask, and gateway IP of the selected route.

   b. Edit the fields using ***Edit Route Page Fields*** on page 98.

   c. Click **Apply**.

      The changes are saved.

Deleting a Static Route

~~Safe@Office 105~~
Safe@Office 110
Safe@Office 225

Note: The “default” route cannot be deleted.

To delete a static route

1. Click **Network** in the main menu, and click the **Static Routes** tab.

   The **Static Routes** page appears, with a listing of existing static routes.

2. In the desired route row, click the Delete 🗑 icon.

   A confirmation message appears.

3. Click **OK**.

   The route is deleted.

Chapter 6

Viewing Reports

This chapter describes the Safe@Office Portal reports.

This chapter includes the following topics:

Viewing the Event Log

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

You can track network activity using the Event Log. The Event Log displays the most recent events and color codes them.

Table 14: Event Log Color Coding

An event marked in this color...	Indicates...
Blue	Changes in your setup that you have made yourself or as a result of a security update implemented by your Service Center
Red	Connection attempts that were blocked by your firewall

An event marked in this color...	Indicates...
Orange	Connection attempts that were blocked by your custom security rules
Green	Traffic accepted by the firewall. By default, accepted traffic is not logged. However, such traffic may be logged if specified by a security policy downloaded from your Service Center.

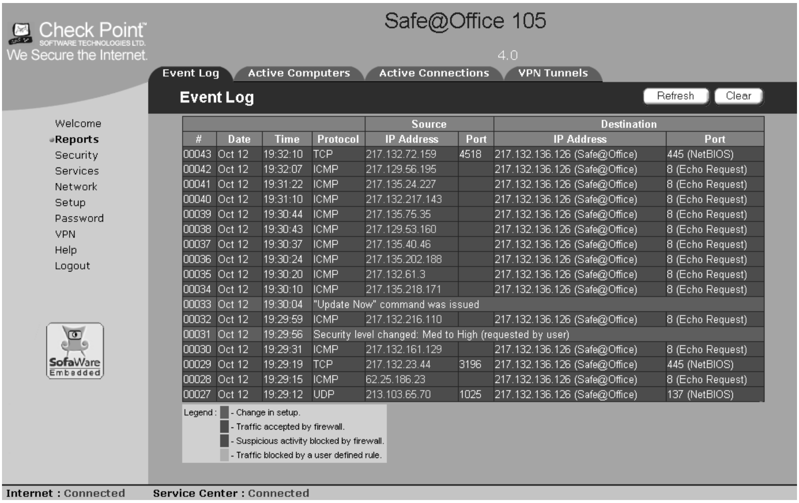
The logs detail the date and the time the event occurred, and its type. If the event is a communication attempt that was rejected by the firewall, the event details include the source and destination IP address, the destination port, and the protocol used for the communication attempt (for example, TCP or UDP).

Note: You can configure the Safe@Office appliance to send event logs to a Syslog server. For information, see ***Configuring Syslog Logging*** on page 204.

To view the event log

- Click **Reports** in the main menu, and click the **Event Log** tab.

  The **Event Log** page appears.



				Source		Destination	
#	Date	Time	Protocol	IP Address	Port	IP Address	Port
00043	Oct 12	19:32:10	TCP	217.132.72.159	4518	217.132.136.126 (Safe@Office)	445 (NetBIOS)
00042	Oct 12	19:32:07	ICMP	217.129.56.195		217.132.136.126 (Safe@Office)	8 (Echo Request)
00041	Oct 12	19:31:22	ICMP	217.135.24.227		217.132.136.126 (Safe@Office)	8 (Echo Request)
00040	Oct 12	19:31:10	ICMP	217.132.217.143		217.132.136.126 (Safe@Office)	8 (Echo Request)
00039	Oct 12	19:30:44	ICMP	217.135.75.35		217.132.136.126 (Safe@Office)	8 (Echo Request)
00038	Oct 12	19:30:43	ICMP	217.129.53.160		217.132.136.126 (Safe@Office)	8 (Echo Request)
00037	Oct 12	19:30:37	ICMP	217.135.40.46		217.132.136.126 (Safe@Office)	8 (Echo Request)
00036	Oct 12	19:30:24	ICMP	217.135.202.188		217.132.136.126 (Safe@Office)	8 (Echo Request)
00035	Oct 12	19:30:20	ICMP	217.132.61.3		217.132.136.126 (Safe@Office)	8 (Echo Request)
00034	Oct 12	19:30:10	ICMP	217.135.218.171		217.132.136.126 (Safe@Office)	8 (Echo Request)
00033	Oct 12	19:30:04	"Update Now" command was issued				
00032	Oct 12	19:29:59	ICMP	217.132.216.110		217.132.136.126 (Safe@Office)	8 (Echo Request)
00031	Oct 12	19:29:56	Security level changed: Med to High (requested by user)				
00030	Oct 12	19:29:31	ICMP	217.132.161.129		217.132.136.126 (Safe@Office)	8 (Echo Request)
00029	Oct 12	19:29:19	TCP	217.132.23.44	3196	217.132.136.126 (Safe@Office)	445 (NetBIOS)
00028	Oct 12	19:29:15	ICMP	62.25.186.23		217.132.136.126 (Safe@Office)	8 (Echo Request)
00027	Oct 12	19:29:12	UDP	213.103.65.70	1025	217.132.136.126 (Safe@Office)	137 (NetBIOS)

Legend : ■ - Change in setup.
■ - Traffic accepted by firewall.
■ - Suspicious activity blocked by firewall.
■ - Traffic blocked by a user defined rule.

Internet : Connected Service Center : Connected

You can do any of the following:

- Click the **Refresh** button to refresh the display.
- Click the **Clear** button to clear all events.
- If an event is highlighted in red, indicating a blocked attack on your network, you can display the attacker's details, by clicking on the IP address of the attacking machine.

  The Safe@Office appliance queries the Internet WHOIS server, and a window displays the name of the entity to whom the IP address is registered and their contact information. This information is useful in tracking down hackers.

Viewing Computers

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

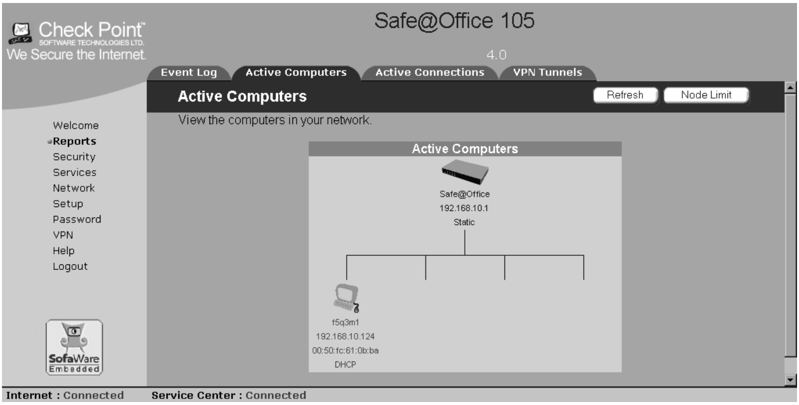
This option allows you to view the currently active computers on your network. The active computers are graphically displayed, each with its name, IP address, and settings (DHCP, Static, etc.).

You can also view node limit information.

To view the active computers

1. Click **Reports** in the main menu, and click the **Active Computers** tab.

   The **Active Computers** page appears.



View the computers in your network.

If you configured High Availability, both the master and backup appliances are shown.

If you are exceeding the maximum number of concurrent computers allowed by your license, a warning message appears, and the computers over the node limit are marked in red. These computers are still protected, but they are blocked from accessing the Internet through the Safe@Office appliance.

Note: Computers that did not communicate through the firewall are not counted for node limit purposes, even though they are protected by the firewall.

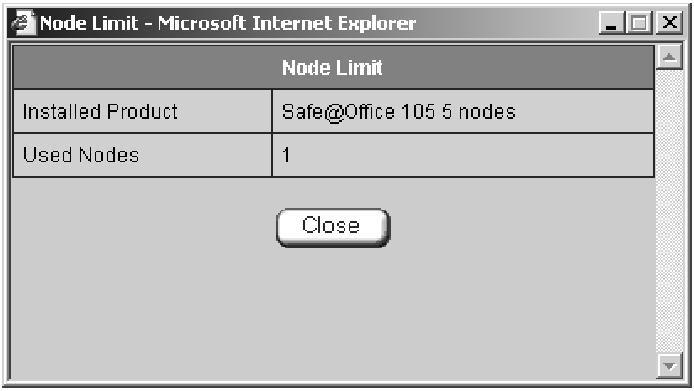
Note: To increase the number of computers allowed by your license, you must upgrade your product. For further information, see ***Upgrading Your Software Product*** on page 197.

If desired, you can click the **Refresh** button to refresh the display.

2. To view node limit information, do the following:

   a. Click **Node Limit**.

      The **Node Limit** window appears with installed software product and the number of nodes used.



Node Limit - Microsoft Internet Explorer

Node Limit	
Installed Product	Safe@Office 105 5 nodes
Used Nodes	1

   b. Click **Close** to close the window.

Viewing Connections

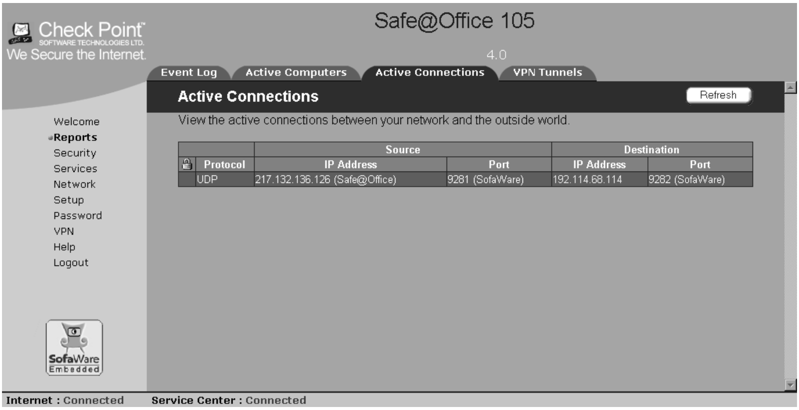
Safe@Office 105 | Safe@Office 110 | Safe@Office 225

This option allows you to view the currently active connections between your network and the external world. The active connections are displayed as a list, specifying source IP address, destination IP address and port, and the protocol used (TCP, UDP, etc.).

To view the active connections

- Click **Reports** in the main menu, and click the **Active Connections** tab.

  The **Active Connections** page appears.



Active Connections

View the active connections between your network and the outside world.

	Source		Destination	
Protocol	IP Address	Port	IP Address	Port
UDP	217.132.136.126 (Safe@Office)	9281 (SofaWare)	192.114.68.114	9282 (SofaWare)

You can do the following:

- Click the **Refresh** button to refresh the display.
- To view information on the destination machine, click its IP address.

  The Safe@Office appliance queries the Internet WHOIS server, and a window displays the name of the entity to whom the IP address is registered and their contact information.

Chapter 7

Setting Your Security Policy

This chapter describes how to set up your Safe@Office appliance security policy.

You can enhance your security policy by subscribing to services such as Web Filtering and E-mail Antivirus scanning. For information on these services and the subscription process, see ***Using Subscription Services*** on page 123.

This chapter includes the following topics:

Setting the Firewall Security Level

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

The firewall security level can be controlled using a simple lever available on the Firewall page. You can set the lever to three states.

Note: If the security policy is remotely managed, this lever might be disabled.

Table 15: Firewall Security Levels

This level…	Does this…	Further Details
Low	Enforces basic control on incoming connections, while permitting all outgoing connections.	All inbound traffic is blocked to the external Safe@Office appliance IP address, except for ICMP echoes ("pings"). All outbound connections are allowed.
Medium	Enforces strict control on all incoming connections, while permitting safe outgoing connections. This is the default level and is recommended for most cases. Leave it unchanged unless you have a specific need for a higher or lower security level.	All inbound traffic is blocked. All outbound traffic is allowed to the Internet except for Windows file sharing (NBT ports 137, 138, 139 and 445).

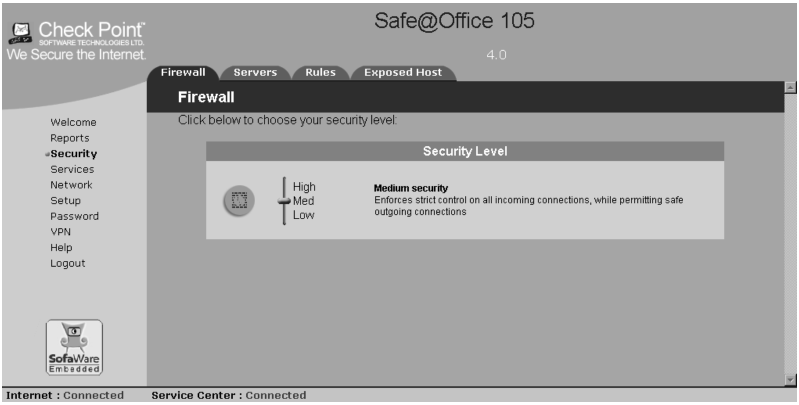
This level...	Does this...	Further Details
High	Enforces strict control on all incoming and outgoing connections.	All inbound traffic is blocked. Restricts all outbound traffic except for the following: Web traffic (HTTP, HTTPS), email (IMAP, POP3, SMTP), ftp, newsgroups, Telnet, DNS, IPSEC IKE and VPN traffic.

Note: The definitions of firewall security levels provided in this table represent the Safe@Office appliance's default security policy. Security updates downloaded from a Service Center may alter this policy and change these definitions.

To change the firewall security level

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

   The **Firewall** page appears.



Firewall

Click below to choose your security level:

Security Level

High
Med
Low

Medium security
Enforces strict control on all incoming connections, while permitting safe outgoing connections

Internet : Connected   Service Center : Connected

2. Drag the security lever to the desired level.

   The Safe@Office appliance security level changes accordingly.

Configuring Servers

Safe@Office **105** Safe@Office **110** Safe@Office **225**

Note: If you do not intend to host any public Internet servers (Web Server, Mail Server etc.) in your network, you can skip this section.

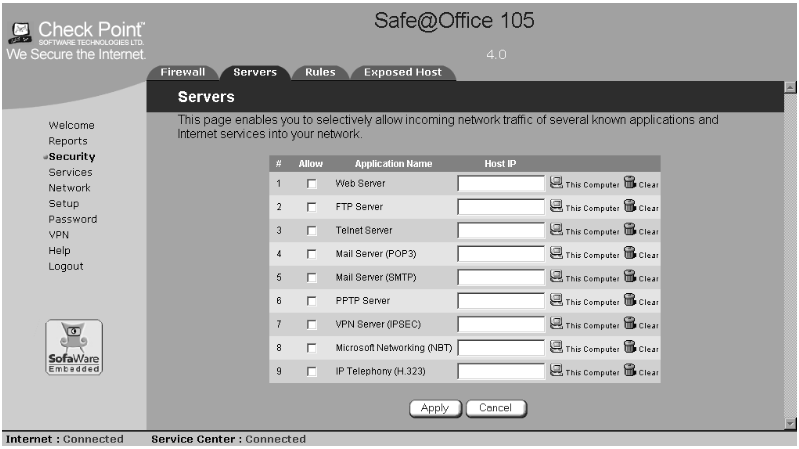
Using the Safe@Office Portal, you can selectively allow incoming network connections into your network. For example, you can set up your own Web server, Mail server or FTP server.

Note: Configuring servers allows you to create simple Allow and Forward rules for common services, and it is equivalent to creating Allow and Forward rules in the **Rules** page. For information on creating rules, see ***Creating Rules*** on page 112.

To allow a service to be run on a specific host

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

   The **Servers** page appears, displaying a list of services and a host IP address for each allowed service.



Servers

This page enables you to selectively allow incoming network traffic of several known applications and Internet services into your network.

#	Allow	Application Name	Host IP		
1	□	Web Server		This Computer	Clear
2	□	FTP Server		This Computer	Clear
3	□	Telnet Server		This Computer	Clear
4	□	Mail Server (POP3)		This Computer	Clear
5	□	Mail Server (SMTP)		This Computer	Clear
6	□	PPTP Server		This Computer	Clear
7	□	VPN Server (IPSEC)		This Computer	Clear
8	□	Microsoft Networking (NBT)		This Computer	Clear
9	□	IP Telephony (H.323)		This Computer	Clear

2. Complete the fields using the information in the table below.
3. Click **Apply**.

   A success message appears, and the selected computer is allowed to run the desired service or application.

Table 16: Servers Page Fields

In this column…	Do this…
Allow	Select the desired service or application.
VPN Only	Select this option to allow only connections made through a VPN.

In this column...	Do this...
Host IP	Type the IP address of the computer that will run the service (one of your network computers) or click the corresponding **This Computer** button to allow your computer to host the service.

To stop the forwarding of a service to a specific host

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

   The **Servers** page appears, displaying a list of services and a host IP address for each allowed service.

2. In the desired service or application's row, click **Clear**.

   The **Host IP** text box of the desired service is cleared.

3. Click **Apply**.

   The service or application is not allowed on the specific host.

Creating Rules

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

The Safe@Office appliance checks the protocol used, the ports range and the destination IP address, when deciding whether to allow or block traffic.

By default, in the Medium security level, the Safe@Office appliance blocks all connection attempts from the Internet (WAN) to the LAN, and allows all outgoing connection attempts from the LAN to the Internet (WAN).

User-defined rules have priority over the default rules.

Adding and Editing Rules

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

Rules provide you with greater flexibility in defining and customizing your security policy.

The following rule types exist:

Table 17: Firewall Rule Types

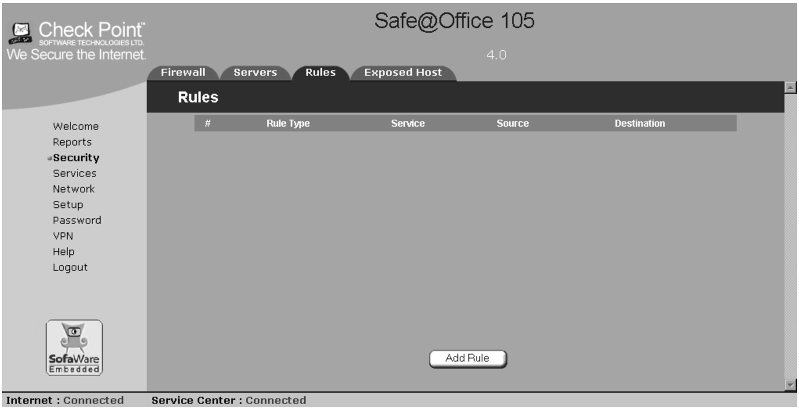
Rule	Description
Allow and Forward	This rule type enables you to do the following: • Permit incoming access from the Internet to a specific service in your internal network. • Forward all such connections to a specific computer in your network. Creating an Allow and Forward rule is equivalent to defining a server in the **Servers** page. **Note:** You must use this type of rule to allow incoming connections if your network uses Hide NAT. **Note**: You cannot specify two Allow and Forward rules that forward the same service to two different destinations.

