c. Click **Apply**.

The changes are saved.

Deleting a Static Route

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

Note: The “default” route cannot be deleted.

To delete a static route

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

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

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

   A confirmation message appears.

3. Click **OK**.

   The route is deleted.

Chapter 6

Viewing Reports

This chapter describes the Safe@Office Portal reports.

This chapter includes the following topics:

Viewing the Event Log

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

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

Table 20: Event Log Color Coding

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

An event marked in this color…	Indicates…
Green	Traffic accepted by the firewall. By default, accepted traffic is not logged. However, such traffic may be logged if specified by a security policy downloaded from your Service Center.

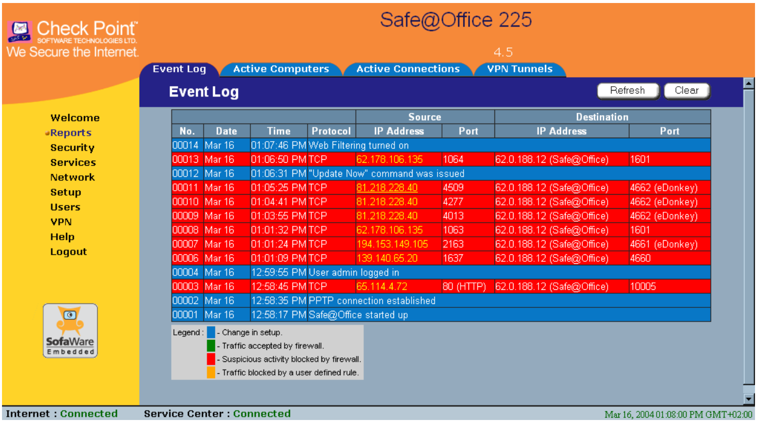
The logs detail the date and the time the event occurred, and its type. If the event is a communication attempt that was rejected by the firewall, the event details include the source and destination IP address, the destination port, and the protocol used for the communication attempt (for example, TCP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

Note: You can configure the Safe@Office appliance to send event logs to a Syslog server. For information, see ***Configuring Syslog Logging*** on page 263.

To view the event log

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

  The **Event Log** page appears.



				Source		Destination	
No.	Date	Time	Protocol	IP Address	Port	IP Address	Port
00014	Mar 16	01:07:46 PM	Web Filtering turned on				
00013	Mar 16	01:06:50 PM	TCP	62.178.106.135	1064	62.0.188.12 (Safe@Office)	1601
00012	Mar 16	01:06:31 PM	"Update Now" command was issued				
00011	Mar 16	01:05:25 PM	TCP	81.218.228.40	4509	62.0.188.12 (Safe@Office)	4662 (eDonkey)
00010	Mar 16	01:04:41 PM	TCP	81.218.228.40	4277	62.0.188.12 (Safe@Office)	4662 (eDonkey)
00009	Mar 16	01:03:55 PM	TCP	81.218.228.40	4013	62.0.188.12 (Safe@Office)	4662 (eDonkey)
00008	Mar 16	01:01:32 PM	TCP	62.178.106.135	1063	62.0.188.12 (Safe@Office)	1601
00007	Mar 16	01:01:24 PM	TCP	194.153.149.105	2163	62.0.188.12 (Safe@Office)	4661 (eDonkey)
00006	Mar 16	01:01:09 PM	TCP	139.140.65.20	1637	62.0.188.12 (Safe@Office)	4660
00004	Mar 16	12:59:55 PM	User admin logged in				
00003	Mar 16	12:58:45 PM	TCP	65.114.4.72	80 (HTTP)	62.0.188.12 (Safe@Office)	10005
00002	Mar 16	12:58:35 PM	PPTP connection established				
00001	Mar 16	12:58:17 PM	Safe@Office started up				

Legend : 🟦 - Change in setup.
🟩 - Traffic accepted by firewall.
🟥 - Suspicious activity blocked by firewall.
🟧 - Traffic blocked by a user defined rule.

Internet : Connected Service Center : Connected Mar 16, 2004 01:08:00 PM GMT+02:00

You can do any of the following:

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

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

Viewing Computers

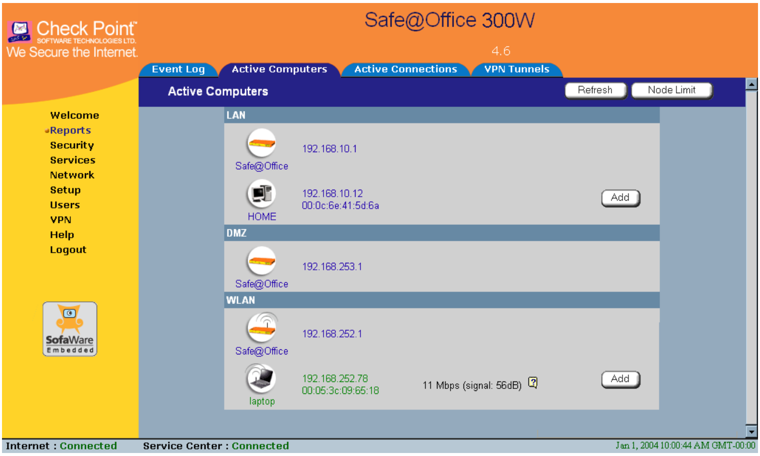
Safe@Office 105 | Safe@Office 110 | Safe@Office 225

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

To view the active computers

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

   The **Active Computers** page appears.



LAN

Safe@Office 192.168.10.1

HOME 192.168.10.12 00:0c:6e:41:5d:6a

DMZ

Safe@Office 192.168.253.1

WLAN

Safe@Office 192.168.252.1

laptop 192.168.252.78 00:05:3c:09:65:18 11 Mbps (signal: 56dB)

Internet : Connected Service Center : Connected Jan 1, 2004 10:00:44 AM GMT-00:00

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

   If you are using Safe@Office 300W, the following is displayed next to wireless computers:

   - Transmission rate in Mbps

- Signal strength in dB
- An information icon - You can mouse-over this icon to see the following statistics:

  Frames OK - The total number of frames that were successfully transmitted and received

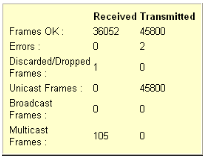
  Errors - The total number of transmitted and received frames for which an error occurred

  Discarded/Dropped Frames - The total number of discarded or dropped frames transmitted and received

  Unicast Frames - The number of unicast frames transmitted and received

  Broadcast Frames - The number of broadcast frames transmitted and received

  Multicast Frames - The number of multicast frames transmitted and received



	Received	**Transmitted**
Frames OK :	36052	45800
Errors :	0	2
Discarded/Dropped Frames :	1	0
Unicast Frames :	0	45800
Broadcast Frames :	0	0
Multicast Frames :	105	0

If you are subscribed to SecureDesk, a status message next to each computer indicates whether the computer complies with the SecureDesk security level conditions. For information on SecureDesk, see ***Using SecureDesk*** on page 183. For an explanation of the status messages, see ***SecureDesk Status Messages*** on page 191.

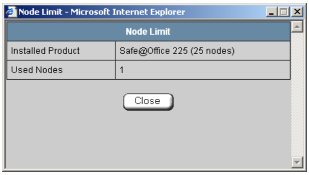
If you are exceeding the maximum number of computers allowed by your license, a warning message appears, and the computers over the node limit are marked in red. These computers are still protected, but they are blocked from accessing the Internet through the Safe@Office appliance.

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

Note: To increase the number of computers allowed by your license, you must upgrade your product. For further information, see ***Upgrading Your Software Product*** on page 258.

2. To refresh the display, click Refresh.
3. To view node limit information, do the following:
   a. Click Node Limit.

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

Node Limit	
Installed Product	Safe@Office 225 (25 nodes)
Used Nodes	1

   b. Click Close to close the window.

Viewing Connections

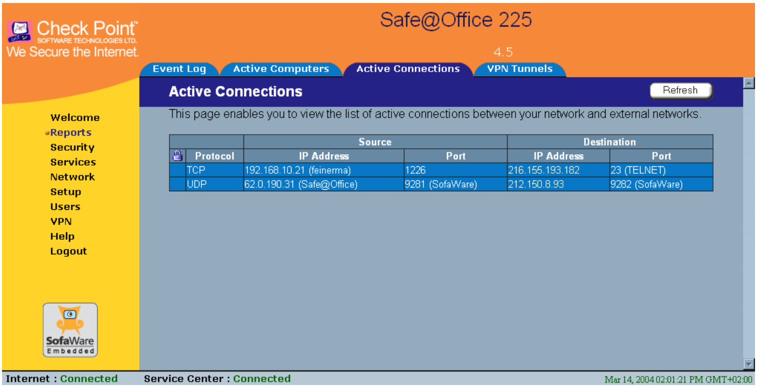
Safe@Office 105 | Safe@Office 110 | Safe@Office 225

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

To view the active connections

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

  The **Active Connections** page appears.



Active Connections

This page enables you to view the list of active connections between your network and external networks.

		Source		Destination	
🔒	Protocol	IP Address	Port	IP Address	Port
	TCP	192.168.10.21 (feinerma)	1226	216.155.193.182	23 (TELNET)
	UDP	62.0.190.31 (Safe@Office)	9281 (SofaWare)	212.150.8.93	9282 (SofaWare)

Internet : Connected Service Center : Connected Mar 14, 2004 02:01:21 PM GMT+02:00

You can do the following:

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

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

Chapter 7

Setting Your Security Policy

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

You can enhance your security policy by subscribing to services such as Web Filtering and Email Antivirus scanning. You can also subscribe to SecureDesk, which includes and enforces the use of McAfee VirusScan ASaP Web-based antivirus service.

For information on subscribing to services and SecureDesk, see ***Using Subscription Services*** on page 165.

This chapter includes the following topics:

Setting the Firewall Security Level

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

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

Table 21: Firewall Security Levels

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

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

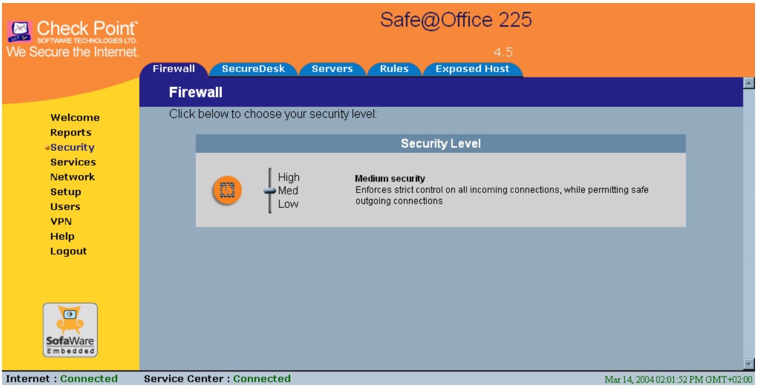
Note: If the security policy is remotely managed, this lever might be disabled.

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

To change the firewall security level

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

   The **Firewall** page appears.



Firewall

Click below to choose your security level:

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

Internet : Connected   Service Center : Connected   Mar 14, 2004 02:01:52 PM GMT+02:00

2. Drag the security lever to the desired level.

   The Safe@Office appliance security level changes accordingly.

Configuring Servers

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

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

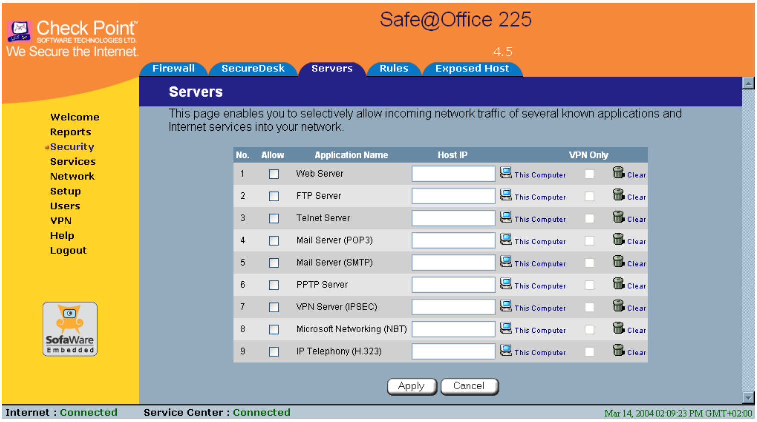
Using the Safe@Office Portal, you can selectively allow incoming network connections into your network. For example, you can set up your own Web server, Mail server or FTP server.

Note: Configuring servers allows you to create simple Allow and Forward rules for common services, and it is equivalent to creating Allow and Forward rules in the Rules page. For information on creating rules, see ***Using Rules*** on page 154.

To allow a service to be run on a specific host

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

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



Servers

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

No.	Allow	Application Name	Host IP		VPN Only	
1	□	Web Server		This Computer	□	Clear
2	□	FTP Server		This Computer	□	Clear
3	□	Telnet Server		This Computer	□	Clear
4	□	Mail Server (POP3)		This Computer	□	Clear
5	□	Mail Server (SMTP)		This Computer	□	Clear
6	□	PPTP Server		This Computer	□	Clear
7	□	VPN Server (IPSEC)		This Computer	□	Clear
8	□	Microsoft Networking (NBT)		This Computer	□	Clear
9	□	IP Telephony (H.323)		This Computer	□	Clear

Internet : Connected Service Center : Connected Mar 14, 2004 02:09:23 PM GMT+02:00

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

3. Click Apply.

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

Table 22: Servers Page Fields

In this column…	Do this…
Allow	Select the desired service or application.

In this column…	Do this…
VPN Only	Select this option to allow only connections made through a VPN.
Host IP	Type the IP address of the computer that will run the service (one of your network computers) or click the corresponding This Computer button to allow your computer to host the service.

To stop the forwarding of a service to a specific host

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

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

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

   The Host IP field of the desired service is cleared.

3. Click Apply.

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

Using Rules

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

The Safe@Office appliance checks the protocol used, the ports range, and the destination IP address, when deciding whether to allow or block traffic. By default, in the Medium security level, the Safe@Office appliance blocks all connection attempts from the Internet (WAN) to the LAN, and allows all outgoing connection attempts from the LAN to the Internet (WAN).

User-defined rules have priority over the default rules and provide you with greater flexibility in defining and customizing your security policy.

The following rule types exist:

Table 23: Firewall Rule Types

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

Rule	Description
Allow	This rule type enables you to do the following: • Permit outgoing access from your internal network to a specific service on the Internet. Note: You can allow outgoing connections for services that are not permitted by the default security policy. • Permit incoming access from the Internet to a specific service in your internal network. • Assign traffic to a QoS class. If Traffic Shaper is enabled for the direction of traffic specified in the rule (incoming or outgoing), then Traffic Shaper will handle relevant connections as specified in the bandwidth policy for the selected QoS class. For example, if Traffic Shaper is enabled for outgoing traffic, and you create an Allow rule associating all outgoing Web traffic with the Urgent QoS class, then Traffic Shaper will handle outgoing Web traffic as specified in the bandwidth policy for the Urgent class. For information on Traffic Shaper and QoS classes, see ***Using Traffic Shaper*** on page 120. This option is only available in Safe@Office 225. Note: You cannot use an Allow rule to permit incoming traffic, if the network or VPN uses Hide NAT. However, you can use Allow rules for static NAT IP addresses.
Block	This rule type enables you to do the following: • Block outgoing access from your internal network to a specific service on the Internet. • Block incoming access from the Internet to a specific service in your internal network.

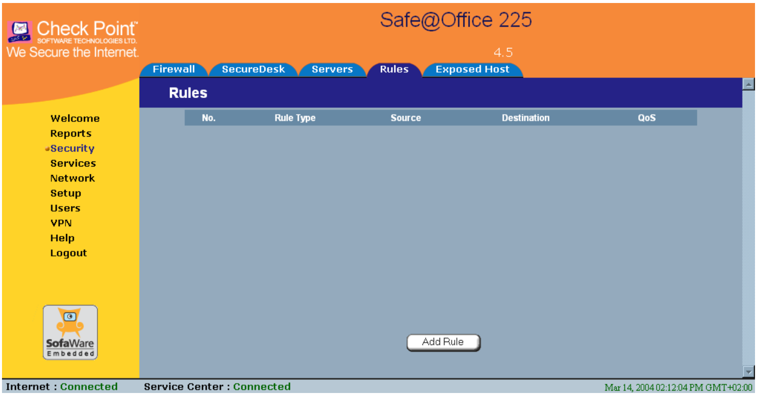
Adding and Editing Rules

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

To add or edit a rule

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

   The **Rules** page appears.

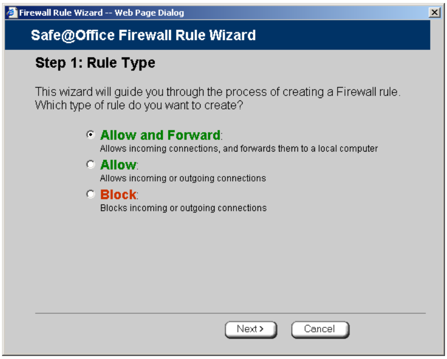
   

   Internet : Connected   Service Center : Connected   Mar 14, 2004 02:12:04 PM GMT+02:00

   If you are using Safe@Office 105 or 110, the **QoS** column does not appear.

2. Click **Add Rule**.

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



Safe@Office Firewall Rule Wizard

Step 1: Rule Type

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

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

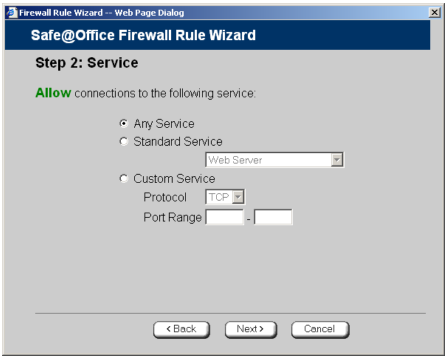
○ Allow:
Allows incoming or outgoing connections

○ Block:
Blocks incoming or outgoing connections

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

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

   The example below shows an Allow rule.



Safe@Office Firewall Rule Wizard

Step 2: Service

Allow connections to the following service:

● Any Service

○ Standard Service

Web Server

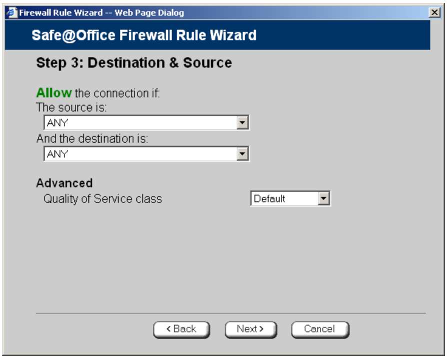
○ Custom Service

Protocol TCP

Port Range -

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

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



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

Step 3: Destination & Source

Allow the connection if:

The source is: ANY

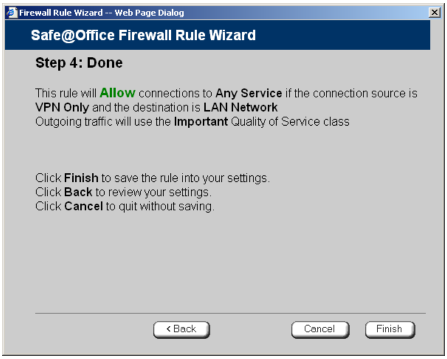
And the destination is: ANY

Advanced

Quality of Service class: Default

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

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



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

Step 4: Done

This rule will **Allow** connections to **Any Service** if the connection source is **VPN Only** and the destination is **LAN Network**
Outgoing traffic will use the **Important** Quality of Service class

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

8. Click **Finish**.

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

Table 24: Firewall Rule Fields

In this field…	Do this…
Any Service	Click this option to specify that the rule should apply to any service.
Standard Service	Click this option to specify that the rule should apply to a specific standard service. You must then select the desired service from the drop-down list.
Custom Service	Click this option to specify that the rule should apply to a specific non-standard service. The Protocol and Port Range fields are enabled. You must fill them in.
Protocol	Select the protocol (ESP, GRE, TCP, UDP or ANY) for which the rule should apply.
Ports	To specify the port range to which the rule applies, type the start port number in the left text box, and the end port number in the right text box. Note: If you do not enter a port range, the rule will apply to all ports. If you enter only one port number, the range will include only that port.

In this field...	Do this...
Source	Select the source of the connections you want to allow/block. To specify an IP address, select Specified IP and type the desired IP address in the filed provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided.
Destination	Select the destination of the connections you want to allow or block. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. This option is not available in Allow and Forward rules.

In this field…	Do this…
Quality of Service Class	Select the QoS class to which you want to assign the specified connections. If Traffic Shaper is enabled, Traffic Shaper will handle these connections as specified in the bandwidth policy for the selected QoS class. If Traffic Shaper is not enabled, this setting is ignored. For information on Traffic Shaper and QoS classes, see ***Using Traffic Shaper*** on page 120. This drop-down list only appears when defining an Allow rule in Safe@Office 225. It contains all QoS classes defined in the portal.
Redirect to port	Select this option to redirect the connections to a specific port. You must then type the desired port in the field provided. This option is called Port Address Translation (PAT), and is only available when defining an Allow and Forward rule.

Deleting Rules

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

To delete an existing rule

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

   The Rules page appears.

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

   A confirmation message appears.

3. Click OK.

   The rule is deleted.

Defining an Exposed Host

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

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

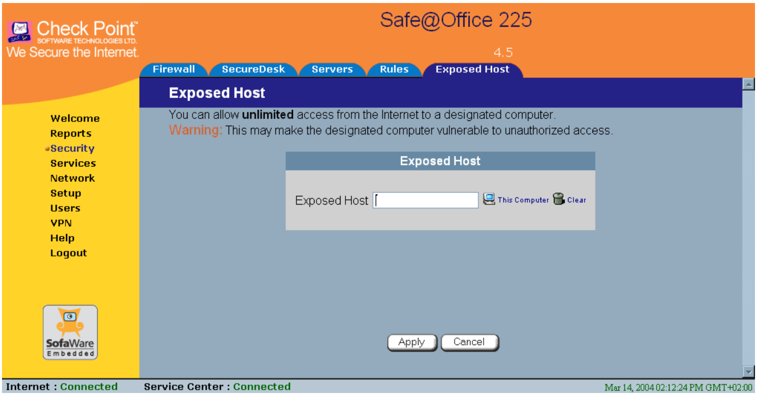
The exposed host receives all traffic that was not forwarded to another computer by use of Allow and Forward rules.

