Check Point Safe@Office

Internet Security Appliance

User Guide

Version 4.6

Part No: 700797, June 2004

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.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply 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 in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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, 200, and 300 product families. The Safe@Office 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.

With the Safe@Office appliance, you can subscribe to additional 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
- Safe@Office 200 series
- Safe@Office 300 series

All three series provide a Web-based management interface, which enables you to manage and configure the Safe@Office appliance operation and options. However, the 200 series and 300 series provide higher firewall and VPN throughput and have a dedicated DMZ port and a serial port. The 300 series also provides two USB ports enabling printer server functionality, and the 300W functions as an access point for a wireless network.

The 100 series includes models Safe@Office 105 and Safe@Office 110. The 200 series includes models Safe@Office 225 and Safe@Office 225U. The 300 series includes models Safe@Office 300 and Safe@Office 300W.

Your 100 and 200 series 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 Remote Access VPN Server which allows a single user to securely access resources protected by the Safe@Office appliance from home or while traveling. 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 Remote Access VPN Server but as a Remote Access VPN Client, enabling employees working

from home to securely connect to the office network. Safe@Office 110 can also be configured as a Site-to-Site 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 and Traffic Shaper. 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. Traffic Shaper allows you to control the flow of communication so that important traffic takes precedence over less important traffic; this enables your business to function with minimum disruption, even when the network is congested.

Safe@Office 225 includes a hardware DMZ port and offers higher VPN and firewall performance than the 100 series. It also supports the use of a dialup modem.

Like Safe@Office 110, Safe@Office 225 is intended for small to medium-sized businesses with extended networks. Safe@Office 225 supports 25 computers.

Safe@Office 225U

Safe@Office 225U provides the same functionality as Safe@Office 225 but supports an unlimited number of computers.

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

Safe@Office 300

Safe@Office 300 provides all the benefits of Safe@Office 225, along with two USB ports for printer server functionality.

Safe@Office 300 is intended for small to medium-sized businesses with extended networks. It can be used by up to 25 computers.

Safe@Office 300W

Safe@Office 300W provides the same functionality as Safe@Office 300, but can function as an access point for a wireless network.

All references to Safe@Office 300 in this guide are also relevant to Safe@Office 300W.

Safe@Office Features and Compatibility

Connectivity

Feature	Safe@ Office 105	Safe@ Office 110	Safe@ Office 225/225U	Safe@ Office 300/300W
Concurrent firewall connections	2,000	2,000	8,000	8,000
LAN Ports	4-ports 10/100 Mbps Fast Ethernet switch			
WAN Port	10/100 Mbps Fast Ethernet	10/100 Mbps Fast Ethernet	10/100 Mbps Fast Ethernet	10/100 Mbps Fast Ethernet
DMZ/WAN2 Port			10/100 Mbps Fast Ethernet	10/100 Mbps Fast Ethernet

Feature	Safe@ Office 105	Safe@ Office 110	Safe@ Office 225/225U	Safe@ Office 300/300W
WLAN Antennas				✓ 300W only
USB Ports				✓
Serial Console Port			✓	✓
Ethernet cable type recognition			✓	✓
Users (nodes)	5	10	25 or Unlimited	25 or Unlimited
Supported Internet connection methods	Static IP, DHCP Client, Cable Modem, PPTP Client, PPPoE Client, Telstra BPA login			
DHCP Server	✓	✓	✓	✓
DHCP relay	✓	✓	✓	✓
MAC Cloning	✓	✓	✓	✓
Backup Internet connection		✓	✓	✓

Feature	Safe@ Office 105	Safe@ Office 110	Safe@ Office 225/225U	Safe@ Office 300/300W
High Availability			✓	✓
Traffic Shaper			✓	✓
Static NAT	✓	✓	✓	✓
Static Routes	✓	✓	✓	✓

Firewall

Feature	Safe@ Office 105	Safe@ Office 110	Safe@ Office 225/225U	Safe@ Office 300/300W
Firewall Type	Check Point Firewall-1 Embedded NG			
Network Address Translation (NAT)	✓	✓	✓	✓
INSPECT Policy Rules	Unlimited	Unlimited	Unlimited	Unlimited
User-defined rules	✓	✓	✓	✓

Feature	Safe@ Office 105	Safe@ Office 110	Safe@ Office 225/225U	Safe@ Office 300/300W
Three levels preset security policies	✓	✓	✓	✓
DoS Protection	✓	✓	✓	✓
Anti-spoofing	✓	✓	✓	✓
Attack Logging	✓	✓	✓	✓
Voice over IP (H.323) Support	✓	✓	✓	✓
Exposed Host	✓	✓	✓	✓
DMZ Network		Logical	Physical	Physical
WLAN Network				✓ 300W only

VPN

Feature	Safe@ Office 105	Safe@ Office 110	Safe@ Office 225/225U	Safe@ Office 300/300W
VPN Type	Check Point VPN-1 Embedded NG			
IPSEC VPN mode	Remote Access Server	Remote Access Client Remote Access Server Site-to-Site	Remote Access Client Remote Access 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	AES/3DES/ DES
Authentication	SHA1/MD5	SHA1/MD5	SHA1/MD5	SHA1/MD5
X.509 Digital Certificates		✓	✓	✓
RADIUS client		✓	✓	✓
Hardware Acceleration			✓	✓

Feature	Safe@ Office 105	Safe@ Office 110	Safe@ Office 225/225U	Safe@ Office 300/300W
Hardware Random Number Generator			✓	✓

Management

Feature	Safe@ Office 105	Safe@ Office 110	Safe@ Office 225/225U	Safe@ Office 300/300W
Web Management	✓	✓	✓	✓
HTTPS Access (local and remote)	✓	✓	✓	✓
Multiple Administrators		✓	✓	✓
CLI	✓	✓	✓	✓
Management Systems	SofaWare SMP	SofaWare SMP	SofaWare SMP	SofaWare SMP

Optional Security Services

Feature	Safe@ Office 105	Safe@ Office 110	Safe@ Office 225/225U	Safe@ Office 300/300W
Firewall security and software updates	✓	✓	✓	✓
Web Filtering *	✓	✓	✓	✓
Email Antivirus protection *	✓	✓	✓	✓
Dynamic DNS Service *	✓	✓	✓	✓
SecureDesk Antivirus Compliance Checking *	✓	✓	✓	✓
VPN Management	✓	✓	✓	✓

Feature	Safe@ Office 105	Safe@ Office 110	Safe@ Office 225/225U	Safe@ Office 300/300W
Firewall security and software updates	✓	✓	✓	✓
Centralized Logging and Intrusion Detection	✓	✓	✓	✓

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

Package Contents

Item	Safe@Office 105, 100, 225/225U	Safe@Office 300	Safe@Office 300W
Safe@Office Internet Security Appliance	✓	✓	✓
Power adapter	✓	✓	✓
CAT5 Straight-through Ethernet cable	✓	✓	✓

Item	Safe@Office 105, 100, 225/225U	Safe@Office 300	Safe@Office 300W
USB cable		✓	✓
Two antennas			✓
Two plastic conical anchors			✓
Two cross-head screws			✓
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.

- When using Safe@Office 300W, a wireless card installed on each wireless client

Getting to Know Your Safe@Office 100 Series

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.

Label	Description
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.

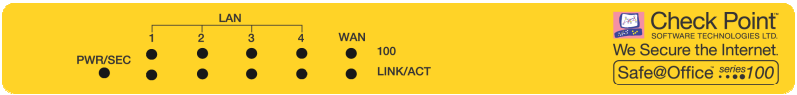


Figure 2: Safe@Office 100 Appliance Front Panel

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
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received

Getting to Know Your Safe@Office 200 Series

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.

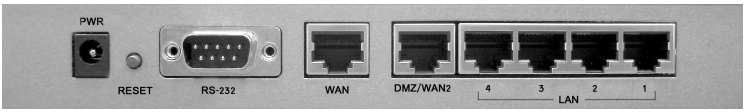


Figure 3: Safe@Office 200 Appliance Rear Panel Items

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.

Label	Description
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
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/WAN 2	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

LED	State	Explanation
	LINK/ACT On, 100 Off	10 Mbps link established for the corresponding port
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
VPN	Flashing (Green)	VPN port in use
Serial	Flashing (Green)	Serial port in use

Getting to Know Your Safe@Office 300 Series Appliance

Rear Panel

All physical connections (network and power) to the Safe@Office appliance are made via the rear panel of your Safe@Office appliance.

The following table lists the Safe@Office 300 appliance's rear panel elements.

Table 5: Safe@Office 300 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.
USB	A USB port
COM1	A serial port
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	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

Label	Description
ANT 1/ ANT 2	Antenna connectors (Safe@Office 300W only)

Front Panel

The Safe@Office 300 appliances includes several status LEDs that enable you to monitor the appliance's operation.

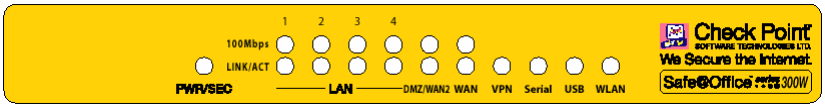


Figure 5: Safe@Office 300 Appliance Front Panel

For an explanation of the Safe@Office 300 appliance's status LEDs, see the table below.

Table 6: Safe@Office 300 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

LED	State	Explanation
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
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
VPN	Flashing (Green)	VPN port in use
Serial	Flashing (Green)	Serial port in use
USB	Flashing (Green)	USB port in use
WLAN (300W only)	Flashing (Green)	WLAN 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 sections below will guide you through the TCP/IP setup and installation process.

Windows 2000/XP

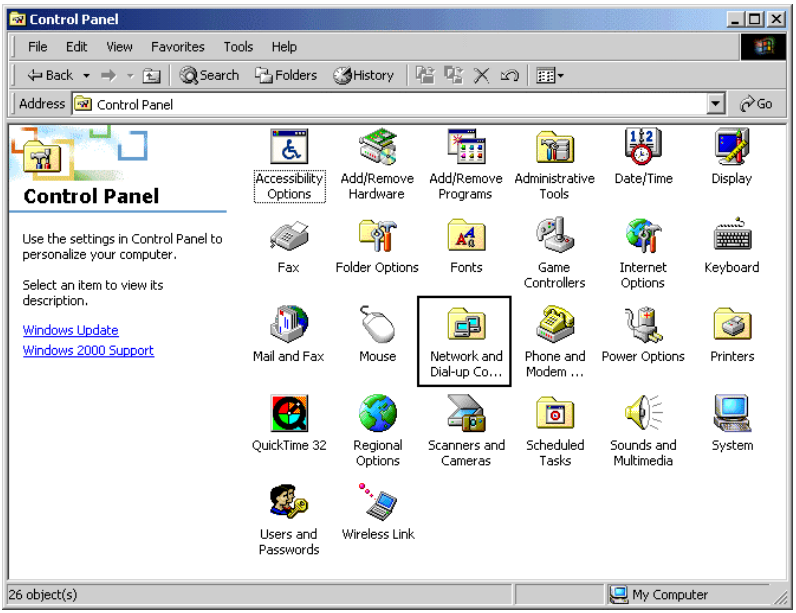
Note: While Windows XP has an "Internet Connection Firewall" option, it is recommended to disable it if you are using a Safe@Office appliance, since the Safe@Office appliance offers better protection.

If you want to subscribe to SecureDesk, you *must* disable the Windows XP firewall before you install the antivirus software. For information on SecureDesk, see ***Using SecureDesk*** on page 183.

Checking the TCP/IP Installation

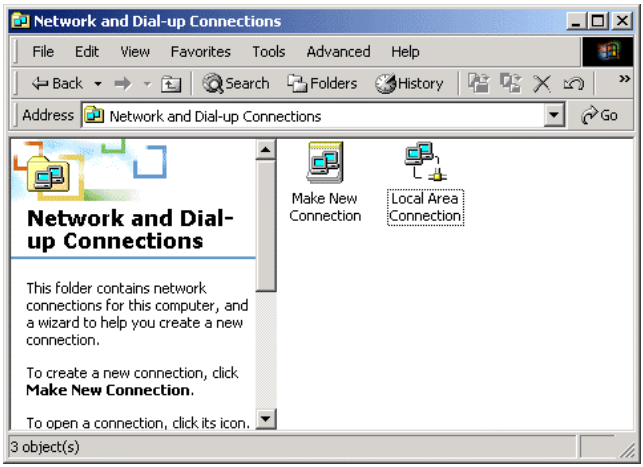
1. Click Start > Settings > Control Panel.

   The Control Panel window appears.



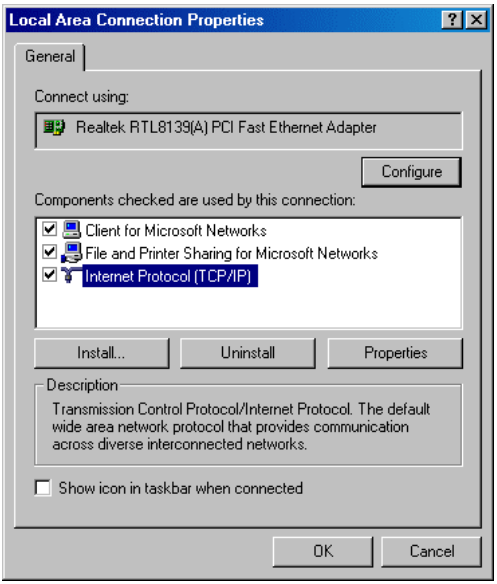
2. Double-click the Network and Dial-up Connections icon.

The Network and Dial-up Connections window appears.



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

The Local Area Connection Properties window appears.