Rule	Description
Allow	This rule type enables you to do the following: • Permit outgoing access from your internal network to a specific service on the Internet. Note: You can allow outgoing connections for services that are not permitted by the default security policy. • Permit incoming access from the Internet to a specific service in your internal network. **Note**: You cannot use an Allow rule to permit incoming traffic, if the network or VPN uses Hide NAT. However, you can use Allow rules for static NAT IP addresses. • You can only define Allow rules in Safe@Office 110 and 225.
Block	This rule type enables you to do the following: • Block outgoing access from your internal network to a specific service on the Internet • Block incoming access from the Internet to a specific service in your internal network

To add or edit a rule

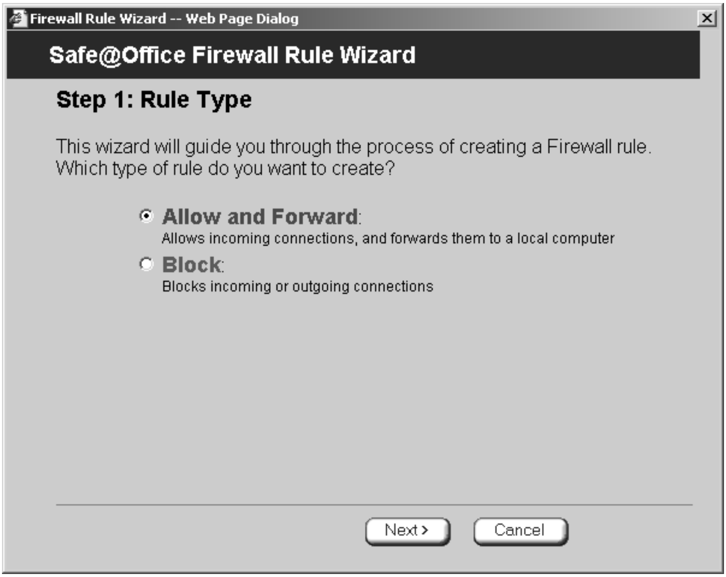
1. Click **Security** in the main menu, and click the **Rules** tab.

The **Rules** page appears.



2. Click **Add Rule**.

   The Firewall Rule wizard opens, with the **Step 1: Rule Type** dialog box displayed.


Firewall Rule Wizard -- Web Page Dialog
Safe@Office Firewall Rule Wizard

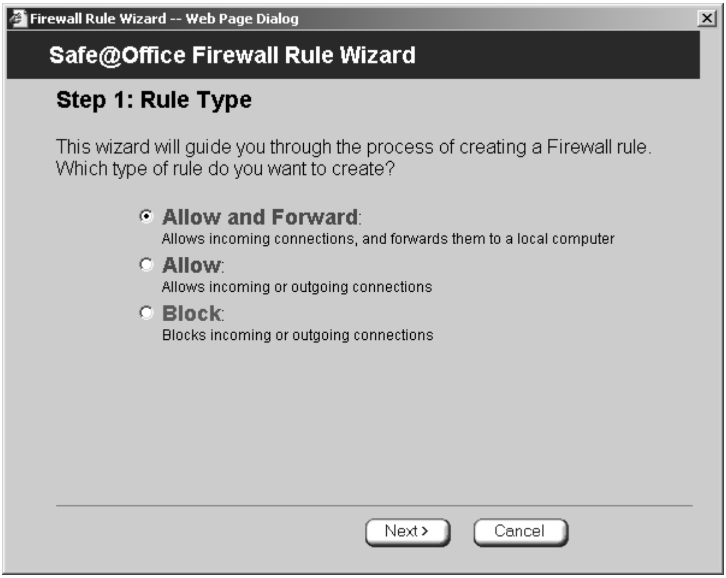
Step 1: Rule Type

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

● **Allow and Forward**: Allows incoming connections, and forwards them to a local computer

○ **Block**: Blocks incoming or outgoing connections

If you are using Safe@Office 110 or 225 the page appears as follows:



Firewall Rule Wizard -- Web Page Dialog

Safe@Office Firewall Rule Wizard

Step 1: Rule Type

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

● Allow and Forward: Allows incoming connections, and forwards them to a local computer

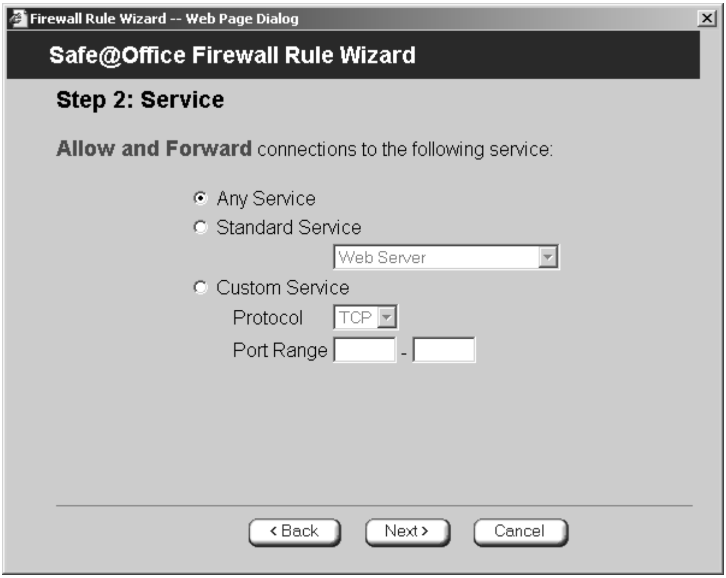
○ Allow: Allows incoming or outgoing connections

○ Block: Blocks incoming or outgoing connections

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

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

The example below shows an Allow and Forward rule.



Firewall Rule Wizard -- Web Page Dialog

Safe@Office Firewall Rule Wizard

Step 2: Service

Allow and Forward connections to the following service:

● Any Service

○ Standard Service

Web Server

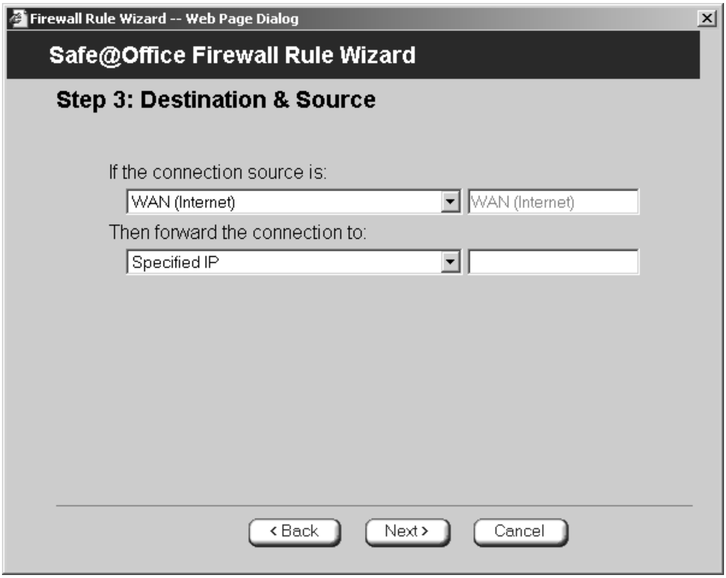
○ Custom Service

Protocol TCP

Port Range -

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

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



Firewall Rule Wizard -- Web Page Dialog

Safe@Office Firewall Rule Wizard

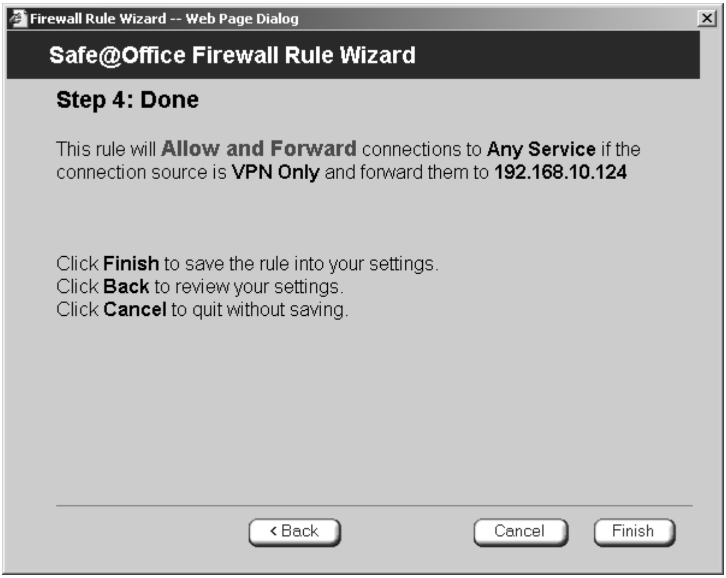
Step 3: Destination & Source

If the connection source is: WAN (Internet) | WAN (Internet)

Then forward the connection to: Specified IP

7. Complete the fields using the relevant information in Table 16.

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



Firewall Rule Wizard -- Web Page Dialog

Safe@Office Firewall Rule Wizard

Step 4: Done

This rule will **Allow and Forward** connections to **Any Service** if the connection source is **VPN Only** and forward them to **192.168.10.124**

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

8. Click **Finish**.

   The new rule appears in the Firewall Rules page.

Table 18: Firewall 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. You must then select the desired service from the drop-down list.

In this field...	Do this...
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 (ESP, GRE, TCP, UDP or ANY) for which the rule should apply.
Ports	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.
Source	Select the source of the connections you want to allow/block. To specify an IP address, select **Specified IP** and type the desired IP address in the text box.
Destination	Select the destination of the connections you want to allow or block. To specify an IP address, select **Specified IP** and type the desired IP address in the text box.

Deleting Rules

Safe@Office 105 Safe@Office 110 Safe@Office 225

To delete an existing rule

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

   The **Rules** page appears.

2. Click the 🗑 icon of the rule you wish to delete.

   A confirmation message appears.

3. Click **OK**.

   The rule is deleted.

Defining an Exposed Host

Safe@Office 105 Safe@Office 110 Safe@Office 225

The Safe@Office appliance allows you to define an exposed host, which is a computer that is not protected by the firewall. This is useful for setting up a public server. It allows **unlimited** incoming and outgoing connections between the Internet and the exposed host computer.

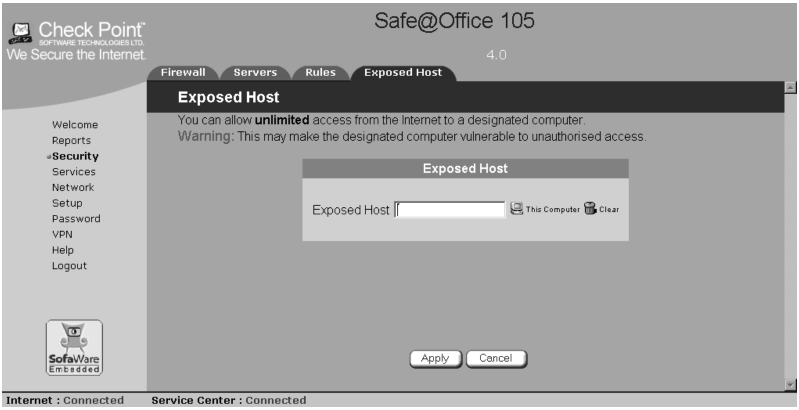
The exposed host receives all traffic that was not forwarded to another computer by use of Allow and Forward rules.

⚠ **Warning** - Entering an IP address may make the designated computer vulnerable to hacker attacks. Defining an exposed host is not recommended unless you are fully aware of the security risks.

To define a computer as an exposed host

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

   The **Exposed Host** page appears.



Exposed Host

You can allow **unlimited** access from the Internet to a designated computer.
Warning: This may make the designated computer vulnerable to unauthorised access.

Exposed Host

Exposed Host

2. In the **Exposed Host** text box, type the IP address of the computer you wish to define as an exposed host. Alternatively, you can click **This Computer** to define your computer as the exposed host.
3. Click **Apply**.

   The selected computer is now defined as an exposed host.

Chapter 8

Using Subscription Services

This chapter explains how to start and use subscription services, such as automatic software and security policy updates, content filtering, email virus scanning, and remote logging.

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

This chapter includes the following topics:

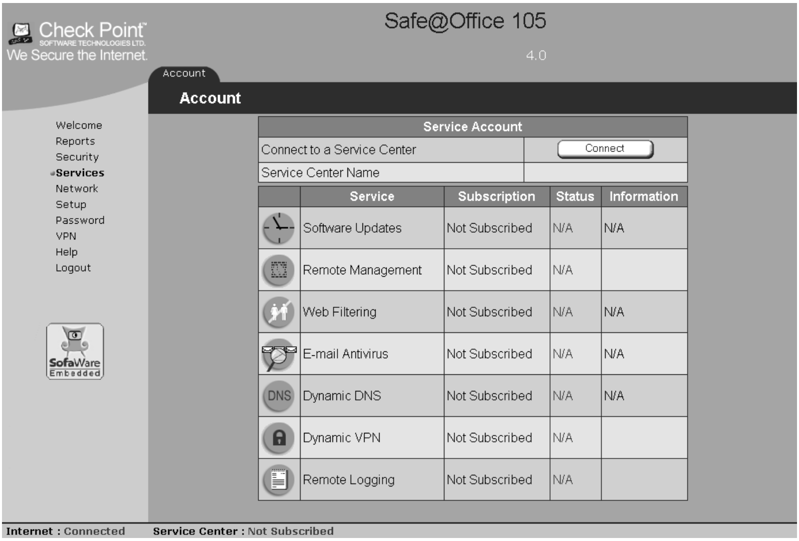
Connecting to a Service Center

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

To connect to a Service Center

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

The **Account** page appears.



Account

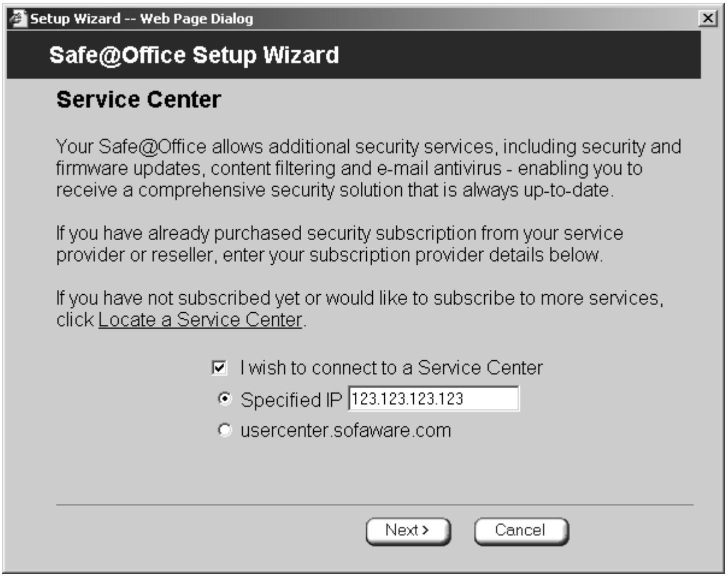
Service Account	
Connect to a Service Center	Connect
Service Center Name	

	Service	Subscription	Status	Information
	Software Updates	Not Subscribed	N/A	N/A
	Remote Management	Not Subscribed	N/A	
	Web Filtering	Not Subscribed	N/A	N/A
	E-mail Antivirus	Not Subscribed	N/A	N/A
DNS	Dynamic DNS	Not Subscribed	N/A	N/A
	Dynamic VPN	Not Subscribed	N/A	
	Remote Logging	Not Subscribed	N/A	

Internet : Connected **Service Center :** Not Subscribed

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

The Setup Wizard opens, with the **Subscription Services** dialog box displayed.



Service Center

Your Safe@Office allows additional security services, including security and firmware updates, content filtering and e-mail 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.

☑ I wish to connect to a Service Center

● Specified IP 123.123.123.123

○ usercenter.sofaware.com

3. Make sure the **I wish to connect to a Service Center** check box is selected.
4. Do one of the following:

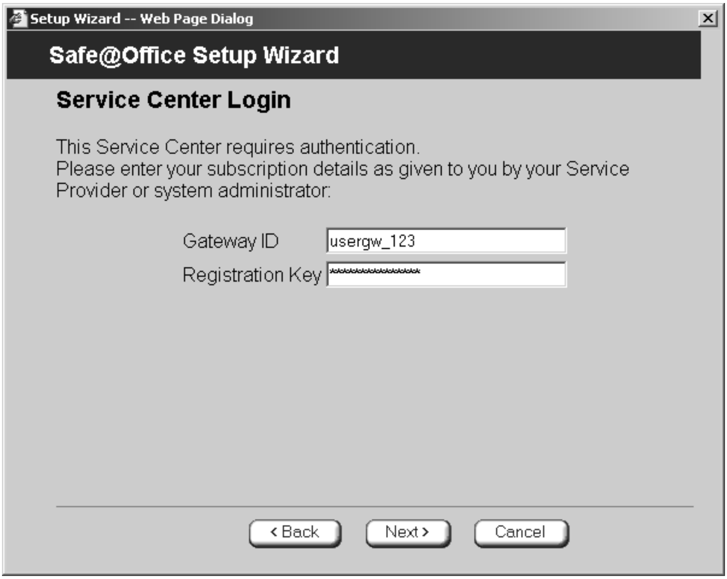
   - To connect to the SofaWare Service Center, select **usercenter.sofaware.com**.
   - To specify a Service Center, do the following:

     1) Select **Specified**.

     2) In the **Specified** text box, 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: ***************

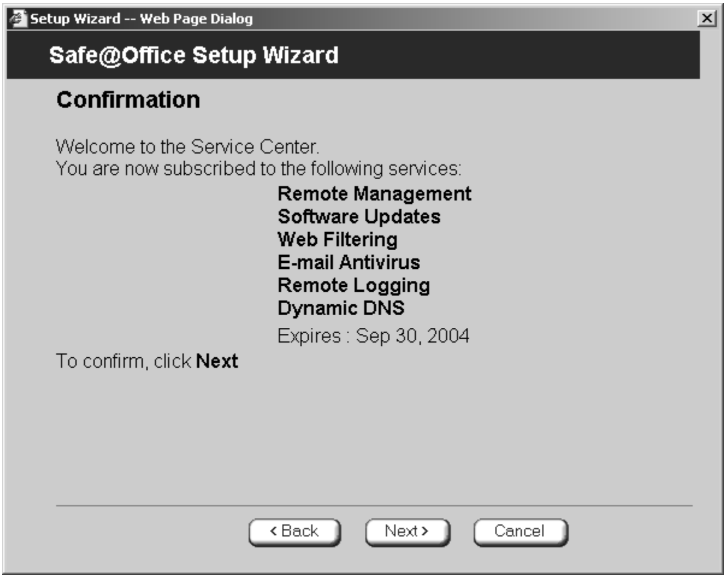
Do the following:

1) Enter your gateway ID and registration key in the appropriate fields, as given to you by your service provider.

2) Click **Next**.

- The **Connecting...** screen appears.

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



Safe@Office Setup Wizard

Confirmation

Welcome to the Service Center.
You are now subscribed to the following services:

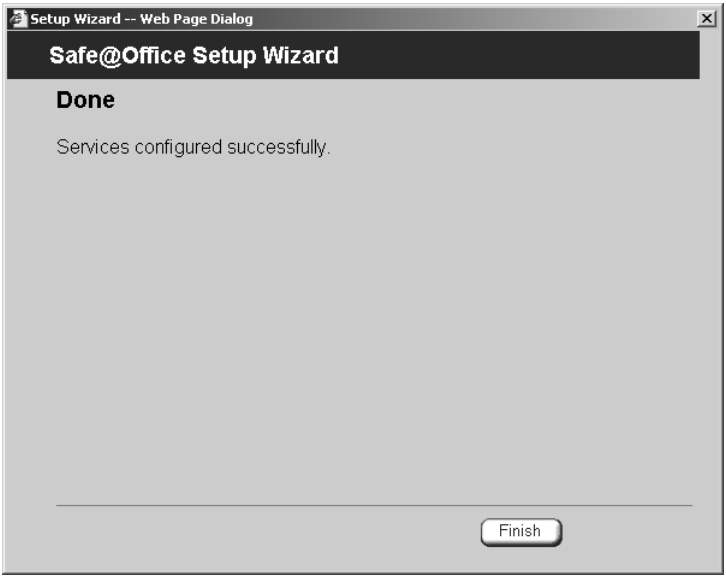
Remote Management
Software Updates
Web Filtering
E-mail Antivirus
Remote Logging
Dynamic DNS

Expires : Sep 30, 2004

To confirm, click **Next**

6. Click **Next**.

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



Setup Wizard -- Web Page Dialog

Safe@Office Setup Wizard

Done

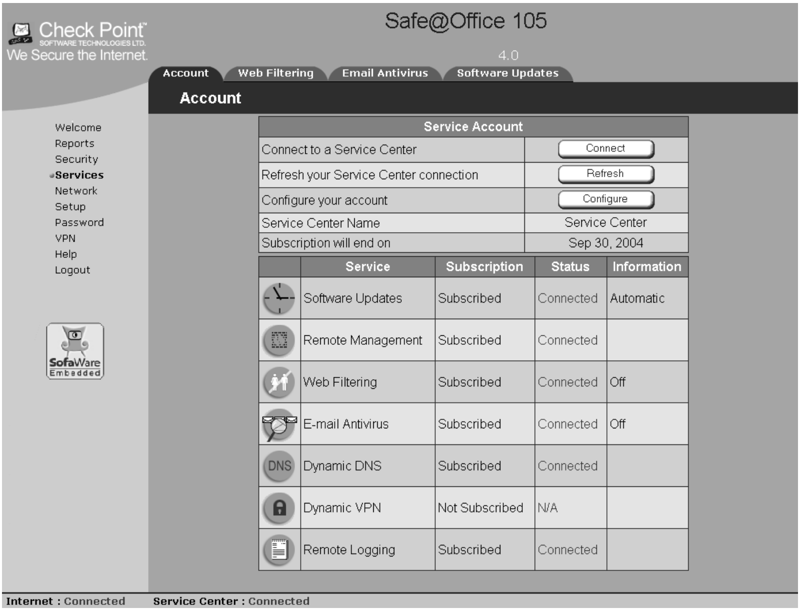
Services configured successfully.