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

To define a computer as an exposed host

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

The Exposed Host page appears.



Exposed Host

You can allow **unlimited** access from the Internet to a designated computer.

Warning: This may make the designated computer vulnerable to unauthorized access.

Exposed Host

Exposed Host [ ]

Internet : Connected Service Center : Connected Mar 14, 2004 02:12:24 PM GMT+02:00

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

   The selected computer is now defined as an exposed host.

Chapter 8

Using Subscription Services

This chapter explains how to start subscription services, and how to use Software Updates, Web Filtering, and Email Antivirus services.

For information on using the SecureDesk service, see ***Using SecureDesk*** on page 183.

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

This chapter includes the following topics:

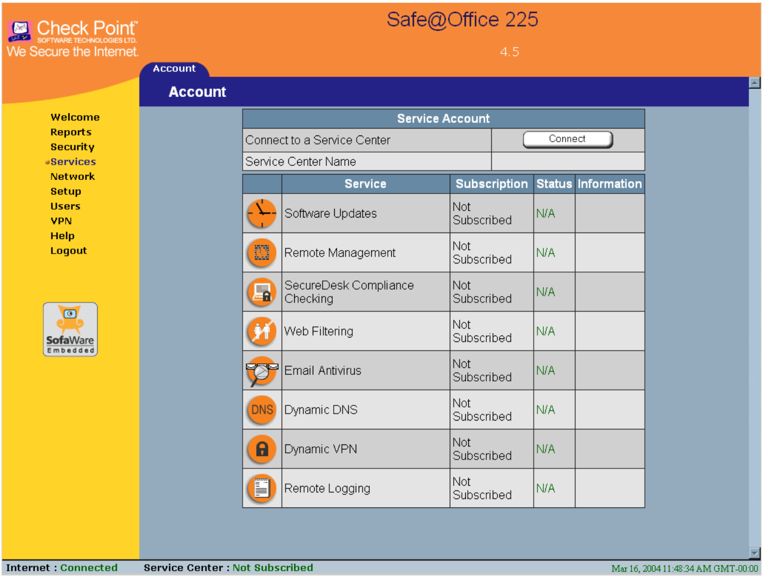
Connecting to a Service Center

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

To connect to a Service Center

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

The **Account** page appears.



Account

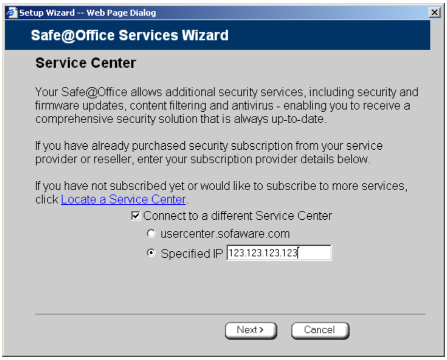
Service Account	
Connect to a Service Center	Connect
Service Center Name	

	Service	Subscription	Status	Information
	Software Updates	Not Subscribed	N/A	
	Remote Management	Not Subscribed	N/A	
	SecureDesk Compliance Checking	Not Subscribed	N/A	
	Web Filtering	Not Subscribed	N/A	
	Email Antivirus	Not Subscribed	N/A	
DNS	Dynamic DNS	Not Subscribed	N/A	
	Dynamic VPN	Not Subscribed	N/A	
	Remote Logging	Not Subscribed	N/A	

Internet : Connected Service Center : Not Subscribed Mar 16, 2004 11:48:34 AM GMT-00:00

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

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



Safe@Office Services Wizard

Service Center

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

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

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

☑ Connect to a different Service Center

○ usercenter.sofaware.com

● Specified IP 123.123.123.123

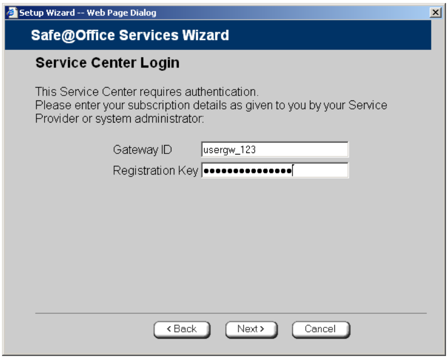
3. Make sure the **Connect to a different Service Center** check box is selected.

4. Do one of the following:

   - To connect to the SofaWare Service Center, select **usercenter.sofaware.com**.
   - To specify a Service Center, select **Specified IP** and then in the **Specified IP** field, enter the desired Service Center's IP address, as given to you by your system administrator.

5. Click **Next**.

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



Service Center Login

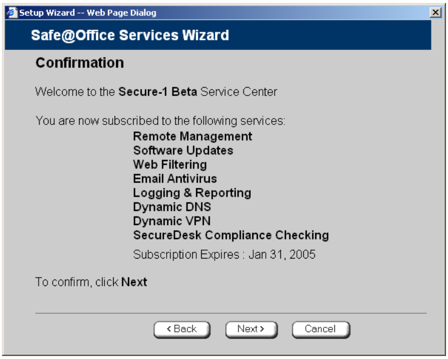
This Service Center requires authentication.
Please enter your subscription details as given to you by your Service Provider or system administrator.

Gateway ID: usergw_123
Registration Key: •••••••••••••••

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

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

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



Confirmation

Welcome to the **Secure-1 Beta** Service Center

You are now subscribed to the following services:

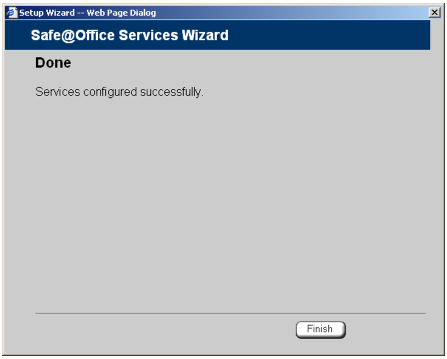
Remote Management
Software Updates
Web Filtering
Email Antivirus
Logging & Reporting
Dynamic DNS
Dynamic VPN
SecureDesk Compliance Checking

Subscription Expires : Jan 31, 2005

To confirm, click **Next**

6. Click **Next**.

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



Done

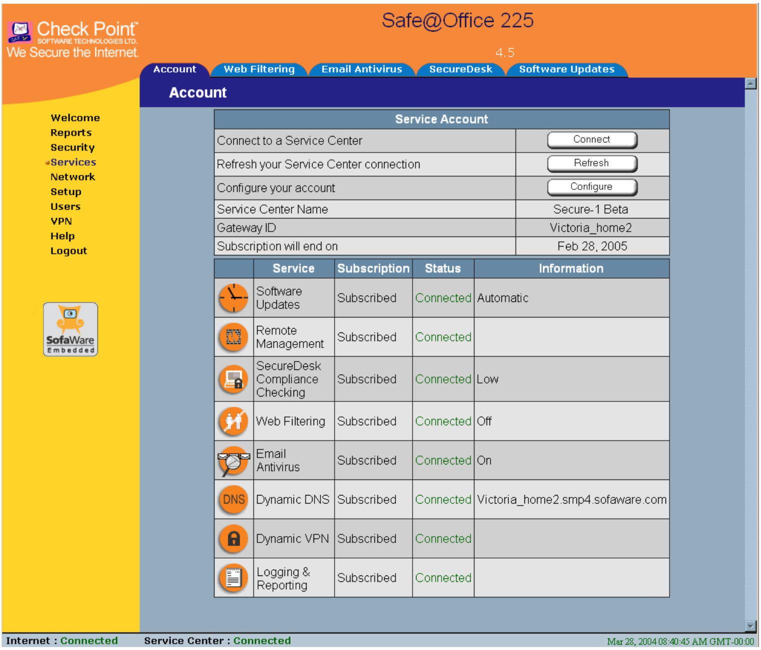
Services configured successfully.

7. Click **Finish**.

   The following things happen:

- If a new firmware is available, the Safe@Office appliance may start downloading it. This may take several minutes. Once the download is complete, the Safe@Office appliance restarts using the new firmware.
- The **Welcome** page appears.

- The services to which you are subscribed are now available on your Safe@Office appliance and listed as such on the Account page. See ***Viewing Services Information*** on page 169 for further information.



Service Account	
Connect to a Service Center	Connect
Refresh your Service Center connection	Refresh
Configure your account	Configure
Service Center Name	Secure-1 Beta
Gateway ID	Victoria_home2
Subscription will end on	Feb 28, 2005

Service	Subscription	Status	Information
Software Updates	Subscribed	Connected	Automatic
Remote Management	Subscribed	Connected	
SecureDesk Compliance Checking	Subscribed	Connected	Low
Web Filtering	Subscribed	Connected	Off
Email Antivirus	Subscribed	Connected	On
Dynamic DNS	Subscribed	Connected	Victoria_home2.smp4.sofaware.com
Dynamic VPN	Subscribed	Connected	
Logging & Reporting	Subscribed	Connected	

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

Viewing Services Information

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

The Account page displays the following information about your subscription.

Table 25: Account Page Fields

This field…	Displays…
Service Center Name	The name of the Service Center to which you are connected (if known).
Gateway ID	Your gateway ID.
Subscription will end on	The date on which your subscription to services will end.
Service	The services available in your service plan.
Subscription	The status of your subscription to each service: • Subscribed • Not Subscribed
Status	The status of each service: • Connected. You are connected to the service through the Service Center. • N/A. The service is not available.
Information	The mode to which each service is set. If you are subscribed to Dynamic DNS, this field displays your gateway's domain name. For further information, see ***Using SecureDesk*** on page 183 , ***Web Filtering*** on page 172, ***Virus Scanning*** on page 175, and ***Automatic and Manual Updates*** on page 179.

Refreshing Your Service Center Connection

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

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

To refresh your Service Center connection

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

   The Account page appears.

2. In the Service Account area, click Refresh.

   The Safe@Office appliance reconnects to the Service Center.

   Your service settings are refreshed.

Configuring Your Account

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

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

To configure your account

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

   The Account page appears.

2. In the Service Account area, click Configure.

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

Your Service Center Web site opens.

3. Follow the on-screen instructions.

Disconnecting from Your Service Center

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

If desired, you can disconnect from your Service Center.

To disconnect from your Service Center

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

   The Account page appears.

2. In the Service Account area, click Connect.

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

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

   The Done screen appears with a success message.

5. Click Finish.

   The following things happen:

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

Web Filtering

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

Note: Web Filtering is only available if you are connected to a Service Center and subscribed to this service.

Enabling/Disabling Web Filtering

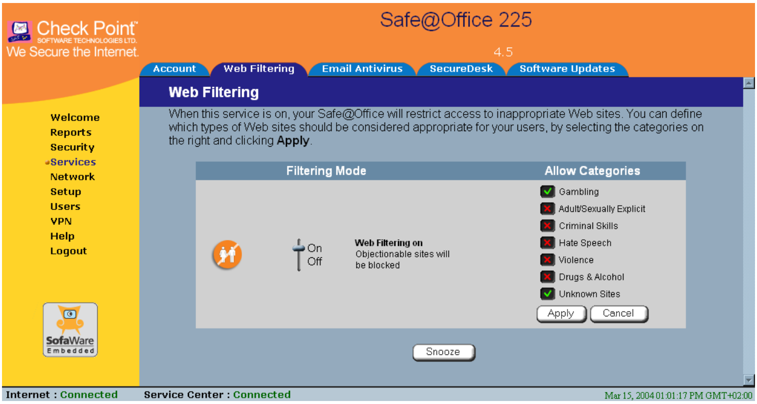
Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

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

To enable/disable Web Filtering

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

   The **Web Filtering** page appears.



Web Filtering

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

Web Filtering on
Objectionable sites will be blocked

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

Internet : Connected   Service Center : Connected   Mar 15, 2004 01:01:17 PM GMT+02:00

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

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

Selecting Categories for Blocking

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

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

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

To allow/block a category

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

Temporarily Disabling Web Filtering

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

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

To temporarily disable Web Filtering

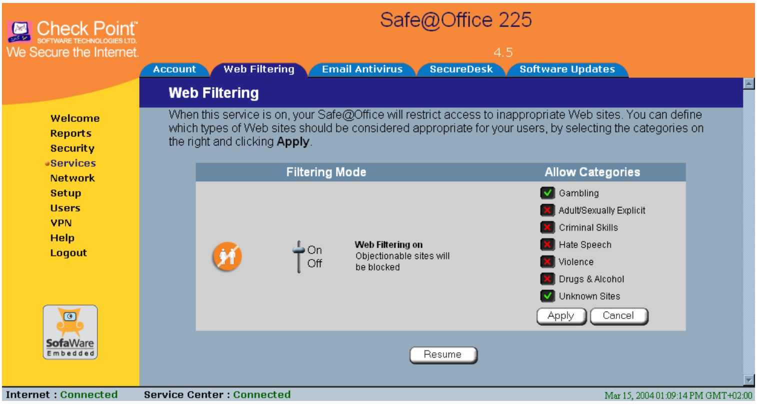
1. Click Services in the main menu, and click the Web Filtering tab.

   The Web Filtering page appears.

2. Click Snooze.

   - Web Filtering is temporarily disabled for all internal network computers.

- The Snooze button changes to Resume.



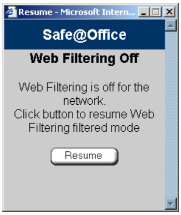
Web Filtering

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

Filtering Mode	Allow Categories
On / Off — **Web Filtering on** Objectionable sites will be blocked	☑ Gambling ☒ Adult/Sexually Explicit ☒ Criminal Skills ☒ Hate Speech ☒ Violence ☒ Drugs & Alcohol ☑ Unknown Sites

Internet : Connected   Service Center : Connected   Mar 15, 2004 01:09:14 PM GMT+02:00

- The Web Filtering Off popup window opens.



Web Filtering Off

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

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

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

Virus Scanning

When the Email Antivirus service is enabled, your email is automatically scanned for the detection and elimination of all known viruses and vandals.

Note: Email Antivirus is only available if you are connected to a Service Center and subscribed to this service.

Enabling/Disabling Email Antivirus

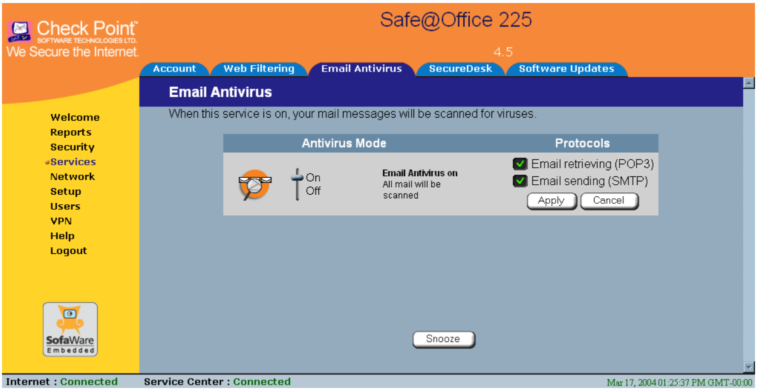
Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

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

To enable/disable Email Antivirus

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

   The **Email Antivirus** page appears.



Email Antivirus

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

Email Antivirus on
All mail will be scanned

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

Internet : Connected   Service Center : Connected   Mar 17, 2004 01:25:37 PM GMT-00:00

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

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

Selecting Protocols for Scanning

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

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

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

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

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

To enable virus scanning for a protocol

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

Temporarily Disabling Email Antivirus

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

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

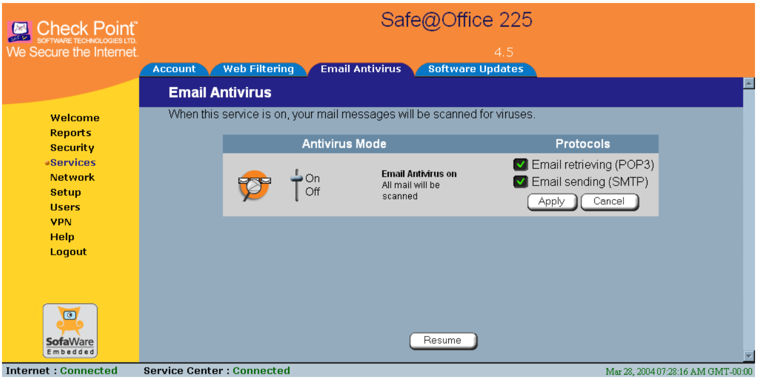
To temporarily disable Email Antivirus

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

   The Email Antivirus page appears.

2. Click **Snooze**.

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



Email Antivirus

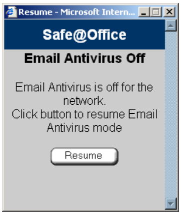
When this service is on, your mail messages will be scanned for viruses.

Antivirus Mode: ○ On ○ Off — Email Antivirus on. All mail will be scanned

Protocols: ☑ Email retrieving (POP3) ☑ Email sending (SMTP)

Internet : Connected Service Center : Connected Mar 28, 2004 07:28:16 AM GMT-00:00

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



Safe@Office

Email Antivirus Off

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

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

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

Automatic and Manual Updates

The Software Updates service enables you to check for new security and software updates.

Note: Software Updates are only available if you are connected to a Service Center and subscribed to this service.

Checking for Software Updates when Locally Managed

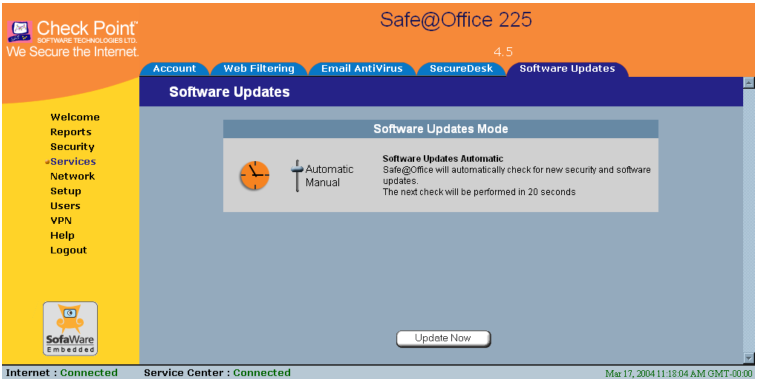
Safe@Office 105 | Safe@Office 110 | Safe@Office 225

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

To configure software updates when locally managed

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

   The **Software Updates** page appears.



Software Updates

Software Updates Mode

Automatic
Manual

Software Updates Automatic
Safe@Office will automatically check for new security and software updates.
The next check will be performed in 20 seconds

Internet : Connected   Service Center : Connected   Mar 17, 2004 11:18:04 AM GMT-00:00

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

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

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

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

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

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

   The system checks for new updates and installs them.

Checking for Software Updates When Remotely Managed

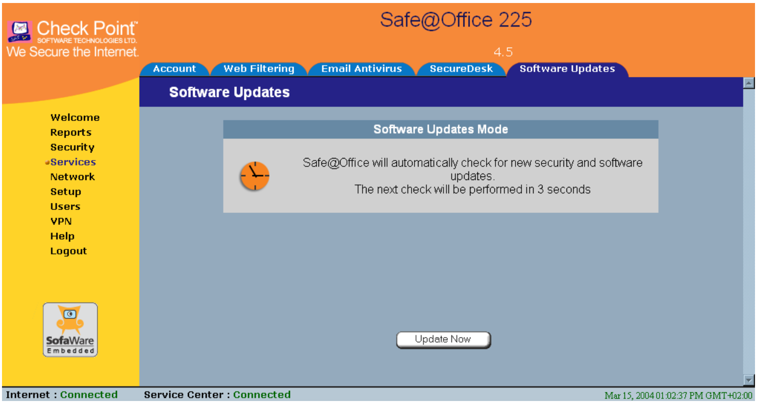
Safe@Office **105** | Safe@Office **110** | Safe@Office **225**

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

To manually check for security and software updates

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

The Software Updates page appears.



Software Updates

Software Updates Mode

Safe@Office will automatically check for new security and software updates.
The next check will be performed in 3 seconds

Internet : Connected Service Center : Connected Mar 15, 2004 01:02:37 PM GMT+02:00

2. Click Update Now.

The system checks for new updates and installs them.

Chapter 9

Using SecureDesk

SecureDesk allows you to make access through the firewall conditional upon the state of a computer's antivirus software. For example, you can configure SecureDesk to allow access for computers on which the antivirus software is enabled but not up-to-date, or to block access for computers on which the antivirus software is up-to-date, but not the most recent build. SecureDesk enables you to quickly and easily install and update antivirus software on all computers in the network simultaneously and reports the status of the antivirus software on each computer.

SecureDesk requires that you install McAfee VirusScan ASaP, a Web-based antivirus service included in the SecureDesk subscription service. SecureDesk monitors the state of the installed VirusScan virus signatures, agent, and engine, and blocks access through the firewall if they do not match the security level set in the Safe@Office Portal. Authorized users can override the block by providing the administrator password via a pop-up window.

If desired, you can 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. To do so you must add the computer or network as a network object. For information on adding network objects and disabling or enabling SecureDesk, see ***Using Network Objects*** on page 129.

Note: SecureDesk is only available if you are connected to a Service Center and subscribed to this service.

This chapter includes the following topics:

Installing McAfee VirusScan ASaP

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

Once you have subscribed to SecureDesk and connected to the Service Center (see ***Connecting to a Service Center*** on page 165), you must install McAfee VirusScan ASaP on all computers in your network.

Note: You must disable the Windows XP "Internet Connection Firewall" option before you install McAfee VirusScan ASaP.