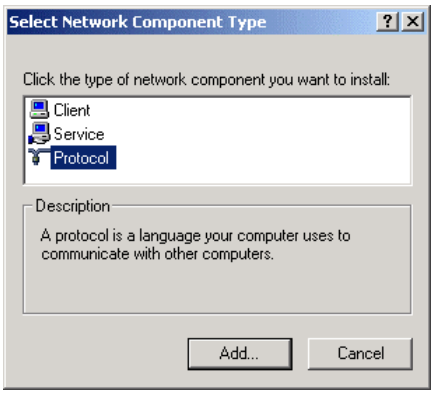


4. In the above window, check if TCP/IP appears in the components list and if it is properly configured with the Ethernet card, installed on your computer. If TCP/IP does not appear in the Components list, you must install it as described in the next section.

Installing TCP/IP Protocol

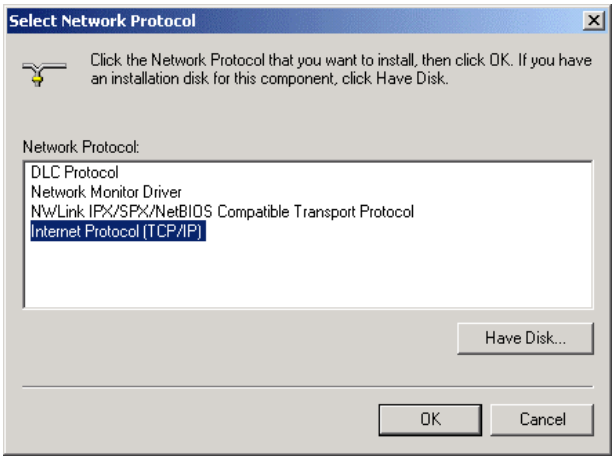
1. In the Local Area Connection Properties window click Install....

   The Select Network Component Type window appears.



2. Choose Protocol and click Add.

   The Select Network Protocol window appears.



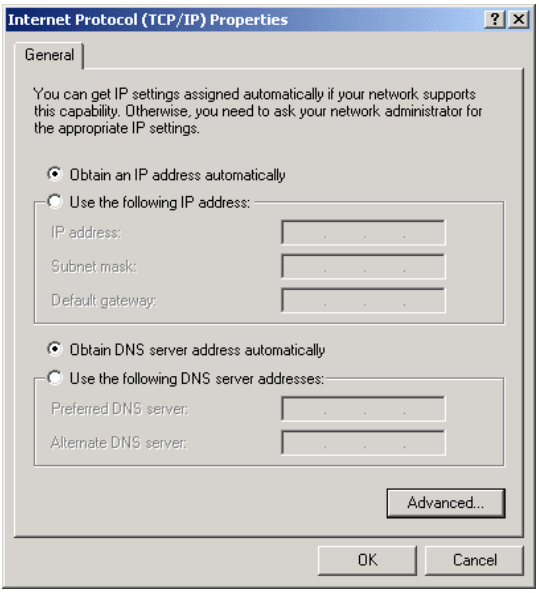
3. Choose Internet Protocol (TCP/IP) and click OK.

   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.



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.

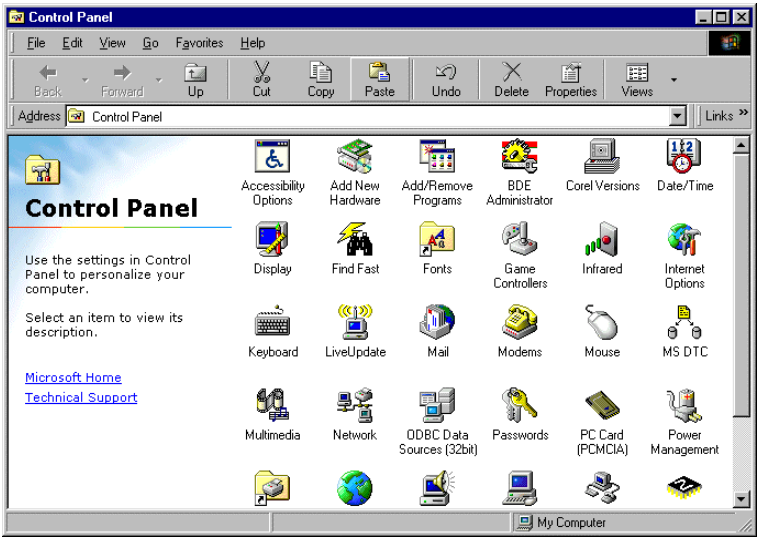
   Your computer is now ready to access your Safe@Office appliance.

Windows 98/Millennium

Checking the TCP/IP Installation

1. Click Start > Settings > Control Panel.

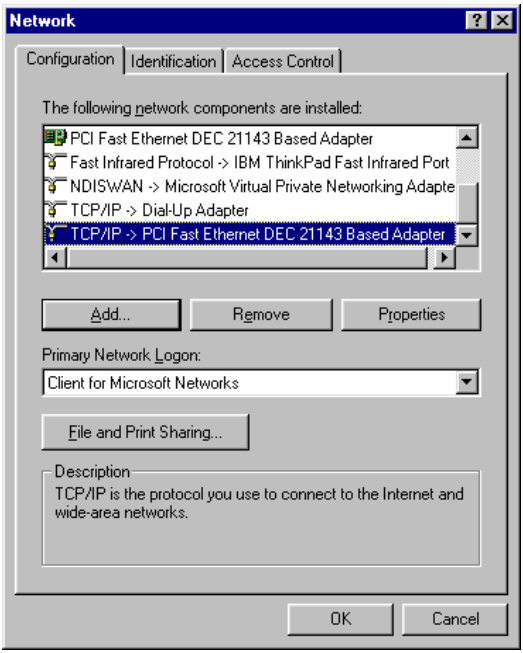
   The Control Panel window appears.



2. Double-click the 

icon.

The Network window appears.



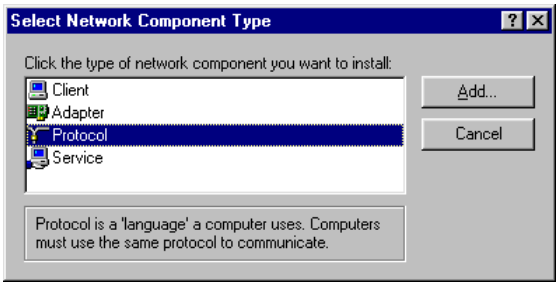
3. In the Network window, check if TCP/IP appears in the network components list and if it is already configured with the Ethernet card, installed on your computer.

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.

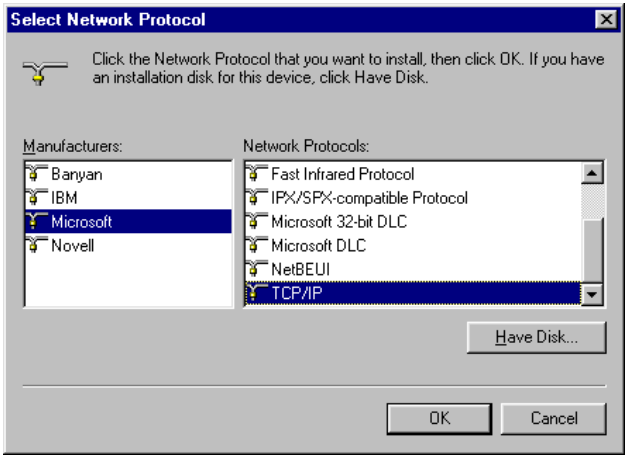
1. In the Network window, click Add.

The Select Network Component Type window appears.



2. Choose Protocol and click Add.

   The Select Network Protocol window appears.



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

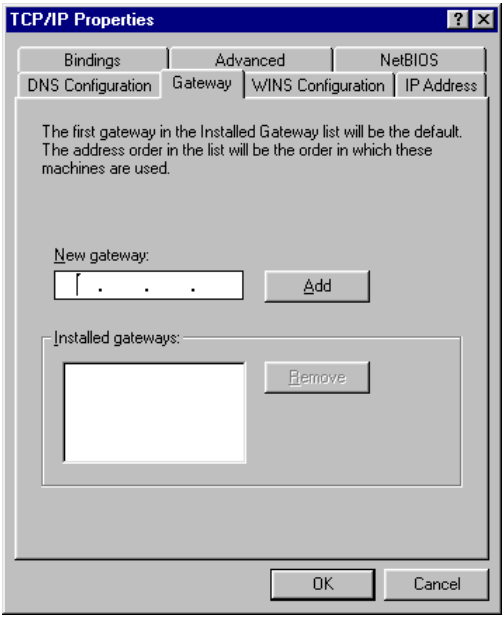
   If Windows asks for original Windows installation files, provide the installation CD and relevant path when required (e.g. D:\win98)

5. Restart your computer if prompted.

TCP/IP Settings

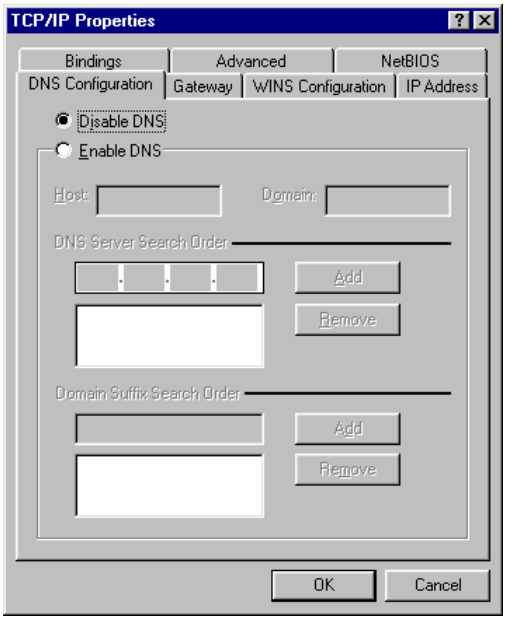
Note: If you are connecting your Safe@Office appliance to an existing LAN, consult your network manager for the correct configurations.

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.

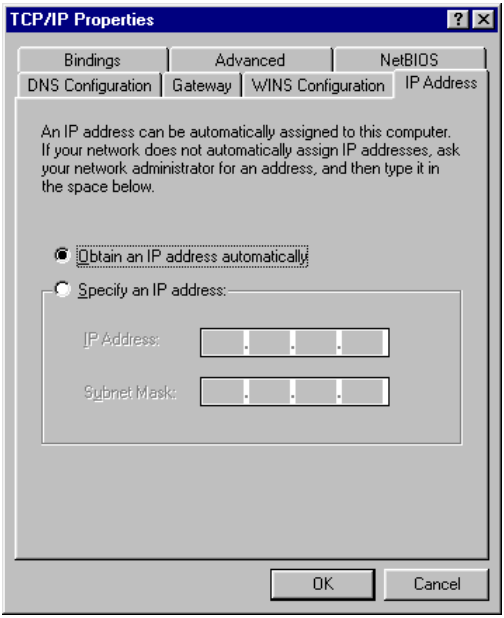


2. Click the Gateway tab, and remove any installed gateways.

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



4. Click the IP Address tab, and 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.)

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

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

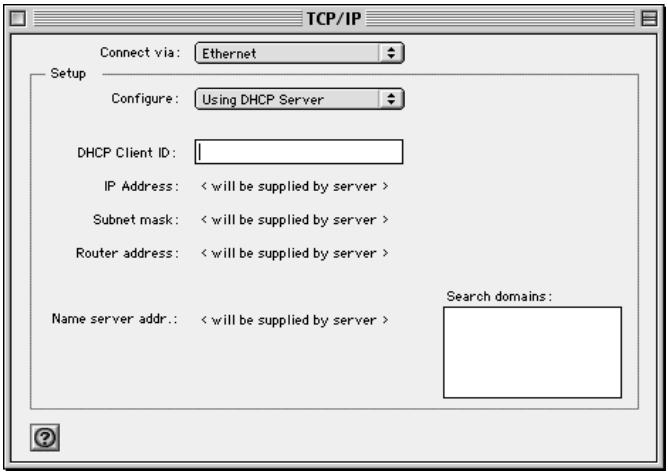
   Your computer is now ready to access your Safe@Office appliance.

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.



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.

Wall Mounting the Appliance

If desired, you can mount your Safe@Office 300 series appliance on the wall.

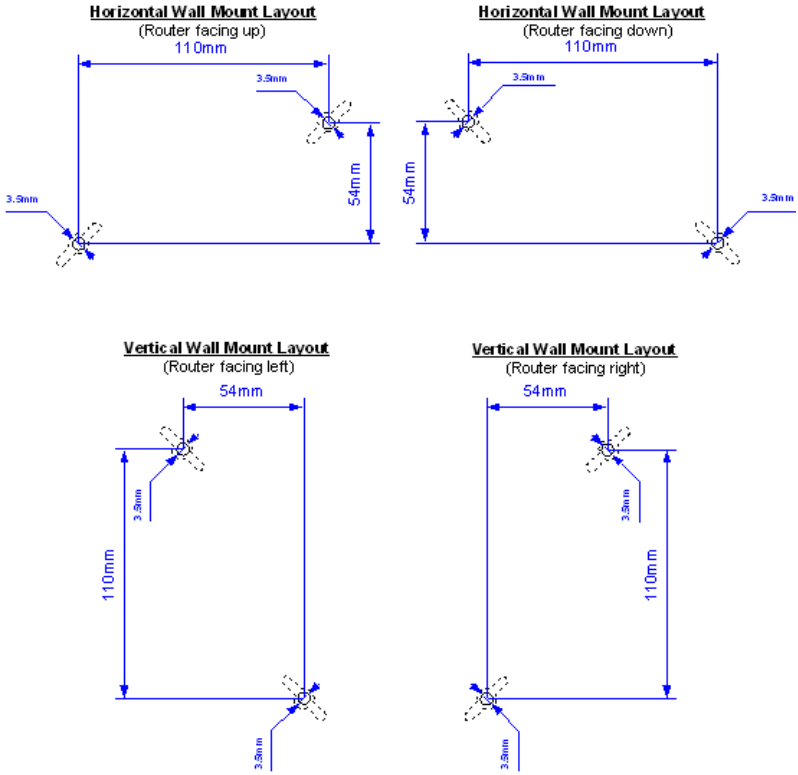
To mount the Safe@Office appliance on the wall

1. Decide where you want to mount your Safe@Office appliance.
2. Decide on the mounting orientation.

   You can mount the appliance on the wall facing up, down, left, or right.