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 130 for further information.



Service Account	
Connect to a Service Center	Connect
Refresh your Service Center connection	Refresh
Configure your account	Configure
Service Center Name	Service Center
Subscription will end on	Sep 30, 2004

	Service	Subscription	Status	Information
	Software Updates	Subscribed	Connected	Automatic
	Remote Management	Subscribed	Connected	
	Web Filtering	Subscribed	Connected	Off
	E-mail Antivirus	Subscribed	Connected	Off
DNS	Dynamic DNS	Subscribed	Connected	
	Dynamic VPN	Not Subscribed	N/A	
	Remote Logging	Subscribed	Connected	

Internet : Connected   Service Center : Connected

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

Viewing Services Information

Safe@Office 105 Safe@Office 110 Safe@Office 225

The **Account** page displays the following information about your subscription.

Table 19: Account Page Fields

This field...	Displays...
Service Center Name	The name of the Service Center to which you are connected (if known).
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. • **N/A.** The service is not available.
Mode	The mode to which each service is set. For further information, see ***Web Filtering*** on page 133, ***Virus Scanning*** on page 136, and ***Automatic and Manual Updates*** on page 139.

Refreshing Your Service Center Connection

Safe@Office 105 Safe@Office 110 Safe@Office 225

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

Safe@Office 105 Safe@Office 110 Safe@Office 225

This option allows you to access your Service Center Web site, which may offer additional configuration options for your account.

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 Web site opens.

3. Follow the on-screen instructions.

Disconnecting from Your Service Center

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

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 Setup Wizard opens, with the first **Subscription Services** dialog box displayed.

3. Clear the **I wish to 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.

Web Filtering

When enabled, access to Web content is restricted according to the categories specified under ‘Allow Categories’. Adult users will be able to view Web pages with no restrictions, only after they have provided the administrator password via the **Web Filtering** pop-up window.

Enabling/Disabling Web Filtering

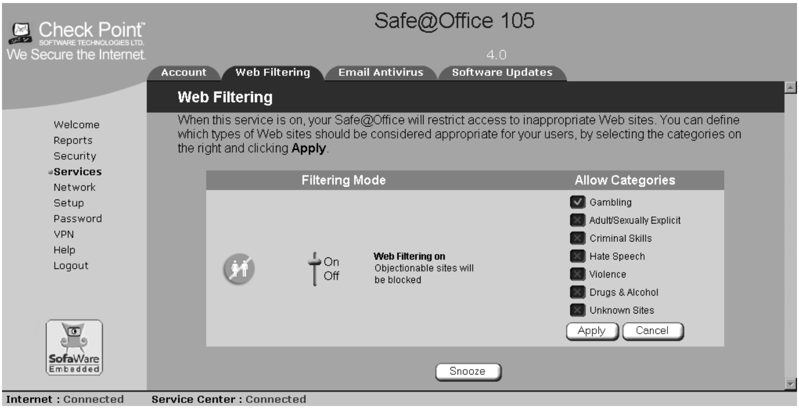
Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

Note: If you are remotely managed, contact your Service Center to change these settings.

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 on the right and clicking **Apply**.

Web Filtering on
Objectionable sites will be blocked

☑ Gambling
☒ Adult/Sexually Explicit
☒ Criminal Skills
☒ Hate Speech
☒ Violence
☒ Drugs & Alcohol
☒ Unknown Sites

Internet : Connected **Service Center :** Connected

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

   Web Filtering is enabled/disabled for all internal network computers.

Selecting Categories for Blocking

Safe@Office 105 Safe@Office 110 Safe@Office 225

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 you are remotely managed, contact your Service Center to change these settings.

To allow/block a category

1. In the **Allow Categories** area, click ☑ or ☒ next to the desired category.
2. Click **Apply**.

Temporarily Disabling Web Filtering

Safe@Office 105 Safe@Office 110 Safe@Office 225

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

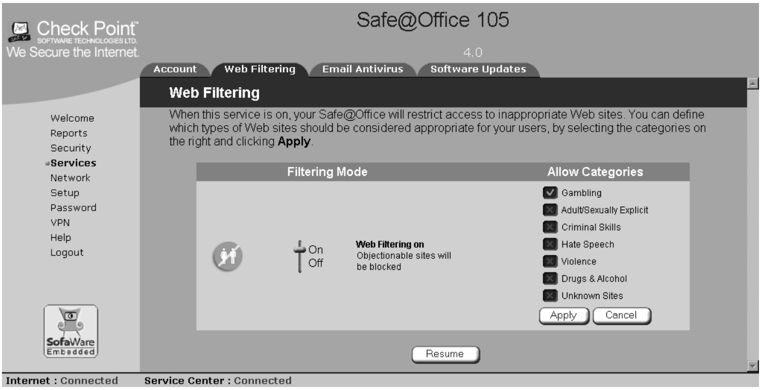
To temporarily disable Web Filtering

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

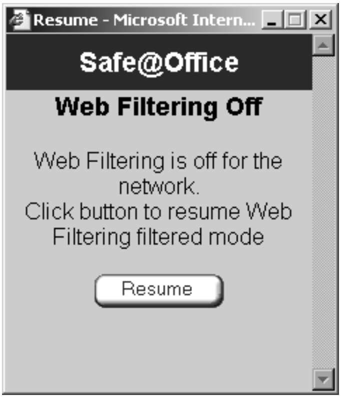
When this service is on, your Safe@Office will restrict access to inappropriate Web sites. You can define which types of Web sites should be considered appropriate for your users, by selecting the categories on the right and clicking **Apply**.

Web Filtering on
Objectionable sites will be blocked

☑ Gambling
☒ Adult/Sexually Explicit
☒ Criminal Skills
☒ Hate Speech
☒ Violence
☒ Drugs & Alcohol
☒ Unknown Sites

Internet : Connected   Service Center : Connected

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



Safe@Office

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.

Virus Scanning

Enabling this option will result in automatic scanning of your email for the detection and elimination of all known viruses and vandals.

Enabling/Disabling Email Antivirus

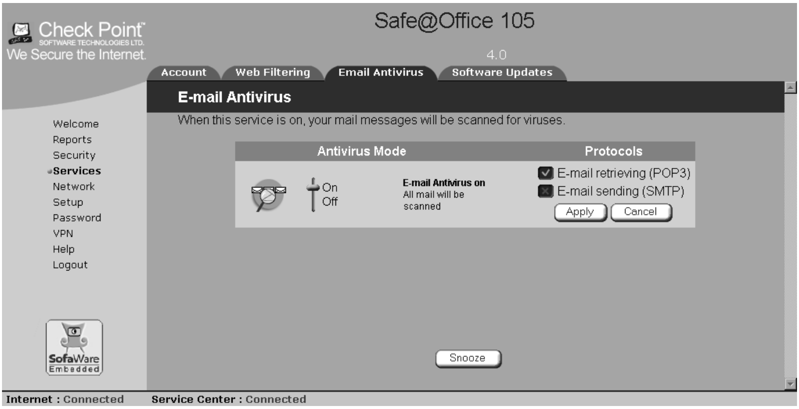
Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

Note: If you are remotely managed, contact your Service Center to change these settings.

To enable/disable Email Antivirus

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

   The **Email Antivirus** page appears.



E-mail Antivirus

When this service is on, your mail messages will be scanned for viruses.

E-mail Antivirus on
All mail will be scanned

☑ E-mail retrieving (POP3)
☒ E-mail sending (SMTP)

Internet : Connected Service Center : Connected

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

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

Selecting Protocols for Scanning

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

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

- **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 you are remotely managed, contact your Service Center to change these settings.

To enable virus scanning for a protocol

1. In the **Protocols** area, click ☑ or ☒ next to the desired protocol.
2. Click **Apply**.

Temporarily Disabling Email Antivirus

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

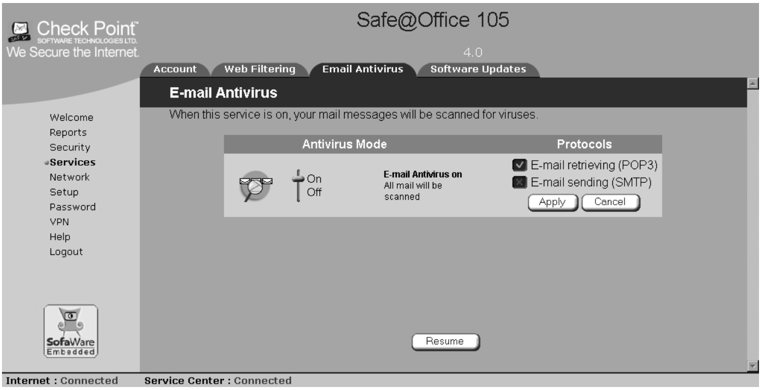
If you are having problems sending or receiving email you can temporarily disable the Email Antivirus service.

To temporarily disable Email Antivirus

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

   The **Email Antivirus** page appears.
2. Click **Snooze**.

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



E-mail Antivirus

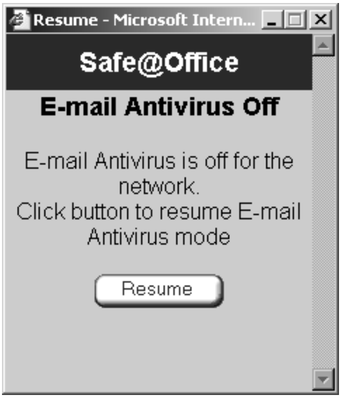
When this service is on, your mail messages will be scanned for viruses.

Antivirus Mode: On / Off — E-mail Antivirus on. All mail will be scanned

Protocols:
☑ E-mail retrieving (POP3)
☒ E-mail sending (SMTP)

Internet : Connected   Service Center : Connected

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



Safe@Office

E-mail Antivirus Off

E-mail Antivirus is off for the network.
Click button to resume E-mail Antivirus mode

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

   - The service is re-enabled for all internal network computers.
   - If you clicked **Resume** in the **Email Antivirus** page, the button changes to **Snooze**.

- If you clicked **Resume** in the **Email Antivirus Off** popup window, the popup window closes.

Automatic and Manual Updates

If you are subscribed to Software Updates, you can check for new security and software updates.

Checking for Software Updates when Locally Managed

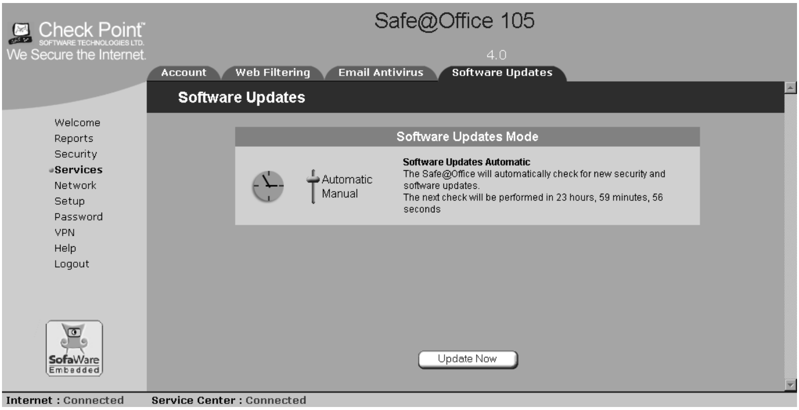
Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

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 Automatic
The Safe@Office will automatically check for new security and software updates.
The next check will be performed in 23 hours, 59 minutes, 56 seconds

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.

Checking for Software Updates When Remotely Managed

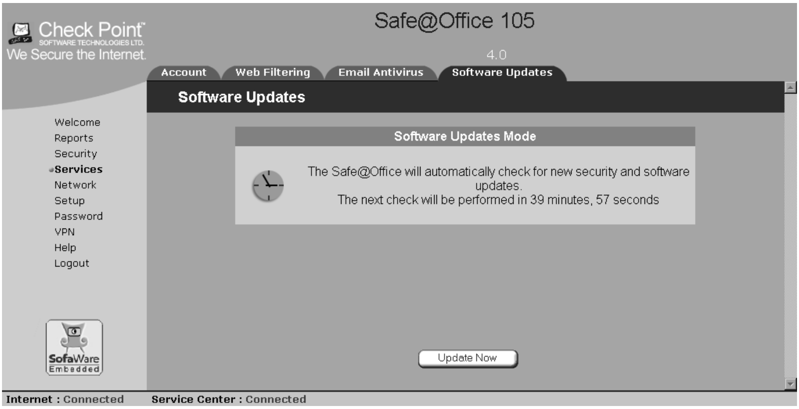
Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

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

The Safe@Office will automatically check for new security and software updates.
The next check will be performed in 39 minutes, 57 seconds

2. Click **Update Now**.

The system checks for new updates and installs them.

Chapter 9

Working With VPNs

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

This chapter includes the following topics:

Overview

A virtual private network (VPN) consists of at least one VPN server or gateway, and several VPN clients. A VPN server makes the office network remotely available to authorized users, such as employees working from home, who connect to the VPN server using VPN clients. A VPN gateway can be connected to another VPN gateway in a permanent, bi-directional relationship. The two connected networks function as a single network.

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.

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.

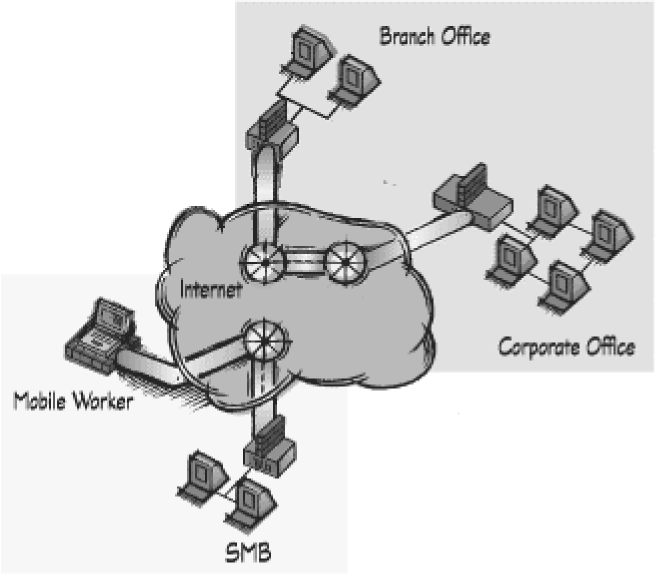


Figure 7: Typical Office VPN

Safe@Office 105 acts as a VPN server for one user, allowing a single remote employee to securely work from home or on the road.

Safe@Office 110 and 225 provide full VPN functionality. They can act as a VPN client, a VPN server for multiple users, or a VPN gateway.

Setting Up Your Safe@Office Appliance as a VPN Server

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

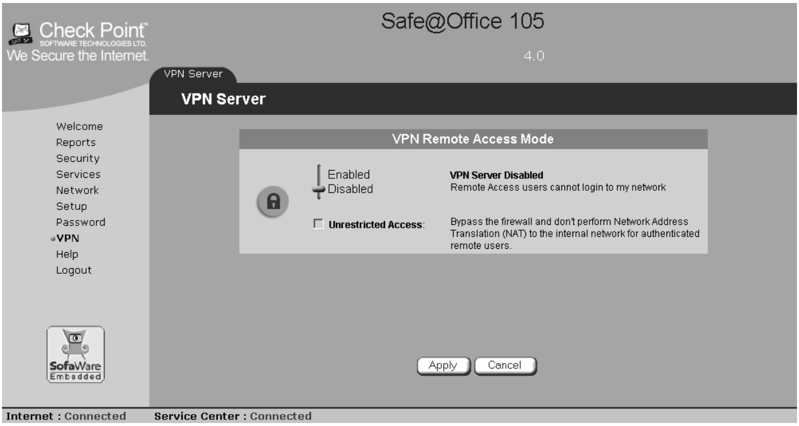
You can make your network remotely available to authorized users by setting up your Safe@Office appliance as a VPN server. Remote access users can connect to the VPN server via Check Point SecuRemote or a Safe@Office appliance in Remote Access VPN mode.

Note: The Check Point SecuRemote VPN client can be downloaded for free from http://www.checkpoint.com/techsupport/downloads_sr.html

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

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

   The **VPN Server** page appears.



VPN Server

VPN Remote Access Mode

Enabled
Disabled

VPN Server Disabled
Remote Access users cannot login to my network

☐ **Unrestricted Access**: Bypass the firewall and don't perform Network Address Translation (NAT) to the internal network for authenticated remote users.

Internet : Connected   **Service Center :** Connected

2. Drag the **Enabled/Disabled** lever to **Enabled**.

   The VPN server is enabled.

   The check box is enabled.

3. To allow authenticated users to access to your internal network without restriction and bypass NAT, select **Unrestricted Access**.
4. Follow the procedure ***Setting Up Remote VPN Access for Users*** on page 188.

Note: Disabling the VPN server will cause all existing VPN tunnels to disconnect.

Adding and Editing VPN Sites

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

You define each VPN site according to the function you want your Safe@Office appliance to perform when connecting to it:

- **VPN client**

  Define the VPN site as a Remote Access VPN site using the procedure below.

- **VPN gateway**

  - On the first VPN site's Safe@Office appliance, define the second VPN site as a Site-to-Site VPN gateway or create a PPPoE tunnel to the second VPN site, using the procedure below.

    Then enable the VPN server using the procedure ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 145.

  - On the second VPN site's Safe@Office appliance, define the first VPN site as a Site-to-Site VPN gateway or create a PPPoE tunnel to the first VPN site, using the procedure below.

    Then enable the VPN server using the procedure ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 145.

To add or edit VPN sites

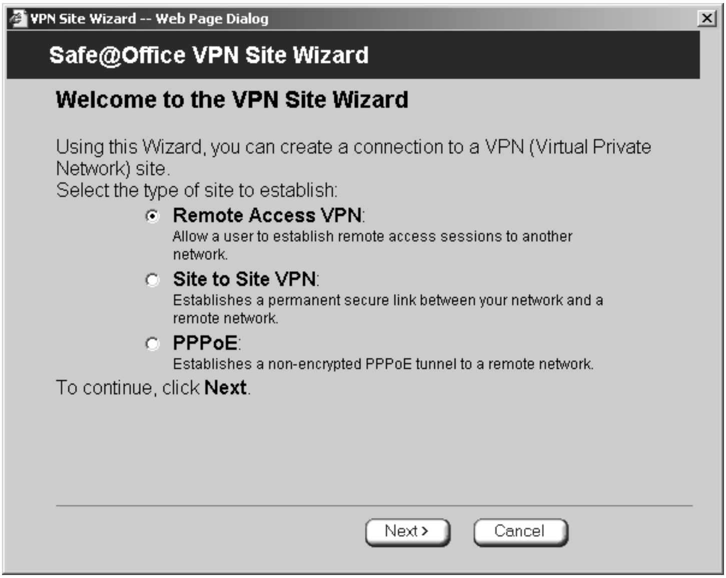
1. Click **VPN** in the main menu, and click the **VPN Sites** tab.

   The **VPN Sites** page appears with a list of VPN sites.