The VirusScan installer automatically uninstalls most antivirus programs before installing VirusScan. For a list of products that the VirusScan installer automatically uninstalls, refer to the *Quick Start Guide*. If your antivirus program does not appear in the list, you must manually uninstall the program before installing VirusScan.

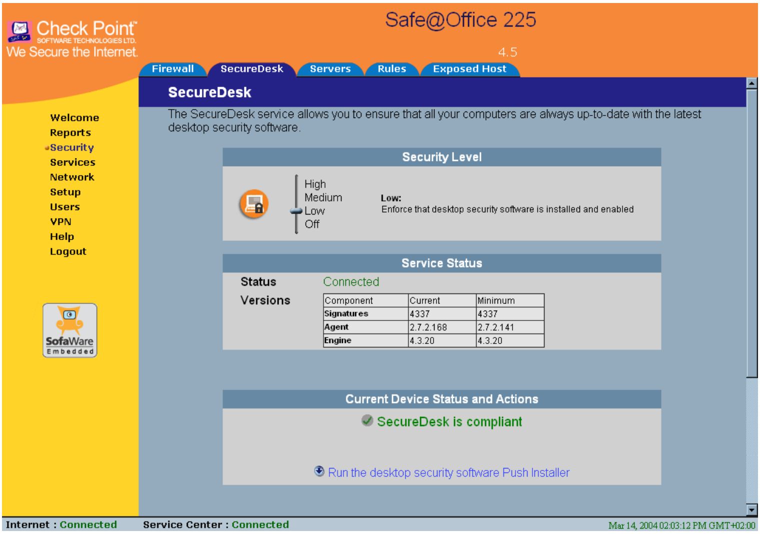
Note: If your current antivirus software is part of a suite of programs, you may have to reinstall the suite without the antivirus component after installing VirusScan.

If VirusScan is already installed on your computer, check whether it complies with the SecureDesk security level conditions using the procedure ***Checking Antivirus Compliancy*** on page 189.

To install McAfee VirusScan ASaP

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

The SecureDesk page appears.



SecureDesk

The SecureDesk service allows you to ensure that all your computers are always up-to-date with the latest desktop security software.

Security Level

High
Medium
Low
Off

Low:
Enforce that desktop security software is installed and enabled

Service Status

Status Connected

Versions

Component	Current	Minimum
Signatures	4337	4337
Agent	2.7.2.168	2.7.2.141
Engine	4.3.20	4.3.20

Current Device Status and Actions

✓ SecureDesk is compliant

Run the desktop security software Push Installer

Internet : Connected Service Center : Connected Mar 14, 2004 02:03:12 PM GMT+02:00

2. Do one of the following:

   - To install VirusScan on this computer only, click Download and install the latest antivirus software.
   - To install VirusScan on all the computers in your network, click Run the desktop security software Push Installer.

   The McAfee Security page opens in a new window, with the McAfee Secure-1 VirusScan ASaP popup window on top.

3. Follow the online instructions to complete installation.

   If antivirus software is already installed, the installer may remove it.

   VirusScan is installed.

For information on troubleshooting installation and using VirusScan, see the User Help. To access VirusScan ASaP User Help, right-click on the VirusScan icon in the taskbar, and select Scan Now > Help.

Updating McAfee VirusScan ASaP on All Computers

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

If the version of VirusScan installed on a computer is not up-to-date, SecureDesk may block access through the firewall for that computer, depending on the SecureDesk security level. You can update the installed version of VirusScan on all computers in the network simultaneously, using the Push Installer.

For information on how to check whether version of VirusScan installed on a computer is up-to-date , see ***Checking Antivirus Compliancy*** on page 189.

To update McAfee VirusScan ASaP on all computers

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

   The SecureDesk page appears.

2. Click Run the desktop security software Push Installer.

   The McAfee Security page opens in a new window, with the McAfee Secure-1 VirusScan ASaP popup window on top.

3. Follow the online instructions to complete updating.

   VirusScan is updated on all computers in the network.

Setting the SecureDesk Security Level

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

The SecureDesk security level determines what conditions a computer's antivirus software must meet before the computer can access the Internet. You control the SecureDesk security level using a simple lever available on the SecureDesk page. You can set the lever to four states.

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

Table 26: SecureDesk Security Levels

This security level...	Enforces these conditions...
Off	None. SecureDesk is disabled, and users can freely access the Internet, regardless of whether antivirus software is installed or not. Note: You can disable SecureDesk for a specific computer or network, using the information in ***Using Network Objects*** on page 129.
Low	Antivirus software must be installed and enabled, but it need not be up-to-date.
Medium	Antivirus software must be installed, enabled, and up-to-date. In order for the antivirus software to qualify as up-to-date, the installed antivirus components' version numbers must be equal to or higher than the version numbers displayed in the Service Status table's Minimum column.

This security level...	Enforces these conditions...
High	The most recent antivirus software must be installed and enabled. In order for the antivirus software to qualify as the most recent, the installed antivirus components' version numbers must match the version numbers displayed in the Service Status table's Current column.

To change the SecureDesk security level

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

   The SecureDesk page appears.

2. Drag the lever to the desired level.

   SecureDesk enforces the new security level conditions.

   If you raised the security level, and the antivirus software installed on your computer does not meet the new security level conditions, the Current Device Status and Actions area displays an appropriate status message, and the Update your antivirus software to the latest version link appears.

   For an explanation of all status messages and their colors, see ***SecureDesk Status Messages*** on page 191.

3. If necessary, update your antivirus software by doing the following:

   a. Click Update your antivirus software to the latest version.

      The McAfee Security page opens in a new window, with the McAfee Secure-1 VirusScan ASaP popup window on top.

   b. Follow the online instructions to complete updating.

VirusScan is updated on all computers in the network.

For information on updating VirusScan on all compters in the network, see ***Updating McAfee VirusScan ASaP on All Computers*** on page 186.

Checking Antivirus Compliancy

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

You can check whether a computer's antivirus software complies with the SecureDesk security level conditions.

To check antivirus compliancy for your computer

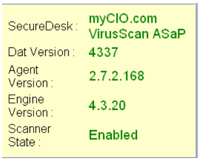
1. Click Security in the main menu, and click the SecureDesk tab.

   The SecureDesk page appears, and the Current Device Status and Actions area displays a color-coded status message indicating whether the computer complies with the SecureDesk security level conditions. For an explanation of the status message and its color, see the table below.

   If the antivirus software installed on your computer does not meet the security level conditions, the Update your antivirus software to the latest version link appears.

2. To view detailed information about the antivirus status and component versions, point to the status message.

   A popup window displays the desired information.

   SecureDesk : myCIO.com VirusScan ASaP
   Dat Version : 4337
   Agent Version : 2.7.2.168
   Engine Version : 4.3.20
   Scanner State : Enabled

3. If necessary, update your antivirus software by doing the following:

   a. Click Update your antivirus software to the latest version.

The McAfee Security page opens in a new window, with the McAfee Secure-1 VirusScan ASaP popup window on top.

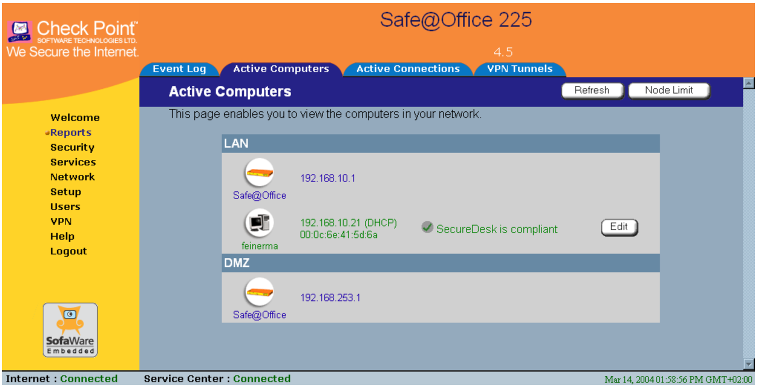
b. Follow the online instructions to complete updating.

VirusScan is updated on all computers in the network.

To check antivirus compliancy for all computers in the network

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

   The Active Computers page appears.



This page enables you to view the computers in your network.

SecureDesk is compliant

A color-coded status message next to each computer indicates whether the computer complies with the SecureDesk security level conditions. For an explanation of the status messages and their colors, see the tables below.

2. To view detailed information about the antivirus status and component versions, point to the status message.

   A popup window displays the desired information.

3. If necessary, update the antivirus software on all computers in the network.

   For instructions, see ***Updating McAfee VirusScan ASaP on All Computers*** on page 186.

Table 27: SecureDesk Status Messages

Message	Explanation
SecureDesk is compliant	The antivirus software complies with the SecureDesk security level conditions, and access through the firewall is not blocked.
Compliant, but SecureDesk not most up-to-date	The antivirus software complies with the SecureDesk security level conditions, and access through the firewall is not blocked. However, the antivirus components' version numbers do not match the version numbers displayed in the Service Status table's Current column. It is recommended to update your software.
Compliant, but SecureDesk scanner is disabled	The antivirus software complies with the SecureDesk security level conditions, and access through the firewall is not blocked. However, the scanner is disabled, and the computer/network is not currently protected from viruses. It is recommended to enable the scanner.

Message	Explanation
SecureDesk not up-to-date	The antivirus software components' version numbers are less than the version numbers displayed in the Service Status table's Minimum column. Access through the firewall may be blocked, depending on whether the SecureDesk security level conditions require that the antivirus software is up-to-date. Update your software.
SecureDesk scanner is disabled	The scanner is disabled, and the computer/network is not currently protected from viruses. Access through the firewall is blocked. Enable the scanner.
SecureDesk not up-to-date and scanner is disabled	The antivirus software components' version numbers are less than the version numbers displayed in the Service Status table's Minimum column, and the scanner is disabled. The computer/network is not currently protected from viruses. Access through the firewall is blocked. Update your software and enable the scanner.

Message	Explanation
SecureDesk is not compliant	The antivirus software does not comply with the SecureDesk security level conditions, and access through the firewall is blocked. Check the SecureDesk security level conditions, and make changes to your antivirus software accordingly. For information on SecureDesk security levels, see ***Setting the SecureDesk Security Level*** on page 186.
SecureDesk scanner not installed	The antivirus engine and virus signatures are installed, but the antivirus scanner is not. Access through the firewall is blocked. Install the scanner.
SecureDesk not installed	VirusScan is not installed, and access through the firewall is blocked. Install the antivirus software.
SecureDesk state is unknown	SecureDesk has not yet determined the antivirus software's state, because the computer is not responding. Access through the firewall is temporarily blocked.

Message	Explanation
Excluded from Antivirus compliance checking	SecureDesk is disabled for this computer/network. Access through the firewall is not blocked. For information on enabling SecureDesk, see ***Using Network Objects*** on page 129.

Table 28: SecureDesk Status Message Color Coding

Color	Explanation
Red	Error. The antivirus software does not comply with the SecureDesk security level conditions, and access through the firewall is blocked.
Orange	Warning. The antivirus software complies with the SecureDesk security level conditions, and access through the firewall is not blocked. However, the state of the antivirus software is not ideal.
Green	OK. The antivirus software complies with the SecureDesk security level conditions, and access through the firewall is not blocked.

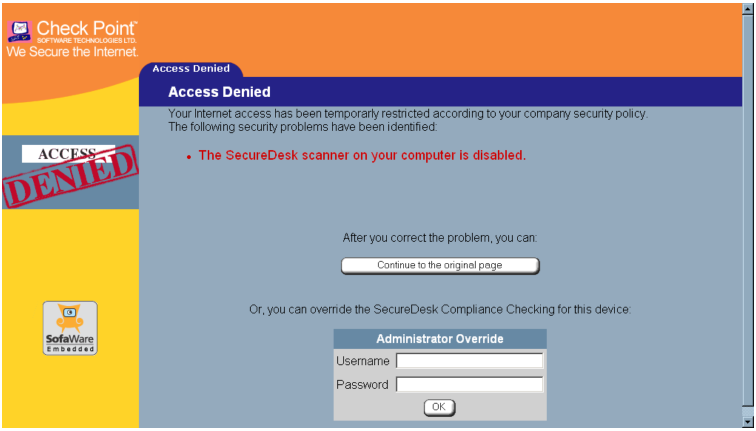
Overriding SecureDesk

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

SecureDesk blocks access through the firewall if your computer's antivirus software does not comply with the SecureDesk security level conditions.

When you attempt to connect to the Internet, the following things happen:

- The Access Denied page appears



Access Denied

Your Internet access has been temporarly restricted according to your company security policy.
The following security problems have been identified:

- The SecureDesk scanner on your computer is disabled.

After you correct the problem, you can:

Continue to the original page

Or, you can override the SecureDesk Compliance Checking for this device:

Administrator Override

Username

Password

OK

- The Event Log specifies that the connection was blocked by SecureDesk.

You can correct the problem by clicking **Download and install the latest antivirus software** to install up-to-date software, and then clicking **Continue to the original page**. Alternatively, Safe@Office administrators with Read/Write permissions can override the block using the procedure below.

To override SecureDesk

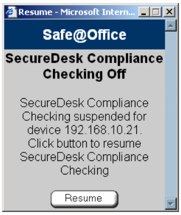
1. In the **Access Denied** page's **Administrator Override** area, in the **Username** field, type your user name.
2. In the **Password** field, type your password.

3. Click **OK**.

   SecureDesk is temporarily disabled for your computer only.

   The page you were blocked from accessing appears.

   The **Antivirus Off** popup window appears.



Safe@Office

SecureDesk Compliance Checking Off

SecureDesk Compliance Checking suspended for device 192.168.10.21. Click button to resume SecureDesk Compliance Checking

4. To re-enable the service, click **Resume** in the popup window.

   The service is re-enabled for your computer.

Viewing SecureDesk Reports

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

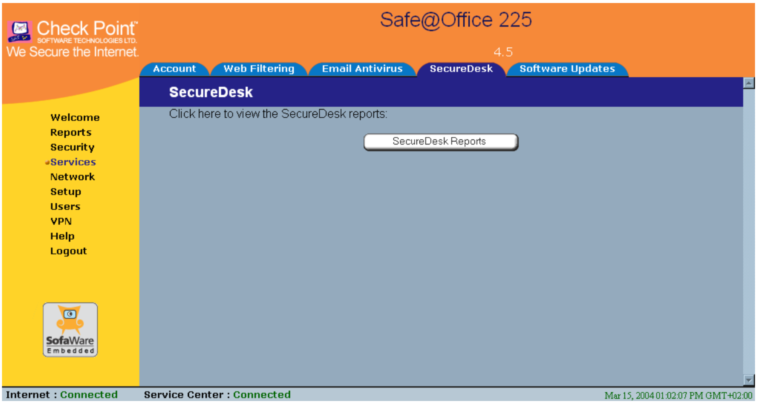
You can view reports on SecureDesk's activities for all computers in your network.

Note: You must be connected to the Internet to view SecureDesk reports.

To view SecureDesk reports

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

The **SecureDesk** page appears.



SecureDesk

Click here to view the SecureDesk reports:

Internet : Connected Service Center : Connected Mar 15, 2004 01:02:07 PM GMT+02:00

2. Click **SecureDesk Reports.**

   A SecureDesk report opens in a new window. This may take some time.

Chapter 10

Working With VPNs

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

This chapter includes the following topics:

Overview

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

The are three types of VPN sites:

- Remote Access VPN Server - Makes a network remotely available to authorized users, who connect to the Remote Access VPN Server using Remote Access VPN Clients, such as Check Point SecuRemote. Unless the Remote Access VPN Server is also a Remote Access VPN Client, it cannot initiate a connection to other VPN sites.

- **Site-to-Site VPN Gateway** - Can connect with another Site-to-Site VPN Gateway in a permanent, bi-directional relationship.
- **Remote Access VPN Client** - Can connect to a Remote Access VPN Server, but other VPN sites cannot initiate a connection to the Remote Access VPN Client. Defining a Remote Access VPN Client is a hardware alternative to using SecuRemote software.

Safe@Office 105 acts as a Remote Access VPN Server for one user, allowing a single remote employee to securely work from home or on the road. Safe@Office 110 and 225 provide full VPN functionality. They can act as a Remote Access VPN Client, a Remote Access VPN Server for multiple users, or a Site-to-Site VPN Gateway.

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

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

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

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

Site-to-Site VPNs

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

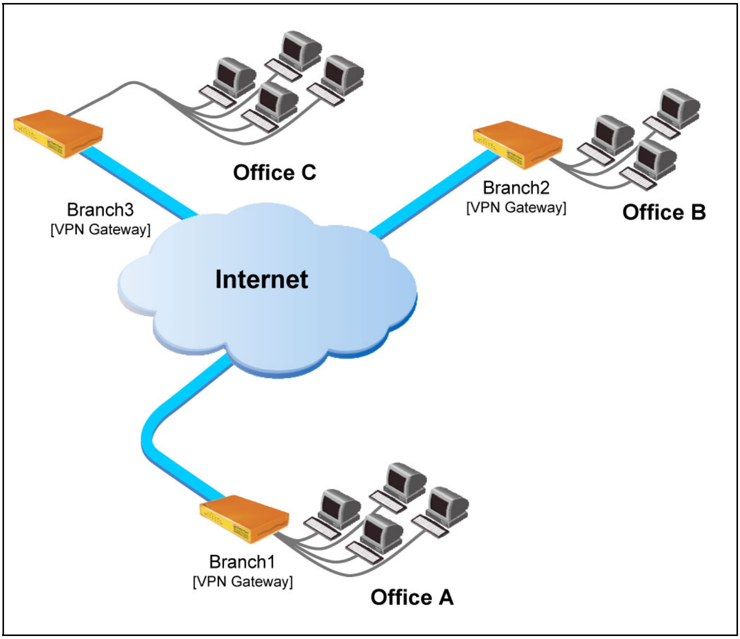


Figure 8: Site-to-Site VPN

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

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

   a. Define the second VPN site as a Site-to-Site VPN Gateway, or create a PPPoE tunnel to the second VPN site, using the procedure ***Adding and Editing VPN Sites*** on page 206.

   b. Enable the Remote Access VPN Server using the procedure ***Setting Up Your Safe@Office Appliance as a Remote Access VPN Server*** on page 204.

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

   a. Define the first VPN site as a Site-to-Site VPN Gateway, or create a PPPoE tunnel to the first VPN site, using the procedure ***Adding and Editing VPN Sites*** on page 206.

   b. Then enable the Remote Access VPN Server using the procedure ***Setting Up Your Safe@Office Appliance as a Remote Access VPN Server*** on page 204.

Remote Access VPNs

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

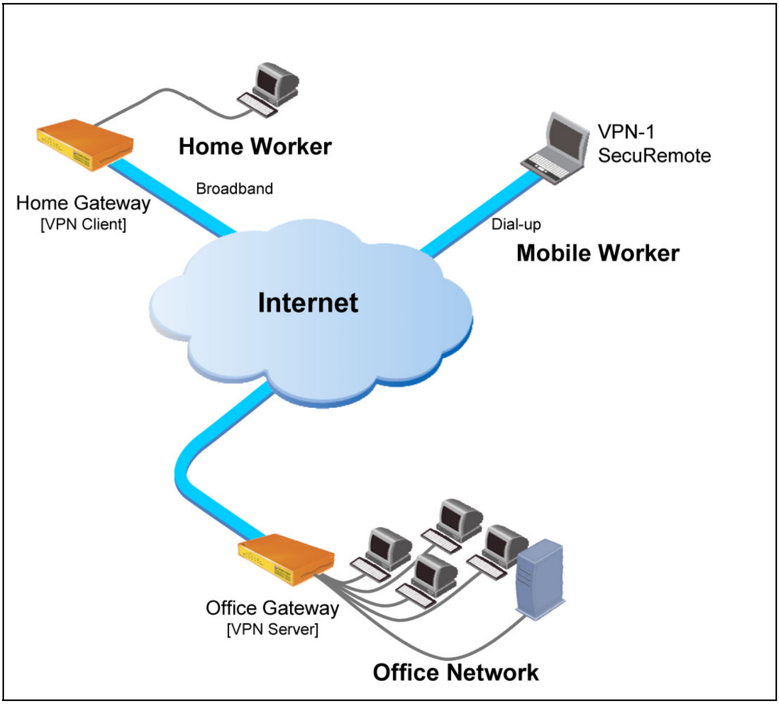


Figure 9: Remote Access VPN

To create a Remote Access VPN with two VPN sites

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

   See ***Adding and Editing VPN Sites*** on page 206.

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

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

   See ***Setting Up Your Safe@Office Appliance as a Remote Access VPN Server*** on page 204.

Setting Up Your Safe@Office Appliance as a Remote Access VPN Server

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

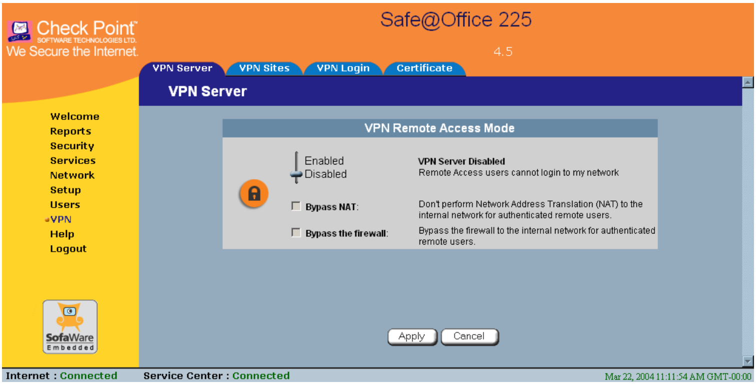
You can make your network remotely available to authorized users by setting up your Safe@Office appliance as a Remote Access VPN Server. Remote access users can connect to the Remote Access VPN Server via Check Point SecuRemote or a via Safe@Office appliance in Remote Access VPN mode.

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

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

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

The VPN Server page appears.



VPN Server

VPN Remote Access Mode

Enabled
Disabled

VPN Server Disabled
Remote Access users cannot login to my network

□ Bypass NAT: Don't perform Network Address Translation (NAT) to the internal network for authenticated remote users.