Note: Facing downwards is not recommended, as dust might accumulate in unused ports.

3. Mark two drill holes on the wall, in accordance with the following sketch:



4. Drill two 3.5 mm diameter holes, approximately 25 mm deep.
5. Insert the two plastic conical anchors you received with your Safe@Office appliance into the holes.
6. Insert the two screws you received with your Safe@Office appliance into the plastic conical anchors, and turn them until they protrude approximately 5 mm from the wall.
7. Align the holes on the Safe@Office appliance's underside with the screws on the wall, then push the appliance in and down.

Your Safe@Office appliance is wall mounted. You can now connect it to your computer. See ***Network Installation*** on page 40.

Network Installation

1. Verify that you have the correct cable type.

   For information, see ***Network Requirements*** on page 13.

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.

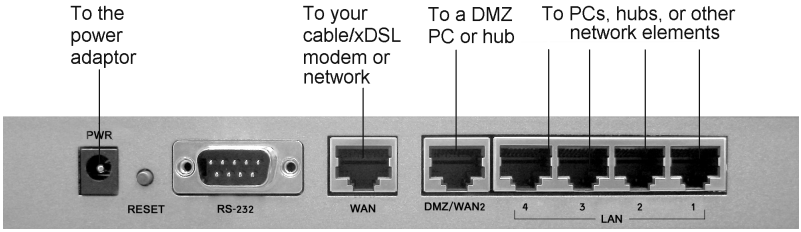


Figure 6: Typical Connection Diagram

5. In Safe@Office appliance 300W, prepare the Safe@Office appliance for a wireless connection:

   a. Connect the antennas that came with your Safe@Office appliance to the ANT1 and ANT2 antenna connectors in the appliance's rear panel.

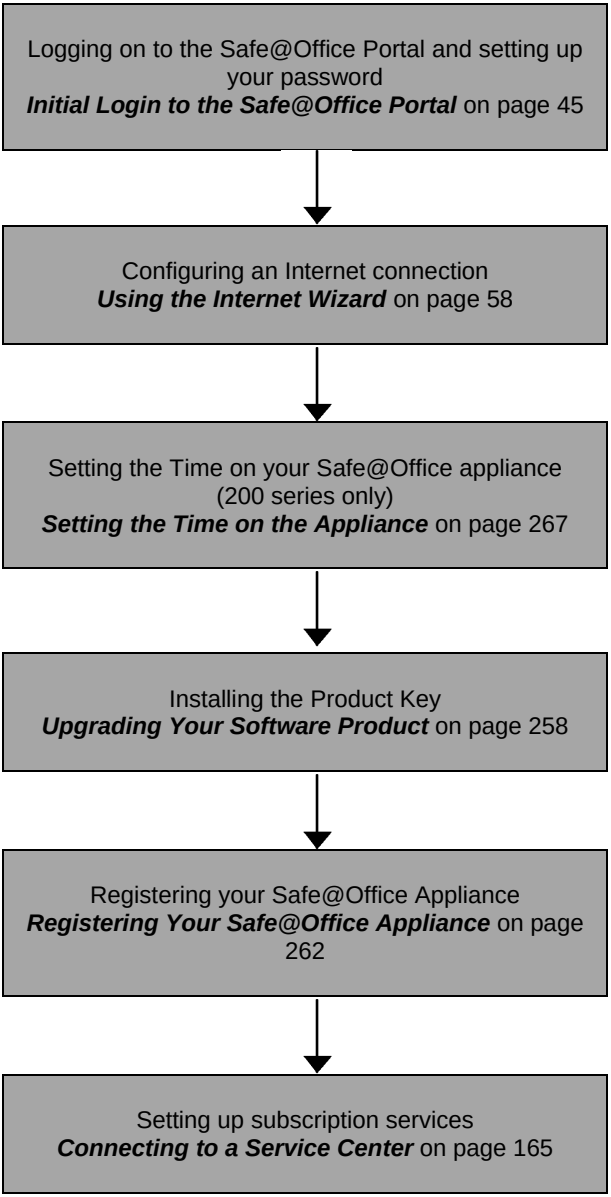
   b. Bend the antennas at the hinges, so that they point upwards.

Setting Up the Safe@Office Appliance

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

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 set up your password, the Safe@Office 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.

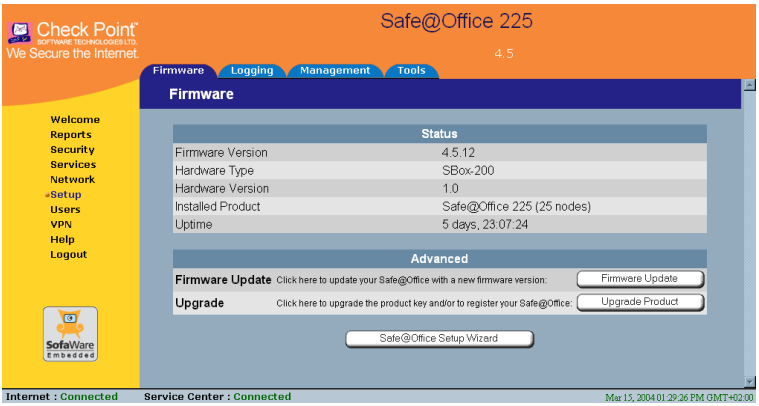

Logging on to the Safe@Office Portal and setting up your password
Initial Login to the Safe@Office Portal on page 45
Configuring an Internet connection
Using the Internet Wizard on page 58
Setting the Time on your Safe@Office appliance (200 series only)
Setting the Time on the Appliance on page 267
Installing the Product Key
Upgrading Your Software Product on page 258
Registering your Safe@Office Appliance
Registering Your Safe@Office Appliance on page 262
Setting up subscription services
Connecting to a Service Center on page 165

You can access the Setup Wizard at any time after initial setup, using the procedure below.

To access the Setup Wizard

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

   The **Firmware** page appears.



2. Click **Safe@Office Setup Wizard.**

3. The **Safe@Office Setup Wizard** opens with the **Welcome** page displayed.

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

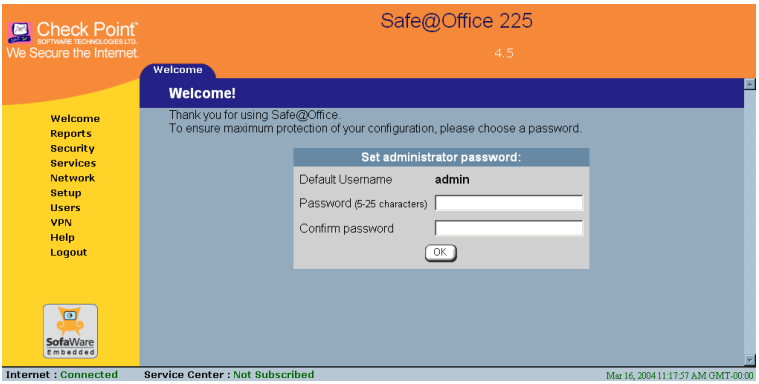
Safe@Office 105 | Safe@Office 110 | Safe@Office 225

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.



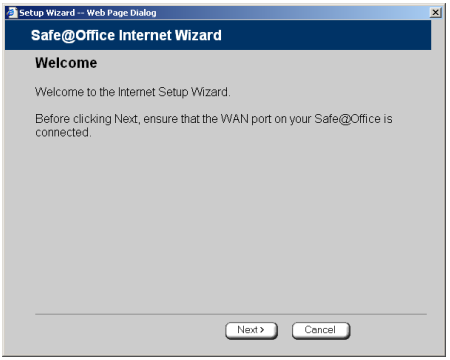
2. Type a password both in the Password and the Confirm Password fields.

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 245.

3. Click OK.

The Safe@Office Setup Wizard opens, with the Welcome screen displayed.



4. Configure your Internet connection using one of the following ways:

   - Internet Wizard

     The Internet Wizard is the first part of the Setup Wizard, and it takes you through basic Internet connection setup, step by step. For information on using the Internet Wizard, see ***Using the Internet Wizard*** on page 58.

     After you have completed the Internet Wizard, the Setup Wizard continues to guide you through appliance setup. For more information, see ***Setting Up the Safe@Office Appliance*** on page 41.

   - Internet Setup

     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 66.

Logging on to the Safe@Office Portal

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

To log on to the Safe@Office Portal

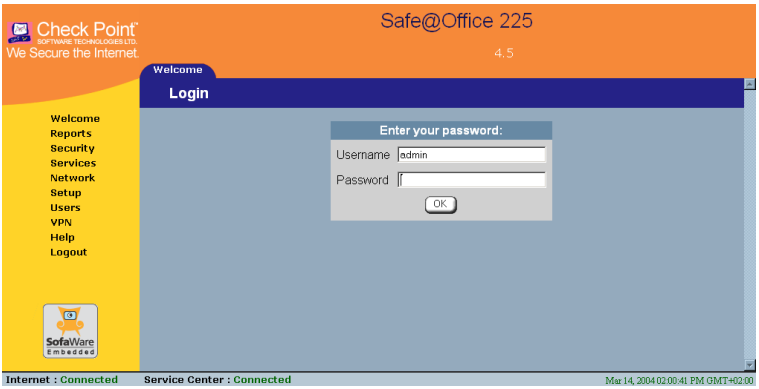
1. Do one of the following:

   - 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 49.

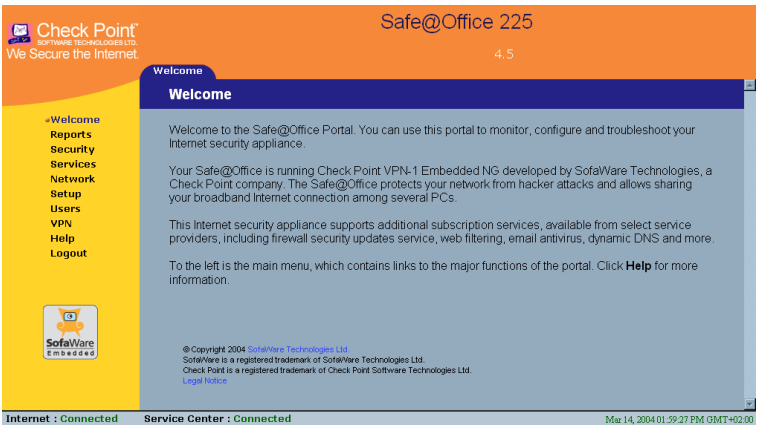
The login page appears.



If you are using Safe@Office 105, the page appears without the Username field.

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

   The Welcome page appears.



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. If desired, 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 45.

Configure HTTPS. See ***Configuring HTTPS*** on page 265.

Note: Your browser must support 128 bit cipher strength. To check your browser's cipher strength, open Internet Explorer and click Help > About Internet Explorer.

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:

a. Click View Certificate.

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

b. Click Install Certificate.

   The Certificate Import Wizard opens.

c. Click Next.

d. Click Next.

e. Click Finish.

f. Click Yes.

g. Click OK.

   The Security Alert dialog box reappears.

h. 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 7: 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.

Figure 7: Safe@Office Portal

Main Menu

The main menu includes the following submenus.

Table 8: 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 9: 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 57.

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

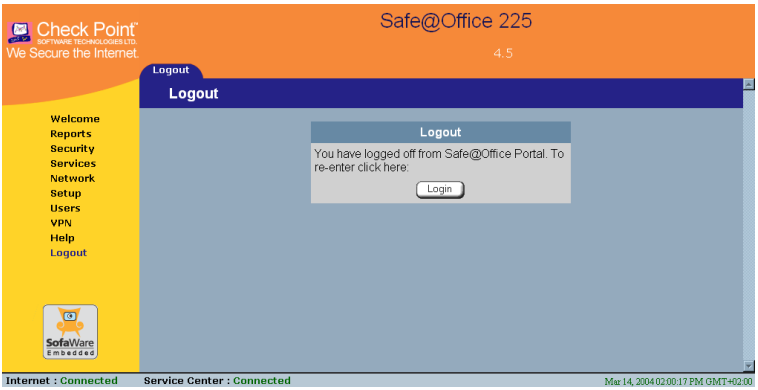
Safe@Office 105 | Safe@Office 110 | Safe@Office 225

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.



  - 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 any of the following setup tools:

- Setup Wizard. Guides you through the Safe@Office appliance setup step by step. The first part of the Setup Wizard is the Internet Wizard. For further information on the Setup Wizard, see ***Setting Up the Safe@Office Appliance*** on page 41.
- Internet Wizard. Guides you through the Internet connection 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. In Safe@Office 225, you can also do the following:
  - Enable Traffic Shaper for traffic flowing through the connection.

    For information on Traffic Shaper, see ***Using Traffic Shaper*** on page 120.
  - Configure a dialup Internet connection.

    Before configuring the connection, you must first set up the modem. For information, see ***Setting Up a Dialup Modem*** on page 84.

Using the Internet Wizard

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

The Internet 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 Internet Wizard starts automatically as part of the Setup Wizard. In this case, you should skip to step 2 in the procedure below.

To set up the Internet connection using the Internet Wizard

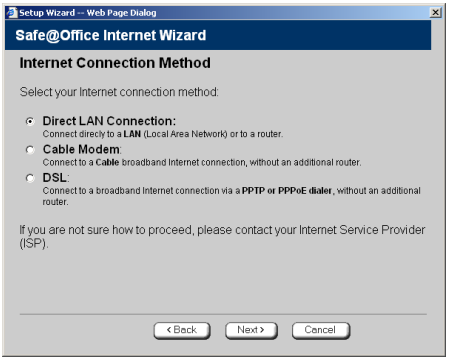
1. Click Network in the main menu, and click the Internet tab.