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 VPN Site Wizard opens, with the **Welcome to the VPN Site Wizard** dialog box displayed.



VPN Site Wizard -- Web Page 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.

○ **PPPoE**:
Establishes a non-encrypted PPPoE tunnel to a remote network.

To continue, click **Next**.

3. Do one of the following:

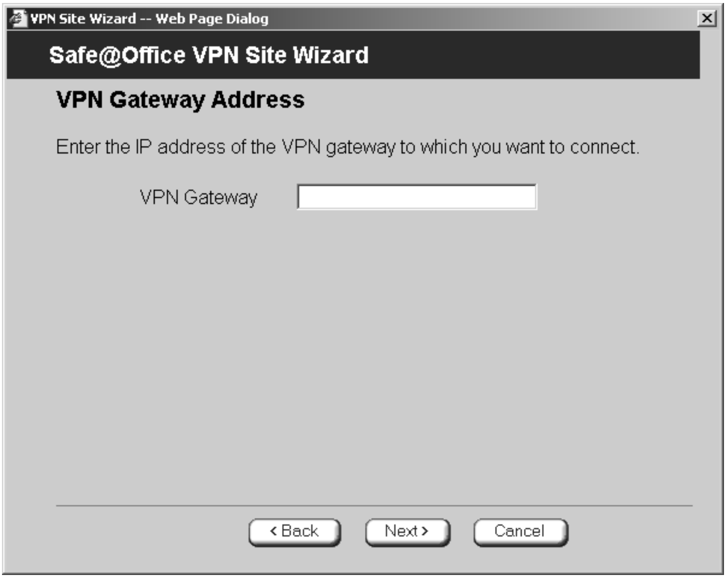
   - Select **Remote Access VPN** to establish remote access from your VPN client to a VPN server or gateway.
   - Select **Site to Site VPN** to create a permanent bi-directional connection to another gateway.

- Select **PPPoE** to create a non-encrypted connection to a PPPoE server.

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 -- Web Page Dialog

Safe@Office VPN Site Wizard

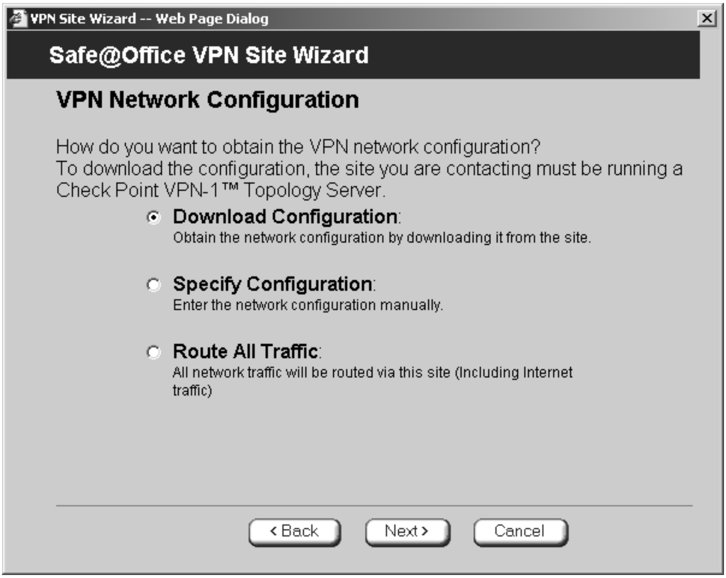
VPN Gateway Address

Enter the IP address of the VPN gateway to which you want to connect.

VPN Gateway

1. Enter the IP address of the VPN gateway to which you want to connect, as given to you by the network administrator.
2. Click **Next**.

The **VPN Network Configuration** dialog box appears.



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.

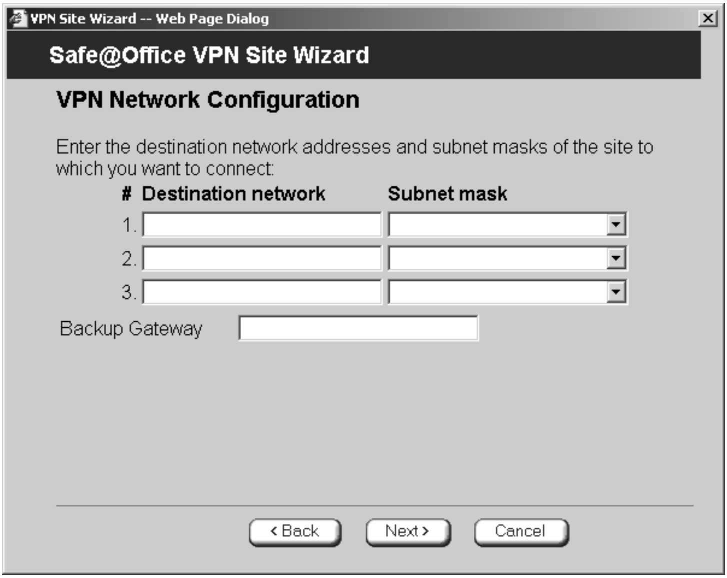
○ **Specify Configuration**: Enter the network configuration manually.

○ **Route All Traffic**: All network traffic will be routed via this site (Including Internet traffic)

3. Specify how you want to obtain the VPN network configuration. Refer to ***VPN Network Configuration Fields*** on page 155.
4. 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 -- Web Page 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:

#	Destination network	Subnet mask
1.		
2.		
3.		

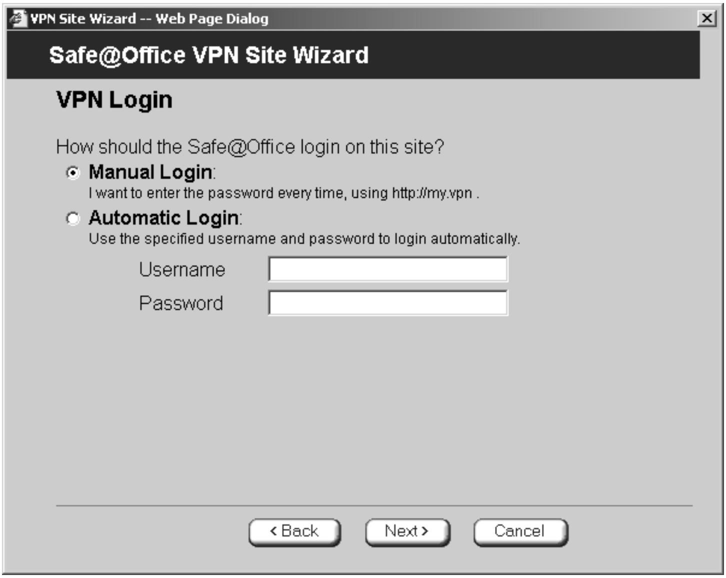
Backup Gateway

Do the following:

1) Complete the fields using the information in ***VPN Network Configuration Fields*** on page 155.

2) Click **Next**.

- The **VPN Login** dialog box appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

VPN Login

How should the Safe@Office login on this site?

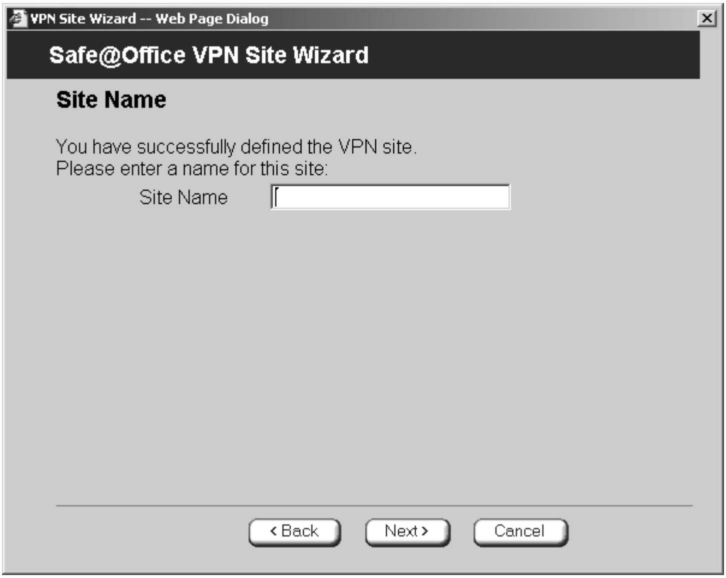
● **Manual Login**:
I want to enter the password every time, using http://my.vpn .

○ **Automatic Login**:
Use the specified username and password to login automatically.

Username
Password

5. Complete the fields using the information in ***VPN Login Fields*** on page 154.
6. Click **Next**.

The **Site Name** dialog box appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

Site Name

You have successfully defined the VPN site.
Please enter a name for this site:

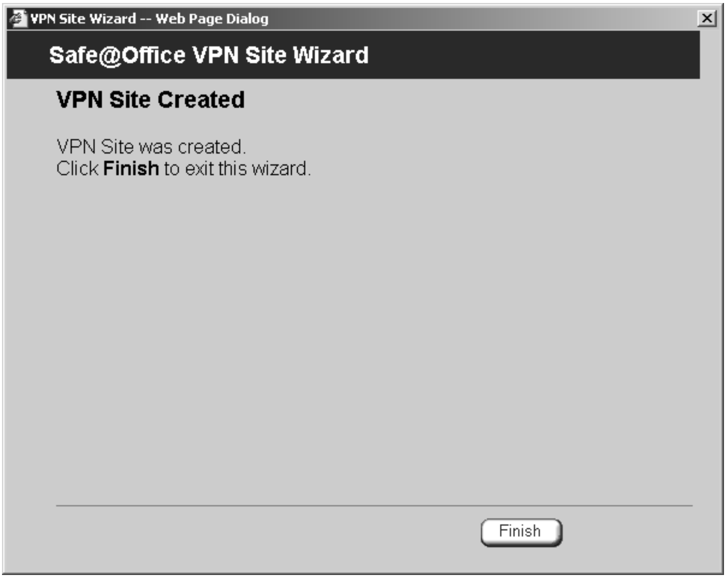
Site Name

7. Enter a name for the VPN site.

   You may choose any name.

8. Click **Next**.

The **VPN Site Created** screen appears.



VPN Site Wizard -- Web Page Dialog
Safe@Office VPN Site Wizard

VPN Site Created

VPN Site was created.
Click **Finish** to exit this wizard.

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.

Table 20: VPN Login Fields

In this field…	Do this…
Manual Login	Click this option to configure the site for Manual Login. Manual Login connects only the computer you are currently logged onto 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 on to a VPN Site*** on page 168.
Automatic Login	Click this option to enable the Safe@Office appliance to log on 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 on to a VPN Site*** on page 168.
Username	Type the user name to be used for logging on to the VPN site.
Password	Type the password to be used for logging on to the VPN site.

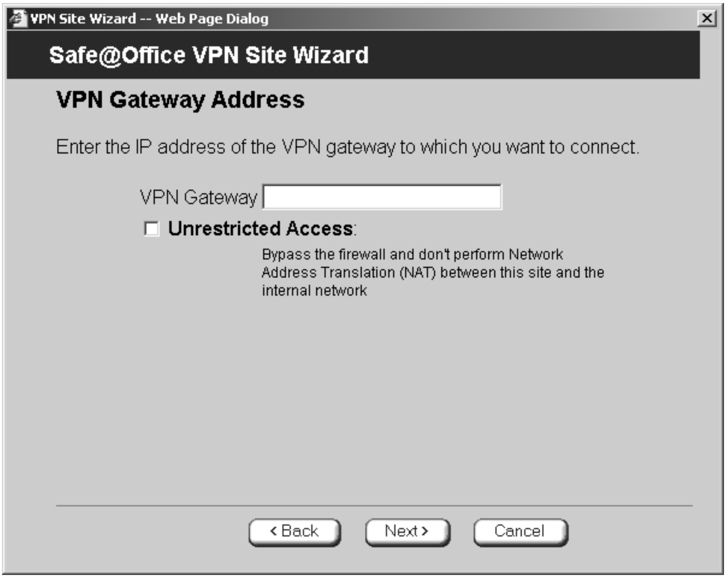
Table 21: VPN Network Configuration Fields

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 VPN server. Note: Downloading the network configuration is only possible if you are connecting to a Check Point VPN-1 or Safe@Office VPN gateway.
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. This option increases network security. 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.
Destination network	Type up to three destination network addresses at the VPN site to which you want to connect.

In this field...	Do this...
Subnet mask	Select the subnet masks for the destination network addresses. Note: Obtain the destination networks and subnet masks from the VPN gateway's system administrator.
Backup Gateway	Type the name of the VPN gateway to use if the primary VPN gateway fails.

Configuring a Site-to-Site VPN Gateway

If you selected **Site to Site VPN**, the **VPN Gateway Address** dialog box appears.



VPN Site Wizard -- Web Page 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

□ **Unrestricted Access**:

Bypass the firewall and don't perform Network Address Translation (NAT) between this site and the internal network

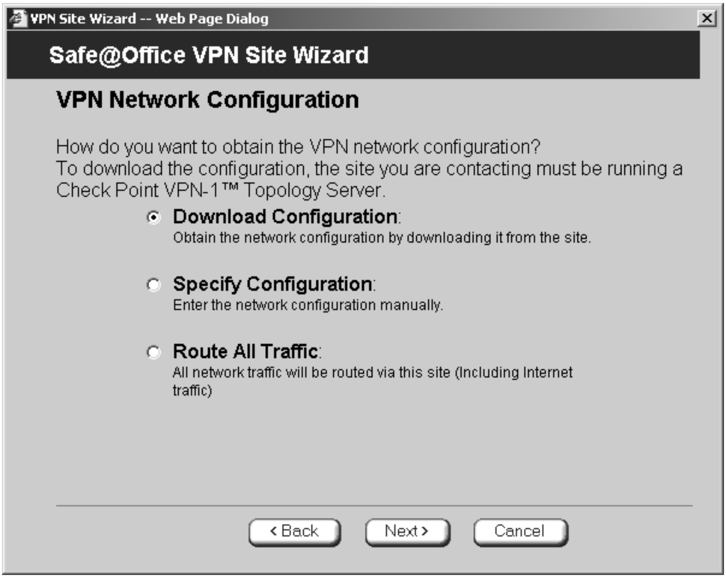
1. In the **VPN Gateway** field, enter the IP address of the VPN gateway to which you want to connect, as given to you by the network administrator.

2. To allow the VPN site to access to your internal network without restriction and bypass NAT, select **Unrestricted Access**.

3. Click **Next**.

   The **Resolving...** screen appears.

   The **VPN Network Configuration** dialog box appears.



VPN Site Wizard -- Web Page 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.

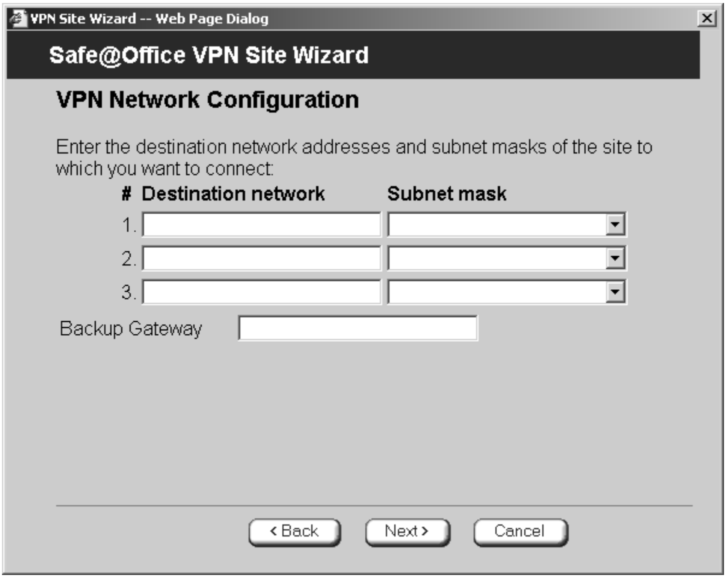
○ Specify Configuration: Enter the network configuration manually.

○ 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 155.

5. Click **Next**.

- If you chose **Specify Configuration**, a second **VPN Network Configuration** dialog box appears.



VPN Site Wizard -- Web Page 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:

#	Destination network	Subnet mask
1.		
2.		
3.		

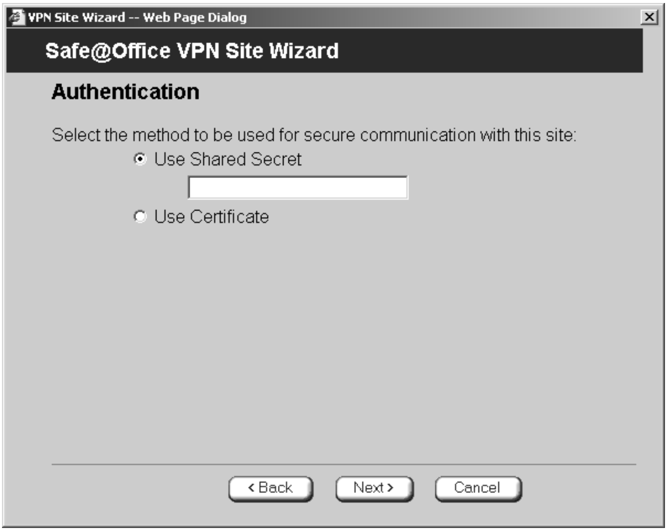
Backup Gateway

Do the following:

1) Complete the fields using the information in ***VPN Network Configuration Fields*** on page 155.

2) Click **Next**.

- The **Authentication** dialog box appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

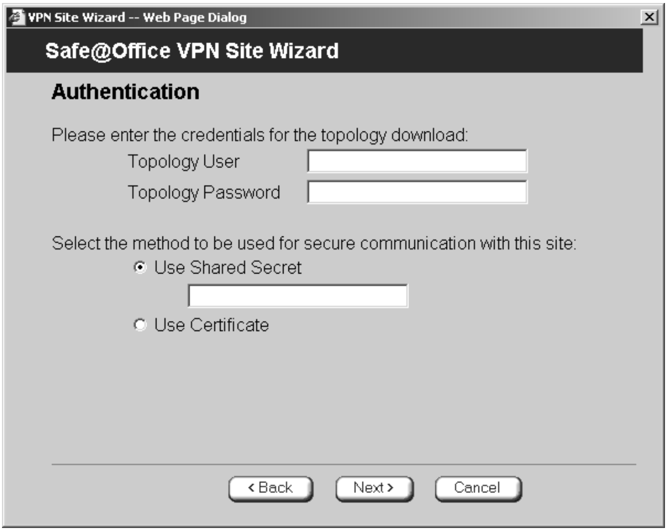
Authentication

Select the method to be used for secure communication with this site:

● Use Shared Secret

○ Use Certificate

If you chose **Download Configuration**, the dialog box appears as follows:



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

Authentication

Please enter the credentials for the topology download:

Topology User

Topology Password

Select the method to be used for secure communication with this site:

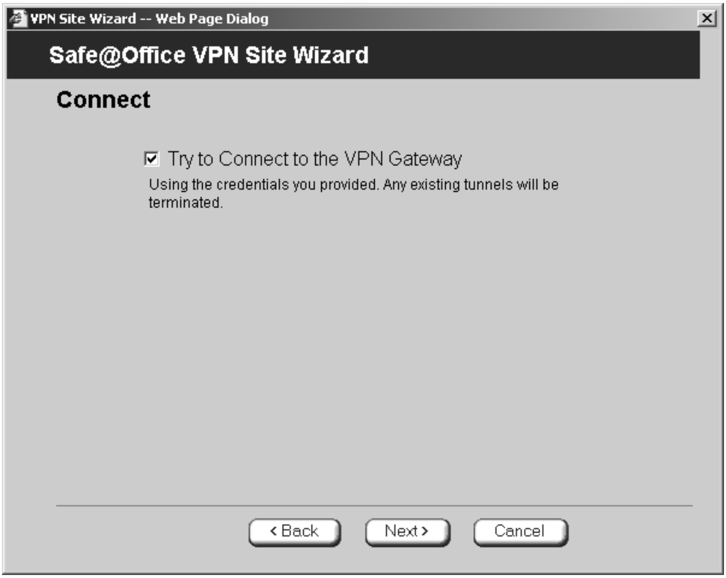
● Use Shared Secret

○ Use Certificate

6. Complete the fields using the table below.

7. Click **Next**.

   The **Connect** dialog box appears.