□ Bypass the firewall: Bypass the firewall to the internal network for authenticated remote users.

Internet : Connected Service Center : Connected Mar 22, 2004 11:11:54 AM GMT-00:00

2. Drag the Enabled/Disabled lever to Enabled.

   The Remote Access VPN Server is enabled.

   The check box is enabled.

3. To allow authenticated users to bypass NAT when connecting to your internal network, select Bypass NAT.

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

5. Follow the procedure ***Setting Up Remote VPN Access for Users*** on page 252.

Note: Disabling the Remote Access VPN Server will cause all existing VPN tunnels to disconnect.

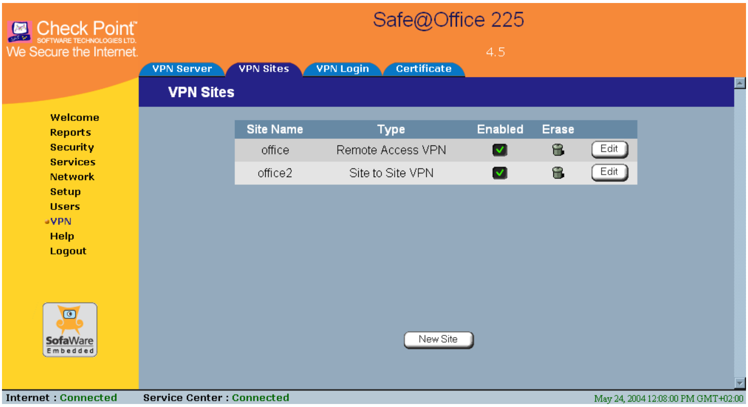
Adding and Editing VPN Sites using Safe@Office 110 and 225

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

To add or edit VPN sites

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

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



VPN Sites

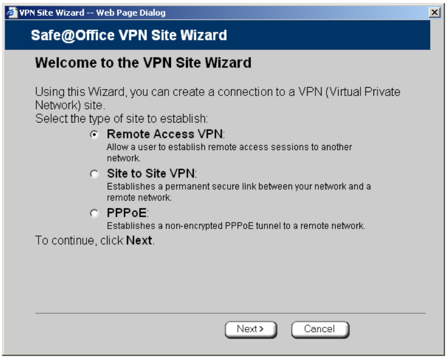
Site Name	Type	Enabled	Erase	
office	Remote Access VPN	☑	🗑	Edit
office2	Site to Site VPN	☑	🗑	Edit

Internet : Connected Service Center : Connected May 24, 2004 12:08:00 PM GMT+02:00

2. Do one of the following:

   - To add a VPN site, click New Site.
   - To edit a VPN site, click Edit in the desired VPN site's row.

The Safe@Office VPN Site Wizard opens, with the Welcome to the VPN Site Wizard dialog box displayed.


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

Welcome to the VPN Site Wizard

Using this Wizard, you can create a connection to a VPN (Virtual Private Network) site.
Select the type of site to establish:

- ● **Remote Access VPN**: Allow a user to establish remote access sessions to another network.
- ○ **Site to Site VPN**: Establishes a permanent secure link between your network and a remote network.
- ○ **PPPoE**: Establishes a non-encrypted PPPoE tunnel to a remote network.

To continue, click **Next**.

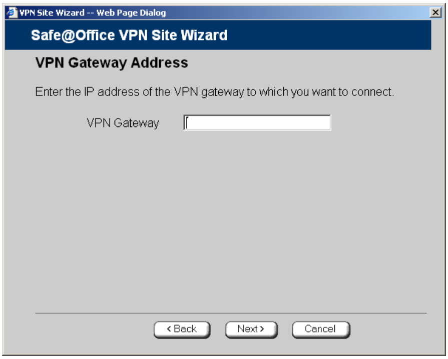
3. Do one of the following:

   - Select Remote Access VPN to establish remote access from your Remote Access VPN Client to a Remote Access VPN Server.
   - Select Site to Site VPN to create a permanent bi-directional connection to another Site-to-Site VPN Gateway.
   - Select PPPoE to create a non-encrypted connection to a PPPoE server.

4. Click Next.

Configuring a Remote Access VPN Site

If you selected Remote Access VPN, the VPN Gateway Address dialog box appears.

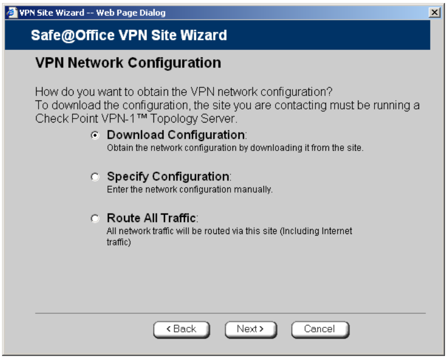

VPN Site Wizard -- Web Page Dialog
Safe@Office VPN Site Wizard
VPN Gateway Address

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

VPN Gateway:

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

   The VPN Network Configuration dialog box appears.


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

How do you want to obtain the VPN network configuration?
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.

● **Download Configuration**:
Obtain the network configuration by downloading it from the site.

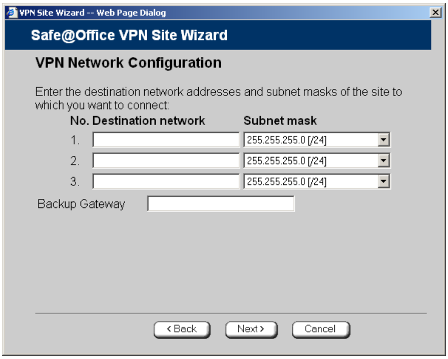
○ **Specify Configuration**:
Enter the network configuration manually.

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

3. Specify how you want to obtain the VPN network configuration. Refer to ***VPN Network Configuration Fields*** on page 215.
4. Click Next.

   The following things happen in the order below:

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



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

VPN Network Configuration

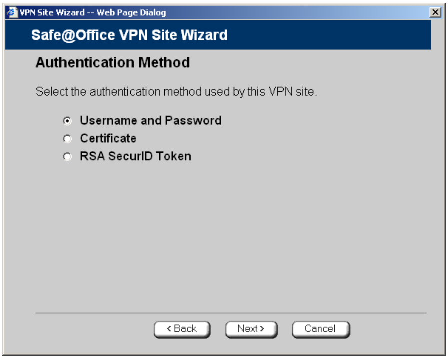
Enter the destination network addresses and subnet masks of the site to which you want to connect:

No.	Destination network	Subnet mask
1.		255.255.255.0 [/24]
2.		255.255.255.0 [/24]
3.		255.255.255.0 [/24]

Backup Gateway

Complete the fields using the information in ***VPN Network Configuration Fields*** on page 215 and click Next.

- The Authentication Method dialog box appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

Authentication Method

Select the authentication method used by this VPN site.

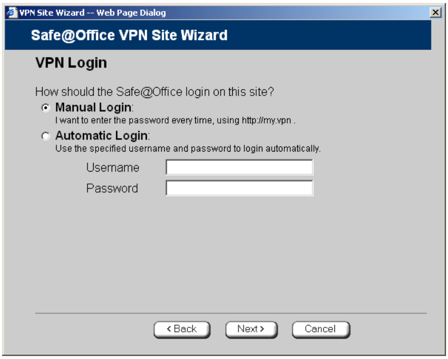
● Username and Password
○ Certificate
○ RSA SecurID Token

5. Complete the fields using the information in ***Authentication Methods Fields*** on page 216.

6. Click Next.

Username and Password Authentication Method

If you selected Username and Password, the VPN Login dialog box appears.


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

VPN Login

How should the Safe@Office login on this site?

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

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

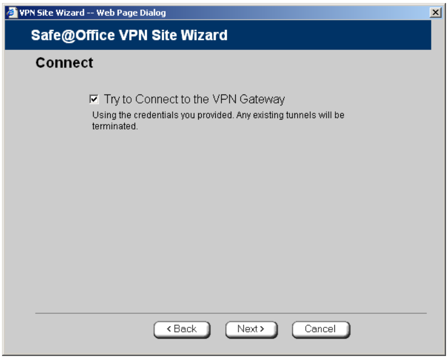
Username

Password

1. Complete the fields using the information in ***VPN Login Fields*** on page 217.

2. Click Next.

   - If you selected Automatic Login, the Connect dialog box appears.


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

Connect

☑ Try to Connect to the VPN Gateway
Using the credentials you provided. Any existing tunnels will be terminated.

Do the following:

1) To try to connect to the Remote Access VPN Server, select the Try to Connect to the VPN Gateway check box.

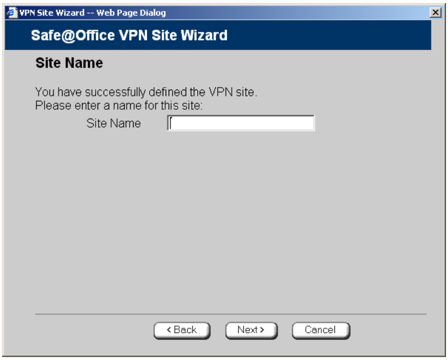
   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels will be terminated.

2) Click **Next**.

If you selected **Try to Connect to the VPN Gateway**, the **Connecting...** screen appears, and then the **Contacting VPN Site** screen appears.

- The **Site Name** dialog box appears.



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

Site Name

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

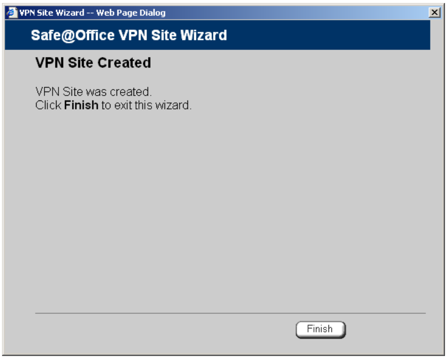
Site Name

3. Enter a name for the VPN site.

   You may choose any name.

4. Click **Next**.

   The **VPN Site Created** screen appears.



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

VPN Site Created

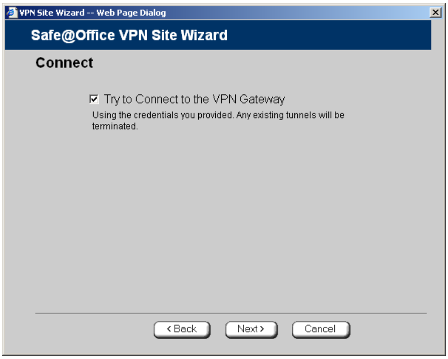
VPN Site was created.
Click **Finish** to exit this wizard.

5. Click **Finish**.

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

Certificate Authentication Method

If you selected **Certificate**, the **Connect** dialog box appears.



VPN Site Wizard -- Web Page Dialog
Safe@Office VPN Site Wizard
Connect
< Back
Next >
Cancel

☑ Try to Connect to the VPN Gateway

Using the credentials you provided. Any existing tunnels will be terminated.

1. To try to connect to the Remote Access VPN Server, select the **Try to Connect to the VPN Gateway** check box.

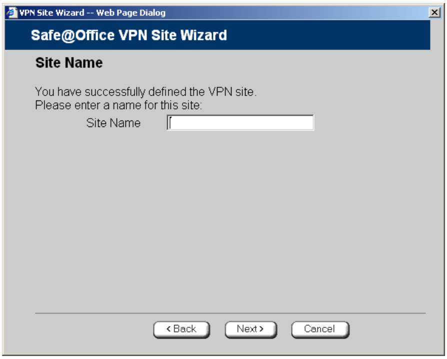
   This allows you to test the VPN connection.

⚠ Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels will be terminated.

2. Click **Next**.

   If you selected **Try to Connect to the VPN Gateway**, the **Connecting**... screen appears, and then the **Contacting VPN Site** screen appears.

The **Site Name** dialog box appears.



VPN Site Wizard -- Web Page Dialog
Safe@Office VPN Site Wizard
< Back
Next >
Cancel

Site Name

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

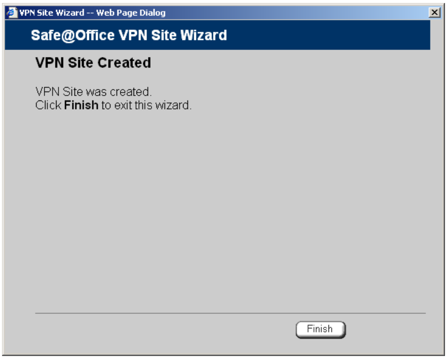
Site Name

3. Enter a name for the VPN site.

   You may choose any name.

4. Click **Next**.

   The **VPN Site Created** screen appears.



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

VPN Site Created

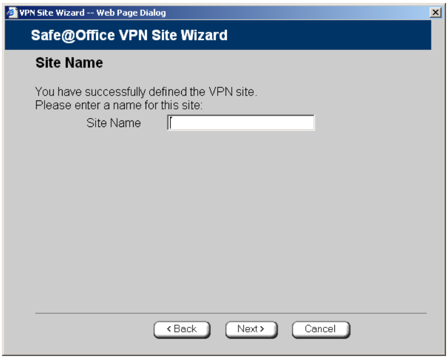
VPN Site was created.
Click **Finish** to exit this wizard.

5. Click **Finish**.

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

RSA SecurID Authentication Method

If you selected RSA SecurID, the Site Name dialog box appears.


VPN Site Wizard -- Web Page Dialog
Safe@Office VPN Site Wizard
< Back
Next >
Cancel

Site Name

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

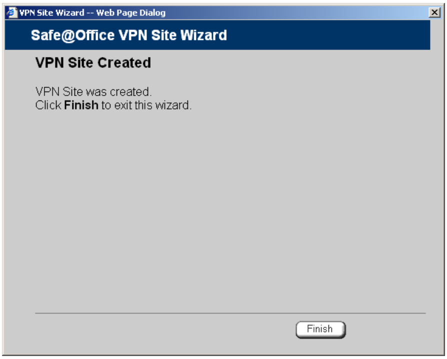
Site Name

1. Enter a name for the VPN site.

   You may choose any name.

2. Click **Next**.

   The **VPN Site Created** screen appears.


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

VPN Site Created

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

3. Click **Finish**.

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

Table 29: VPN Network Configuration Fields

In this field…	Do this…
Download Configuration	Click this option to obtain the network configuration by downloading it from the VPN site. This option will automatically configure your VPN settings, by downloading the network topology definition from the Remote Access VPN Server. Note: Downloading the network configuration is only possible if you are connecting to a Check Point VPN-1 or Safe@Office Site-to-Site VPN Gateway.
Specify Configuration	Click this option to provide the network configuration manually.
Route All Traffic	Click this option to route all network traffic through the VPN site. For example, if your VPN consists of a central office and a number of remote offices, and the remote offices are only allowed to access Internet resources through the central office, you can choose to route all traffic from the remote offices through the central office. Note: You can only configure one VPN site to route all traffic.
Destination network	Type up to three destination network addresses at the VPN site to which you want to connect.

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

Table 30: Authentication Methods Fields

In this field…	Do this…
Username and Password	Select this option to use a user name and password for VPN authentication. In the next step, you can specify whether you want to log on to the VPN site automatically or manually.
Certificate	Select this option to use a certificate for VPN authentication. If you select this option, a certificate must have been installed. (Refer to ***Installing a Certificate*** on page 237 for more information about certificates and instructions on how to install a certificate.)

In this field...	Do this...
RSA SecurID Token	Select this option to use an RSA SecurID token for VPN authentication. When authenticating to the VPN site, you must enter a four-digit PIN code and the SecurID passcode shown in your SecurID token's display. The RSA SecurID token generates a new passcode every minute. SecurID is only supported in Remote Access manual login mode.

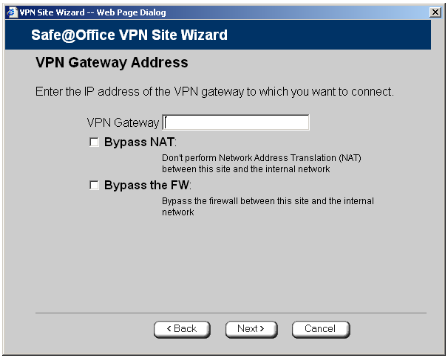
Table 31: VPN Login Fields

In this field...	Do this...
Manual Login	Click this option to configure the site for Manual Login. Manual Login connects only the computer you are currently logged onto to the VPN site, and only when the appropriate user name and password have been entered. For further information on Automatic and Manual Login, see, ***Logging on to a VPN Site*** on page 233.

In this field...	Do this...
Automatic Login	Click this option to enable the Safe@Office appliance to log on to the VPN site automatically. You must then fill in the Username and Password fields. Automatic Login provides all the computers on your internal network with constant access to the VPN site. For further information on Automatic and Manual Login, see ***Logging on to a VPN Site*** on page 233.
Username	Type the user name to be used for logging on to the VPN site.
Password	Type the password to be used for logging on to the VPN site.

Configuring a Site-to-Site VPN Gateway

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



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

VPN Gateway Address

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

VPN Gateway

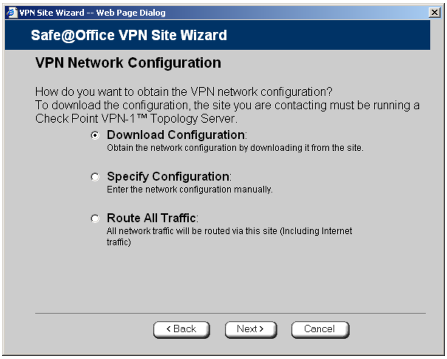
□ Bypass NAT:
Don't perform Network Address Translation (NAT) between this site and the internal network

□ Bypass the FW:
Bypass the firewall between this site and the internal network

1. Complete the fields using the information in ***VPN Gateway Address Fields*** on page 226.

2. Click Next.

   The VPN Network Configuration dialog box appears.



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

VPN Network Configuration

How do you want to obtain the VPN network configuration?
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.

● Download Configuration:
Obtain the network configuration by downloading it from the site.

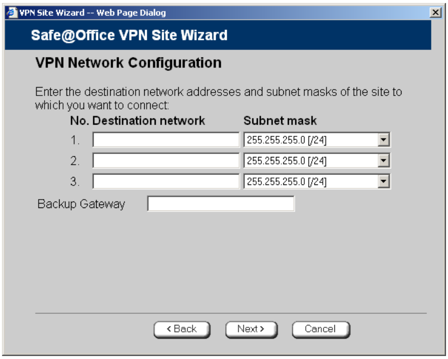
○ Specify Configuration:
Enter the network configuration manually.

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

3. Specify how you want to obtain the VPN network configuration. Refer to ***VPN Network Configuration Fields*** on page 215.

4. Click Next.

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



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

VPN Network Configuration

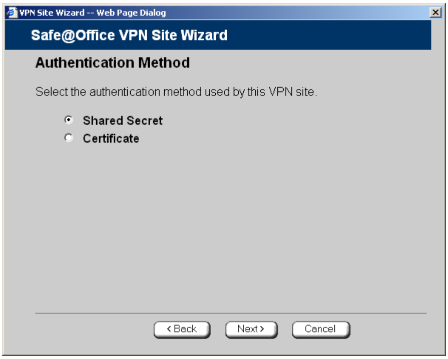
Enter the destination network addresses and subnet masks of the site to which you want to connect:

No.	Destination network	Subnet mask
1.		255.255.255.0 [/24]
2.		255.255.255.0 [/24]
3.		255.255.255.0 [/24]

Backup Gateway

Complete the fields using the information in ***VPN Network Configuration Fields*** on page 215, and then click Next.

- The Authentication Method dialog box appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

Authentication Method

Select the authentication method used by this VPN site.

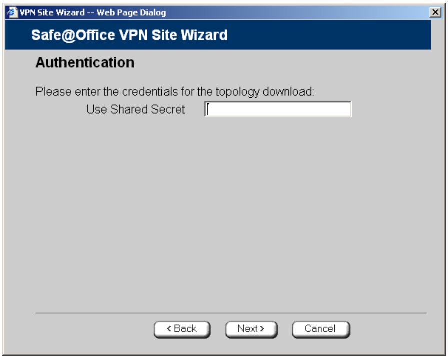
● Shared Secret
○ Certificate

5. Complete the fields using the information in ***Authentication Methods Fields*** on page 227.

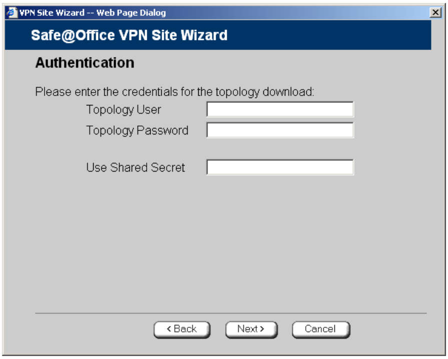
6. Click Next.

Shared Secret Authentication Method

If you selected Shared Secret, the Authentication dialog box appears.

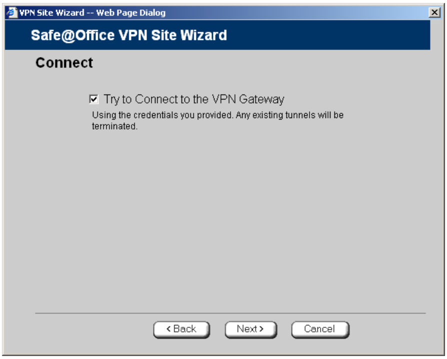

VPN Site Wizard -- Web Page Dialog
Safe@Office VPN Site Wizard
Authentication
Please enter the credentials for the topology download:
Use Shared Secret
< Back
Next >
Cancel

If you chose Download Configuration, the dialog box contains additional fields.


VPN Site Wizard -- Web Page Dialog
Safe@Office VPN Site Wizard
Authentication
Please enter the credentials for the topology download:
Topology User
Topology Password
Use Shared Secret
< Back
Next >
Cancel

1. Complete the fields using the information in ***VPN Authentication Fields*** on page 228 and click Next.

The **Connect** dialog box appears.