   The Internet page appears
2. Click Internet Wizard.

The Internet Wizard opens with the Welcome page displayed.

3. Click Next.

   The Internet Connection Method dialog box appears.



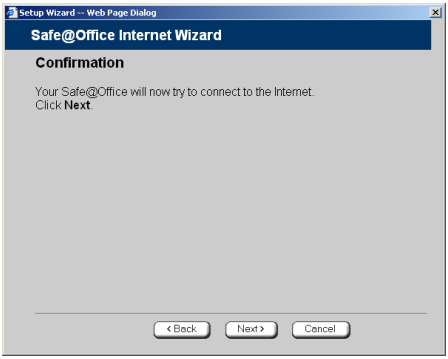
4. Select the Internet connection method you want to use for connecting to the Internet.

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.



1. Click Next.

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

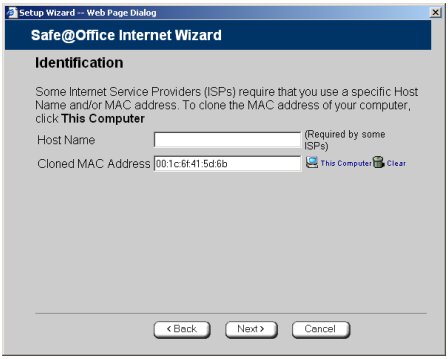
   The Connecting... screen appears.

   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.



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.

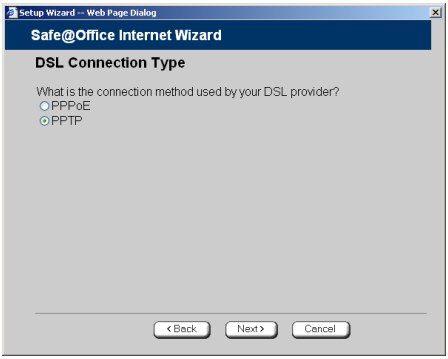
The system attempts to connect to the Internet.

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.



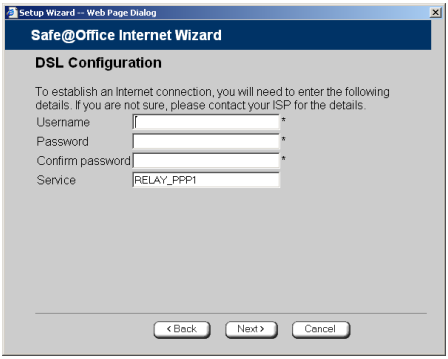
1. Select the connection method used by your DSL provider.

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.



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.

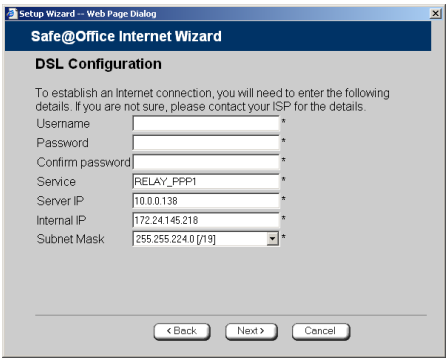
Table 10: PPPoE Connection Fields

In this field…	Do this…
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password.

In this field…	Do this…
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.



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 11: 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.

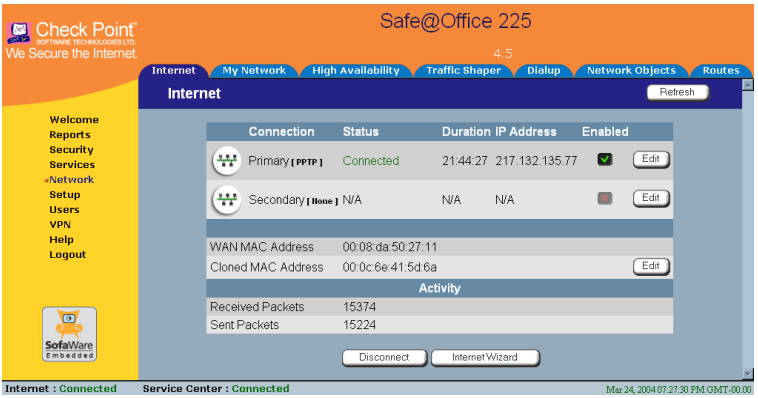
Using Internet Setup

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.

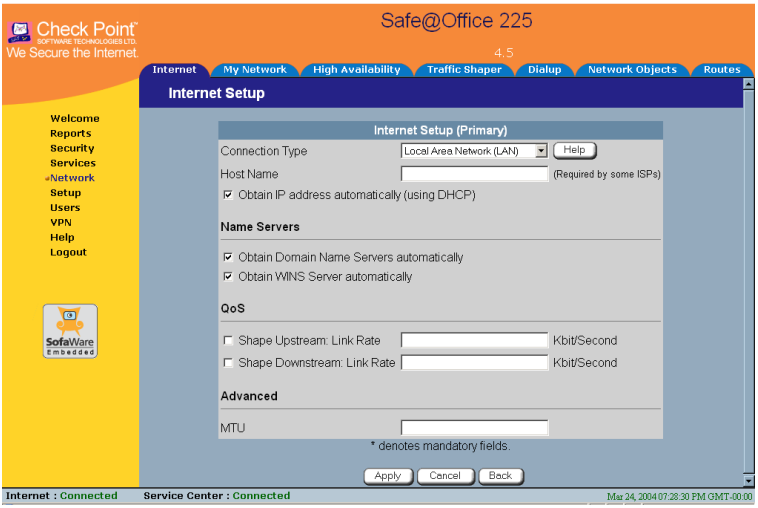


   If you are using Safe@Office 105, the secondary connection does not appear.

2. If your ISP restricts connections to specific, recognized MAC addresses, clone a MAC address using the procedure ***Cloning a MAC Address*** on page 86.

3. Next to the Internet connection, click Edit.

The **Internet Setup** page appears.

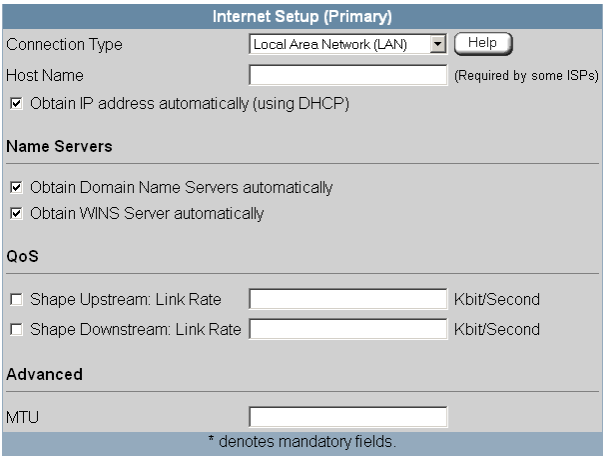


4. From the **Connection Type** drop-down list, select the Internet connection type you are using/intend to use.

   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.

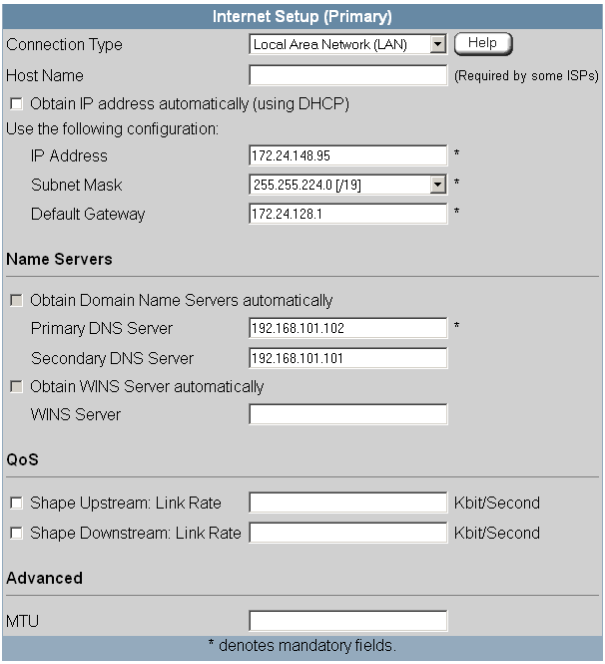
Using a LAN Connection



Note: The QoS area only appears in the Safe@Office 200 series.

1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 79.

New fields appear, depending on the check boxes you selected.

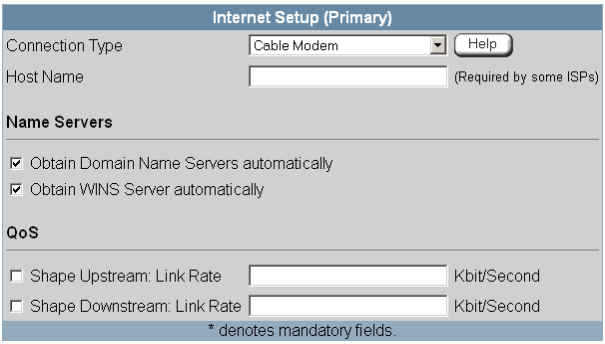


2. Click Apply.

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

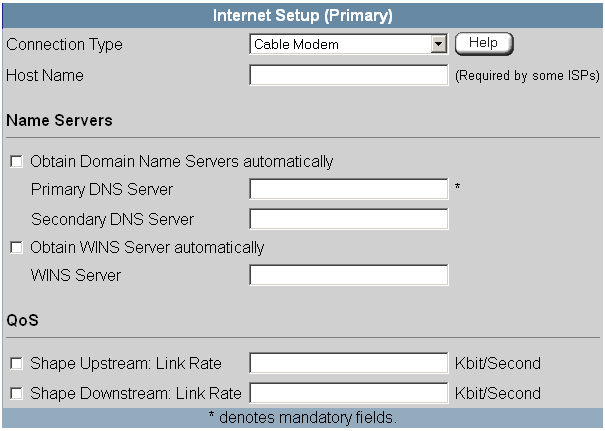
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a Cable Modem Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 79.

   New fields appear, depending on the check boxes you selected.

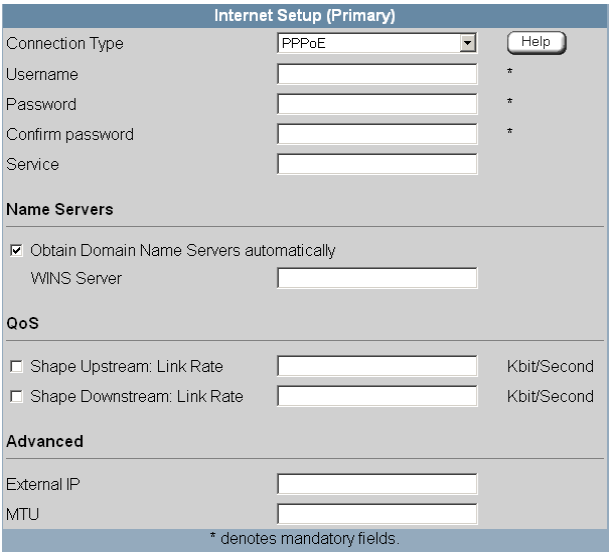


2. Click Apply.

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

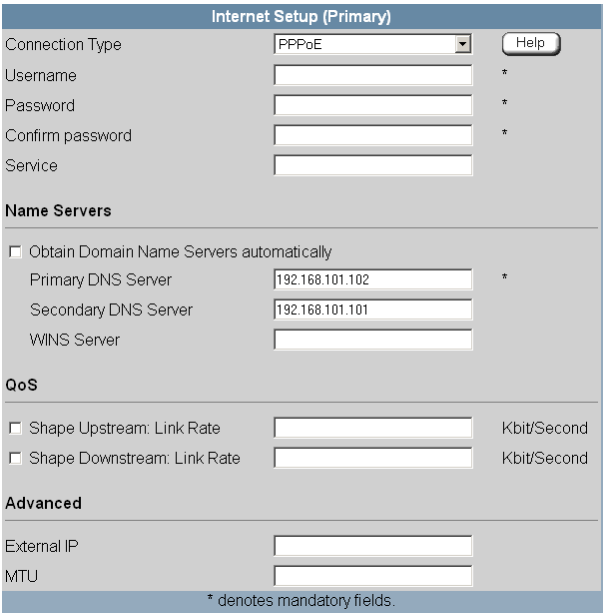
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPPoE Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 79.

New fields appear, depending on the check boxes you selected.