VPN Site Wizard -- Web Page 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.

8. If you don't want to try to connect to the VPN gateway, clear 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 will be terminated.

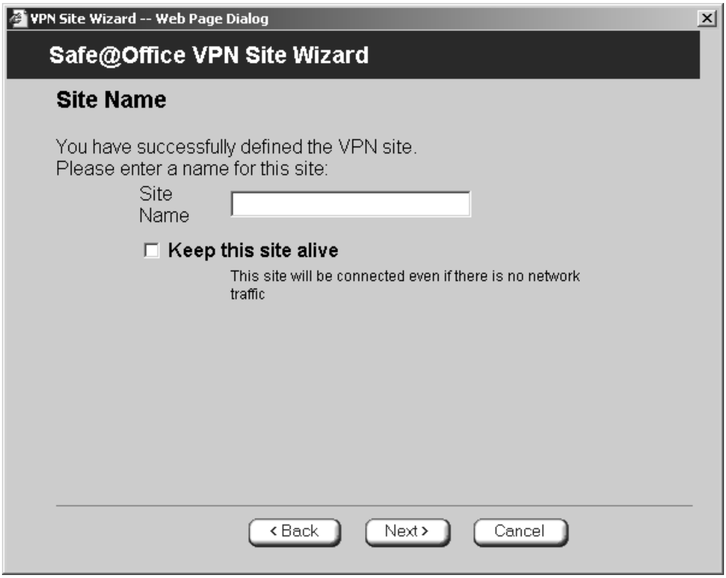
9. Click **Next**.

   - 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 -- Web Page 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

10. Enter a name for the VPN site.

    You may choose any name.

11. 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**.

12. Click **Next**.

    The **VPN Site Created** screen appears.

13. Click **Finish**.

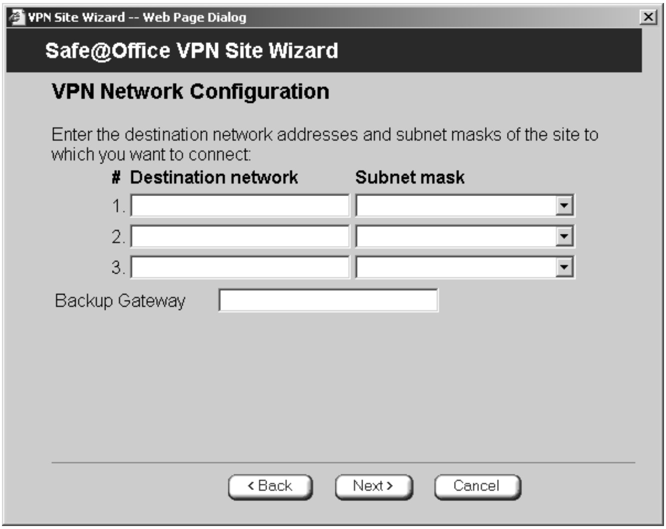
    The **VPN Sites** page reappears. If you added a VPN site, the new site appears in the **VPN Sites** list. If you edited a VPN site, the modifications are reflected in the **VPN Sites** list.

Table 22: 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	Select this option to use a shared secret for VPN authentication. If you select this option, you must fill in the **Shared Secret** field.
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.
Use 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 172 for more information about certificates and instructions on how to install a certificate.)

Creating a PPPoE Tunnel

If you selected PPPoE, the **VPN Network Configuration** dialog box appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

VPN Network Configuration

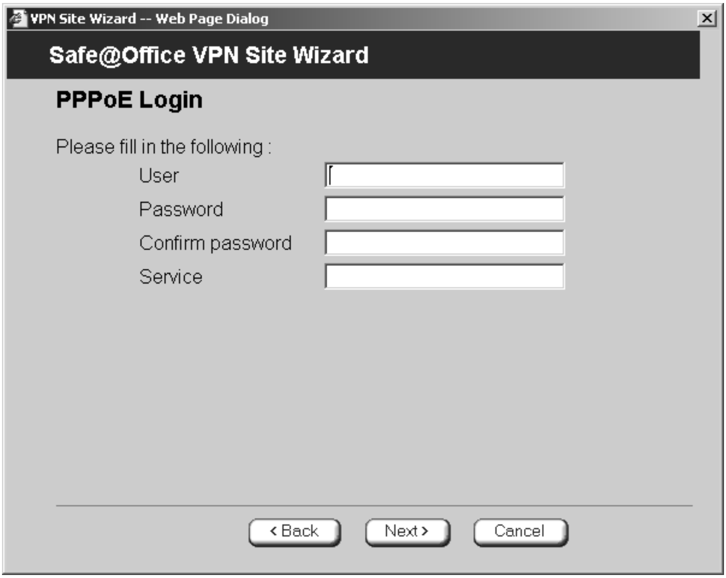
Enter the destination network addresses and subnet masks of the site to which you want to connect:

#	Destination network	Subnet mask
1.		
2.		
3.		

Backup Gateway

1. Complete the fields using the information in ***VPN Network Configuration Fields*** on page 155.
2. Click **Next**.

The **PPPoE Login** page appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

PPPoE Login

Please fill in the following :

User

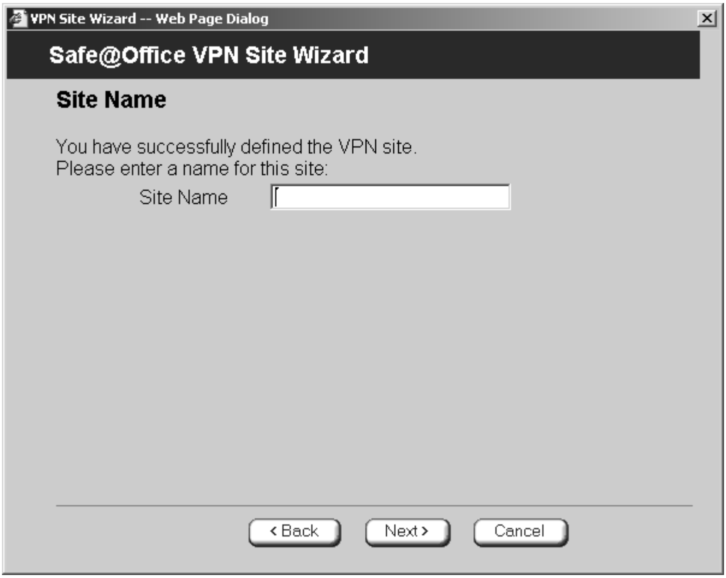
Password

Confirm password

Service

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

The **Site Name** dialog box appears.



VPN Site Wizard -- Web Page Dialog
Safe@Office VPN Site Wizard
Site Name

You have successfully defined the VPN site.
Please enter a name for this site:

Site Name

5. Enter a name for the VPN site.

   You may choose any name.

6. Click **Next**.

   The **VPN Site Created** screen appears.

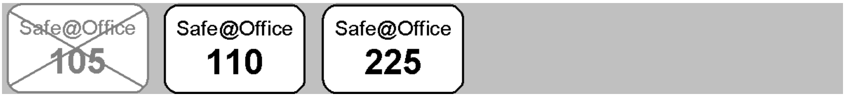
7. Click **Finish**.

   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 23: PPPoE Login Fields

In this field…	Do this…
User	The PPPoE username.
Password	The PPPoE password.
Service	The service name configured in the PPPoE server. You only need to fill in this field if there is more than one PPPoE server in the WAN network. **Note:** If you do not fill in this field, the first PPPoE server found is used.

Deleting a VPN Site



To 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 VPN sites.

2. In the desired VPN site's row, click the Delete 🗑 icon.

   A confirmation message appears.

3. Click **OK**.

   The VPN site is deleted.

Enabling/Disabling a VPN Site

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

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 on to a VPN Site

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

You need to manually log on to Remote Access VPN sites configured for Manual Login. You do not need to manually log on to a Remote Access VPN site 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 on and traffic is sent to the VPN site, a VPN tunnel is established. Only the computer from which you logged on can use the tunnel. To share the tunnel with other computers in your home network, you must log on 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 on through the Safe@Office Portal

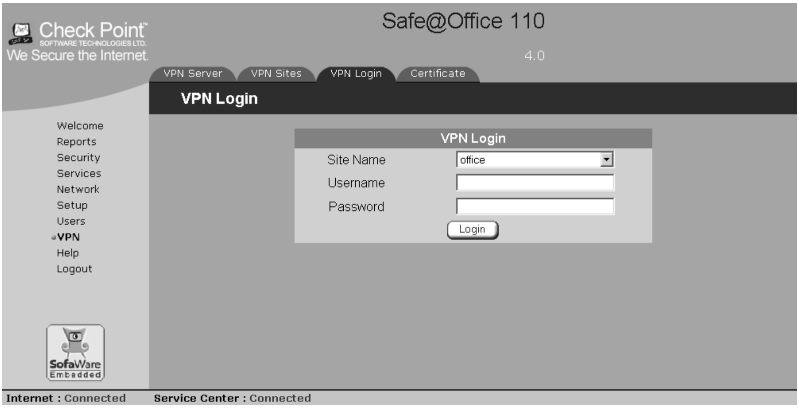
~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

Note: You can only login to sites that are configured for Manual Login.

To manually log on to a VPN site through the Safe@Office Portal

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

The **VPN Login** page appears.



VPN Login

Site Name	office
Username	
Password	

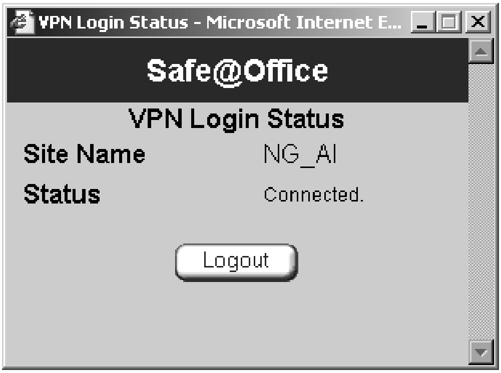
2. From the **Site Name** list, select the site to which you want to log on.

Note: Disabled VPN sites will not appear in the Site list.

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.

- Once the Safe@Office appliance has finished connecting, the **VPN Login Status** box appears. The **Status** field displays “Connected”.



VPN Login Status - Microsoft Internet E...

Safe@Office

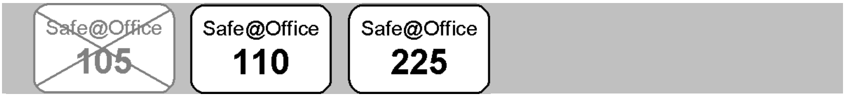
VPN Login Status

Site Name NG_AI

Status Connected.

- The **VPN Login Status** box remains open until you manually log off the VPN site.

Logging on through the my.vpn page

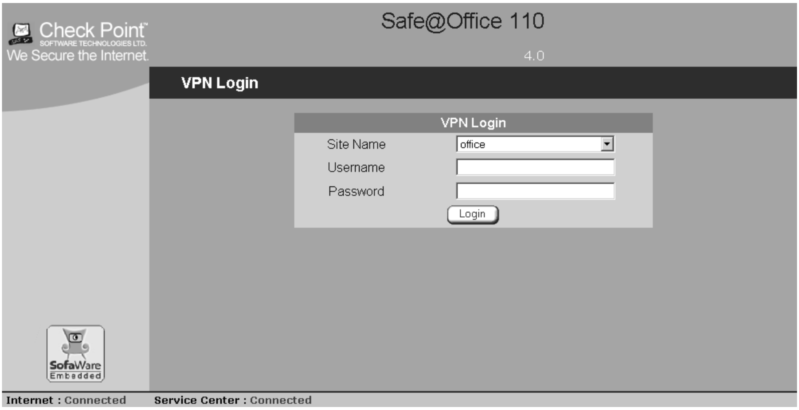


Note: You don’t need to know the my.firewall page administrator’s password in order to use the my.vpn page.

To manually log on to a VPN site through the my.vpn page

1. Direct your web browser to http://my.vpn

The **VPN Login** screen appears.



VPN Login

VPN Login

Site Name: office

Username:

Password:

Login

Internet : Connected   Service Center : Connected

2. In the **Site Name** list, select the site to which you want to log on.
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 off of the VPN site.

Logging off a VPN Site

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

You need to manually log off a VPN site if the VPN site is a Remote Access VPN site configured for Manual Login.

To log off 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.

Installing a Certificate

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

A digital certificate is a secure means of authenticating the Safe@Office appliance to other 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 Distinguishing 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 Safe@Office appliance supports certificates encoded in the PKCS#12 (Personal Information Exchange Syntax Standard) format. The PKCS#12 file must have a ".p12" file extension

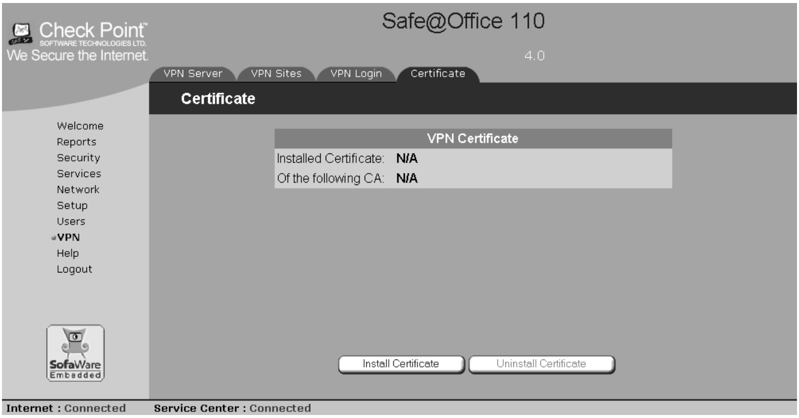
Note: To use certificates authentication, each Safe@Office appliance should have a unique certificate. Do not use the same certificate for more than one gateway.

If you do not have a PKCS#12, obtain it from your network security administrator.

To install a certificate

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

   The **Certificate** page appears, with instructions on how to install the certificate.



Certificate

VPN Certificate

Installed Certificate: N/A

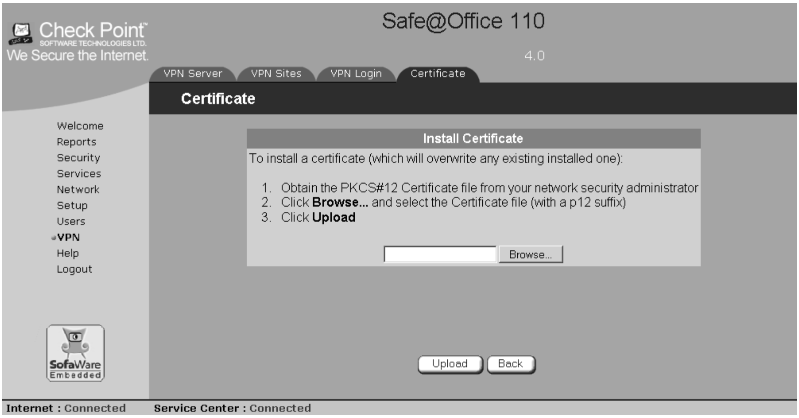
Of the following CA: N/A

Internet : Connected

Service Center : Connected

2. Click **Install Certificate**.

A **Certificate** page appears as follows:



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 **Upload**

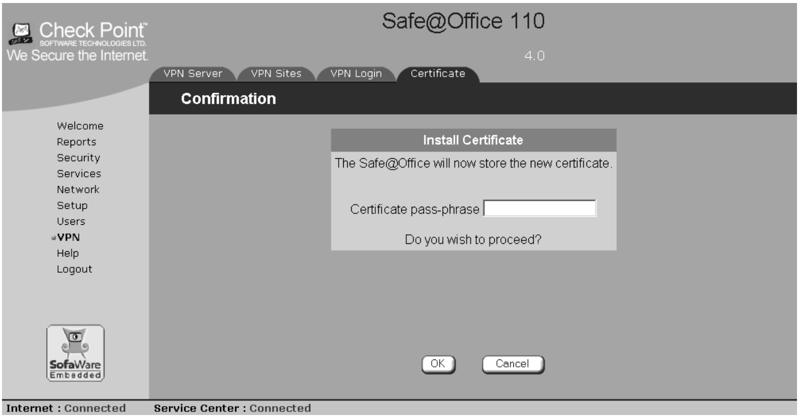
Internet : Connected **Service Center :** Connected

3. Click **Browse** to open a file browser from which to locate and select the file.

   The filename that you selected is displayed.

4. Click **Upload**.

   You are requested to enter the pass-phrase.



The Safe@Office will now store the new certificate.

Certificate pass-phrase

Do you wish to proceed?

Internet : Connected **Service Center :** Connected

5. Type the pass-phrase you received from the network security administrator.

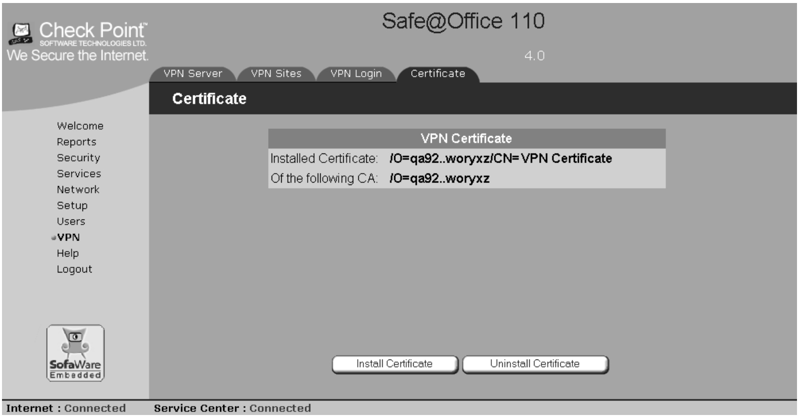
6. Click **OK**.

   The certificate is installed.

A success message appears.

7. Click **OK**.

   The name of the CA that issued the certificate and the name of the gateway to which this certificate was issued appear.



Certificate

VPN Certificate

Installed Certificate: /O=qa92..woryxz/CN=VPN Certificate

Of the following CA: /O=qa92..woryxz

Internet : Connected Service Center : Connected

Uninstalling a Certificate

~~Safe@Office 105~~ | Safe@Office 110 | Safe@Office 225

You cannot uninstall the certificate if there is a VPN site currently defined to use certificate authentication.

When a certificate is currently installed, the **Certificate** page presents two options:

- **Install Certificate**: Allows you to install a new certificate. The current certificate will be replaced.
- **Uninstall Certificate**: Allows you to uninstall the current certificate. Therefore, no certificate exists on the Safe@Office appliance, and you will not be able to connect to the VPN if a certificate is still required.

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**.

Viewing VPN Tunnels

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

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, Site-to-Site VPN gateways and PPPoE tunnels:** 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.

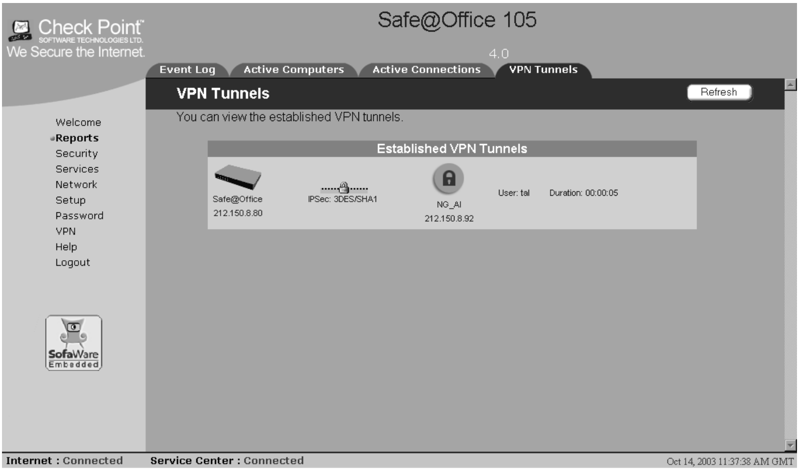
Note: Although the VPN tunnel is automatically closed, the site remains open, and if you attempt to communicate with the site, the tunnel will be reestablished.