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

Connect

☑ Try to Connect to the VPN Gateway

Using the credentials you provided. Any existing tunnels will be terminated.

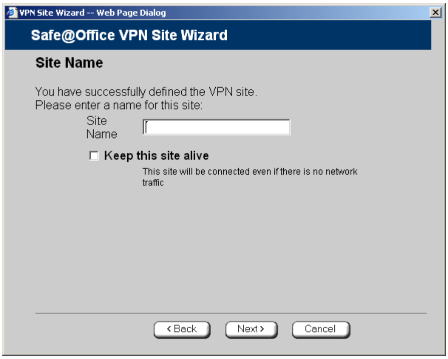
2. To try to connect to the Remote Access VPN Server, select the **Try to Connect to the VPN Gateway** check box.

   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels will be terminated.

3. Click **Next**.

   - If you selected **Try to Connect to the VPN Gateway**, the **Connecting**... screen appears, and then the **Contacting VPN Site** screen appears.
   - The **Site Name** dialog box appears.



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

Site Name

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

Site Name:

□ Keep this site alive

This site will be connected even if there is no network traffic

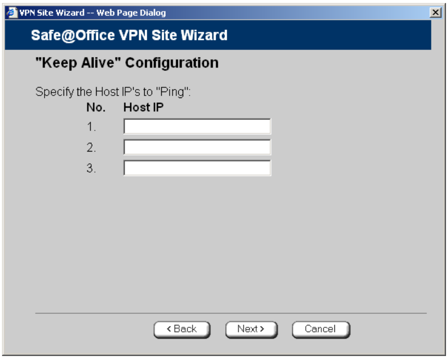
4. Enter a name for the VPN site.

   You may choose any name.

5. To keep the tunnel to the VPN site alive even if there is no network traffic between the Safe@Office appliance and the VPN site, select **Keep this site alive**.

6. Click **Next**.

   - If you selected **Keep this site alive**, and previously you chose **Download Configuration**, the **"Keep Alive" Configuration** dialog box appears.

     VPN Site Wizard -- Web Page Dialog

     Safe@Office VPN Site Wizard

     "Keep Alive" Configuration

     Specify the Host IP's to "Ping":

No.	Host IP
1.	
2.	
3.	

     Do the following:

     1) Type up to three IP addresses which the Safe@Office appliance should ping in order to keep the tunnel to the VPN site alive.

     2) Click **Next**.

   - The **VPN Site Created** screen appears.

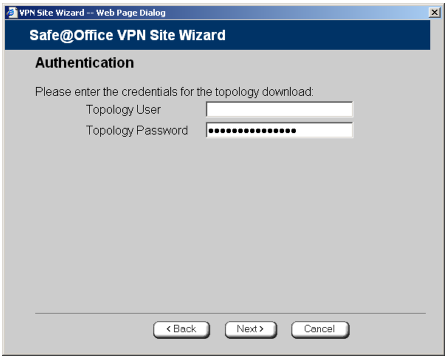
7. Click **Finish**.

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

Certificate Authentication Method

If you selected Certificate, the following things happen:

- If you chose Download Configuration, the Authentication dialog box appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

Authentication

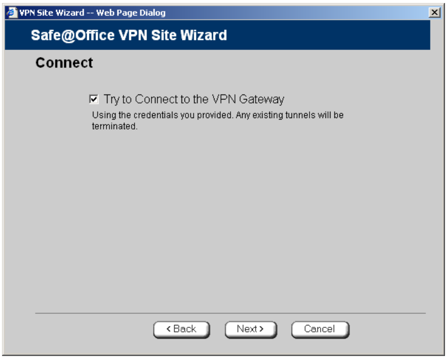
Please enter the credentials for the topology download:

Topology User:

Topology Password: ••••••••••••••••

Complete the fields using the information in ***VPN Authentication Fields*** on page 228 and click Next.

- The Connect dialog box appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

Connect

☑ Try to Connect to the VPN Gateway

Using the credentials you provided. Any existing tunnels will be terminated.

1. To try to connect to the Remote Access VPN Server, select the Try to Connect to the VPN Gateway check box.

   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels will be terminated.

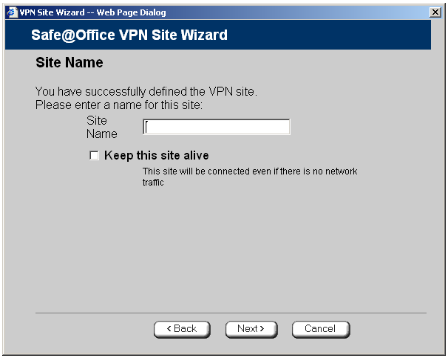
2. Click **Next**.

- If you selected **Try to Connect to the VPN Gateway**, the following things happen:

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

- The **Contacting VPN Site** screen appears.

- The **Site Name** dialog box appears.



Safe@Office VPN Site Wizard

Site Name

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

Site Name:

☐ Keep this site alive

This site will be connected even if there is no network traffic

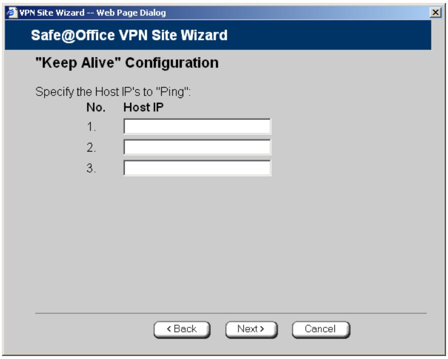
3. Enter a name for the VPN site.

   You may choose any name.

4. To keep the tunnel to the VPN site alive even if there is no network traffic between the Safe@Office appliance and the VPN site, select **Keep this site alive**.

5. Click **Next**.

- If you selected Keep this site alive, and previously you chose Download Configuration, the "Keep Alive" Configuration dialog box appears.



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

"Keep Alive" Configuration

Specify the Host IP's to "Ping":

No.	Host IP
1.	
2.	
3.	

Do the following:

1) Type up to three IP addresses which the Safe@Office appliance should ping in order to keep the tunnel to the VPN site alive.
2) Click Next.

- The VPN Site Created screen appears.

6. Click Finish.

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

Table 32: VPN Gateway Address Fields

In this field…	Do this…
Gateway Address	Type the IP address of the Site-to-Site VPN Gateway to which you want to connect, as given to you by the network administrator.

In this field...	Do this...
Bypass NAT	Select this option to allow the VPN site to bypass NAT when connecting to your internal network.
Bypass the FW	Select this option to allow the VPN site to bypass the firewall and access your internal network without restriction.

Table 33: Authentication Methods Fields

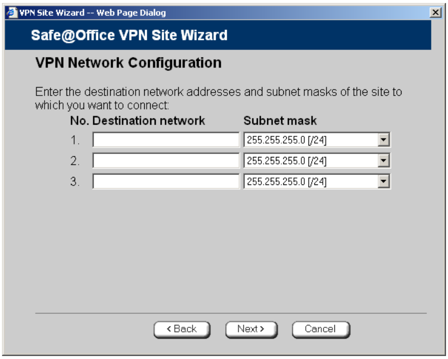
In this field...	Do this...
Shared Secret	Select this option to use a shared secret for VPN authentication. A shared secret is a string used to identify VPN sites to each other.
Certificate	Select this option to use a certificate for VPN authentication. If you select this option, a certificate must have been installed. (Refer to ***Installing a Certificate*** on page 237 for more information about certificates and instructions on how to install a certificate.)

Table 34: VPN Authentication Fields

In this field…	Do this…
Topology User	Type the topology user's user name.
Topology Password	Type the topology user's password.
Use Shared Secret	Type the shared secret to use for secure communications with the VPN site. This shared secret is a string used to identify the VPN sites to each other. The secret can contain spaces and special characters.

Creating a PPPoE Tunnel

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


VPN Site Wizard -- Web Page Dialog
Safe@Office VPN Site Wizard
< Back
Next >
Cancel

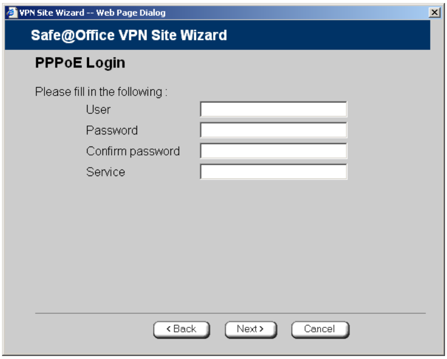
VPN Network Configuration

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

No.	Destination network	Subnet mask
1.		255.255.255.0 [/24]
2.		255.255.255.0 [/24]
3.		255.255.255.0 [/24]

1. Complete the fields using the information in ***VPN Network Configuration Fields*** on page 215.
2. Click Next.

The **PPPoE Login** page appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

PPPoE Login

Please fill in the following :

User

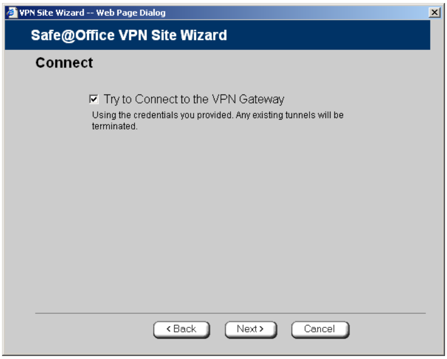
Password

Confirm password

Service

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

   The **Connect** dialog box appears.



VPN Site Wizard -- Web Page Dialog

Safe@Office VPN Site Wizard

Connect

☑ Try to Connect to the VPN Gateway

Using the credentials you provided. Any existing tunnels will be terminated.

5. If you don’t want to try to connect to the VPN site, clear the **Try to Connect to the VPN Gateway** check box.

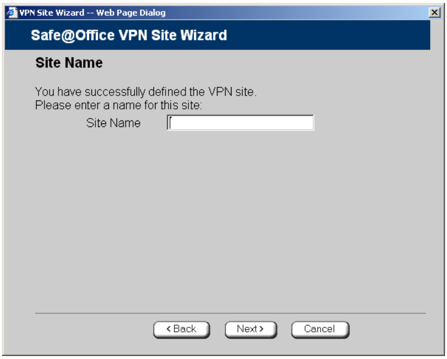
   This allows you to test the VPN connection.

Warning: If you try to connect to the VPN site before completing the wizard, all existing tunnels will be terminated.

6. Click **Next**.

If you selected Try to Connect to the VPN Gateway, the Connecting... screen appears, and then the Contacting VPN Site screen appears.

The Site Name dialog box appears.


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

Site Name

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

Site Name

7. Enter a name for the VPN site.

   You may choose any name.

8. Click Next.

   The VPN Site Created screen appears.

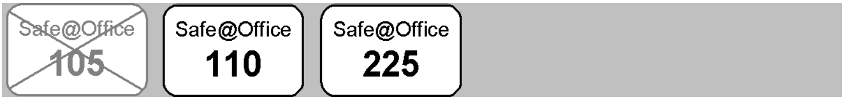
9. Click Finish.

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

Table 35: PPPoE Login Fields

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

Deleting a VPN Site



To delete a VPN site

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

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

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

   A confirmation message appears.

3. Click OK.

   The VPN site is deleted.

Enabling/Disabling a VPN Site

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

You can only connect to VPN sites that are enabled.

To enable/disable a VPN site

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

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

2. To enable a VPN site, do the following:

   a. Click the ☒ icon in the desired VPN site's row.

      A confirmation message appears.

   b. Click **OK**.

      The icon changes to ☑, and the VPN site is enabled.

3. To disable a VPN site, do the following:

Note: Disabling a VPN site eliminates the tunnel and erases the network topology.

   a. Click the ☑ icon in the desired VPN site's row.

      A confirmation message appears.

   b. Click **OK**.

      The icon changes to ☒, and the VPN site is disabled.

Logging on to a VPN Site

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

You need to manually log on to Remote Access VPN Servers configured for Manual Login. You do not need to manually log on to a Remote Access VPN Server configured for Automatic Login or a Site-to-Site VPN Gateway: all the computers on your network have constant access to it.

Manual Login can be done through either the Safe@Office Portal or the my.vpn page. When you log on and traffic is sent to the VPN site, a VPN tunnel is established. Only the computer from which you logged on can use the tunnel. To share the tunnel with other computers in your home network, you must log on to the VPN site from those computers, using the same user name and password.

Note: You must use a single user name and password for each VPN destination gateway.

Logging on through the Safe@Office Portal

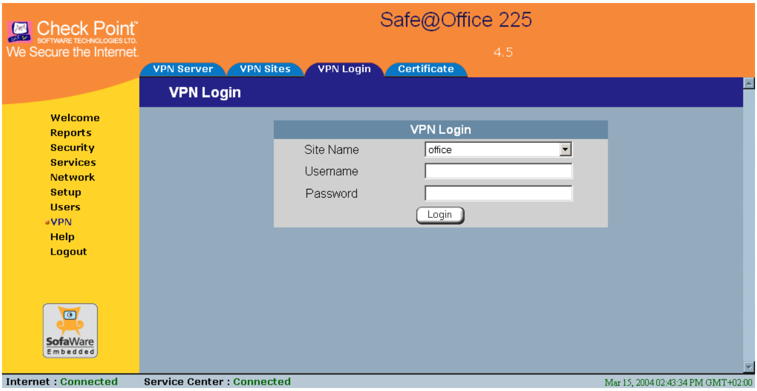
~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

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

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

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

The VPN Login page appears.



VPN Login

Site Name: office

Username:

Password:

Internet : Connected   Service Center : Connected   Mar 15, 2004 02:43:34 PM GMT+02:00

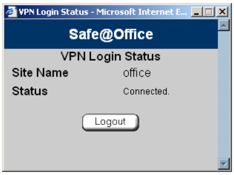
2. From the **Site Name** list, select the site to which you want to log on.

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

3. Enter your user name and password in the appropriate fields.

4. Click **Login**.

   - If the Safe@Office appliance is configured to automatically download the network configuration, the Safe@Office appliance downloads the network configuration.
   - If when adding the VPN site you specified a network configuration, the Safe@Office appliance attempts to create a tunnel to the VPN site.
   - Once the Safe@Office appliance has finished connecting, the **VPN Login Status** box appears. The **Status** field displays “Connected”.



VPN Login Status

Site Name: office

Status: Connected.

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

Logging on through the my.vpn page

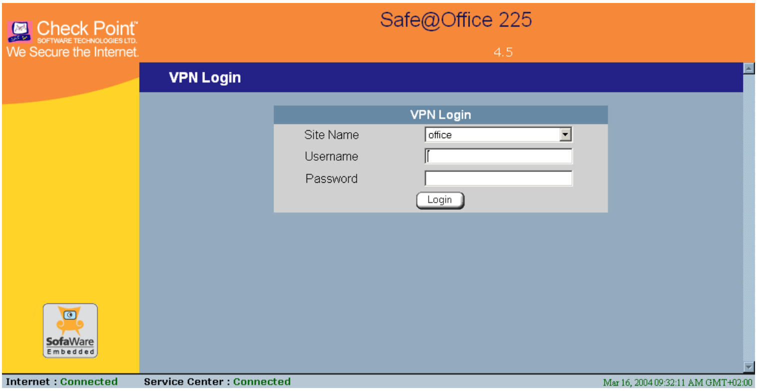
~~Safe@Office 105~~ Safe@Office 110 Safe@Office 225

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

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

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

   The **VPN Login** screen appears.



Site Name: office

Username:

Password:

Internet : Connected   Service Center : Connected   Mar 16, 2004 09:32:11 AM GMT+02:00

2. In the **Site Name** list, select the site to which you want to log on.
3. Enter your user name and password in the appropriate fields.
4. Click **Login**.

- If the Safe@Office appliance is configured to automatically download the network configuration, the Safe@Office appliance downloads the network configuration.

- If when adding the VPN site you specified a network configuration, the Safe@Office appliance attempts to create a tunnel to the VPN site.
- The **VPN Login Status** box appears. The **Status** field tracks the connection's progress.
- Once the Safe@Office appliance has finished connecting, the **Status** field changes to "Connected".
- The **VPN Login Status** box remains open until you manually log off of the VPN site.

Logging off a VPN Site

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

You need to manually log off a VPN site in the following cases:

- You are using Safe@Office 105.
- The VPN site is a Remote Access VPN site configured for Manual Login.

To log off a VPN site

- In the **VPN Login Status** box, click **Logout**.

  All open tunnels from the Safe@Office appliance to the VPN site are closed, and the **VPN Login Status** box closes.

Note: Closing the browser or dismissing the VPN Login Status box will also terminate the VPN session within a short time.

Installing a Certificate

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

A digital certificate is a secure means of authenticating the Safe@Office appliance to other Site-to-Site VPN Gateways. The certificate is issued by the Certificate Authority (CA) to entities such as gateways, users, or computers. The entity then uses the certificate to identify itself and provide verifiable information.

For instance, the certificate includes the Distinguishing Name (DN) (identifying information) of the entity, as well as the public key (information about itself). After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

The Safe@Office appliance supports certificates encoded in the PKCS#12 (Personal Information Exchange Syntax Standard) format. The PKCS#12 file must have a ".p12" file extension

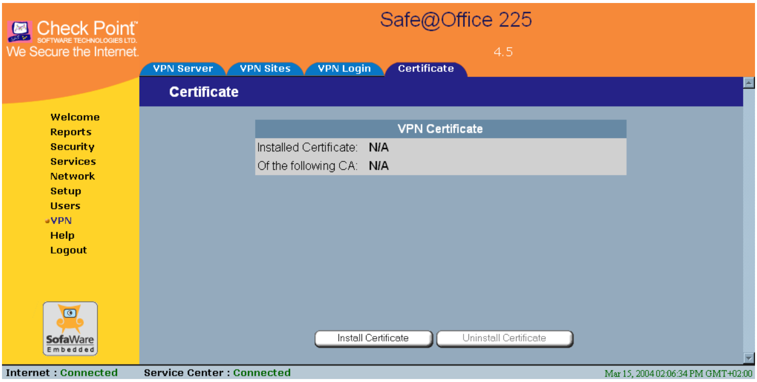
Note: To use certificates authentication, each Safe@Office appliance should have a unique certificate. Do not use the same certificate for more than one gateway.

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

To install a certificate

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

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



Certificate

VPN Certificate

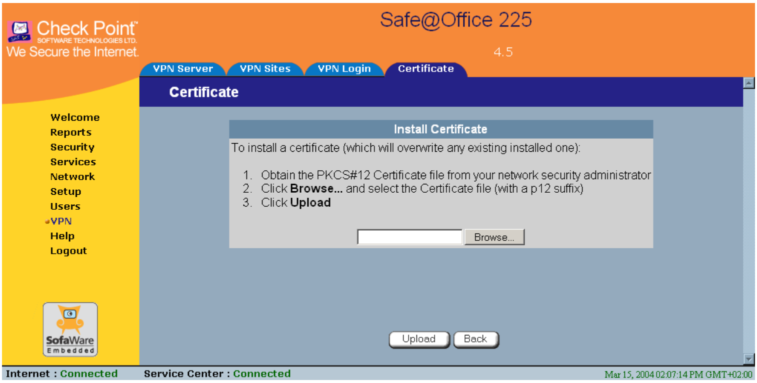
Installed Certificate: N/A

Of the following CA: N/A

Internet : Connected Service Center : Connected Mar 15, 2004 02:06:34 PM GMT+02:00

2. Click **Install Certificate.**

   A **Certificate** page requests you to specify a certificate file for upload.



Certificate

Install Certificate

To install a certificate (which will overwrite any existing installed one):

1. Obtain the PKCS#12 Certificate file from your network security administrator
2. Click **Browse...** and select the Certificate file (with a p12 suffix)
3. Click **Upload**

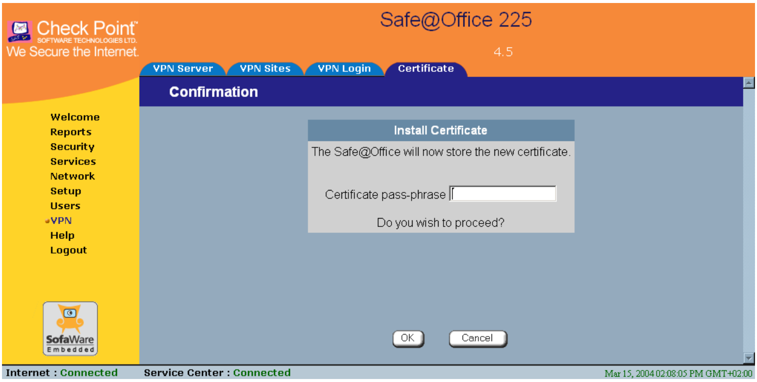
Internet : Connected Service Center : Connected Mar 15, 2004 02:07:14 PM GMT+02:00

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

   The filename that you selected is displayed.

4. Click **Upload**.

You are requested to enter the pass-phrase.



Confirmation

Install Certificate

The Safe@Office will now store the new certificate.

Certificate pass-phrase

Do you wish to proceed?

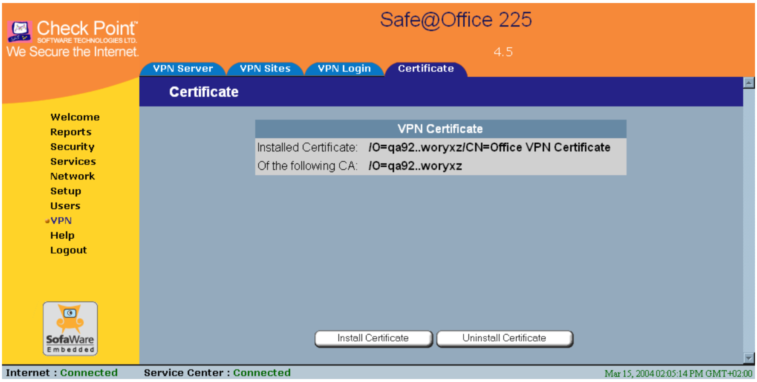
Internet : Connected Service Center : Connected Mar 15, 2004 02:08:05 PM GMT+02:00

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

   The certificate is installed.