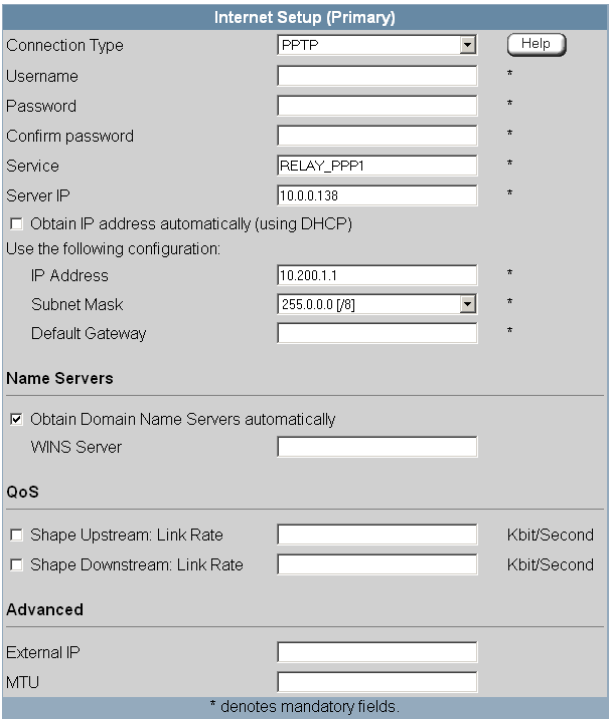


2. Click Apply.

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

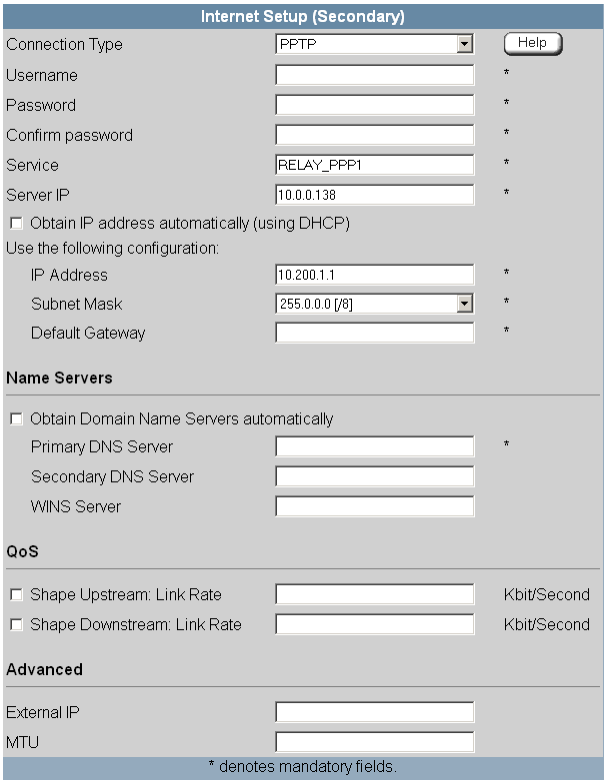
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPTP Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 79.

New fields appear, depending on the check boxes you selected.



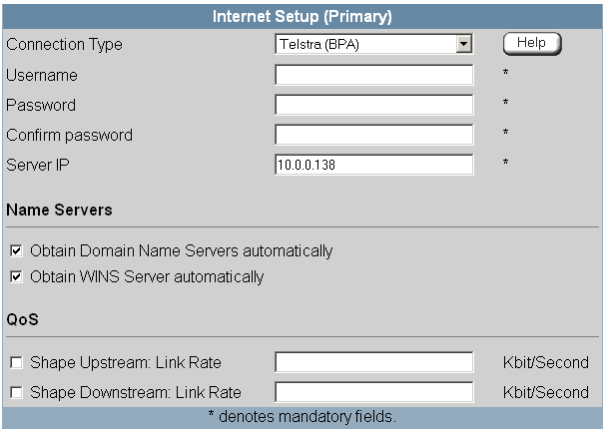
2. Click Apply.

   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”.

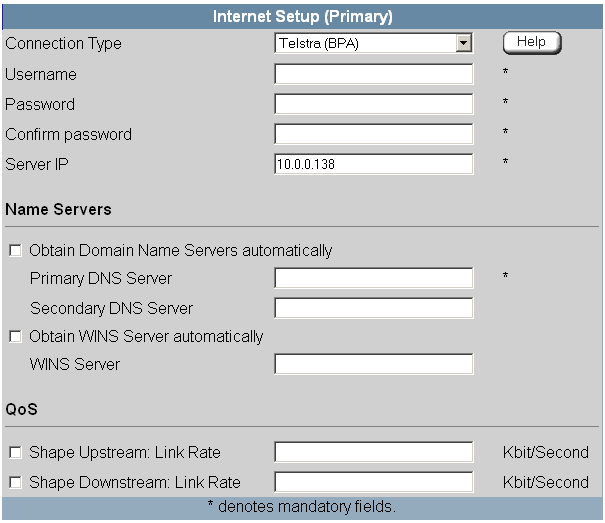
Using a Telstra (BPA) Connection

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



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 79.

New fields appear, depending on the check boxes you selected.



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.

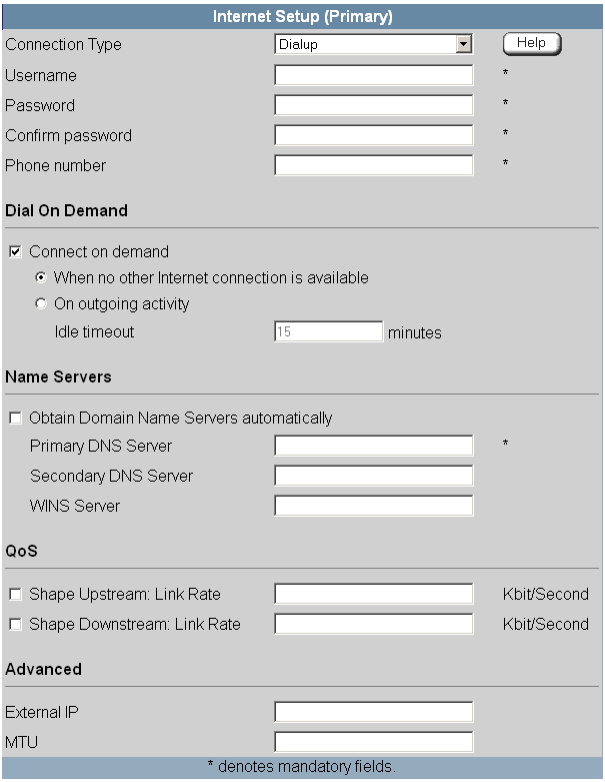
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a Dialup Connection

To use this connection type, you must first set up the dialup modem. For information, see ***Setting Up a Dialup Modem*** on page 84.

1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 79.

New fields appear, depending on the check boxes you selected.



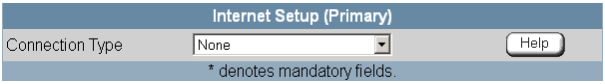
2. Click Apply.

   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.



- Click Apply.

Table 12: 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.
Service	Type your service name. If your ISP has not provided you with a service name, leave this field empty.
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.

In this field…	Do this…
Phone Number	If you selected Dialup, type the phone number that the modem should dial, as given by your ISP.
Dial On Demand	
Connect on demand	Select this option if you do not want the dialup modem to be constantly connected to the Internet. The modem will dial a connection only under certain conditions. This option is useful when configuring a dialup backup connection. For information, see ***Setting Up a Dialup Backup Connection*** on page 92.
When no other Internet connection is available	Select this option to specify that the dialup modem should only dial a connection if no other connection exists, and the Safe@Office appliance is not acting as a Backup appliance. If another connection opens, or if the Safe@Office appliance becomes a Backup appliance, the dialup modem will disconnect. For information on configuring the appliance as a Backup or Master, see ***Configuring High Availability*** on page 117.

In this field…	Do this…
On outgoing activity	Select this option to specify that the dialup modem should only dial a connection if no other connection exists, and there is outgoing activity (that is, packets need to be transmitted to the Internet). If another connection opens, or if the connection times out, the dialup modem will disconnect.
Idle timeout	Type the amount of time (in minutes) that the connection can remain idle. Once this period of time has elapsed, the dialup modem will disconnect.
Name Servers	
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.
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 servers.
Obtain WINS Server automatically	Clear this option if you want the Safe@Office appliance to obtain an IP address automatically using DHCP, but not to automatically configure the WINS server.
IP Address	Type the static IP address of your Safe@Office appliance.

In this field…	Do this…
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.
Primary DNS Server	Type the Primary DNS server IP address.
Secondary DNS Server	Type the Secondary DNS server IP address.
WINS Server	Type the WINS server IP address.
QoS	
Shape Upstream: Link Rate	Select this option to enable Traffic Shaper for outgoing traffic. Then type a rate (in kilobits/second) slightly lower than your Internet connection's maximum measured upstream speed in the field provided. It is recommended to try different rates in order to determine which one provides the best results. For information on using Traffic Shaper, see ***Using Traffic Shaper*** on page 120.

In this field...	Do this...
Shape Downstream: Link Rate	Select this option to enable Traffic Shaper for incoming traffic. Then type a rate (in kilobits/second) slightly lower than your Internet connection's maximum measured downstream speed in the field provided. It is recommended to try different rates in order to determine which one provides the best results. Note: Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping received packets. This makes the shaping of inbound traffic less accurate than the shaping of outbound traffic. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary. For information on using Traffic Shaper, see ***Using Traffic Shaper*** on page 120.
Advanced	
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.

In this field…	Do this…
MTU	This 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.

Setting Up a Dialup Modem

You can use a dialup modem as a primary or secondary Internet connection method. This is useful in locations where broadband Internet access is unavailable.

When used as a backup Internet connection, the modem can be automatically disconnected when not in use. For information on setting up a dialup backup connection, see ***Setting Up a Dialup Backup Connection*** on page 92.

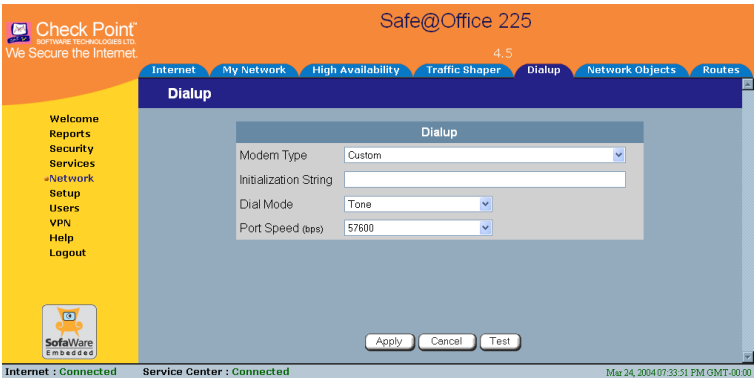
To set up a dialup modem

1. Connect a regular or ISDN dialup modem to your Safe@Office appliance's serial port.

   For information on locating the serial port, see ***Rear Panel*** on page 17.

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

The Dialup page appears.



3. Complete the fields using the information in the table below.
4. Click Apply.
5. To check that that the values you entered are correct, click Test.

   The Dialup page displays a message indicating whether the test succeeded.
6. Configure a Dialup Internet connection using the information in ***Using Internet Setup*** on page 66.

Table 13: Dialup Fields

In this field…	Do this…
Modem Type	Select the modem type. If you selected Custom, the Installation String field is enabled. Otherwise, it is filled in with the correct installation string for the modem type.

In this field…	Do this…
Initialization String	Type the installation string for the custom modem type. Is you selected a standard modem type, this field is read-only.
Dial Mode	Select the dial mode the modem uses.
Port Speed	Select the modem's port speed (in bits per second).

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.

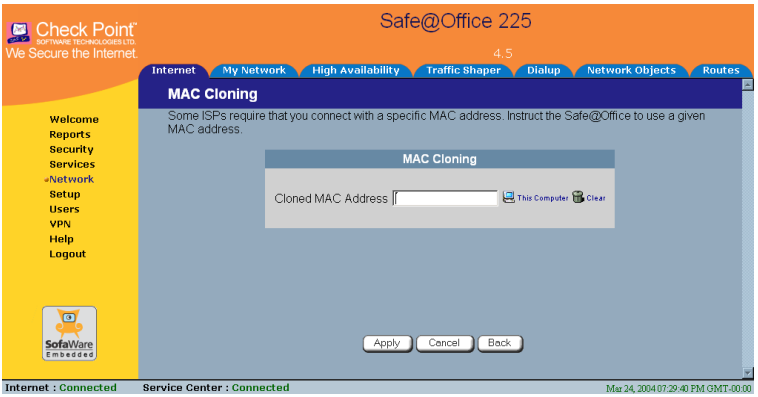
To clone a MAC address

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.



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

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

   The Internet page appears.

   For an explanation of the fields on this page, see the table below.

2. To refresh the information on this page, click Refresh.

Table 14: 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.

Field	Description
Enabled	Indicates whether or not the connection is enabled. For further information, see ***Enabling/Disabling the Internet Connection*** on page 89
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 86.
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 89.

Configuring a Backup Internet Connection

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.

Note: You can configure different DNS servers for the primary and secondary 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.

Setting Up a LAN or Broadband Backup Connection

To set up a LAN or broadband 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 66.

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

Setting Up a Dialup Backup Connection

If desired, you can use a dialup modem as the secondary Internet connection method. The Safe@Office appliance automatically dials the modem if the primary Internet connection fails.

To set up a dialup backup Internet connection

1. Setup a dialup modem.

   For instructions, see ***Setting Up a Dialup Modem*** on page 84.

2. Configure a LAN or broadband primary Internet connection.

   For instructions, see ***Using Internet Setup*** on page 66.

3. Configure a Dialup secondary Internet connection.

   For instructions, see ***Using Internet Setup*** on page 66.

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 277.

Configuring a 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.

Note: The DHCP server only serves computers that are configured to obtain an IP address automatically. If a computer is not configured to obtain an IP address automatically, it is recommended to assign it an IP address outside of the DHCP address range. If you do assign it an IP address within the DHCP address range, the DHCP server will not assign this IP address to another computer.

If you already have a DHCP server in your internal network, and you want to use it instead of the Safe@Office DHCP server, you must disable the Safe@Office DHCP server, since you cannot have two DHCP servers or relays on the same network segment.

If you want to use a DHCP server on the Internet or via a VPN, instead of the Safe@Office DHCP server, you can configure DHCP relay. When in DHCP relay mode, the Safe@Office appliance relays information from the desired DHCP server to the devices on your network.

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

Note: You can perform DHCP reservation using network objects. For information, see ***Using Network Objects*** on page 129.