- **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 on to the site*. All open tunnels connecting to the site are closed when you manually log off.

To view VPN tunnels

- Click **Reports** in the main menu, and click the **VPN Tunnels** tab.

  The **VPN Tunnels** page appears with a table of open tunnels to VPN sites.



VPN Tunnels

You can view the established VPN tunnels.

Established VPN Tunnels

Safe@Office 212.150.8.80	IPSec: 3DES/SHA1	NG_AI 212.150.8.92	User: tal	Duration: 00:00:05

The **VPN Tunnels** page includes the information described in ***VPN Tunnels Page Fields*** on page 178.

You can refresh the table by clicking **Refresh**.

Table 24: VPN Tunnels Page Fields

This field...	Displays...
	The Safe@Office appliance Internet IP address.
	The security protocol (IPSec), 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: Security protocol: Encryption type/Authentication type 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.
	The name and IP address of the VPN gateway to which the tunnel is connected.
User	The user logged on to the VPN site.

This field…	Displays…

Duration	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

Chapter 10

Managing Users

This chapter describes how to manage Safe@Office appliance users. In Safe@Office 105, there is a single user called "admin", whose password can be changed; in Safe@Office 110 and 225, you can define multiple users and assign them various permissions.

This chapter includes the following topics:

Changing Your Password

You can change your password at any time. How this task is performed depends on the Safe@Office model you are using.

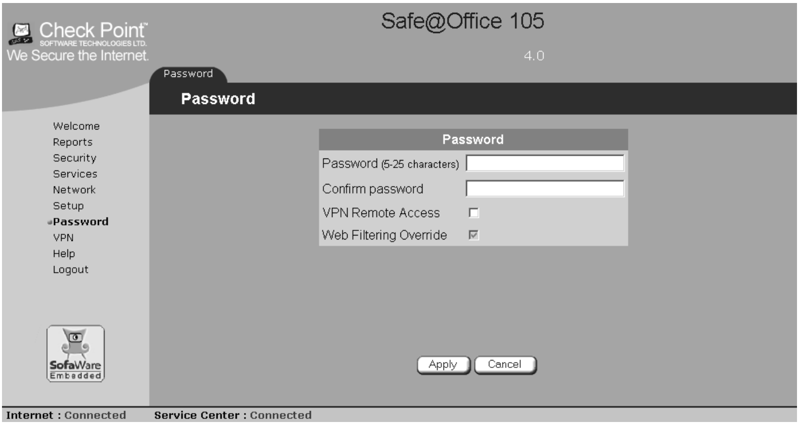
Using Safe@Office 105

Safe@Office 105 ~~Safe@Office 110~~ ~~Safe@Office 225~~

To change your password

1. Click **Password** in the main menu.

The **Password** page appears.



Password

Password (5-25 characters)	
Confirm password	
VPN Remote Access	☐
Web Filtering Override	☑

2. Edit the **Password** and **Confirm password** fields.

Note: Use 5 to 25 characters (letters or numbers) for the new password.

3. Click **Apply**.

   Your changes are saved.

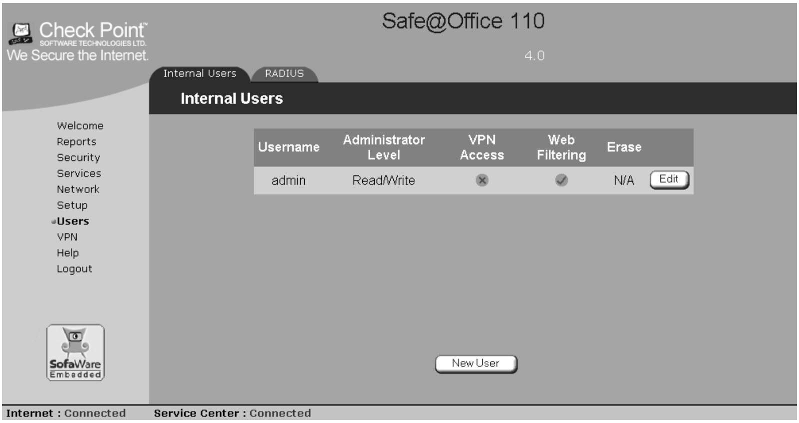
Using Safe@Office 110 and 225

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

To change your password

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

   The **Internal Users** page appears.



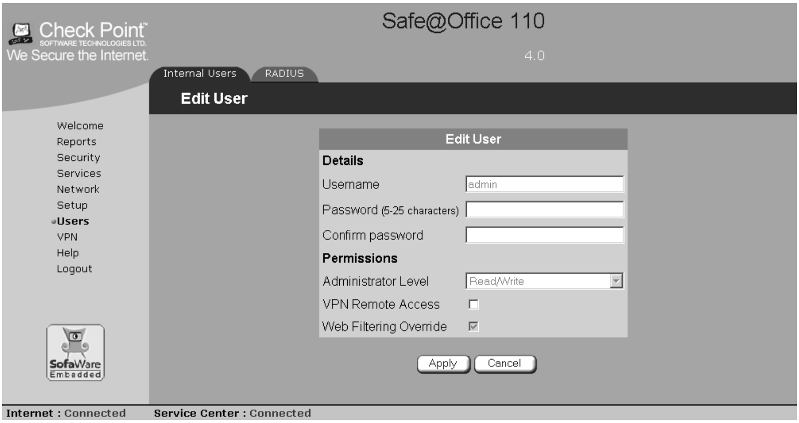
Internal Users

Username	Administrator Level	VPN Access	Web Filtering	Erase	
admin	Read/Write	☒	✓	N/A	Edit

Internet : Connected Service Center : Connected

2. In the row of your username, click **Edit**.

The **Edit User** page appears.



Edit User

Edit User

Details

Username: admin

Password (5-25 characters):

Confirm password:

Permissions

Administrator Level: Read/Write

VPN Remote Access ☐

Web Filtering Override ☑

Internet : Connected   Service Center : Connected

3. Edit the **Password** and **Confirm password** fields.

Note: Use 5 to 25 characters (letters or numbers) for the new password.

4. Click **Apply**.

   Your changes are saved.

Adding Users

~~Safe@Office 105~~ | Safe@Office 110 | Safe@Office 225

To add a user

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

   The **Internal Users** page appears.

2. Click **New User**.

   The **Edit User** page appears. The options that appear on the page are dependant on the software and services you are using.

3. Complete the fields using the information in ***Edit User Page Fields*** on page 186.
4. Click **Apply**.

   The new user is saved.

   The **Edit User** page appears.

Viewing and Editing Users

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

To view or edit users

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

   The **Internal Users** page appears.
2. In the desired user's row, click **Edit**.

   The **Edit User** page appears with the user's details. The options that appear on the page are dependant on the software and services you are using.
3. To edit the user's details, do the following:
   a. Edit the fields using ***Edit User Page Fields*** on page 186.
   b. Click **Apply**.

      The changes are saved.
4. To return to the **Users** page without making any changes, click **Cancel**.

Table 25: Edit User Page Fields

In this field…	Do this…
Username	Enter a username for the user. You cannot change the “admin” user’s username.
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.
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/Write**: The user can log on to the Safe@Office Portal and modify system settings. • **Read Only**: The user can log on to the Safe@Office Portal, but cannot modify system settings. For example, you could assign this administrator level to technical support personnel who need to view the Event Log. The default level is **No Access**. The “admin” user’s Administrator Level (Read/Write) cannot be changed.

In this field...	Do this...
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 ***Setting Up Remote VPN Access for Users*** on page 188. This option only appears in Safe@Office 110 and 225.
Web Filtering Override	Select this option to allow the user to override Web Filtering. This option only appears if the Web Filtering service is defined. This option cannot be changed for the "admin" user.

Deleting Users

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

Note: The "admin" user cannot be deleted.

To delete a user

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

   The **Internal Users** page appears.

2. In the desired user's row, click the Delete 🗑 icon.

   A confirmation message appears.

3. Click **OK**.

   The user is deleted.

Setting Up Remote VPN Access for Users

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

If you are using your Safe@Office appliance as a VPN server, you can allow users to access it remotely through their VPN clients (a Check Point SecureClient, Check Point SecuRemote, or another Embedded NG 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 145.

   List continue

2. Add the user to the system, using the procedure ***Adding Users*** on page 184. You must select the **VPN Remote Access** option.

Note: When using Safe@Office 105, there is only one pre-defined user called 'admin', and you cannot create additional users.

Using RADIUS Authentication

~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

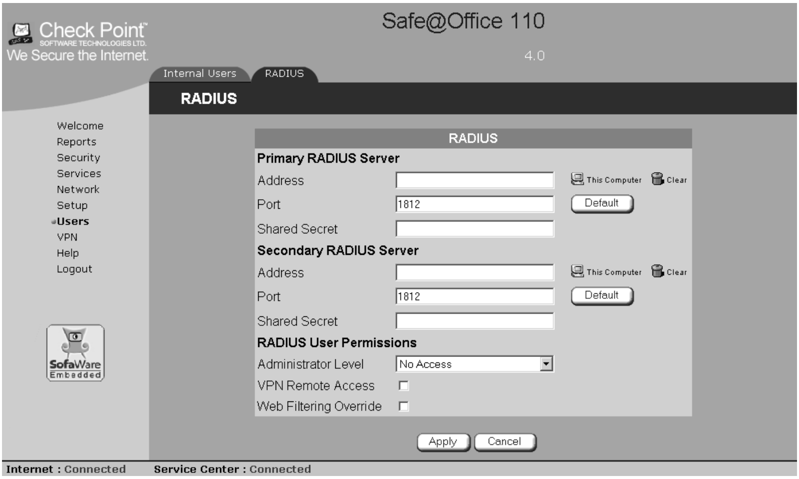
You can use RADIUS to authenticate both Safe@Office appliance users and VPN clients trying to connect to the Safe@Office appliance.

When a user accesses the Safe@Office Portal and tries to log on, 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 on.

To use RADIUS authentication

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

   The **RADIUS** page appears.



RADIUS

RADIUS

Primary RADIUS Server

Address

Port 1812

Shared Secret

Secondary RADIUS Server

Address

Port 1812

Shared Secret

RADIUS User Permissions

Administrator Level No Access

VPN Remote Access □

Web Filtering Override □

Internet : Connected   Service Center : Connected

2. Complete the fields using ***RADIUS Page Fields*** on page 190.
3. Click **Apply**.

Table 26: RADIUS Page Fields

In this field…	Do this…
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. To reset this field to the default (port 1812), click **Default**.
Shared Secret	Type the shared secret to use for secure communication with the RADIUS server.

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/Write**: The user can log on to the Safe@Office Portal and modify system settings. • **Read Only**: The user can log on to the Safe@Office Portal, but cannot modify system settings. The default level is **No Access**.
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.

Chapter 11

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

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

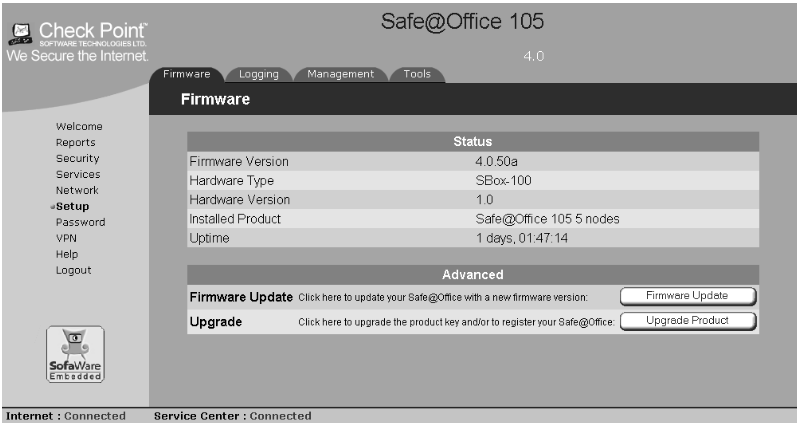
The firmware is the software program embedded in the Safe@Office appliance.

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.



Firmware

Status	
Firmware Version	4.0.50a
Hardware Type	SBox-100
Hardware Version	1.0
Installed Product	Safe@Office 105 5 nodes
Uptime	1 days, 01:47:14

Advanced

Firmware Update Click here to update your Safe@Office with a new firmware version:

Upgrade Click here to upgrade the product key and/or to register your Safe@Office:

Internet : Connected   Service Center : Connected

The **Firmware** page displays the following information:

Table 27: Firmware Status Fields

This field…	Displays…	For example…
Firmware Version	The current version of the firmware	4.0
Hardware Type	The type of the current Safe@Office appliance hardware	200 series
Hardware Version	The current hardware version of the Safe@Office appliance	1.0

This field...	Displays...	For example...
Installed Product	The licensed software and the number of allowed nodes	Safe@Office 225 unlimited nodes
Uptime	The time that elapsed from the moment the unit was turned on	01:21:15

Updating the Firmware

Safe@Office 105 Safe@Office 110 Safe@Office 225

If you are subscribed to Software Updates, firmware updates are performed automatically. These updates include new product features and protection against new security threats. Check with your reseller for the availability of Software Updates and other services. For information on subscribing to services, see ***Starting Your Subscription Services*** on page 123.

If you are not subscribed to the Software Updates service, you must update your firmware manually.

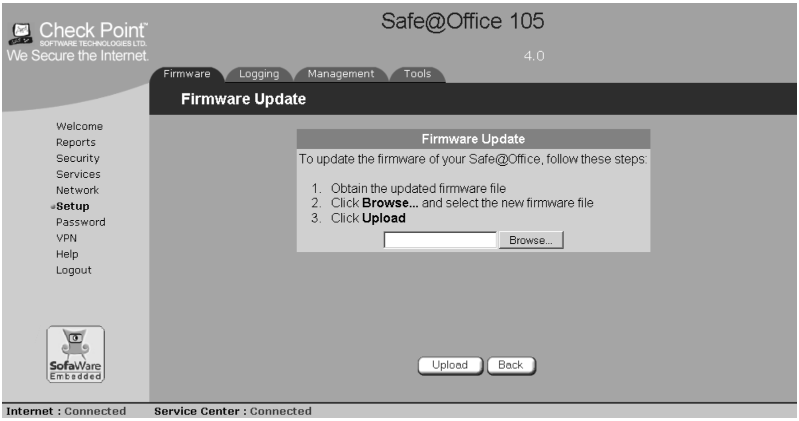
To update your Safe@Office appliance firmware manually

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

To update the firmware of your Safe@Office, follow these steps:

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

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. This takes about one minute. At the end of the process the Safe@Office appliance restarts automatically.

Upgrading Your Software Product

Safe@Office 105

Safe@Office 110

Safe@Office 225

Upgrading your Safe@Office appliance is a very simple process. After purchasing an upgrade, you will receive a new Product Key that will enable you to use the upgraded product on the same Safe@Office appliance you have today. For example, if you are using Safe@Office 105, you can purchase an upgrade to Safe@Office 110 and enjoy extended VPN features on your existing Safe@Office appliance. Likewise, you can upgrade from Safe@Office 225 to 225U without changing your hardware.

Note: You can only upgrade within the same appliance hardware type.

Note: To purchase an upgrade, contact your Safe@Office appliance provider.

To upgrade your product, you must install the new Product Key.

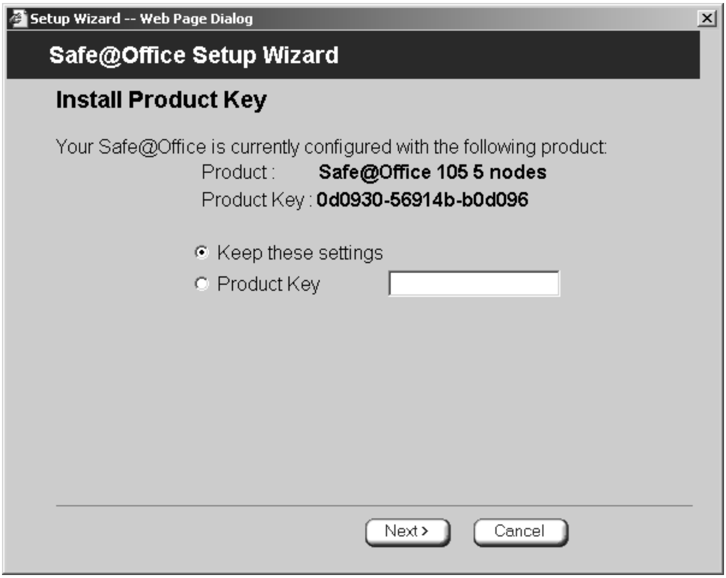
To install a Product Key

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

   The **Firmware** page appears.

2. Click **Upgrade Product**.

The Setup Wizard opens, with the **Install Product Key** dialog box displayed.



Setup Wizard -- Web Page Dialog

Safe@Office Setup Wizard

Install Product Key

Your Safe@Office is currently configured with the following product:

Product : **Safe@Office 105 5 nodes**

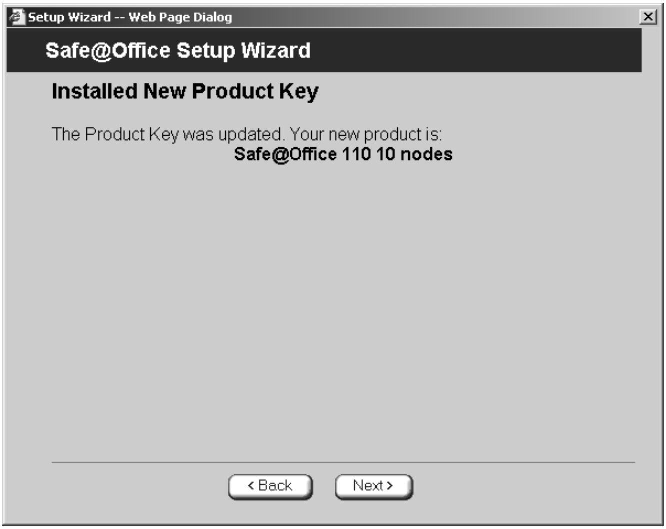
Product Key : **0d0930-56914b-b0d096**

● Keep these settings

○ Product Key

3. Click **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 -- Web Page Dialog

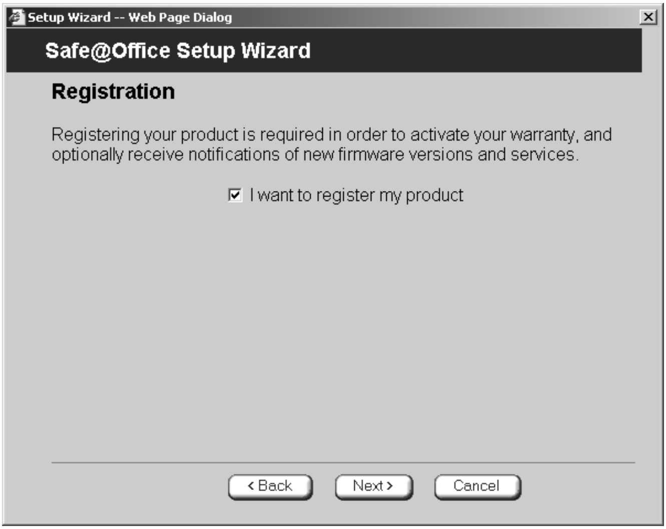
Safe@Office Setup Wizard

Installed New Product Key

The Product Key was updated. Your new product is:
Safe@Office 110 10 nodes

6. Click **Next**.

   The first **Registration** dialog box appears.



Setup Wizard -- Web Page Dialog

Safe@Office Setup Wizard

Registration

Registering your product is required in order to activate your warranty, and optionally receive notifications of new firmware versions and services.