   A success message appears.
7. Click OK.

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



Certificate

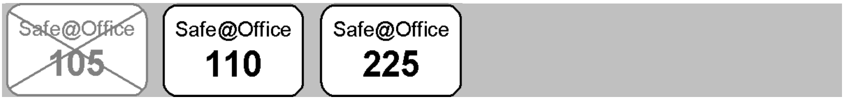
VPN Certificate

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

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

Internet : Connected Service Center : Connected Mar 15, 2004 02:05:14 PM GMT+02:00

Uninstalling a Certificate



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

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

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

To uninstall a certificate

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

   The Certificate page appears with the name of the currently installed certificate.

2. Click Uninstall.

   A confirmation message appears.

3. Click OK.

   The certificate is uninstalled.

   A success message appears.

4. Click OK.

Viewing VPN Tunnels

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

You can view a list of currently established VPN tunnels. VPN tunnels are created and closed as follows:

- Remote Access VPN sites configured for Automatic Login, Site-to-Site VPN Gateways and PPPoE tunnels

  A tunnel is created whenever your computer attempts any kind of communication with a computer at the VPN site. The tunnel is closed when not in use for a period of time.

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

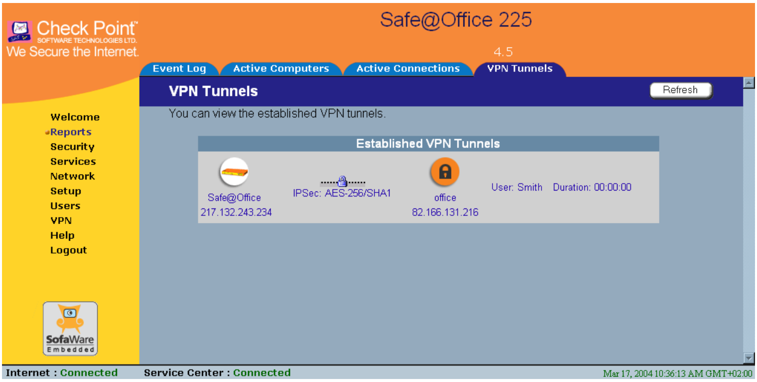
- Remote Access VPN sites configured for Manual Login

  A tunnel is created whenever your computer attempts any kind of communication with a computer at the VPN site, *after you have manually logged on to the site*. All open tunnels connecting to the site are closed when you manually log off.

To view VPN tunnels

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

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



VPN Tunnels

You can view the established VPN tunnels.

Established VPN Tunnels

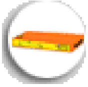
Safe@Office 217.132.243.234 — IPSec: AES-256/SHA1 — office 82.166.131.216 — User: Smith — Duration: 00:00:00

Internet : Connected   Service Center : Connected   Mar 17, 2004 10:36:13 AM GMT+02:00

The **VPN Tunnels** page includes the information described in the table below.

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

Table 36: VPN Tunnels Page Fields

This field…	Displays…
	The Safe@Office appliance Internet IP address.

This field...	Displays...
🔒	The security protocol (IPSec), the type of encryption used to secure the connection, and the type of Message Authentication Code (MAC) used to verify the integrity of the message. This information is presented in the following format: Security protocol: Encryption type/Authentication type Note: All VPN settings are automatically negotiated between the two sites. The encryption and authentication schemes used for the connection are the strongest of those used at the two sites. Your Safe@Office appliance supports AES, 3DES, and DES encryption schemes, and MD5 and SHA authentication schemes.
🔒	The name and IP address of the VPN gateway to which the tunnel is connected.
User	The user logged on to the VPN site.

Duration	The time at which the tunnel was established.
	This information is presented in the format hh:mm:ss, where:
	hh=hours
	mm=minutes
	ss=seconds

Chapter 11

Managing Users

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

This chapter includes the following topics:

Changing Your Password

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

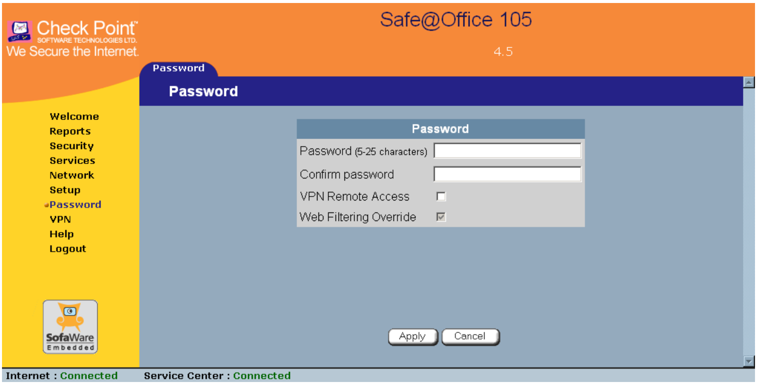
Using Safe@Office 105

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

To change your password

1. Click Password in the main menu.

The **Password** page appears.



Password

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

Internet : Connected   Service Center : Connected

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

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

3. Click **Apply**.

   Your changes are saved.

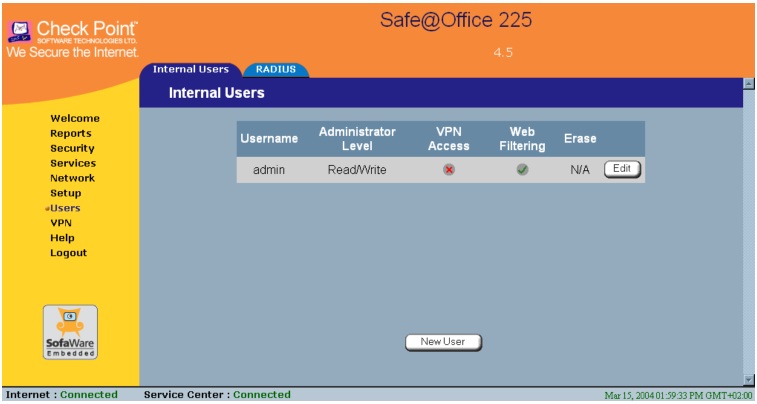
Using Safe@Office 110 and 225

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

To change your password

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

The **Internal Users** page appears.

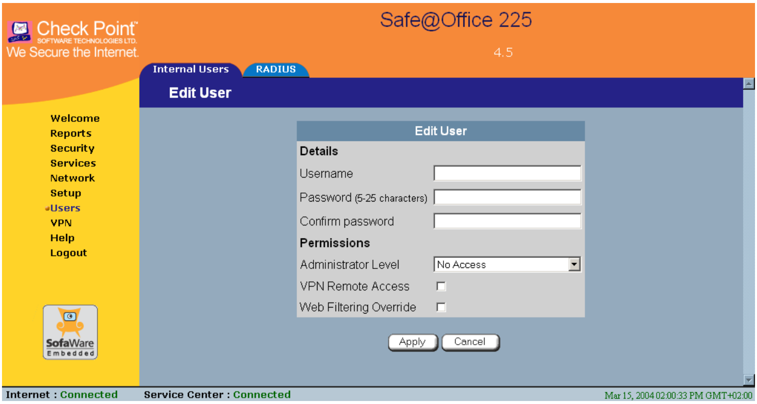


Username	Administrator Level	VPN Access	Web Filtering	Erase	
admin	Read/Write	☒	✓	N/A	Edit

Internet : Connected Service Center : Connected Mar 15, 2004 01:59:33 PM GMT+02:00

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

   The **Edit User** page appears.



Edit User

Details

Username

Password (5-25 characters)

Confirm password

Permissions

Administrator Level: No Access

VPN Remote Access ☐

Web Filtering Override ☐

Internet : Connected Service Center : Connected Mar 15, 2004 02:00:33 PM GMT+02:00

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

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

4. Click **Apply**.

   Your changes are saved.

Adding Users

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

To add a user

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

   The Internal Users page appears.

2. Click New User.

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

3. Complete the fields using the information in ***Edit User Page Fields*** on page 249.

4. Click Apply.

   The new user is saved.

Viewing and Editing Users

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

To view or edit users

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

   The Internal Users page appears.

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

   The Edit User page appears with the user's details. The options that appear on the page are dependant on the software and services you are using.

3. To edit the user's details, do the following:

a. Edit the fields using ***Edit User Page Fields*** on page 249.

b. Click Apply.

The changes are saved.

4. To return to the Users page without making any changes, click Cancel.

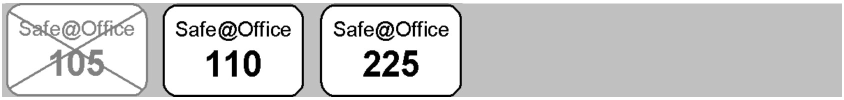
Table 37: Edit User Page Fields

In this field...	Do this...
Username	Enter a username for the user.
Password	Enter a password for the user. Use five to 25 characters (letters or numbers) for the new password.
Confirm Password	Re-enter the user’s password.

In this field...	Do this...
Administrator Level	Select the user's level of access to the Safe@Office Portal. The levels are: • No Access: The user cannot access the Safe@Office Portal. • Read/Write: The user can log on to the Safe@Office Portal and modify system settings. • Read Only: The user can log on to the Safe@Office Portal, but cannot modify system settings or export the appliance configuration via the Setup>Tools page. For example, you could assign this administrator level to technical support personnel who need to view the Event Log. The default level is No Access. The "admin" user's Administrator Level (Read/Write) cannot be changed.
VPN Remote Access	Select this option to allow the user to connect to this Safe@Office appliance using their VPN client. For further information on setting up VPN remote access, see ***Setting Up Remote VPN Access for Users*** on page 252. This option only appears in Safe@Office 110 and 225.

In this field...	Do this...
Web Filtering Override	Select this option to allow the user to override Web Filtering. This option only appears if the Web Filtering service is defined. This option cannot be changed for the "admin" user.

Deleting Users



Note: The "admin" user cannot be deleted.

To delete a user

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

   The **Internal Users** page appears.

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

   A confirmation message appears.

3. Click **OK**.

   The user is deleted.

Setting Up Remote VPN Access for Users

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

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

To set up remote VPN access for a user

1. Enable your Remote Access VPN Server, using the procedure ***Setting Up Your Safe@Office Appliance as a Remote Access VPN Server*** on page 204.
2. Add the user to the system, using the procedure ***Adding Users*** on page 248. You must select the VPN Remote Access option.

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

Using RADIUS Authentication

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

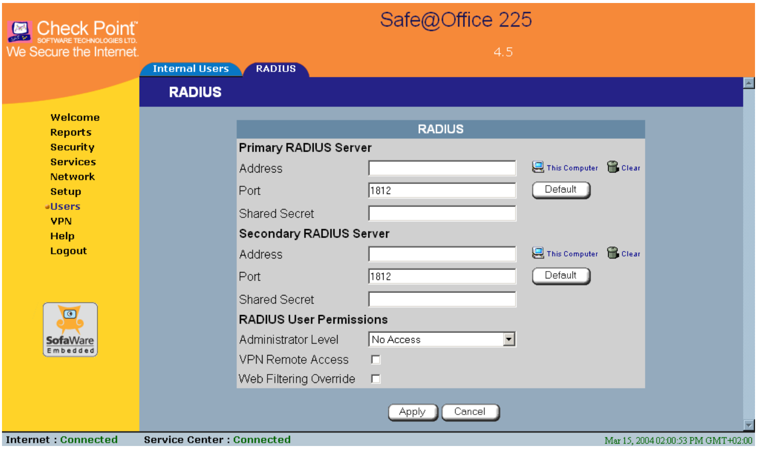
You can use RADIUS to authenticate both Safe@Office appliance users and Remote Access VPN Clients trying to connect to the Safe@Office appliance.

When a user accesses the Safe@Office Portal and tries to log on, the Safe@Office appliance sends the entered user name and password to the RADIUS server. The server then checks whether the RADIUS database contains a matching user name and password pair. If so, then the user is logged on.

To use RADIUS authentication

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

   The **RADIUS** page appears.



RADIUS

Primary RADIUS Server

Address	
Port	1812
Shared Secret	

Secondary RADIUS Server

Address	
Port	1812
Shared Secret	

RADIUS User Permissions

Administrator Level	No Access
VPN Remote Access	□
Web Filtering Override	□

Internet : Connected Service Center : Connected Mar 15, 2004 02:00:53 PM GMT+02:00

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

Table 38: RADIUS Page Fields

In this field…	Do this…
Address	Type the IP address of the computer that will run the RADIUS service (one of your network computers) or click the corresponding **This Computer** button to allow your computer to host the service. To clear the text box, click **Clear**.

In this field...	Do this...
Port	Type the port number on the RADIUS server's host computer. To reset this field to the default (port 1812), click Default.
Shared Secret	Type the shared secret to use for secure communication with the RADIUS server.
Administrator Level	Select the level of access to the Safe@Office Portal to assign to all users authenticated by the RADIUS server. The levels are: • No Access: The user cannot access the Safe@Office Portal • Read/Write: The user can log on to the Safe@Office Portal and modify system settings. • Read Only: The user can log on to the Safe@Office Portal, but cannot modify system settings. The default level is No Access.
Web Filtering Override	Select this option to allow all users authenticated by the RADIUS server to override Web Filtering. This option only appears if the Web Filtering service is defined.

Chapter 12

Maintenance

This chapter describes the tasks required for maintenance and diagnosis of your Safe@Office appliance.

This chapter includes the following topics:

Viewing Firmware Status

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

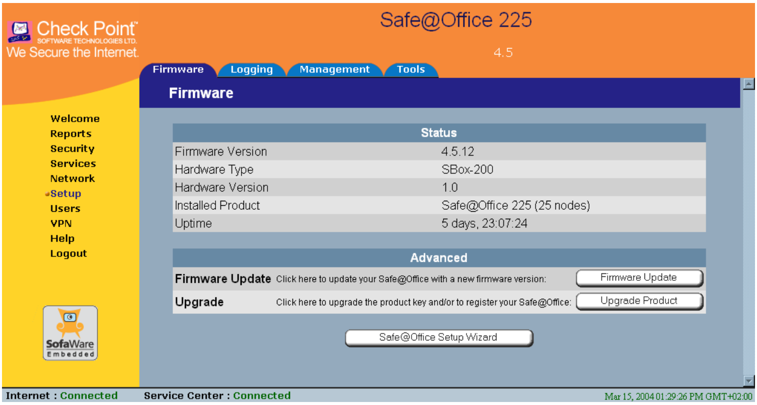
The firmware is the software program embedded in the Safe@Office appliance.

You can view your current firmware version and additional details.

To view the firmware status

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

  The **Firmware** page appears.



Firmware

Status	
Firmware Version	4.5.12
Hardware Type	SBox-200
Hardware Version	1.0
Installed Product	Safe@Office 225 (25 nodes)
Uptime	5 days, 23:07:24

Advanced

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

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

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

Table 39: Firmware Status Fields

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

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

Updating the Firmware

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

If you are subscribed to Software Updates, firmware updates are performed automatically. These updates include new product features and protection against new security threats. Check with your reseller for the availability of Software Updates and other services. For information on subscribing to services, see ***Connecting to a Service Center*** on page 165.

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

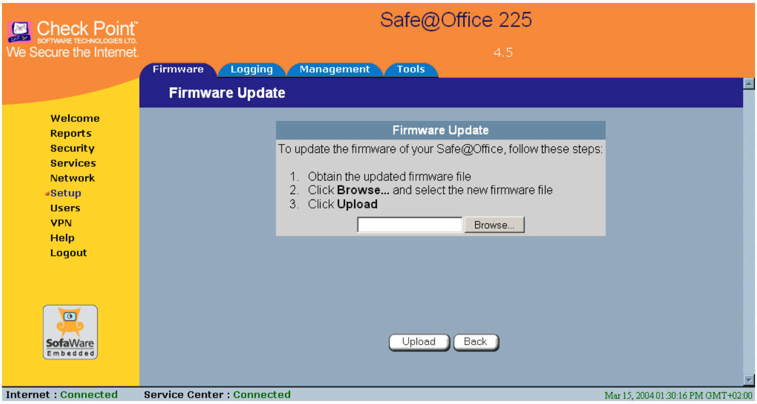
To update your Safe@Office firmware manually

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

   The Firmware page appears.

2. Click Firmware Update.

The **Firmware Update** page appears.



Firmware Update

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

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

3. Click **Browse**.

   A browse window appears.

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

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

5. Click **Upload**.

   Your Safe@Office appliance firmware is updated. This may take a few minutes. At the end of the process the Safe@Office appliance restarts automatically.

Upgrading Your Software Product

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

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

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

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

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

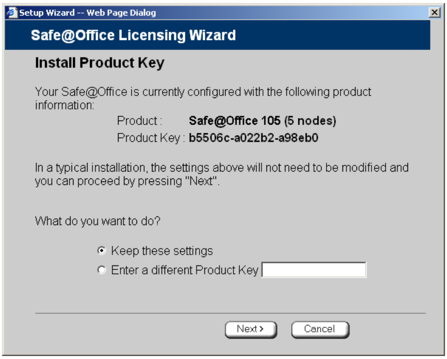
To install a Product Key

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

   The **Firmware** page appears.

2. Click **Upgrade Product.**

   The **Safe@Office Licensing Wizard** opens, with the **Install Product Key** dialog box displayed.

   Install Product Key

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

   Product : **Safe@Office 105 (5 nodes)**
   Product Key : **b5506c-a022b2-a98eb0**

   In a typical installation, the settings above will not need to be modified and you can proceed by pressing "Next".

   What do you want to do?

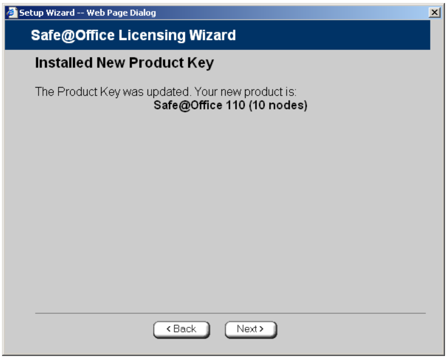
   ● Keep these settings
   ○ Enter a different Product Key

3. Click **Enter a different Product Key.**

4. In the **Product Key** field, enter the new Product Key.

5. Click **Next.**

The **Installed New Product Key** dialog box appears.

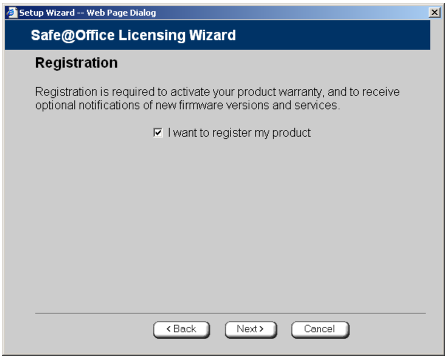


Installed New Product Key

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

6. Click **Next**.

   The first **Registration** dialog box appears.



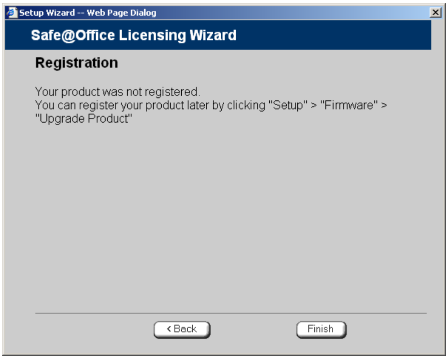
Registration

Registration is required to activate your product warranty, and to receive optional notifications of new firmware versions and services.

☑ I want to register my product

7. Do one of the following:

- To register your Safe@Office appliance later on, clear the **I want to register my product** check box and then click **Next.**



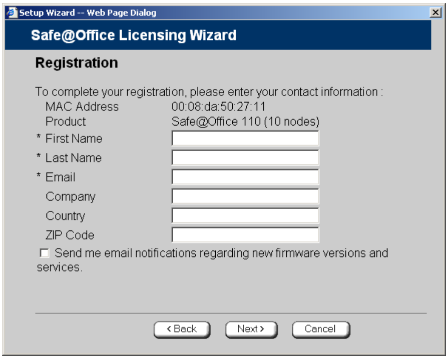
Registration

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

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

1) Click **Next.**

   A second **Registration** dialog box appears.



Registration

To complete your registration, please enter your contact information :

MAC Address	00:08:da:50:27:11
Product	Safe@Office 110 (10 nodes)
* First Name	
* Last Name	
* Email	
Company	
Country	
ZIP Code	

□ Send me email notifications regarding new firmware versions and services.

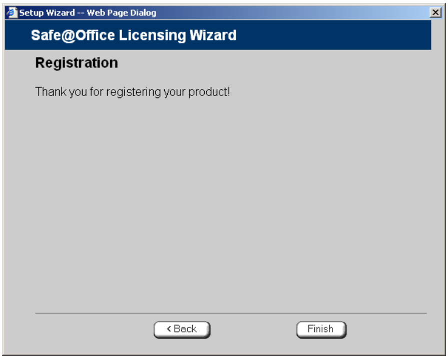
2) Enter your contact information in the appropriate fields.

3) To receive email notifications regarding new firmware versions and services, select the check box.

4) Click **Next.**

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

The third **Registration** dialog box appears.



Setup Wizard -- Web Page Dialog

Safe@Office Licensing Wizard

Registration

Thank you for registering your product!

8. Click **Finish.**

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

Registering Your Safe@Office Appliance

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

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

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

To register your Safe@Office appliance

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

   The **Firmware** page appears.

2. Click **Upgrade Product.**

The Safe@Office Licensing Wizard opens, with the Install Product Key dialog box displayed.

3. Select Keep these settings.
4. Click Next.

   The first Registration dialog box appears.
5. Verify that the I want to register my product check box is selected.
6. Click Next.

   A second Registration dialog box appears.
7. Enter your contact information in the appropriate fields.
8. To receive email notifications regarding new firmware versions and services, select the check box.
9. Click Next.

   The Registration... screen appears.