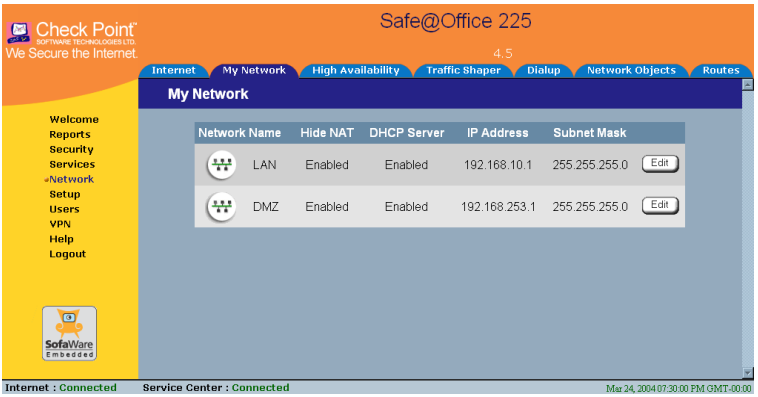
Enabling/Disabling the Safe@Office DHCP Server

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

To enable/disable the Safe@Office DHCP server

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

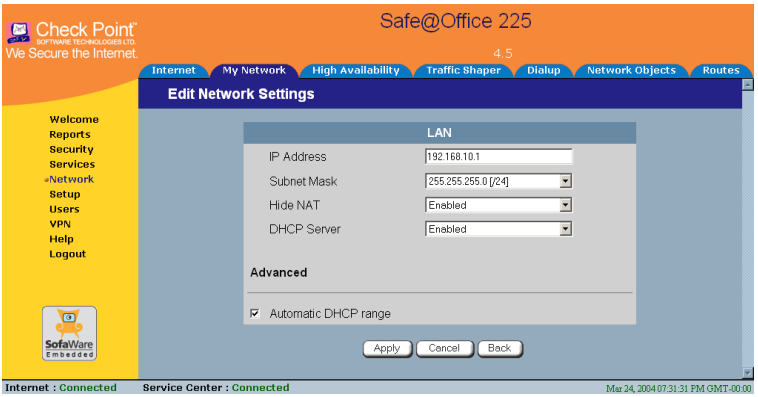
   The My Network page appears.



   If you are using Safe@Office 105, the page appears without the DMZ area.

2. In the desired network's row, click Edit.

The Edit Network Settings page appears.



3. From the DHCP Server list, select Enabled or Disabled.
4. Click Apply.

   A warning message appears.
5. Click OK.

   A success message appears
6. If your computer is configured to obtain its IP address automatically (using DHCP), and either the Safe@Office DHCP server or another DHCP server is enabled, restart your computer.

   If you enabled the DHCP server, your computer obtains an IP address in the DHCP address range.

Configuring the DHCP Address Range

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

By default, the Safe@Office DHCP server automatically sets the DHCP address range. The DHCP address range is the range of IP addresses that the DHCP server can assign to network devices. IP addresses outside of the DHCP address range are reserved for statically addressed computers.

If desired, you can set the Safe@Office DHCP range manually.

To configure the DHCP address range

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

   The My Network page appears.

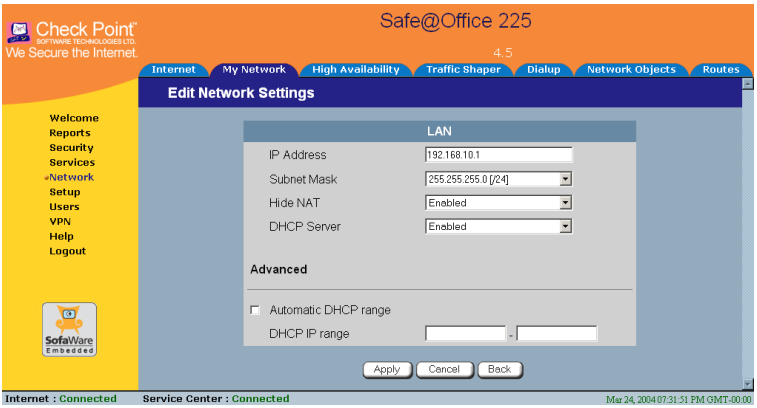
2. In the desired network's row, click Edit.

   The Edit Network Settings page appears.

3. To set the DHCP range manually:

   a. Clear the Automatic DHCP range check box.

   The DHCP IP range fields appear.



   b. In the DHCP IP range fields, type the desired DHCP range.

4. To allow the DHCP server to set the IP address range, select the Automatic DHCP range check box.

5. Click Apply.

   A warning message appears.

6. Click OK.

   A success message appears

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

   Your computer obtains an IP address in the new DHCP address range.

Configuring DHCP Relay

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

To configure DHCP relay

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

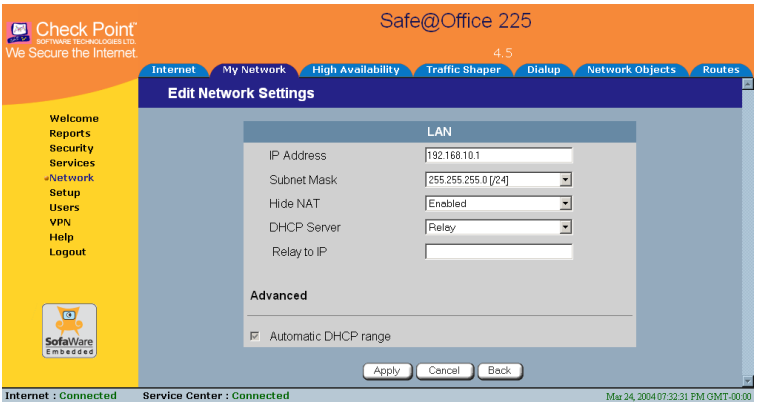
   The My Network page appears.

2. In the desired network's row, click Edit.

   The Edit Network Settings page appears.

3. In the DHCP Server list, select Relay.

   The Automatic DHCP range check box is disabled, and the Relay to IP field appears.



4. In the Relay to IP field, type the IP address of the desired DHCP server.

5. Click Apply.

   A warning message appears.

6. Click OK.

A success message appears

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

   Your computer obtains an IP address in the DHCP address range.

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. In the LAN network's row, click Edit.

   The Edit Network Settings page appears.

3. To change the Safe@Office appliance's internal IP address, enter the new IP address in the IP Address field.

4. To change the internal network range, enter a new value in the 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.

The default internal network range is 192.168.10.*.

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 34, on page 30.

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. In the desired network's row, click Edit.

   The Edit Network Settings page appears.

3. From the Hide NAT list, select Enabled or Disabled.

4. Click Apply.

   A warning message appears.

5. 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

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 and WLAN

networks. You can easily customize this behavior by creating firewall user rules. For further information, see ***Using Rules*** on page 154.

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.

Note: If you are using Safe@Office 225, you can enable the DHCP server for the DMZ network.

If you are using Safe@Office 110, 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 34, on page 30.

Note: 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(s) as follows:

   - If you are using Safe@Office 110, connect the DMZ computers to any of the appliance's LAN ports.
   - If you are using Safe@Office 225, 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 DMZ network's row, click Edit.

The Edit Network Settings page appears.

4. In the Mode drop-down list, select Enabled.

   The fields are enabled.

5. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 101.

6. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 94.

7. In the IP Address field, type the IP address of the DMZ network's default gateway.

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

8. In the Subnet Mask field, type the DMZ's internal network range.
9. Click Apply.

   A warning message appears.

10. Click OK.

    A success message appears.

Configuring a WLAN Network

In addition to the LAN and DMZ networks, you can define a wireless internal network called a WLAN (wireless LAN) network, when using Safe@Office 300W.

By default, all traffic is allowed from the LAN network to the WLAN network, and no traffic is allowed from the WLAN network to the LAN or DMZ networks. You can easily customize this behavior by creating firewall user rules. For further information, see ***Using Rules*** on page 154.

By default, access from the WLAN network to Safe@Office Portal (my.firewall and my.vpn) is not allowed. You can enable access from the WLAN to the Safe@Office Portal in either of the following ways:

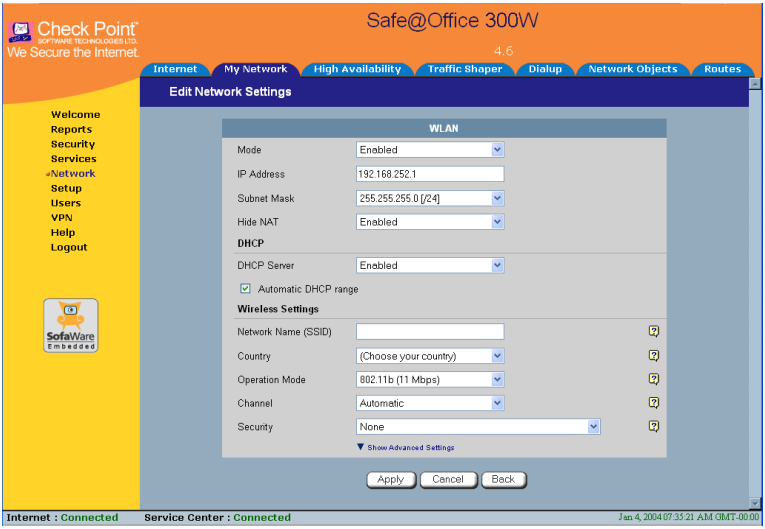
- In the Management page, select ANY in either the SSH or HTTPS drop-down list.
- Create a custom firewall rule to allow the desired protocols from the WLAN, or from an IP address in the WLAN.

To configure a WLAN network

1. Prepare the appliance for a wireless connection as described in ***Network Installation*** on page 40.
2. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
3. In the WLAN network's row, click Edit.

   The Edit Network Settings page appears.



4. In the Mode drop-down list, select Enabled.

   The fields are enabled.
5. If desired, enable or disable Hide NAT.

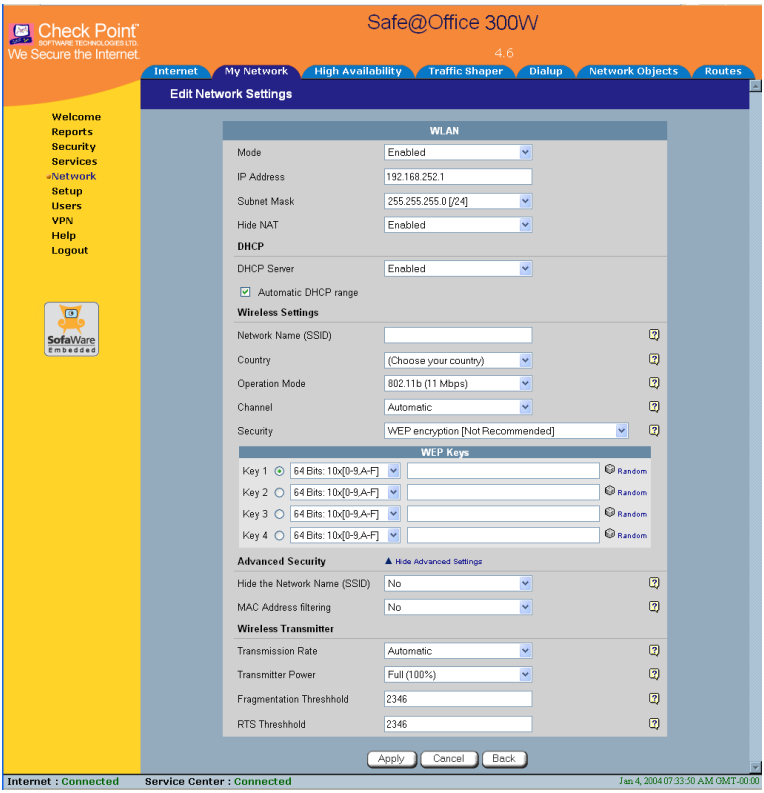
   See ***Enabling/Disabling Hide NAT*** on page 101.

6. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 94.

7. Complete the fields using the information in the table below.

   New fields appear depending on the options you selected.



8. Click Apply.

   A warning message appears.

9. Click OK.

   A success message appears.

10. Prepare the wireless clients by doing one of the following:

- If you selected the 802.1X or WPA security mode, configure RADIUS servers.

  See ***Using RADIUS Authentication*** on page 252.

- If you selected the WEP security mode, give the WEP key to the wireless clients.
- If you selected the WPA-PSK security mode, give the passphrase to the wireless clients.

11. The wireless clients' administrators should configure the wireless clients and connect them to the WLAN.

    Refer to the wireless cards' documentation for details.

Note: Some wireless cards have "Infrastructure" and "Ad-hoc" modes. These modes are also called "Access Point" and "Peer to Peer". Choose the "Infrastructure" or "Access Point" mode.

Note: The wireless cards' region and the Safe@Office appliance's region must both match the region of the world where you are located. If you purchased your Safe@Office appliance in a different region, contact technical support.

Table 15: WLAN Settings Fields

In this field…	Do this…
IP Address	Type the IP address of the WLAN network's default gateway. Note: The WLAN network must not overlap the LAN network.
Subnet Mask	Type the WLAN's internal network range.
Wireless Settings	
Network Name (SSID)	Type the network name (SSID) that identifies your wireless network. It can be up to 32 alphanumeric characters long and is case-sensitive.
Country	Select the country where you are located. Warning: Choosing an incorrect country may result in the violation of government regulations.

In this field…	Do this…
Operation Mode	Select an operation mode: • 802.11b (11Mbps) - Operates in the 2.4 GHz range and offers a rate of 11 Mbps (in theory). • 802.11g (54 Mbps) - Operates in the 2.4 GHz range, and offers a rate of 54 Mbps (in theory). Compatible with 802.11b. • Turbo G (108 Mbps) - Operates in the 2.4 GHz range, and offers a rate of 54 Mbps (in theory). Compatible with 802.11b and 802.11g. Each operation mode indicates a wireless protocol (such as Turbo G), followed by the maximum bandwidth (such as 108 Mbps). The list of modes is dependent on the selected country. Note: The actual data transfer speed is usually significantly lower than the maximum bandwidth. Important: The client wireless cards must support the selected operation mode.