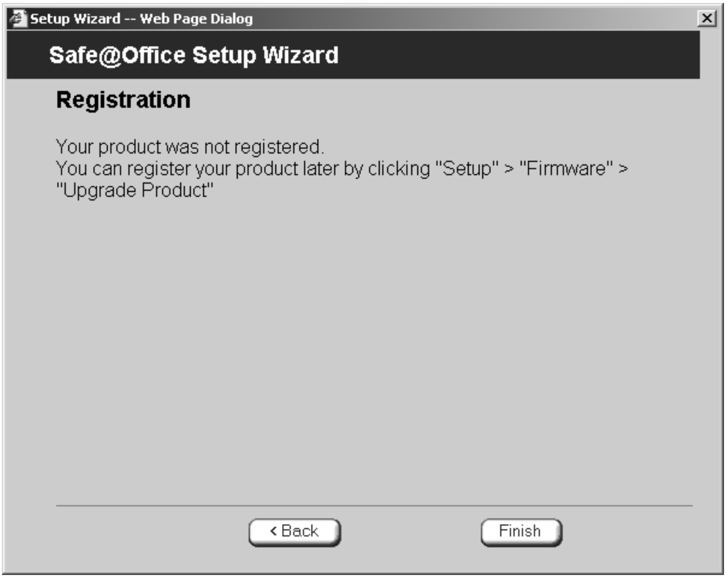
☑ I want to register my product

7. Do one of the following:

   - To register your Safe@Office appliance later on, do the following:

     1) Clear the **I want to register my product** check box.

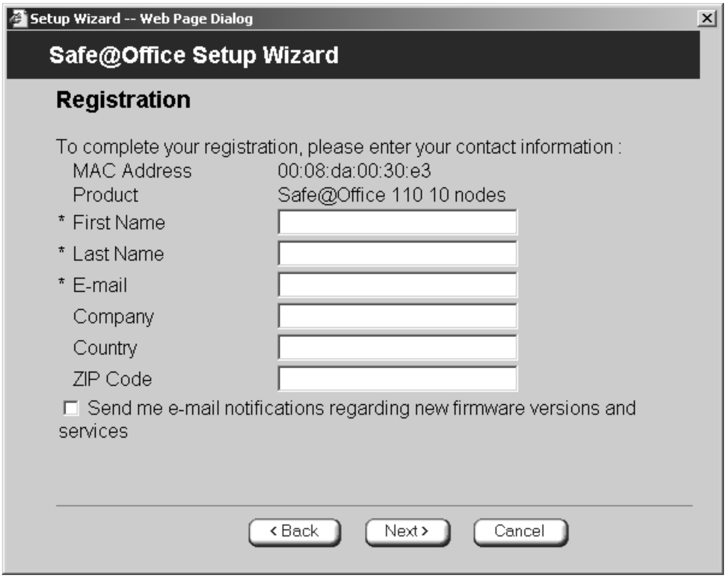
     2) Click **Next**.



Your product was not registered.
You can register your product later by clicking "Setup" > "Firmware" > "Upgrade Product"

- To register your Safe@Office appliance now, click **Next**.

  A second **Registration** dialog box appears.



Registration

To complete your registration, please enter your contact information :

MAC Address	00:08:da:00:30:e3
Product	Safe@Office 110 10 nodes
* First Name	
* Last Name	
* E-mail	
Company	
Country	
ZIP Code	

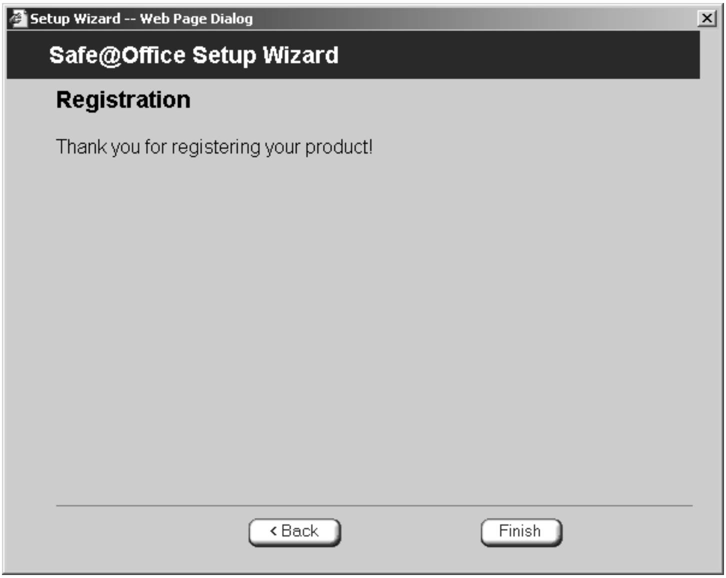
□ Send me e-mail notifications regarding new firmware versions and services

Do the following:

1) Enter your contact information in the appropriate fields.
2) To receive email notifications regarding new firmware versions and services, select the check box.
3) Click **Next**.

   The **Registration...** screen appears.

The third **Registration** dialog box appears.



Setup Wizard -- Web Page Dialog

Safe@Office Setup Wizard

Registration

Thank you for registering your product!

8. Click **Finish**.

   Your Safe@Office appliance is restarted and the **Welcome** page appears.

Registering Your Safe@Office Appliance

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

If you want to activate your warranty and optionally receive notifications of new firmware versions and services, you must register your Safe@Office appliance.

Privacy Statement: Check Point is committed to protecting your privacy. We use the information we collect about you to process orders and to improve our ability to serve your needs. We will under no circumstances sell, lease, or otherwise disclose any of your personal or contact details without your explicit permission.

To register your Safe@Office appliance

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

   The **Firmware** page appears.

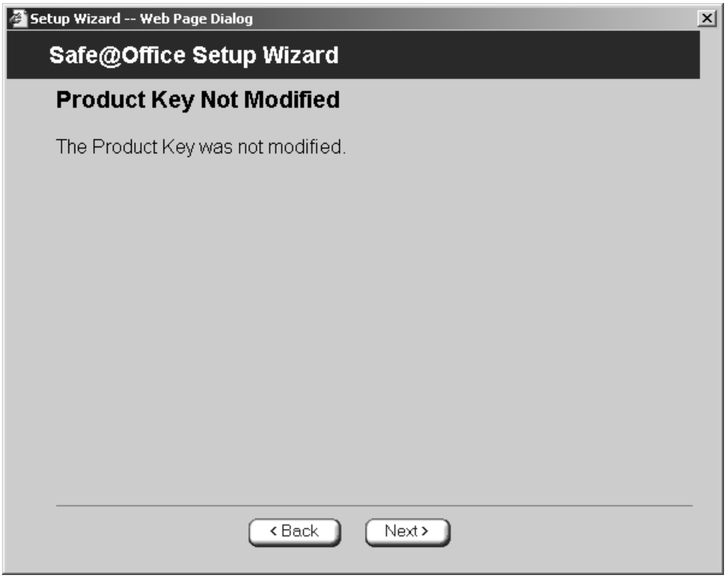
2. Click **Upgrade Product**.

   The Setup Wizard opens, with the **Install Product Key** dialog box displayed.

3. Select **Keep these settings**.

4. Click **Next**.

   The **Product Key Not Modified** screen appears.



Product Key Not Modified

The Product Key was not modified.

5. Click **Next**.

   The first **Registration** dialog box appears.

6. Verify that the **I want to register my product** check box is selected.

7. Click **Next**.

   A second **Registration** dialog box appears.

8. Enter your contact information in the appropriate fields.
9. To receive email notifications regarding new firmware versions and services, select the check box.
10. Click **Next**.

    The **Registration...** screen appears.

    The third **Registration** dialog box appears.
11. Click **Finish**.

    Your Safe@Office appliance is restarted and the **Welcome** page appears.

Configuring Syslog Logging

Safe@Office **105** Safe@Office **110** Safe@Office **225**

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).

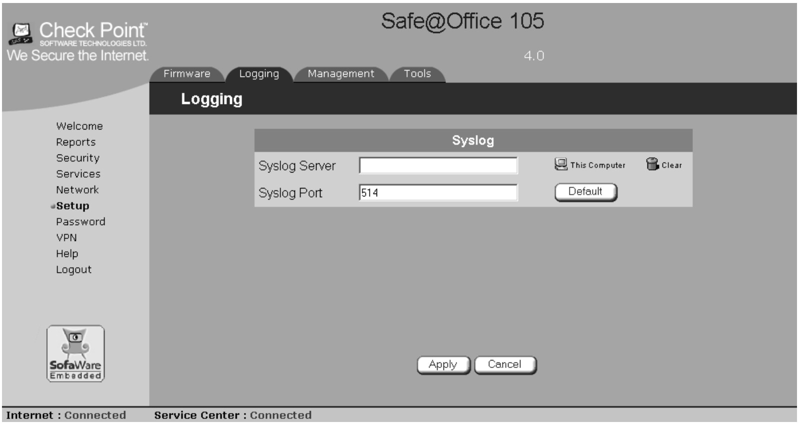
This same information is also available in the Event Log page (see ***Viewing the Event Log*** on page 101). However, the Event Log can only display up to 100 logs, while a Syslog server can store an unlimited number of logs. Furthermore, Syslog servers can provide useful tools for managing your logs.

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.



Syslog Server:
Syslog Port: 514

2. Complete the fields using the information in the table below.
3. Click **Apply**.

Table 28: 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.

In this field...	Do this...
Default	Click to reset the **Syslog Port** field to the default (port 514 UDP).

Configuring HTTPS

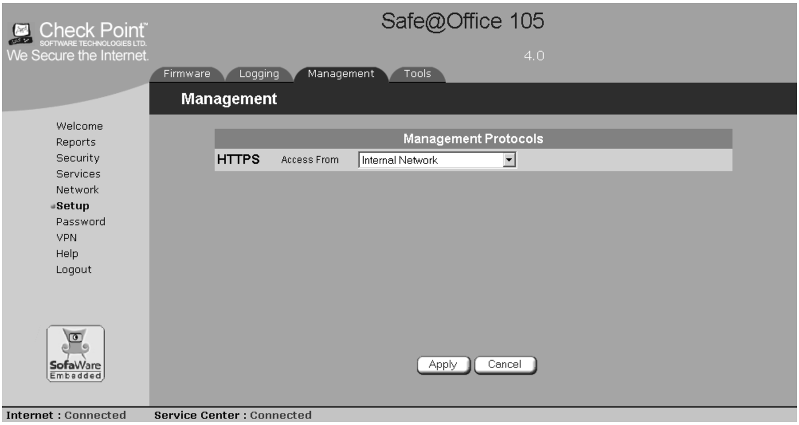
Safe@Office **105** Safe@Office **110** Safe@Office **225**

You can enable Safe@Office appliance users to access the Safe@Office Portal from the Internet. To do so, you must first configure HTTPS.

To configure HTTPS

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

   The **Management** page appears.



Management Protocols

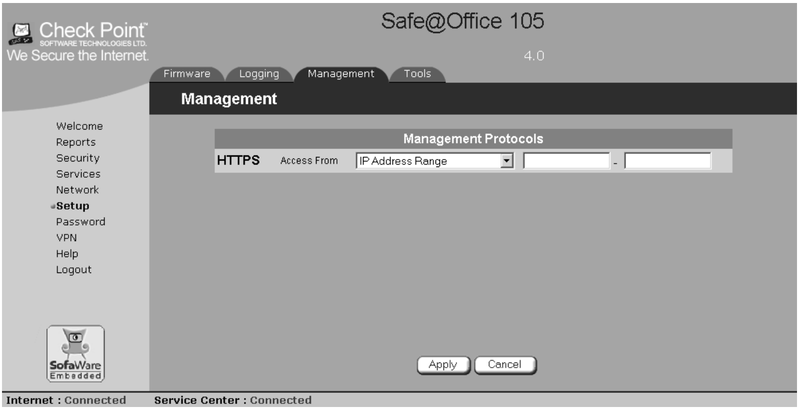
HTTPS Access From: Internal Network

Internet : Connected Service Center : Connected

2. Specify from where HTTPS access to the Safe@Office Portal should be granted. See the table below for information.

Warning: If remote HTTPS is enabled, your Safe@Office appliance settings can be changed remotely, so make sure all Safe@Office appliance users' passwords are unguessable.

If you selected **IP Address Range**, additional fields appear.



HTTPS Access From: IP Address Range

Internet : Connected   Service Center : Connected

3. If you selected **IP Address Range**, enter the desired IP address range in the fields provided.

4. Click **Apply**.

The HTTPS configuration is saved. You can now access the Safe@Office Portal through the Internet, using the procedure ***Accessing the Safe@Office Portal Remotely*** on page 40.

Table 29: HTTPS Access Options

Select this option…	To allow HTTPS access from…
Internal Network	The internal network only. This disables remote HTTPS capability. Note: You can use HTTPS to access the Safe@Office Portal from your internal network, by surfing to https://my.firewall.
Internal Network and VPN	The internal network and your VPN.
IP Address Range	A particular range of IP addresses. Additional fields appear, in which you can enter the desired IP address range.
ANY	Any IP address.

Setting the Time on the Appliance

~~Safe@Office 105~~ ~~Safe@Office 110~~ Safe@Office 225

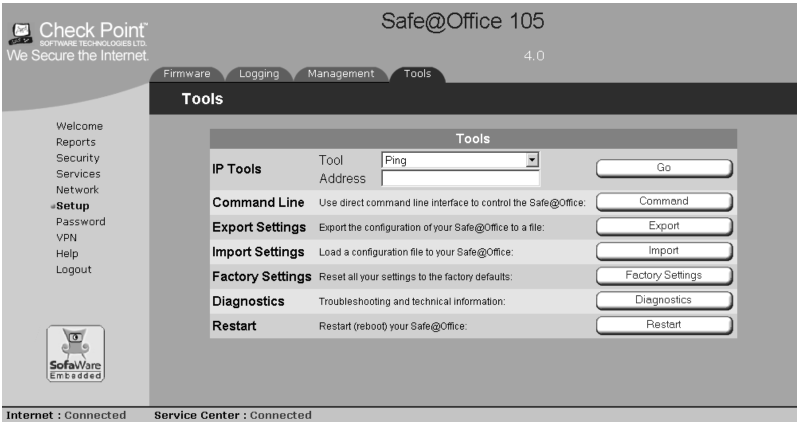
You set the time displayed in the Safe@Office 225 Portal during initial appliance setup. If desired, you can change the date and time displayed in the Safe@Office 225 Portal using the procedure below.

Note: The Safe@Office 100 series takes the time from your local computer and you do not have to manually set the time.

To set the time

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

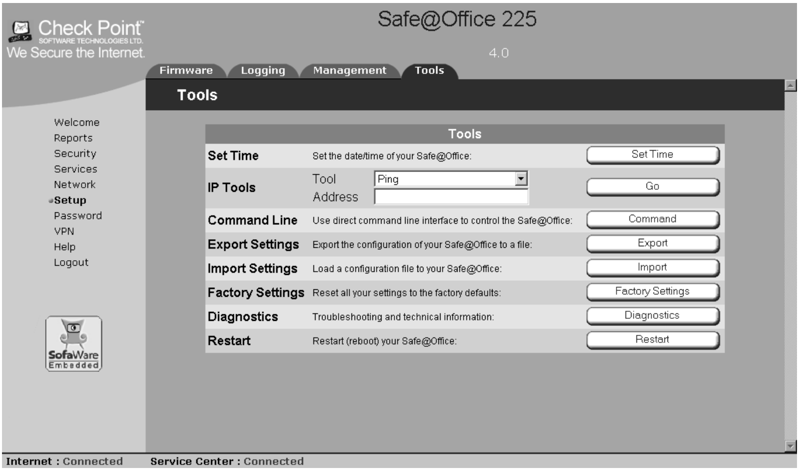
   The **Tools** page appears.



Tools		
IP Tools	Tool: Ping Address:	Go
Command Line	Use direct command line interface to control the Safe@Office:	Command
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
Restart	Restart (reboot) your Safe@Office:	Restart

Internet : Connected   Service Center : Connected

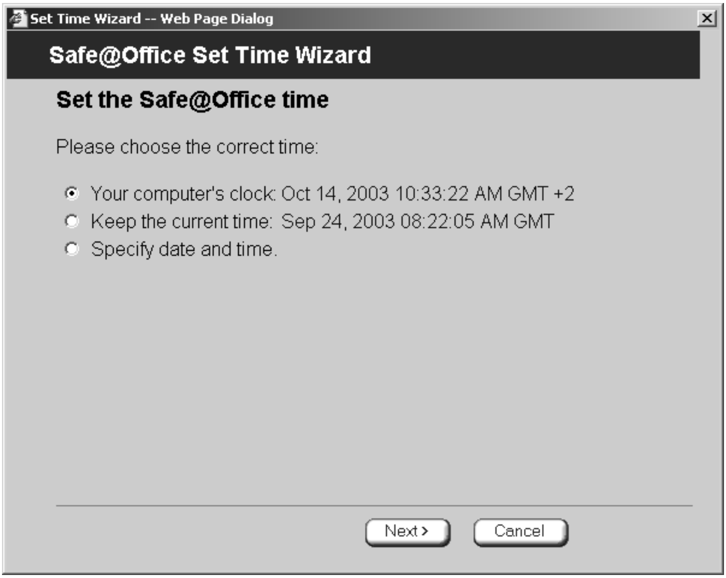
If you are using Safe@Office 225, the page appears as follows:



Tools		
Set Time	Set the date/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
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
Restart	Restart (reboot) your Safe@Office:	Restart

2. Click **Set Time**.

The Safe@Office Set Time Wizard opens displaying the **Set the Safe@Office time** dialog box.


Set Time Wizard -- Web Page Dialog
Safe@Office Set Time Wizard
Next >
Cancel

Set the Safe@Office time

Please choose the correct time:

● Your computer's clock: Oct 14, 2003 10:33:22 AM GMT +2

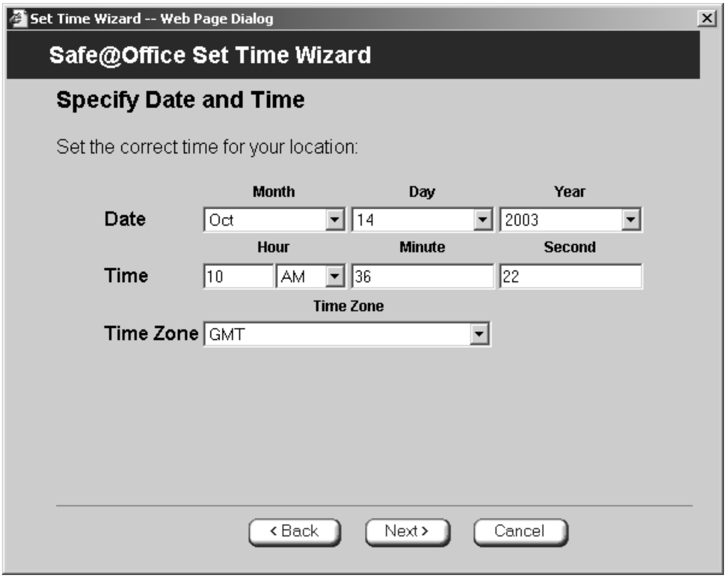
○ Keep the current time: Sep 24, 2003 08:22:05 AM GMT

○ Specify date and time.

3. Complete the fields using the information in the table below.
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 -- Web Page Dialog

Safe@Office Set Time Wizard

Specify Date and Time

Set the correct time for your location:

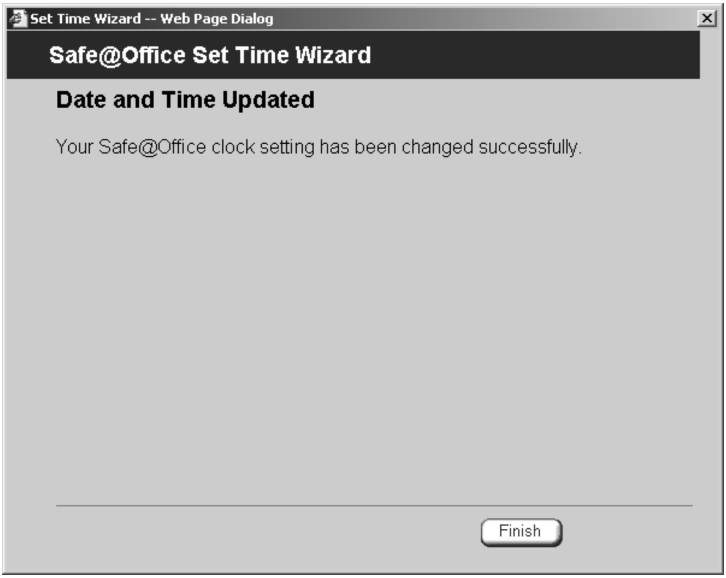
	Month	Day	Year
Date	Oct	14	2003
	Hour	Minute	Second
Time	10 AM	36	22
	Time Zone		
Time Zone	GMT		

Do the following:

1) Set the date, time, and time zone in the fields provided.