   The third Registration dialog box appears.
10. Click Finish.

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

Configuring Syslog Logging

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

You can configure the Safe@Office appliance to send event logs to a Syslog server residing in your internal network or on the Internet. The logs detail the date and the time each event occurred. If the event is a communication attempt that was rejected by the firewall, the event details include the source and destination IP address, the destination port, and the protocol used for the communication attempt (for example, TCP or UDP).

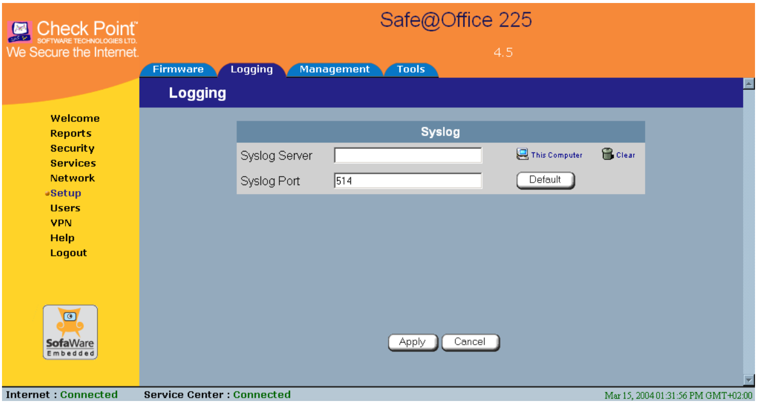
This same information is also available in the Event Log page (see ***Viewing the Event Log*** on page 141). However, while the Event Log can display hundreds of logs, a Syslog server can store an unlimited number of logs. Furthermore, Syslog servers can provide useful tools for managing your logs.

Note: Kiwi Syslog Daemon is freeware and can be downloaded from http://www.kiwisyslog.com. For technical support, contact Kiwi Enterprises.

To configure Syslog logging

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

   The **Logging** page appears.



Logging

Syslog

Syslog Server

Syslog Port 514

Internet : Connected Service Center : Connected Mar 15, 2004 01:31:56 PM GMT+02:00

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

Table 40: Logging Page Fields

In this field...	Do this...
Syslog Server	Type the IP address of the computer that will run the Syslog service (one of your network computers), or click **This Computer** to allow your computer to host the service.

In this field...	Do this...
Clear	Click to clear the Syslog Server field.
Syslog Port	Type the port number of the Syslog server.
Default	Click to reset the Syslog Port field to the default (port 514 UDP).

Configuring HTTPS

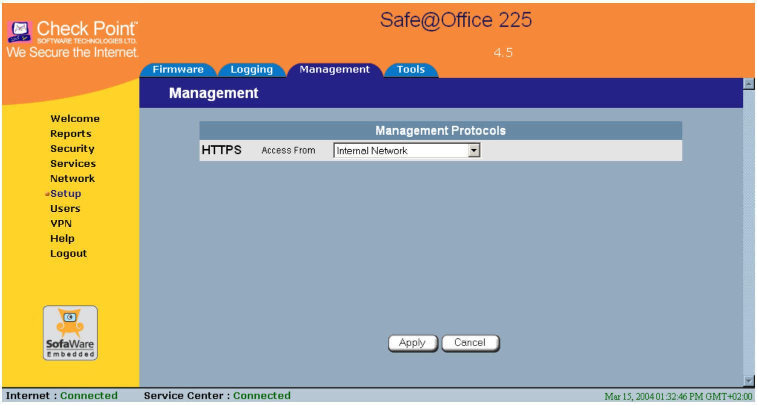
Safe@Office 105 | Safe@Office 110 | Safe@Office 225

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

To configure HTTPS

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

   The Management page appears.



Management Protocols

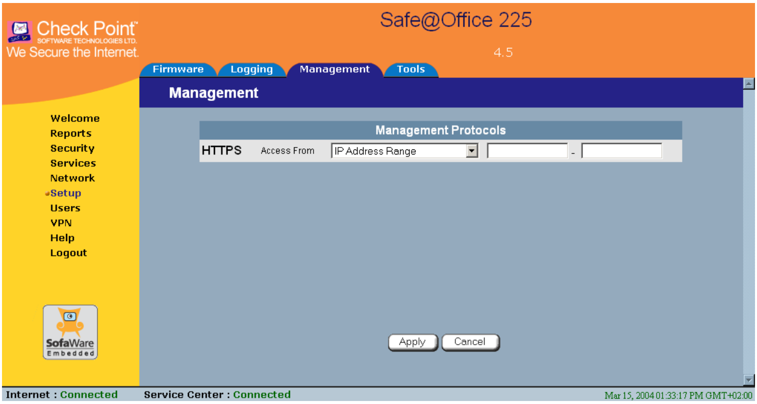
HTTPS Access From Internal Network

Internet : Connected Service Center : Connected Mar 15, 2004 01:32:46 PM GMT+02:00

2. Specify from where HTTPS access to the Safe@Office Portal should be granted. See ***HTTPS Access Options*** on page 267 for information.

Warning: If remote HTTPS is enabled, your Safe@Office appliance settings can be changed remotely, so make sure all Safe@Office appliance users' passwords are unguessable.

If you selected IP Address Range, additional fields appear.



HTTPS Access From: IP Address Range [ ] - [ ]

Internet : Connected Service Center : Connected Mar 15, 2004 01:33:17 PM GMT+02:00

3. If you selected IP Address Range, enter the desired IP address range in the fields provided.
4. Click Apply.

   The HTTPS configuration is saved. You can now access the Safe@Office Portal through the Internet, using the procedure ***Accessing the Safe@Office Portal Remotely*** on page 49.

Table 41: HTTPS Access Options

Select this option…	To allow HTTPS access from…
Internal Network	The internal network only. This disables remote HTTPS capability. Note: You can use HTTPS to access the Safe@Office Portal from your internal network, by surfing to https://my.firewall.
Internal Network and VPN	The internal network and your VPN.
IP Address Range	A particular range of IP addresses. Additional fields appear, in which you can enter the desired IP address range.
ANY	Any IP address.

Setting the Time on the Appliance

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

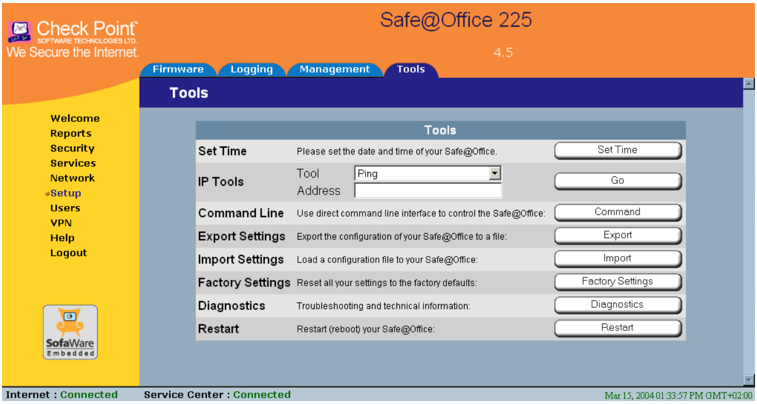
You set the time displayed in the Safe@Office 225 Portal during initial appliance setup. If desired, you can change the date and time displayed in the Safe@Office 225 Portal using the procedure below.

Note: The Safe@Office 100 series takes the time from your local computer and you do not have to manually set the time.

To set the time

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

   The **Tools** page appears.



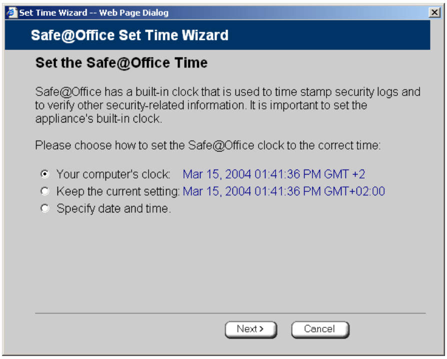
Tools		
Set Time	Please set the date and time of your Safe@Office.	Set Time
IP Tools	Tool: Ping Address:	Go
Command Line	Use direct command line interface to control the Safe@Office:	Command
Export Settings	Export the configuration of your Safe@Office to a file:	Export
Import Settings	Load a configuration file to your Safe@Office:	Import
Factory Settings	Reset all your settings to the factory defaults:	Factory Settings
Diagnostics	Troubleshooting and technical information:	Diagnostics
Restart	Restart (reboot) your Safe@Office:	Restart

Internet : Connected   Service Center : Connected   Mar 15, 2004 01:33:57 PM GMT+02:00

   If you are using Safe@Office 105 or 110, the page appears without the **Set Time** button.

2. Click **Set Time**.

The **Safe@Office Set Time Wizard** opens displaying the **Set the Safe@Office time** dialog box.


Set Time Wizard -- Web Page Dialog
Safe@Office Set Time Wizard
Next >
Cancel

Set the Safe@Office Time

Safe@Office has a built-in clock that is used to time stamp security logs and to verify other security-related information. It is important to set the appliance's built-in clock.

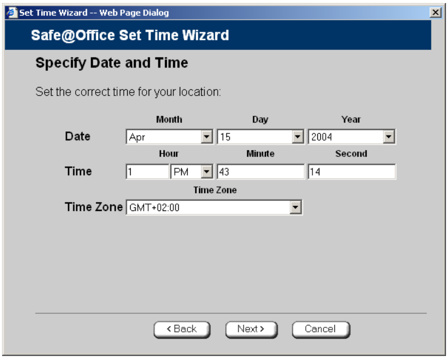
Please choose how to set the Safe@Office clock to the correct time:

- ● Your computer's clock: Mar 15, 2004 01:41:36 PM GMT +2
- ○ Keep the current setting: Mar 15, 2004 01:41:36 PM GMT+02:00
- ○ Specify date and time.

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

The following things happen in the order below:

- If you selected **Specify date and time**, the **Specify Date and Time** dialog box appears.


Set Time Wizard -- Web Page Dialog
Safe@Office Set Time Wizard
< Back
Next >
Cancel

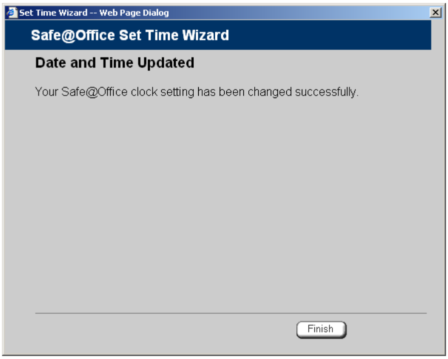
Specify Date and Time

Set the correct time for your location:

	Month	Day	Year
Date	Apr	15	2004
	Hour	Minute	Second
Time	1 PM	43	14
	Time Zone		
Time Zone	GMT+02:00		

Set the date, time, and time zone in the fields provided, then click **Next.**

- The Date and Time Updated window appears.



Safe@Office Set Time Wizard

Date and Time Updated

Your Safe@Office clock setting has been changed successfully.

5. Click **Finish**.

Table 42: Set Time Wizard Fields

Select this option…	To allow HTTPS access from…
Your computer's clock	Set the appliance time to your computer’s system time. Your computer’s system time is displayed to the right of this option.
Keep the current time	Do not change the appliance’s time. The current appliance time is displayed to the right of this option.
Specify date and time	Set the appliance to a specific date and time.

Controlling the Appliance via the Command Line

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

The Safe@Office Portal enables you to control your appliance via the command line interface.

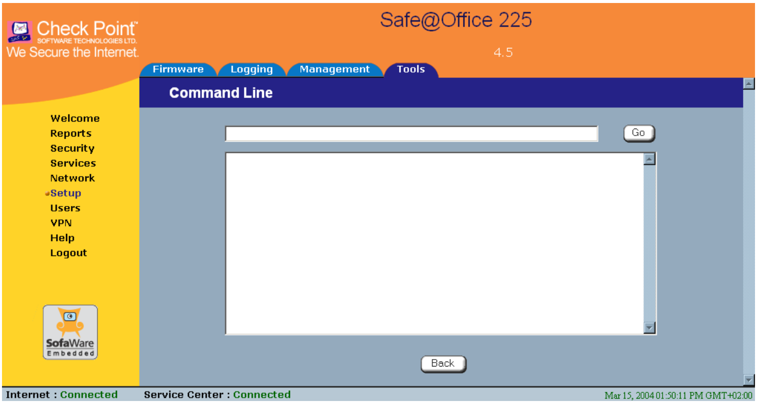
To control the appliance via the command line

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

   The Tools page appears.

2. Click Command.

   The Command Line page appears.



3. In the upper field, type a command.

   You can view a list of supported commands using the command help.

   For information on all commands, refer to the *Embedded NG CLI Reference Guide*.

4. Click Go.

The command is implemented.

Using Diagnostic Tools

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

The Safe@Office appliance is equipped with a set of diagnostic tools that are useful for troubleshooting Internet connectivity.

Table 43: Diagnostic Tools

Use this tool...	To do this...
Ping	Check that a specific IP address or DNS name can be reached via the Internet.
Traceroute	Display a list of all routers used to connect from the Safe@Office appliance to a specific IP address or DNS name.
WHOIS	Display the name and contact information of the entity to whom a specific IP address or DNS name is registered. This information is useful in tracking down hackers.

To use a diagnostic tool

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

   The Tools page appears.

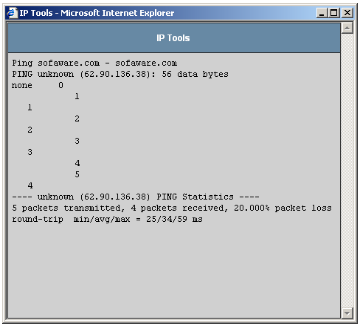
2. In the Tools drop-down list, select the desired tool.
3. In the Address field, type the IP address or DNS name for which to run the tool.

4. Click **Go**.

- If you selected **Ping**, the following things happen:

  The Safe@Office appliance sends packets to the specified the IP address or DNS name.

  The IP Tools window opens and displays the percentage of packet loss and the amount of time it each packet took to reach the specified host and return (round-trip) in milliseconds.

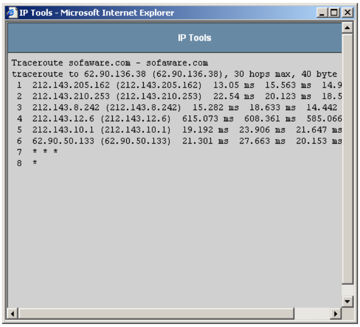
  

```
Ping sofaware.com - sofaware.com
PING unknown (62.90.136.38): 56 data bytes
none     0
            1
   1
            2
   2
            3
   3
            4
            5
   4
---- unknown (62.90.136.38) PING Statistics ----
5 packets transmitted, 4 packets received, 20.000% packet loss
round-trip  min/avg/max = 25/34/59 ms
```

- If you selected **Traceroute**, the following things happen:

  The Safe@Office appliance connects to the specified IP address or DNS name.

  The **IP Tools** window opens and displays a list of routers used to make the connection.

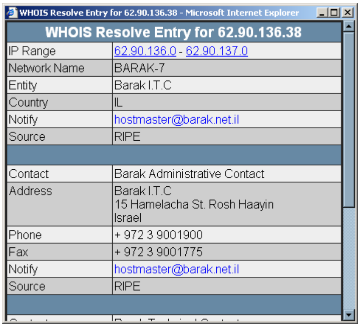
  

```
Traceroute sofaware.com - sofaware.com
traceroute to 62.90.136.38 (62.90.136.38), 30 hops max, 40 byte
 1  212.143.205.162 (212.143.205.162)  13.05 ms  15.563 ms  14.9
 2  212.143.210.253 (212.143.210.253)  22.54 ms  20.123 ms  18.5
 3  212.143.8.242 (212.143.8.242)  15.282 ms  18.633 ms  14.442
 4  212.143.12.6 (212.143.12.6)  615.073 ms  608.361 ms  585.066
 5  212.143.10.1 (212.143.10.1)  19.192 ms  23.906 ms  21.647 ms
 6  62.90.50.133 (62.90.50.133)  21.301 ms  27.663 ms  20.153 ms
 7  * * *
 8  *
```

- If you selected WHOIS, the following things happen:

  The Safe@Office appliance queries the Internet WHOIS server.

  A window displays the name of the entity to whom the IP address or DNS name is registered and their contact information.



WHOIS Resolve Entry for 62.90.136.38 - Microsoft Internet Explorer

WHOIS Resolve Entry for 62.90.136.38	
IP Range	62.90.136.0 - 62.90.137.0
Network Name	BARAK-7
Entity	Barak I.T.C
Country	IL
Notify	hostmaster@barak.net.il
Source	RIPE
Contact	Barak Administrative Contact
Address	Barak I.T.C 15 Hamelacha St. Rosh Haayin Israel
Phone	+ 972 3 9001900
Fax	+ 972 3 9001775
Notify	hostmaster@barak.net.il
Source	RIPE

Backing Up the Safe@Office Appliance Configuration

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

You can export the Safe@Office appliance configuration to a *.cfg file, and use this file to backup and restore Safe@Office appliance settings, as needed. The configuration file includes all your settings.

Exporting the Safe@Office Appliance Configuration

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

Exporting the Safe@Office appliance configuration creates a configuration file.

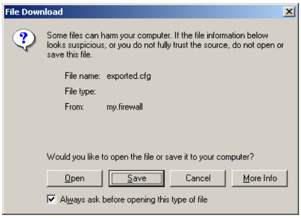
To export the Safe@Office appliance configuration

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

   The **Tools** page appears.

2. Click **Export**.

   A standard **File Download** dialog box appears.



File Download

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

File name: exported.cfg

File type:

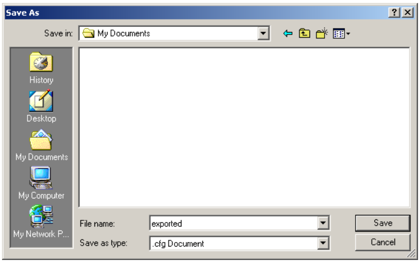
From: my.firewall

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

☑ Always ask before opening this type of file

3. Click **Save**.

   The **Save As** dialog box appears.



Save As

Save in: My Documents

File name: exported

Save as type: .cfg Document

4. Browse to a destination directory of your choice.

5. Type a name for the configuration file and click **Save**.

   The *.cfg configuration file is created and saved to the specified directory.

Importing the Safe@Office Appliance Configuration

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

In order to restore your Safe@Office appliance's configuration from a configuration file, you must import the file.

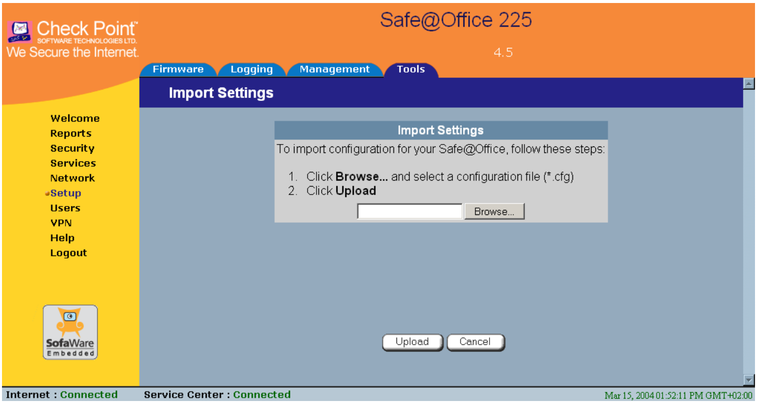
To import the Safe@Office appliance configuration

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

   The **Tools** page appears.

2. Click **Import**.

   The **Import Settings** page appears.



Import Settings

To import configuration for your Safe@Office, follow these steps:

1. Click **Browse...** and select a configuration file (*.cfg)
2. Click **Upload**

3. Do one of the following:

   - In the **Import Settings** field, type the full path to the configuration file.

   Or

   - Click **Browse**, and browse to the configuration file.

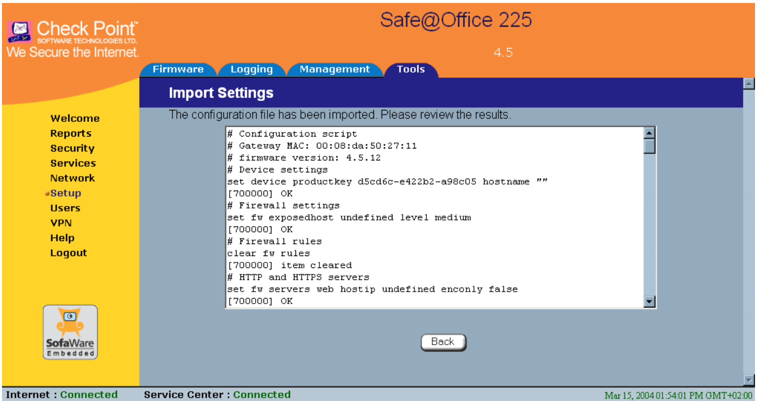
4. Click **Upload**.

A confirmation message appears.

5. Click OK.

The Safe@Office appliance settings are imported.

The Import Settings page displays the configuration file's content and the result of implementing each configuration command.



Import Settings

The configuration file has been imported. Please review the results.

```
# Configuration script
# Gateway MAC: 00:08:da:50:27:11
# firmware version: 4.5.12
# Device settings
set device productkey d5cd6c-e422b2-a98c05 hostname ""
[700000] OK
# Firewall settings
set fw exposedhost undefined level medium
[700000] OK
# Firewall rules
clear fw rules
[700000] item cleared
# HTTP and HTTPS servers
set fw servers web hostip undefined enconly false
[700000] OK
```

Internet : Connected   Service Center : Connected   Mar 15, 2004 01:54:01 PM GMT+02:00

Resetting the Safe@Office Appliance to Defaults

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

You can reset the Safe@Office appliance to its default settings. When you reset your Safe@Office appliance, it reverts to the state it was originally in when you purchased it. You can choose to keep the current firmware or to revert to the firmware version that shipped with the Safe@Office appliance.