In this field…	Do this…
Channel	Select the radio frequency to use for the wireless connection: • Automatic - The Safe@Office appliance automatically selects a channel. This is the default. • A specific channel - The list of channels is dependent on the selected country and operation mode. Note: If there is another wireless network in the vicinity, the two networks may interfere with one another. To avoid this problem, the networks should be assigned channels that are at least 25 MHz (5 channels) apart.

In this field…	Do this…
Security	Select the security protocol to use: • None - No security method is used. This option is not recommended, because it allows unauthorized users to access your network. • WEP encryption - In the WEP (Wired Equivalent Privacy) encryption security method, wireless clients must use a pre-shared key to connect to your network. This option is not recommended, due to known security flaws. If you select this option, the WEP Keys area opens, and you must configure at least one WEP key. The wireless clients must be configured with this key as well. • 802.1X: RADIUS authentication, no encryption - In the 802.1x security method, wireless clients (supplicants) attempting to connect to the access point (authenticator) must first be authenticated by RADIUS servers (authentication servers). All messages are passed in EAP (Extensible Authentication Protocol). To use this security method, you must configure RADIUS servers. See ***Using RADIUS Authentication.*** on page 252

In this field…	Do this…
	• WPA: RADIUS authentication, encryption - The WPA (Wi-Fi Protected Access) security method uses MIC (message integrity check) to ensure the integrity of messages, and TKIP (Temporal Key Integrity Protocol) to enhance data encryption. Furthermore, WPA includes 802.1x and EAP authentication, based on a central RADIUS authentication server. To use this security method, you must configure RADIUS servers. See ***Using RADIUS Authentication.*** on page 252 • WPA-PSK: password authentication, encryption - The WPA-PSK security mode is a variation of WPA that does not require an authentication server. WPA-PSK periodically changes and authenticates encryption keys. This is called *rekeying*. If you select this option, the Passphrase field appears. The wireless clients must be configured with this passphrase as well.
Passphrase	Type the passphrase for accessing the network. This must be between 8 and 63 characters. It can contain spaces and special characters, and is case-sensitive.
Show/Hide Advanced Settings	Click to show/hide advanced WLAN settings. The Advanced Security and Wireless Transmitter areas are displayed.

In this field…	Do this…
WEP Keys	
Key 1, 2, 3, 4 radio button	Click the radio button next to the desired WEP key.
64 Bits:10x[0-9, A-F]	Select the WEP key length from the drop-down list. The possible key lengths are: • 64 Bits - The key length is 10 characters. • 128 Bits - The key length is 26 characters. • 152 Bits - The key length is 32 characters. Note: Some wireless card vendors call these lengths 40/104/128, respectively.
Key 1, 2, 3, 4 text box	Type the WEP key, or click Random to randomly generate a key matching the selected length. The key is composed of characters 0-9 and A-F, and is not case-sensitive.

In this field…	Do this…
Advanced Security	
Hide the Network Name (SSID)	Specify whether you want to hide your network's SSID, by selecting one of the following: • Yes - Hide the SSID. Only devices to which your SSID is known can connect to your network. • No - Do not hide the SSID. Any device within within range can detect your network name using the wireless network discovery features of some products, such as Microsoft Windows XP, and attempt to connect to your network. This is the default. Note: Hiding the SSID does not provide strong security, because your SSID can still be discovered using specialized test equipment such as wireless sniffers. Therefore, it is not recommended to rely on this setting alone for security.

In this field…	Do this…
MAC Address filtering	Specify whether you want to enable MAC address filtering, by selecting one of the following: • Yes - Enable MAC address filtering. Only MAC addresses that you added as network objects can connect to your network. For information on network objects, see ***Using Network Objects*** on page 129. • No - Disable MAC address filtering. This is the default. Note: MAC address filtering does not provide strong security, therefore it is not recommended to rely on this setting alone for security.
Wireless Transmitter	
Transmission Rate	Select the transmission rate: • Automatic - The Safe@Office appliance automatically selects a rate. This is the default. • A specific rate
Transmitter Power	Select the transmitter power. Setting a higher transmitter power increases the access point's range. A lower power reduces interference with other access points in the vicinity. The default value is Full, providing a maximum range of 300m, under ideal outdoor conditions. It is not necessary to change this value, unless there are other access points in the vicinity.

In this field…	Do this…
Fragmentation Threshold	Type the smallest IP packet size (in bytes) that requires that the IP packet be split into smaller fragments. If you are experiencing significant radio interference, set the threshold to a low value (around 1000), to reduce error penalty and increase overall throughput. Otherwise, set the threshold to a high value (around 2000), to reduce overhead. The default value is 2346.
RTS Threshold	Type the smallest IP packet size for which a client must send an RTS (Request To Send) before sending the IP packet. If multiple wireless clients are in range of the access point, but not in range of each other, they might send data to the access point simultaneously, thereby causing data collisions and failures. RTS ensures that the channel is clear before the each packet is sent. If your network is congested, and the users are distant from one another, set the RTS threshold to a low value (around 500). Setting a value equal to the fragmentation threshold effectively disables RTS. The default value is 2346.

Configuring High Availability

You can install two Safe@Office 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 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 93.
- 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.

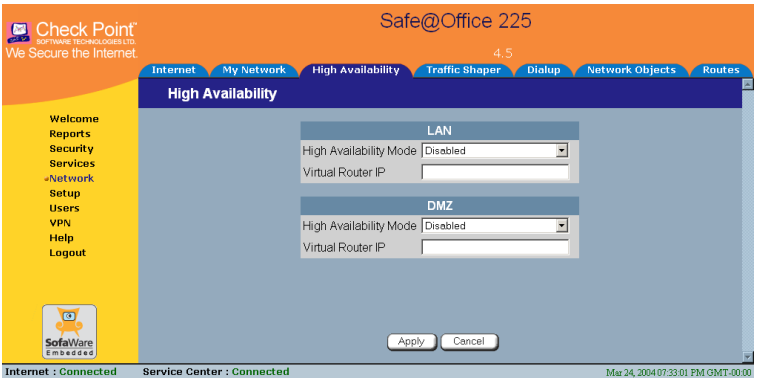
      For further information, see ***Changing IP Addresses*** on page 100.

   b. Configure the LAN network range.

      For further information, see ***Changing IP Addresses*** on page 100.

   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 Master.

e. In the Virtual Router IP field, 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 100.

      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 100.

   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 field, 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 Traffic Shaper

Traffic Shaper is a bandwidth management solution that allows you to set bandwidth policies to control the flow of communication. Traffic Shaper ensures that important traffic takes precedence over less important traffic, so that your business can continue to function with minimum disruption, despite network congestion.

Traffic Shaper uses Stateful Inspection technology to access and analyze data derived from all communication layers. This data is used to classify traffic in up to eight user-defined Quality of Service (QoS) classes. Traffic Shaper divides available bandwidth among the classes according to weight. For example, suppose Web traffic is deemed three times as important as FTP traffic, and these services are assigned weights of 30 and 10 respectively. If the lines are congested, Traffic Shaper will maintain the ratio of bandwidth allocated to Web traffic and FTP traffic at 3:1.

If a specific class is not using all of its bandwidth, the leftover bandwidth is divided among the remaining classes, in accordance with their relative weights. In the example above, if only one Web and one FTP connection are active and they are competing, the Web connection will receive 75% (30/40) of the leftover bandwidth, and the FTP connection will receive 25% (10/40) of the leftover bandwidth. If the Web connection closes, the FTP connection will receive 100% of the bandwidth.

Traffic Shaper allows you to give a class a bandwidth limit. A class's bandwidth limit is the maximum amount of bandwidth that connections belonging to that class may use together. Once a class has reached its bandwidth limit, connections belonging to that class will not be allocated further bandwidth, even if there is unused bandwidth available. For example, you can limit all traffic used by Peer-To-Peer file-sharing applications to a specific rate, such as 512 kilobit per second. Traffic Shaper also allows you to assign a "Delay Sensitivity" value to a class, indicating whether connections belonging to the class should be given precedence over connections belonging to other classes.

Traffic Shaper supports DiffServ (Differentiated Services) Packet Marking. DiffServ marks packets as belonging to a certain Quality of Service class. These packets are then granted priority on the public network according to their class.

To use Traffic Shaper

1. Enable Traffic Shaper for the Internet connection.

   You can enable Traffic Shaper for incoming or outgoing connections.

   See ***Using Internet Setup*** on page 66.

2. Define QoS classes that reflect your communication needs. Alternatively, use the four built-in QoS classes.

   See ***Adding and Editing a Class*** on page 122.

3. Use Allow rules to assign different types of connections to QoS classes.

   For example, if Traffic Shaper is enabled for outgoing traffic, and you create an Allow rule associating all outgoing VPN traffic with the Urgent QoS class, then Traffic Shaper will handle outgoing VPN traffic as specified in the bandwidth policy for the Urgent class.

   See ***Adding and Editing Rules*** on page 157.

Note: Traffic Shaper must be enabled for the direction of traffic specified in the rule.

Note: If you do not assign a connection type to a class, Traffic Shaper automatically assigns the connection type to the built-in "Default" class.

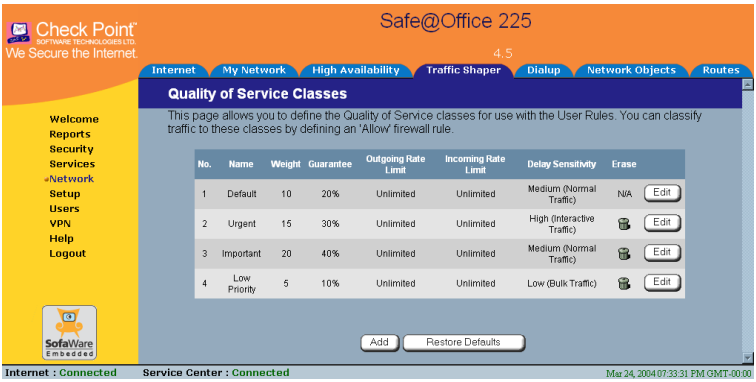
Adding and Editing a Class

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

To add or edit a QoS class

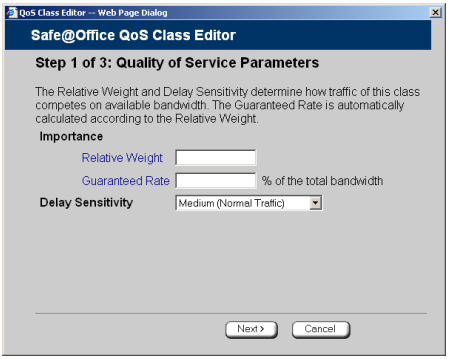
1. Click **Network** in the main menu, and click the **Traffic Shaper** tab.

   The **Quality of Service Classes** page appears.



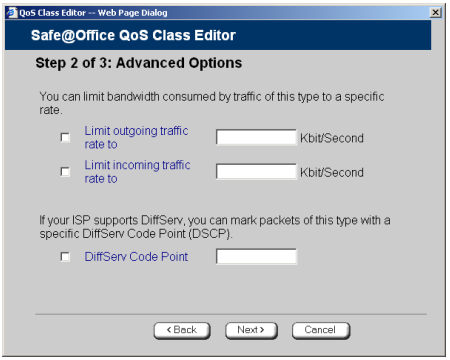
2. Click **Add**.

The Safe@Office QoS Class Editor wizard opens, with the Step 1 of 3: Quality of Service Parameters dialog box displayed.



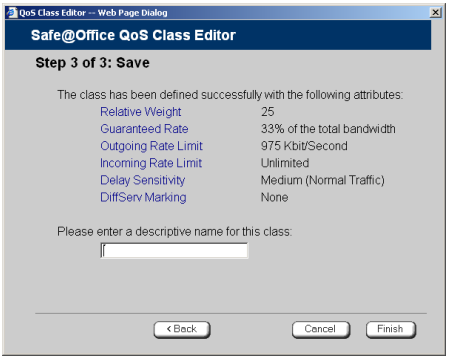
3. Complete the fields using the relevant information in the table below.
4. Click Next.

   The Step 2 of 3: Advanced Options dialog box appears.



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

The Step 3 of 3: Save dialog box appears with a summary of the class.



7. Type a name for the class.

   For example, if you are creating a class for high priority Web connections, you can name the class "High Priority Web".

8. Click Finish.

   The new class appears in the Quality of Service Classes page.

Table 16: QoS Class Fields

In this field...	Do this...
Relative Weight	Type a value indicating the class's importance relative to the other defined classes. For example, if you assign one class a weight of 100, and you assign another class a weight of 50, the first class will be allocated twice the amount of bandwidth as the second when the lines are congested. When you complete this field, the Guaranteed Rate field is filled in automatically.

In this field…	Do this…
Guaranteed Rate	The percentage of bandwidth that the class is guaranteed, out of the total amount of bandwidth. For example, if there are only two classes, and you assign one class a weight of 100 and the other class a weight of 50, the first class's guaranteed rate will be 66% and the second class's guaranteed rate will be 33%. This field is read-only and is shown for informational purposes. Note: Traffic Shaper may not enforce guaranteed rates and relative weights for incoming traffic as accurately as for outgoing traffic. This is because Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping received packets. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary. For information on enabling Traffic Shaper for incoming and outgoing traffic, see ***Using Internet Setup*** on page 66.