2) Click **Next**.

- The **Date and Time Updated** window appears.



Set Time Wizard -- Web Page Dialog

Safe@Office Set Time Wizard

Date and Time Updated

Your Safe@Office clock setting has been changed successfully.

5. Click **Finish**.

Table 30: Set Time Wizard Fields

Select this option…	To do this…
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.

Select this option...	To do this...
Keep the current time	Do not change the appliance's time. The current appliance time is displayed to the right of this option.
Specify date and time	Set the appliance to a specific date and time.

Controlling the Appliance via the Command Line

Safe@Office 105 | Safe@Office 110 | Safe@Office 225

The Safe@Office Portal enables you to control your appliance via the command line interface.

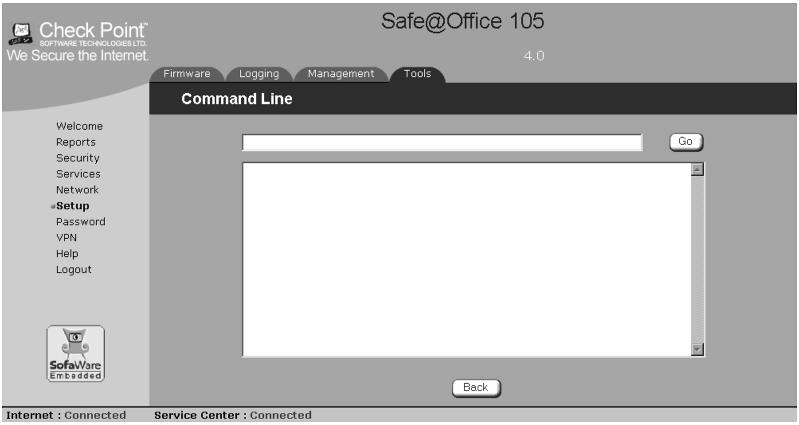
To control the appliance via the command line

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

   The **Tools** page appears.

2. Click **Command**.

The **Command Line** page appears.



3. In the upper text box type a command.

   You can view a list of supported commands using the command **help**.

4. Click **Go**.

   The command is implemented.

Using Diagnostic Tools

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

The Safe@Office appliance is equipped with a set of diagnostic tools that are useful for troubleshooting Internet connectivity.

Table 31: Diagnostic Tools

Use this tool...	To do this...
Ping	Check that a specific IP address or DNS name can be reached via the Internet.

Use this tool...	To do this...
Traceroute	Display a list of all routers used to connect from the Safe@Office appliance to a specific IP address or DNS name.
WHOIS	Display the name and contact information of the entity to whom a specific IP address or DNS name is registered. This information is useful in tracking down hackers.

To use a diagnostic tool

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

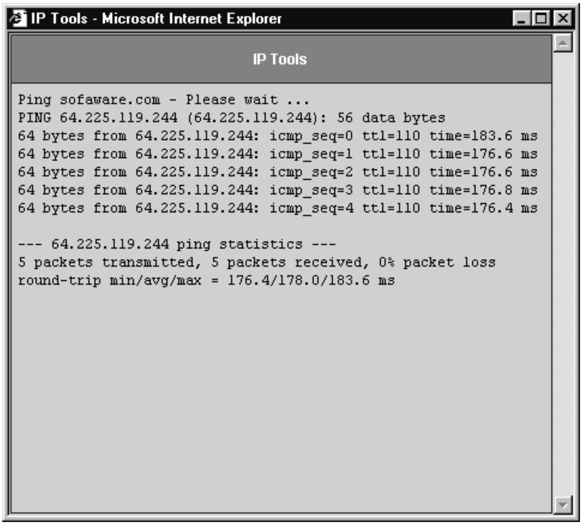
   The **Tools** page appears.

2. In the **Tools** 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 each packet took to reach the specified host and return (round-trip) in milliseconds.



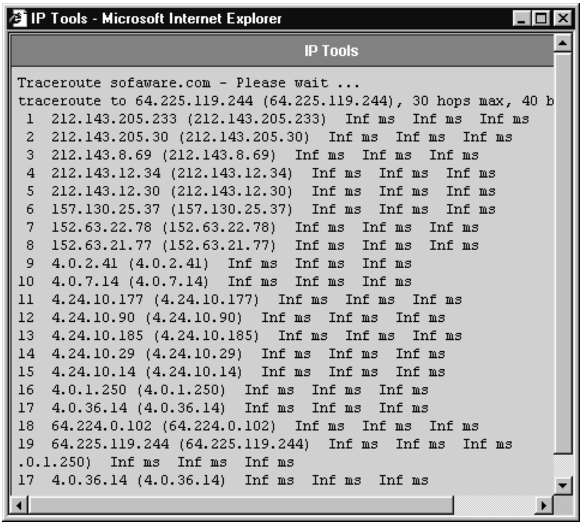
```
Ping sofaware.com - Please wait ...
PING 64.225.119.244 (64.225.119.244): 56 data bytes
64 bytes from 64.225.119.244: icmp_seq=0 ttl=110 time=183.6 ms
64 bytes from 64.225.119.244: icmp_seq=1 ttl=110 time=176.6 ms
64 bytes from 64.225.119.244: icmp_seq=2 ttl=110 time=176.6 ms
64 bytes from 64.225.119.244: icmp_seq=3 ttl=110 time=176.8 ms
64 bytes from 64.225.119.244: icmp_seq=4 ttl=110 time=176.4 ms

--- 64.225.119.244 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 176.4/178.0/183.6 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.

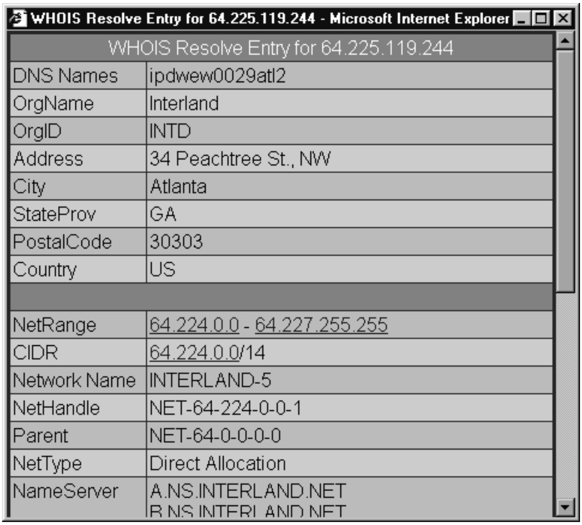


```
Traceroute sofaware.com - Please wait ...
traceroute to 64.225.119.244 (64.225.119.244), 30 hops max, 40 b
 1  212.143.205.233 (212.143.205.233)  Inf ms  Inf ms  Inf ms
 2  212.143.205.30 (212.143.205.30)  Inf ms  Inf ms  Inf ms
 3  212.143.8.69 (212.143.8.69)  Inf ms  Inf ms  Inf ms
 4  212.143.12.34 (212.143.12.34)  Inf ms  Inf ms  Inf ms
 5  212.143.12.30 (212.143.12.30)  Inf ms  Inf ms  Inf ms
 6  157.130.25.37 (157.130.25.37)  Inf ms  Inf ms  Inf ms
 7  152.63.22.78 (152.63.22.78)  Inf ms  Inf ms  Inf ms
 8  152.63.21.77 (152.63.21.77)  Inf ms  Inf ms  Inf ms
 9  4.0.2.41 (4.0.2.41)  Inf ms  Inf ms  Inf ms
10  4.0.7.14 (4.0.7.14)  Inf ms  Inf ms  Inf ms
11  4.24.10.177 (4.24.10.177)  Inf ms  Inf ms  Inf ms
12  4.24.10.90 (4.24.10.90)  Inf ms  Inf ms  Inf ms
13  4.24.10.185 (4.24.10.185)  Inf ms  Inf ms  Inf ms
14  4.24.10.29 (4.24.10.29)  Inf ms  Inf ms  Inf ms
15  4.24.10.14 (4.24.10.14)  Inf ms  Inf ms  Inf ms
16  4.0.1.250 (4.0.1.250)  Inf ms  Inf ms  Inf ms
17  4.0.36.14 (4.0.36.14)  Inf ms  Inf ms  Inf ms
18  64.224.0.102 (64.224.0.102)  Inf ms  Inf ms  Inf ms
19  64.225.119.244 (64.225.119.244)  Inf ms  Inf ms  Inf ms
.0.1.250)  Inf ms  Inf ms  Inf ms
17  4.0.36.14 (4.0.36.14)  Inf ms  Inf ms  Inf ms
```

- 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 whom the IP address or DNS name is registered and their contact information.


WHOIS Resolve Entry for 64.225.119.244 - Microsoft Internet Explorer

WHOIS Resolve Entry for 64.225.119.244	
DNS Names	ipdwew0029atl2
OrgName	Interland
OrgID	INTD
Address	34 Peachtree St., NW
City	Atlanta
StateProv	GA
PostalCode	30303
Country	US
NetRange	64.224.0.0 - 64.227.255.255
CIDR	64.224.0.0/14
Network Name	INTERLAND-5
NetHandle	NET-64-224-0-0-1
Parent	NET-64-0-0-0-0
NetType	Direct Allocation
NameServer	A.NS.INTERLAND.NET B.NS.INTERLAND.NET

Backing Up the Safe@Office Appliance Configuration

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

You can export the Safe@Office appliance configuration to a *.cfg file, and use this file to backup and restore Safe@Office appliance settings, as needed. The configuration file includes all your settings.

Exporting the Safe@Office Appliance Configuration

Safe@Office **105** Safe@Office **110** Safe@Office **225**

Exporting the Safe@Office appliance configuration creates a configuration file.

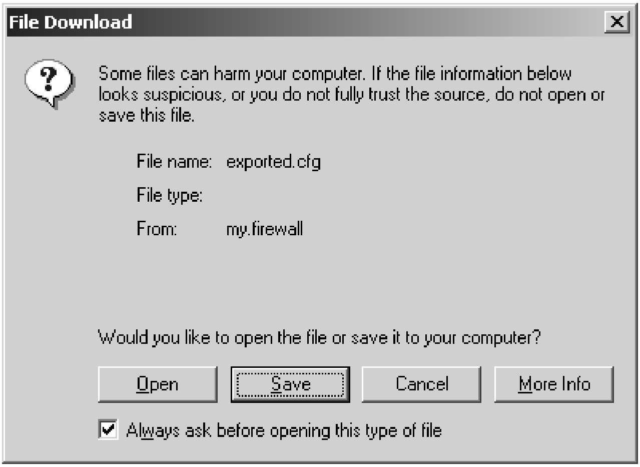
To export the Safe@Office appliance configuration

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.



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

File name: exported.cfg

File type:

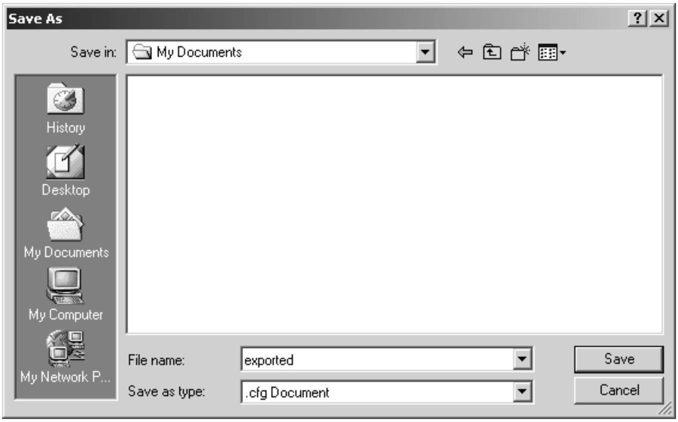
From: my.firewall

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

☑ Always ask before opening this type of file

3. Click **Save**.

The **Save As** dialog box appears.



Save As

Save in: My Documents

File name: exported

Save as type: .cfg Document

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.

Importing the Safe@Office Appliance Configuration

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

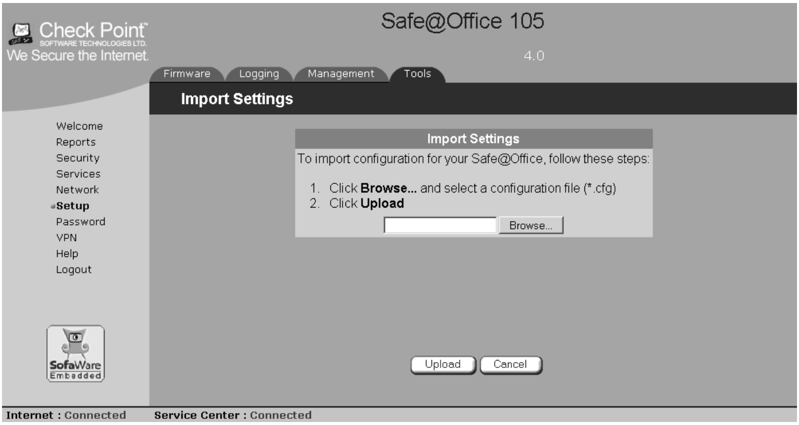
In order to restore your Safe@Office appliance's configuration from a configuration file, you must import the file.

To import the Safe@Office appliance configuration

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.

   A success message appears.

6. Click **OK**.

   The **Tools** page reappears.

Resetting the Safe@Office Appliance to Defaults

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

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, and your firmware reverts to the version that shipped with the Safe@Office appliance.

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.

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.

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.

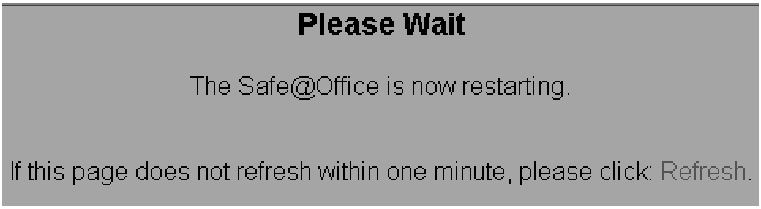
   The **Tools** page appears.

2. Click **Factory Settings**.

   A confirmation message appears.

3. Click **OK**.

- The **Please Wait** screen appears.



Please Wait

The Safe@Office is now restarting.

If this page does not refresh within one minute, please click: Refresh.

- The Safe@Office appliance returns to its factory defaults.
- The Safe@Office appliance is restarted (the PWR/SEC LED flashes quickly).

  This may take up to a minute.
- 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 (PWR/SEC LED flashes slowly or illuminates steadily in green light).

   For information on the appliance's front and rear panels, see ***Getting to Know Your Safe@Office 100 Series*** on page 10 or ***Getting to Know Your Safe@Office 200 Series*** on page 13.

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, or the Safe@Office appliance might not function properly until you reboot it as described below.

Running Diagnostics

Safe@Office **105** Safe@Office **110** Safe@Office **225**

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 copy and paste it into the body an email and send it to technical support.

To run diagnostics

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 refresh the contents of the window, click **Refresh**.

   The contents are refreshed.

4. To close the window, click **Close**.

Rebooting the Safe@Office Appliance

Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

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 **Tools** tab.

   The **Tools** page appears.

2. Click **Restart**.

   A confirmation message appears.

3. Click **OK**.

   - The **Please Wait** screen appears.
   - The Safe@Office appliance is restarted (the PWR/SEC LED flashes quickly).

     This may take up to a minute.
   - The **Login** page appears.

Chapter 12

Troubleshooting

This chapter provides solutions to common problems you may encounter while using the Safe@Office appliance.

This chapter includes the following topics:

Connectivity

I cannot access the Internet. What should I do?

- Check if the PWR/SEC LED is green. If not, check the power connection to the Safe@Office appliance.
- Check if the WAN LINK/ACT LED is green. If not, check the network cable to the modem and make sure the modem is turned on.
- Check if the LAN LINK/ACT LED for the 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 19.

- If Web Filtering or Email Anti Virus scanning 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 following the procedure ***Viewing Computers*** on page 104.

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 49.

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 49.
- 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 49.

I cannot access http://my.firewall or http://my.vpn. What should I do?

- Verify that the Safe@Office appliance is operating (PWR/SEC LED is active)
- Check if the LAN LINK/ACT LED for the port used by your computer is on. If not, check if the network cable linking your computer to the Safe@Office appliance is connected properly.

Note: You may need to use a crossed cable when connecting the Safe@Office appliance to another hub/switch.

- 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 19.
- 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 222.

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, such as Wireless access.
- 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
  - 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.

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.

I cannot connect to the LAN network from the DMZ network. What should I do?

By default, connections from the DMZ network to the LAN network are blocked. To allow traffic from the DMZ to the LAN, configure appropriate firewall rules. For instructions, see ***Creating Rules*** on page 112.

Service Center and Upgrades

I purchased Safe@Office 110, but I only have Safe@Office 105 functionality. What should I do?

Your have not installed your product key. For further information, see ***Upgrading Your Software Product*** on page 197.

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 Active 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.

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 222.

Why are the date and time displayed incorrectly?

In the Safe@Office 100 series, when a computer on the LAN connects to the Safe@Office Portal, the Safe@Office appliance adjusts its date and time to match that of the computer. If the date and time displayed in the Safe@Office Portal are incorrect, it probably means that the date and time on the computer connected to the Safe@Office Portal are incorrect.

In the Safe@Office 200 series, you can adjust the time on the **Setup** page's **Tools** tab. For information, see ***Setting the Time on the Appliance*** on page 209.

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:

- Turn the Safe@Office appliance security 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*** on page 121.

When you have finished using the application, make sure to clear the exposed host setting, otherwise your security might be compromised.

Chapter 13

Specifications

This chapter includes the following topics:

Technical Specifications

Table 32: Safe@Office Appliance Attributes

Attribute	Details
General	
Dimensions (width x height x depth)	20.32 x 3.05 x 12.19 cm (8.0 x 1.2 x 4.8 inches)
Weight	0.7 kg (1.56 lbs)
Supply voltage	110VAC (90 to 132 VAC)
	100VAC
	230VAC (200 to 265 VAC)
Line voltage frequency, AC	50/60 Hz (47 to 63 Hz)
Max. Power Consumption	13.5W (100 series) / 7.5W (200 series)

Attribute	Details
Retail box dimensions (width x height x depth)	31 x 10 x 16 cm (12.4 x 4 x 6.4 inches)
Retail box weight	1.3 kg (2.9 lbs)
Environmental Conditions	
Temperature: Storage/Transport	- 20°C to +70°C
Temperature: Operation	+ 5°C to +45°C
Humidity: Storage/Operation	5% to 90% at 25°C (no condensation)
Applicable Standards	
Shock & Vibration	ETSI 300 019-2-3 CLASS 3.1 & Bellcore GR 63 (NEBS)
Safety	EN60950/IEC 60950
Quality	ISO9001

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:

EN 50081-1:1992, EN 50082-1:1997, EN 61000-6-1:2001, EN 61000-6-3:2001, EN 55022:1998, EN 55024:1998, EN 61000-3-2: 1995, EN 61000-3-3: 1995, EN 61000-4-2:1995, EN 61000-4-3:1996/A2:2001, EN 61000-4-4:1995, EN 61000-4-5:1995, EN 61000-4-6:1996, EN 61000-4-7:1993, EN 61000-4-8:1993, EN 61000-4-9:1993, EN 61000-4-10:1993, EN 61000-4-11:1994,EN 61000-4-12:1995, EN 60950: 1992.

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.

Changes or modifications not expressly approved by the manufacturer could void the user’s authority to operate the equipment.

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.

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

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 Distinguishing 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 certifcates, 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 Appliance.

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 VPN client and a VPN server.

Index