In this field...	Do this...
Delay Sensitivity	Select the degree of precedence to give this class in the transmission queue: • Low (Bulk Traffic) - Traffic that is not sensitive to long delays. For example, SMTP traffic (outgoing email). • Medium (Normal Traffic) - Normal traffic • High (Interactive Traffic) - Traffic that is highly sensitive to delay. For example, IP telephony, videoconferencing, and interactive protocols that require quick user response, such as telnet. Traffic Shaper serves delay-sensitive traffic with a lower latency. That is, Traffic Shaper attempts to send packets with a "High (Interactive Traffic)" level before packets with a "Medium (Normal Traffic)" or "Low (Bulk Traffic)" level.
Limit outgoing traffic rate to	Select this option to limit the rate of outgoing traffic belonging to this class. Then type the maximum rate (in kilobits/second) in the field provided.
Limit incoming traffic rate to	Select this option to limit the rate of incoming traffic belonging to this class. Then type the maximum rate (in kilobits/second) in the field provided.

In this field…	Do this…
DiffServ Code Point	Select this option to mark packets belonging to this class with a DiffServ Code Point (DSCP), which is an integer between 0 and 63. Then type the DSCP in the field provided. The marked packets will be given priority on the public network according to their DSCP. To use this option, your ISP or private WAN must support DiffServ. You can obtain the correct DSCP value from your ISP or private WAN administrator.

Deleting Classes

You cannot delete a class that is currently used by a rule. You can determine whether a class is in use or not, by viewing the Rules page.

To delete an existing QoS class

1. Click Network in the main menu, and click the Traffic Shaper tab.

   The Quality of Service Classes page appears.

2. Click the  icon of the class you wish to delete.

   A confirmation message appears.

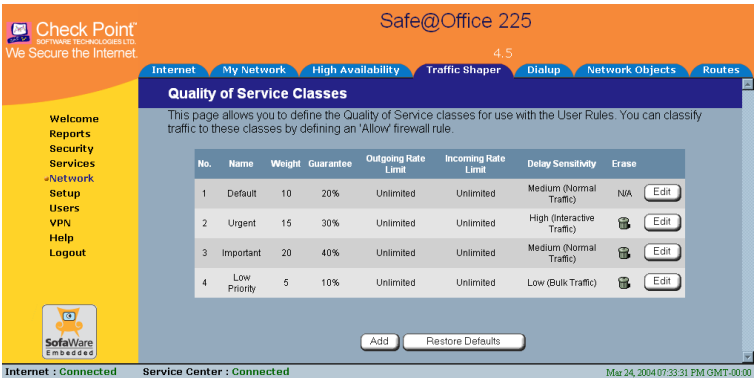
3. Click OK.

   The class is deleted.

Restoring Traffic Shaper Defaults

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

The Safe@Office appliance provides four built-in QoS classes:



If desired, you can reset the Traffic Shaper bandwidth policy to use these classes, and restore the classes to their default settings (shown above).

Note: This will delete any additional classes you defined in Traffic Shaper and reset all rules to use the Default class.

If one of the additional classes is currently used by a rule, you cannot reset Traffic Shaper to defaults. You can determine whether a class is in use or not, by viewing the Rules page.

To restore Traffic Shaper defaults

1. Click Network in the main menu, and click the Traffic Shaper tab.

   The Quality of Service Classes page appears.

2. Click Restore Defaults.

   A confirmation message appears.

3. Click OK.

Using Network Objects

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

You can add individual computers or networks as network objects. This enables you to configure various settings for the computer or network represented by the network object.

You can configure the following settings for a network object:

- Static NAT (or One-to-One NAT)

  Static 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 ***Using Rules*** on page 154.

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.

- Assign the network object's IP address to a MAC address

  Normally, the Safe@Office DHCP server consistently assigns the same IP address to a specific computer. However, if the Safe@Office DHCP server runs out of IP addresses and the computer is down, then the DHCP server may reassign the IP address to a different computer.

  If you want to guarantee that a particular computer's IP address remains constant, you can reserve the IP address for use by the computer's MAC address only. This is called *DHCP reservation*, and it is useful if you are hosting a public Internet server on your network.

- Exclude the network object from SecureDesk enforcement

  If you are subscribed to SecureDesk, you can choose to disable SecureDesk for a specific computer or network. For example, you might want to disable SecureDesk for a printer with an IP address, or for a computer with an operating system that VirusScan does not support.

  If you disable SecureDesk for a computer or network, the firewall will allow access from that computer or network, regardless of whether the installed antivirus software complies with the SecureDesk security level conditions.

Note: To disable SecureDesk for all computers, set the security level to Off. For instructions on setting the security level, see ***Setting the SecureDesk Security Level*** on page 186.

For information on SecureDesk, see ***Using SecureDesk*** on page 183.

Adding and Editing Network Objects

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

You can add or edit network objects via:

- The Network Objects page

  This page enables you to add both individual computers and networks.

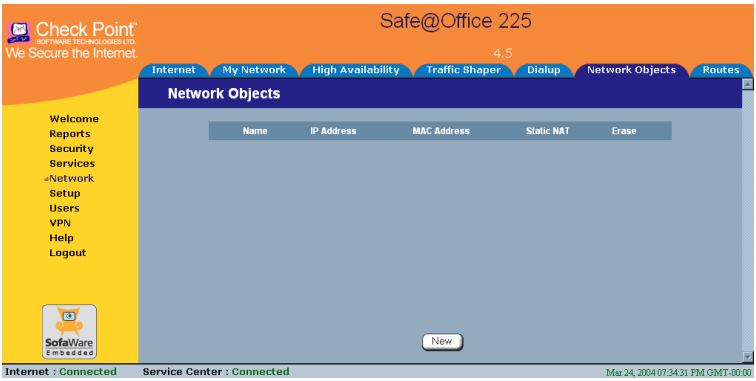
- The Active Computers page

  This page enables you to add only individual computers as network objects. The computer's details are filled in automatically in the wizard.

To add or edit a network object via the Network Objects page

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

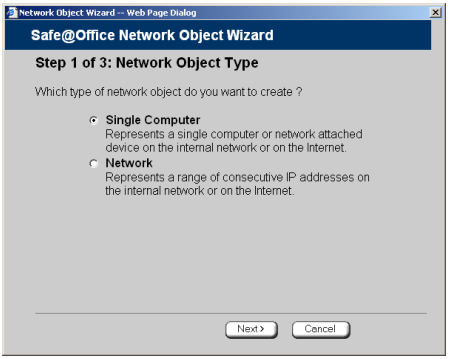
   The Network Objects page appears with a list of network objects.



2. Do one of the following:

   - To add a network object, click New.
   - To edit an existing network object, click Edit next to the desired computer in the list.

The Safe@Office Network Object Wizard opens, with the Step 1: Network Object Type dialog box displayed.

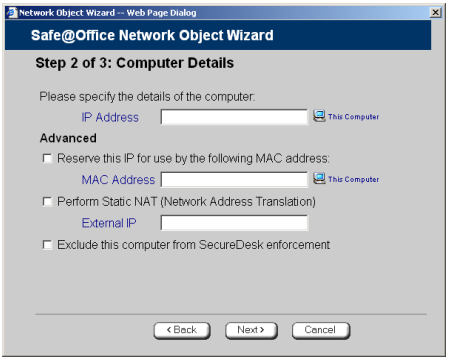


3. Do one of the following:

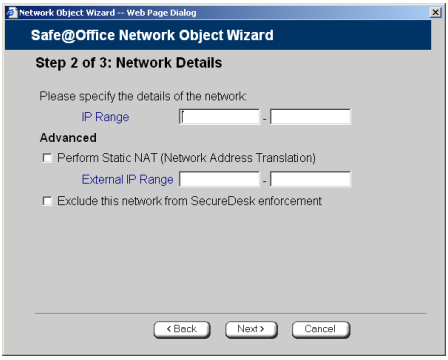
   - To specify that the network object should represent a single computer or device, click Single Computer.
   - To specify that the network object should represent a network, click Network.

4. Click Next.

   The Step 2: Computer Details dialog box appears. If you chose Single Computer, the dialog box includes the Perform Static NAT option.

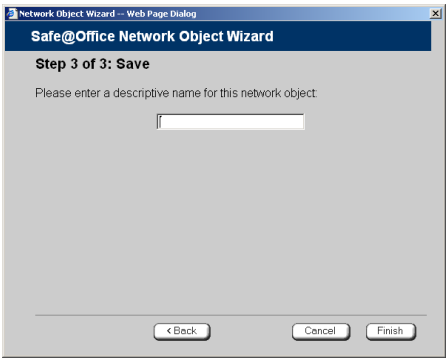


If you chose Network, the dialog box does not include this option.



5. Complete the fields using the information in the tables below.
6. Click Next.

   The Step 3: Save dialog box appears.

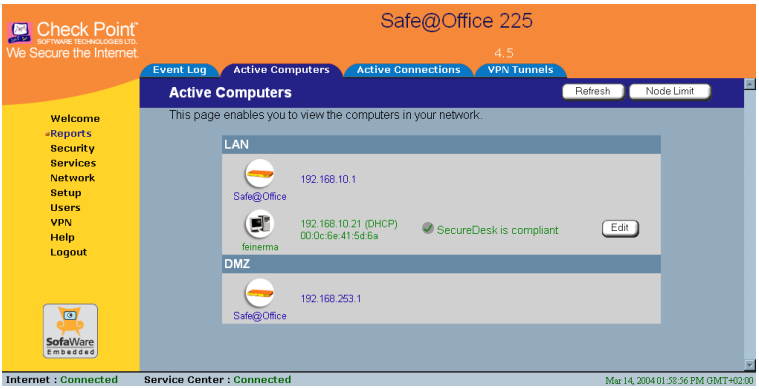


7. Type a name for the network object in the field.
8. Click Finish.

To add or edit a network object via the Active Computers page

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

The Active Computers page appears.



If a computer has not yet been added as a network object, the Add button appears next to it. If a computer has already been added as a network object, the Edit button appears next to it.

2. Do one of the following:

   - To add a network object, click Add next to the desired computer.
   - To edit a network object, click Edit next to the desired computer.

   The Safe@Office Network Object Wizard opens, with the Step 2: Computer Details dialog box displayed.

   The computer's IP address and MAC address are automatically filled in.

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

   The Step 3: Save dialog box appears with the network object's name. If you are adding a new network object, this name is the computer's name.

5. To change the network object name, type the desired name in the field.
6. Click Finish.

   The new object appears in the Network Objects page.

Table 17: Network Object Fields for a Single Computer

In this field...	Do this...
IP Address	Type the IP address of the local computer, or click This Computer to specify your computer.
Reserve this IP for use by the following MAC address	Select this option to assign the network object's IP address to a MAC address.
MAC Address	Type the MAC address you want to assign to the network object's IP address, or click This Computer to specify your computer's MAC address.
Perform Static NAT (Network Address Translation)	Select this option to map the local computer's IP address to an Internet IP address. You must then fill in the External IP field.
External IP	Type the Internet IP address to which you want to map the local computer's IP address.
Exclude this computer from SecureDesk enforcement	Select this option to disable SecureDesk for the computer. For information on SecureDesk, see ***Using SecureDesk*** on page 183.

Table 18: Network Object Fields for a Network

In this field...	Do this...
IP Range	Type the range of local computer IP addresses in the network.
Perform Static NAT (Network Address Translation)	Select this option to map the network's IP address range to a range of Internet IP addresses of the same size. You must then fill in the External IP Range field.
External IP Range	Type the Internet IP address range to which you want to map the network's IP address range.
Exclude this network from SecureDesk enforcement	Select this option to disable SecureDesk for the network. For information on SecureDesk, see ***Using SecureDesk*** on page 183.

Viewing and Deleting Network Objects

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

To view or delete a network object

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

   The Network Objects page appears with a list of network objects.

2. To delete a network object, do the following:

   a. In the desired network object's row, click the Delete icon.

A confirmation message appears.

b. Click OK.

The network object 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 68.

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

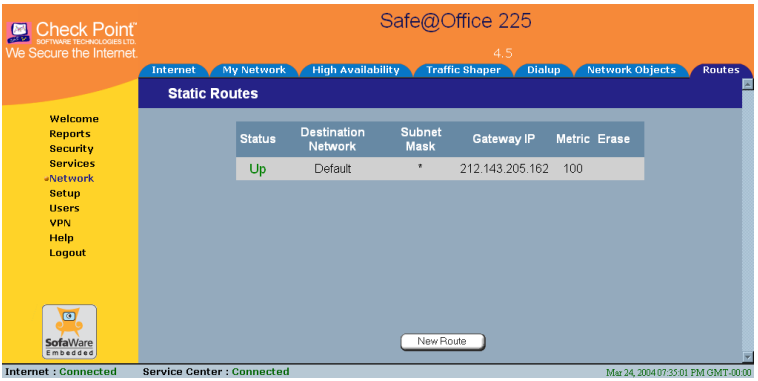
Adding a Static Route

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

To add a static route

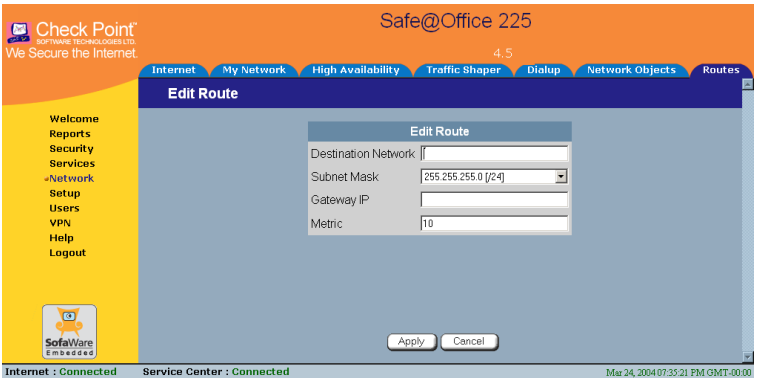
1. Click Network in the main menu, and click the Routes tab.

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



2. Click **New Route**.

   The **Edit Route** page appears.



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

   The new static route is saved.

Table 19: 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.
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

To edit a static route

1. Click Network in the main menu, and click the 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 139.