Warning: This operation erases all your settings and password information. You will have to set a new password and reconfigure your Safe@Office appliance for Internet connection. For information on performing these tasks, see ***Setting Up the Safe@Office Appliance*** on page 41.

You can reset the Safe@Office appliance to defaults via the Web management interface (software) or by manually pressing the Reset button (hardware) located at the back of the Safe@Office appliance.

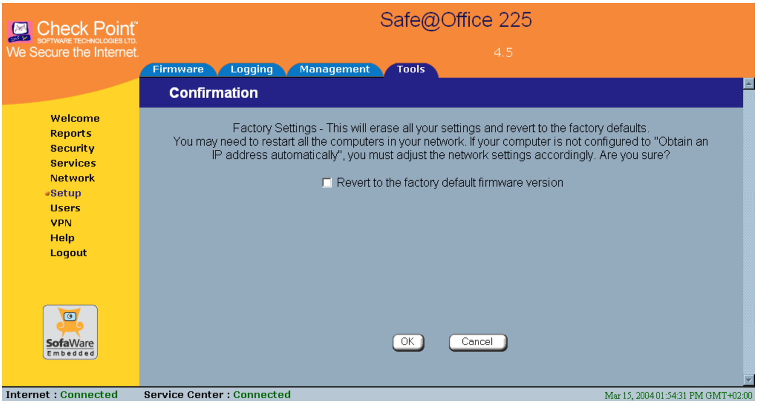
To reset the Safe@Office appliance to factory defaults via the Web interface

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

   The **Tools** page appears.

2. Click **Factory Settings.**

   A confirmation message appears.



Confirmation

Factory Settings - This will erase all your settings and revert to the factory defaults.
You may need to restart all the computers in your network. If your computer is not configured to "Obtain an IP address automatically", you must adjust the network settings accordingly. Are you sure?

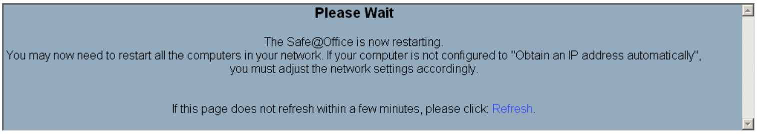
□ Revert to the factory default firmware version

Internet : Connected   Service Center : Connected   Mar 15, 2004 01:54:31 PM GMT+02:00

3. To revert to the firmware version that shipped with the appliance, select the check box.

4. Click **OK**.

   - The **Please Wait** screen appears.



Please Wait

The Safe@Office is now restarting.
You may now need to restart all the computers in your network. If your computer is not configured to "Obtain an IP address automatically", you must adjust the network settings accordingly.

If this page does not refresh within a few minutes, please click: Refresh.

   - The Safe@Office appliance returns to its factory defaults.

- The Safe@Office appliance is restarted (the PWR/SEC LED flashes quickly).

  This may take a few minutes.

- The Login page appears.

To reset the Safe@Office appliance to factory defaults using the Reset button

1. Make sure the Safe@Office appliance is powered on.
2. Using a pointed object, press the RESET button on the back of the Safe@Office appliance steadily for seven seconds and then release it.
3. Allow the Safe@Office appliance to boot-up until the system is ready (PWR/SEC LED flashes slowly or illuminates steadily in green light).

   For information on the appliance's front and rear panels, see ***Getting to Know Your Safe@Office 100 Series*** on page 14 or ***Getting to Know Your Safe@Office 200 Series*** on page 17.

⚠ Warning: If you choose to reset the Safe@Office appliance by disconnecting the power cable and then reconnecting it, be sure to leave the Safe@Office appliance disconnected for at least three seconds, or the Safe@Office appliance might not function properly until you reboot it as described below.

Running Diagnostics

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

You can view technical information about your Safe@Office appliance’s hardware, firmware, license, network status, and Service Center.

This information is useful for troubleshooting. You can copy and paste it into the body an email and send it to technical support.

To run diagnostics

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

   The **Tools** page appears.

2. Click **Diagnostics**.

   Technical information about your Safe@Office appliance appears in a new window.

3. To refresh the contents of the window, click **Refresh**.

   The contents are refreshed.

4. To close the window, click **Close**.

Rebooting the Safe@Office Appliance

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

If your Safe@Office appliance is not functioning properly, rebooting it may solve the problem.

To reboot the Safe@Office appliance

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

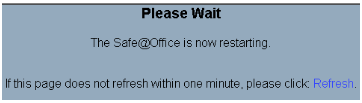
   The **Tools** page appears.

2. Click **Restart**.

   A confirmation message appears.

3. Click **OK**.

   - The **Please Wait** screen appears.



Please Wait

The Safe@Office is now restarting.

If this page does not refresh within one minute, please click: Refresh.

- The Safe@Office appliance is restarted (the PWR/SEC LED flashes quickly).

  This may take a few minutes.

- The Login page appears.

Chapter 13

Troubleshooting

This chapter provides solutions to common problems you may encounter while using the Safe@Office appliance.

This chapter includes the following topics:

Connectivity

I cannot access the Internet. What should I do?

- Check if the PWR/SEC LED is green. If not, check the power connection to the Safe@Office appliance.
- Check if the WAN LINK/ACT LED is green. If not, check the network cable to the modem and make sure the modem is turned on.
- Check if the LAN LINK/ACT LED for the port used by your computer is green. If not, check if the network cable linking your computer to the Safe@Office appliance is connected properly. Try replacing the cable or connecting it to a different LAN port.
- Using your web browser, go to http://my.firewall and see whether "Connected" appears on the Status Bar. Make sure that your Safe@Office appliance network settings are configured as per your ISP directions.
- Check your TCP/IP configuration according to ***Installing and Setting up the Safe@Office Appliance*** on page 25.
- If Web Filtering or Email Anti Virus scanning are on, try turning them off.

- Check if you have defined firewall rules which block your Internet connectivity.
- Check with your ISP for possible service outage.
- Check whether you are exceeding the maximum number of computers allowed by your license, by following the procedure ***Viewing Computers*** on page 144.

I cannot access my DSL broadband connection. What should I do?

DSL equipment comes in two flavors: bridges (commonly known as DSL modems) and routers. Some DSL equipment can be configured to work both ways.

- If you connect to your ISP using a PPPoE or PPTP dialer defined in your operating system, your equipment is most likely configured as a DSL bridge. Configure a PPPoE or PPTP type DSL connection.
- If you were not instructed to configure a dialer in your operating system, your equipment is most likely configured as a DSL router. Configure a LAN connection, even if you are using a DSL connection.

For instructions, see ***Configuring the Internet Connection*** on page 57.

I cannot access my Cable broadband connection. What should I do?

- Some cable ISPs require you to register the MAC address of the device behind the cable modem. You may need to clone your Ethernet adapter MAC address onto the Safe@Office appliance. For instructions, see ***Configuring the Internet Connection*** on page 57.
- Some cable ISPs require using a hostname for the connection. Try reconfiguring your Internet connection and specifying a hostname. For further information, see ***Configuring the Internet Connection*** on page 57.

I cannot access http://my.firewall or http://my.vpn. What should I do?

- Verify that the Safe@Office appliance is operating (PWR/SEC LED is active)
- Check if the LAN LINK/ACT LED for the port used by your computer is on. If not, check if the network cable linking your computer to the Safe@Office appliance is connected properly.

Note: You may need to use a crossed cable when connecting the Safe@Office appliance to another hub/switch.

- Try surfing to 192.168.10.1 instead of to my.firewall.

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

- Check your TCP/IP configuration according to ***Installing and Setting up the Safe@Office Appliance*** on page 25.
- Restart your Safe@Office appliance and your broadband modem by disconnecting the power and reconnecting after 5 seconds.
- If your web browser is configured to use an HTTP proxy to access the Internet, add "my.firewall" or "my.vpn" to your proxy exceptions list.

My network seems extremely slow. What should I do?

- The Ethernet cables may be faulty. For proper operation, the Safe@Office appliance requires STP CAT5 (Shielded Twisted Pair Category 5) Ethernet cables. Make sure that this specification is printed on your cables.

- Your Ethernet card may be faulty or incorrectly configured. Try replacing your Ethernet card.

- There may be an IP address conflict in your network. Check that the TCP/IP settings of all your computers are configured to obtain an IP address automatically.

I changed the network settings to incorrect values and am unable to correct my error. What should I do?

Reset the network to its default settings using the button on the back of the Safe@Office appliance unit. See ***Resetting the Safe@Office Appliance to Defaults*** on page 277.

I am using the Safe@Office appliance behind another NAT device, and I am having problems with some applications. What should I do?

By default, the Safe@Office appliance performs Network Address Translation (NAT). It is possible to use the Safe@Office appliance behind another device that performs NAT, such as a DSL router or Wireless router, but the device will block all incoming connections from reaching your Safe@Office appliance.

To fix this problem, do ONE of the following. (The solutions are listed in order of preference.)

- Consider whether you really need the router. The Safe@Office appliance can be used as a replacement for your router, unless you need it for some additional functionality that it provides, such as Wireless access.
- If possible, disable NAT in the router. Refer to the router's documentation for instructions on how to do this.
- If the router has a "DMZ Computer" or "Exposed Host" option, set it to the Safe@Office appliance's external IP address.
- Open the following ports in the NAT device:
  - UDP 9281/9282
  - UDP 500
  - TCP 256
  - TCP 264
  - ESP IP protocol 50
  - TCP 981

I cannot receive audio or video calls through the Safe@Office appliance. What should I do?

To enable audio/video, you must configure an IP Telephony (H.323) virtual server. For instructions, see ***Configuring Servers*** on page 152.

I run a public Web server at home but it cannot be accessed from the Internet. What should I do?

Configure a virtual Web Server. For instructions, see ***Configuring Servers*** on page 152.

I cannot connect to the LAN network from the DMZ network. What should I do?

By default, connections from the DMZ network to the LAN network are blocked. To allow traffic from the DMZ to the LAN, configure appropriate firewall rules. For instructions, see ***Using Rules*** on page 154.

Service Center and Upgrades

I purchased Safe@Office 110, but I only have Safe@Office 105 functionality. What should I do?

Your have not installed your product key. For further information, see ***Upgrading Your Software Product*** on page 258.

I have exceeded my node limit. What does this mean? What should I do?

Your Product Key specifies a maximum number of nodes that you may connect to the Safe@Office appliance.

The Safe@Office appliance tracks the cumulative number of nodes on the internal network that have communicated through the firewall. When the Safe@Office appliance encounters an IP address that exceeds the licensed node limit, the Active Computers page displays a warning message and marks nodes over the node limit in red. These nodes will not be able to access the Internet through the Safe@Office appliance, but will be protected. The Event Log page also warns you that you have exceeded the node limit.

To upgrade your Safe@Office appliance to support more nodes, purchase a new Product Key. Contact your reseller for upgrade information.

While trying to connect to a Service Center, I received the message “The Service Center did not respond”. What should I do?

- If you are using a Service Center other than the Check Point Service Center, check that the Service Center IP address is typed correctly.
- The Safe@Office appliance connects to the Service Center using UDP ports 9281/9282. If the Safe@Office appliance is installed behind another firewall, make sure that these ports are open.

Other Problems

I have forgotten my password. What should I do?

Reset your Safe@Office appliance to factory defaults using the Reset button as detailed in ***Resetting the Safe@Office Appliance to Defaults*** on page 277.

Why are the date and time displayed incorrectly?

In the Safe@Office 100 series, when a computer on the LAN connects to the Safe@Office Portal, the Safe@Office appliance adjusts its date and time to match that of the computer. If the date and time displayed in the Safe@Office Portal are incorrect, it probably means that the date and time on the computer connected to the Safe@Office Portal are incorrect.

In the Safe@Office 200 series, you can adjust the time on the Setup page's Tools tab. For information, see ***Setting the Time on the Appliance*** on page 267.

I cannot use a certain network application. What should I do?

Look at the Event Log page. If it lists blocked attacks, do the following:

- Turn the Safe@Office appliance security to Low and try again.
- If the application still does not work, set the computer on which you want to use the application to be the exposed host.

  For instructions, see ***Defining an Exposed Host*** on page 163.

When you have finished using the application, make sure to clear the exposed host setting, otherwise your security might be compromised.

I installed McAfee VirusScan ASaP, but the SecureDesk status message says "SecureDesk not installed". What should I do?

If you are using Windows XP, then the Windows XP firewall probably prevented VirusScan from being installed correctly. Do the following:

1. Uninstall McAfee VirusScan ASaP via the Control Panel.
2. Disable the Windows XP Internet Connection Firewall option.
3. Re-install McAfee VirusScan ASaP using the information in ***Installing McAfee VirusScan ASaP*** on page 184.

Chapter 14

Specifications

This chapter includes the following topics:

Technical Specifications

Table 44: Safe@Office Appliance Attributes

Attribute	Safe@Office 105/110/ 255/225U	Safe@Office 300	Safe@Office 300W
General			
Dimensions (width x height x depth)	20.32 x 3.05 x 12.19 cm (8 x 1.2 x 4.8 inches)	20 x 3.1 x 13.24 cm (7.9 x 1.2 x 5.2 inches)	20 x 3.1 x 15.5 cm (7.9 x 1.2 x 6.1 inches)
Weight	0.7 kg (1.56 lbs)	0.64 kg	0.69 kg (1.55 lbs)

Attribute	Safe@Office 105/110/ 255/225U	Safe@Office 300	Safe@Office 300W
Supply voltage	110VAC (90 to 132 VAC) 100VAC 230VAC (200 to 265 VAC)	100 ~ 240 VAC	100 to 240VAC
Line voltage frequency, AC	50/60 Hz (47 to 63 Hz)	50/60 Hz	50/60 Hz
Max. Power Consumption	13.5W (100series)/7.5W (200series)	MAX 5.75W (MAX 1.15A) w/o external USB devices (USB – MAX 1A)	MAX 8W (MAX1.6A) w/o external USB devices (USB – MAX 1A)
Retail box dimensions (width x height x depth)	31 x 10 x 16 cm (12.4 x 4 x 6.4 inches)	29 x 25 x 76 cm (11.4 x 9.8 x 3 inches)	29 x 25 x 7.6 cm (11.4 x 9.8 x 3 inches)
Retail box weight	1.3 kg (2.9 lbs)	1.3 kg (2.9 lbs)	1.35 kg (3 lbs)
Environmental Conditions			

Attribute	Safe@Office 105/110/ 255/225U	Safe@Office 300	Safe@Office 300W
Temperature: Storage/Transport	- 20°C to +70°C	- 5°C to +70°C	- 5°C to +70°C
Temperature: Operation	+ 5°C to +45°C	- 5°C ~ 50°C	- 5°C ~ 50°C
Humidity: Storage/Operation	5% to 90% at 25°C (no condensation)	0% ~ 90%	0% ~ 90%
Applicable Standards			
Shock & Vibration	ETSI 300 019-2-3 CLASS 3.1 & Bellcore GR 63 (NEBS)	CNS1219 C6343	CNS1219 C6343
Safety	EN60950/ IEC 60950	EN60950/ IEC 60950	EN60950/ IEC 60950

Attribute	Safe@Office 105/110/ 255/225U	Safe@Office 300	Safe@Office 300W
Quality	ISO9001	ISO9001:2000 TL9000-HW R3.0 ISO14001 Ohsas18001: 1999	ISO9001:2000 TL9000-HW R3.0 ISO14001 Ohsas18001: 1999

CE Declaration of Conformity

SofaWare Technologies Ltd., 3 Hilazon St., Ramat-Gan Israel, hereby declares that this equipment is in conformity with the essential requirements specified in Article 3.1 (a) and 3.1 (b) of:

- Directive 89/336/EEC (EMC Directive)
- Directive 73/23/EEC (Low Voltage Directive – LVD)
- Directive 99/05/EEC (Radio Equipment and Telecommunications Terminal Equipment Directive)

In accordance with the following standards:

Table 45: Safe@Office Appliance Standards

Safe@Office 105/110/ 255/225U	Safe@Office 300	Safe@Office 300W
EN 50081-1:1992 EN 50082-1:1997 EN 61000-6-1:2001 EN 61000-6-3:2001 EN 55022:1998 EN 55024:1998 EN 61000-3-2: 1995	EN55022: 1994+A1: 1995+A2: 1997 EN 61000-3-2:2000 EN 61000-3-3:1995+ A1:2001 EN55024: 1998+A1: 2001+A2: 2003 IEC 61000-4-2:2001	EN 300 328 V 1.4.1(2003-04) EN 301 489-1 V 1.4.1(2002-08) EN 301 489-17 V 1.2.1(2002-08) EN 55022:1994+A1: 1995+A2 1997, Class B EN 61000-3-2:2000 EN 61000-3-3:1995+A1: 2001

Safe@Office 105/110/255/225U	Safe@Office 300	Safe@Office 300W
EN 61000-3-3: 1995 EN 61000-4-2:1995 EN 61000-4-3:1996/A2:2001 EN 61000-4-4:1995 EN 61000-4-5:1995 EN 61000-4-6:1996 EN 61000-4-7:1993 EN 61000-4-8:1993 EN 61000-4-9:1993 EN 61000-4-10:1993 EN 61000-4-11:1994 EN 61000-4-12:1995 EN 60950: 1992	IEC 61000-4-3:2002+A1:2002 IEC 61000-4-4:1995+A1:2002+A2:2001 IEC 61000-4-5:2001 IEC 61000-4-6:2001 IEC 61000-4-8:2001 IEC 61000-4-11:2001 EN 60950-1:2001	EN 61000-4-2:1995+A1:1998+A2:2001 EN 61000-4-3:1996+A1:1998+A2: 2001 EN 61000-4-4:1995+A1:2001+A2: 2001 EN 61000-4-5:1995+A1:2001 EN 61000-4-6:1996+A1:2001 EN 61000-4-11:1994+A1: 2001 EN 60950-1: 2001

The "CE" mark is affixed to this product to demonstrate conformance to the R&TTE Directive 99/05/EEC (Radio Equipment and Telecommunications Terminal Equipment Directive) and FCC Part 15 Class B.

The product has been tested in a typical configuration. For a copy of the Original Signed Declaration (in full conformance with EN45014), please contact SofaWare at the above address.

Federal Communications Commission Radio Frequency Interference Statement

This equipment complies with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Shielded cables must be used with this equipment to maintain compliance with FCC regulations.

Changes or modifications not expressly approved by the manufacturer could void the user’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

Glossary of Terms

A

ADSL Modem

A device connecting a computer to the Internet via an existing phone line. ADSL (Asymmetric Digital Subscriber Line) modems offer a high-speed 'always-on' connection.

C

CA

The Certificate Authority (CA) issues certificates to entities such as gateways, users, or computers. The entity later uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the Distinguishing Name (DN) (identifying information) of the entity, as well as the public key (information about itself), and possibly the IP address.

After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

Cable Modem

A device connecting a computer to the Internet via the cable television network. Cable modems offer a high-speed 'always-on' connection.

Certificate Authority

The Certificate Authority (CA) issues certificates to entities such as gateways, users, or computers. The entity later uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the Distinguishing Name (DN) (identifying information) of the entity, as well as the public key (information about itself), and possibly the IP address.

After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

Cracking

An activity in which someone breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is that whatever resides on the computer can be viewed and sensitive data can be stolen without anyone knowing about it. Sometimes, tiny programs are 'planted' on the computer that are designed to watch out for, seize and then transmit to another computer, specific types of data.

D

DHCP

Any machine requires a unique IP address to connect to the Internet using Internet Protocol. Dynamic Host Configuration Protocol (DHCP) is a communications protocol that assigns Internet Protocol (IP) addresses to computers on the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer.

DMZ

A DMZ (demilitarized zone) is an internal network defined in addition to the LAN network and protected by the Safe@Office appliance.

DNS

The Domain Name System (DNS) refers to the Internet domain names, or easy-to-remember "handles", that are translated into IP addresses.

An example of a Domain Name is 'www.sofaware.com'.

Domain Name System

Domain Name System. The Domain Name System (DNS) refers to the Internet domain names, or easy-to-remember "handles", that are translated into IP addresses.

An example of a Domain Name is 'www.sofaware.com'.

E

Exposed Host

An exposed host allows one computer to be exposed to the Internet. An example of using an exposed host would be exposing a public server, while preventing outside users from getting direct access form this server back to the private network.

F

Firmware

Software embedded in a device.

G

Gateway

A network point that acts as an entrance to another network.

H

Hacking

An activity in which someone breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is that whatever resides on the computer can be viewed and sensitive data can be stolen without anyone knowing about it. Sometimes, tiny programs are 'planted' on the computer that are designed to watch out for, seize and then transmit to another computer, specific types of data.

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL.

A protocol for accessing a secure Web server. It uses SSL as a sublayer under the regular HTTP application. This directs messages to a secure port number rather than the default Web port number, and uses a public key to encrypt data

HTTPS is used to transfer confidential user information.

Hub

A device with multiple ports, connecting several PCs or network devices on a network.

I

IP Address

An IP address is a 32-bit number that identifies each computer sending or receiving data packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IP Spoofing

A technique where an attacker attempts to gain unauthorized access through a false source address to make it appear as though communications have originated in a part of the network with higher access privileges. For example, a packet originating on the Internet may be masquerading as a local packet with the source IP address of an internal host. The firewall can protect against IP spoofing attacks by limiting network access based on the gateway interface from which data is being received.

IPSEC

IPSEC is the leading Virtual Private Networking (VPN) standard. IPSEC enables individuals or offices to establish secure communication channels ('tunnels') over the Internet.

ISP

An ISP (Internet service provider) is a company that provides access to the Internet and other related services.

L

LAN

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single server within a small geographic area.

M

MAC Address

The MAC (Media Access Control) address is a computer's unique hardware number. When connected to the Internet from your computer, a mapping relates your IP address to your computer's physical (MAC) address on the LAN.

Mbps

Megabits per second. Measurement unit for the rate of data transmission.

MTU

The Maximum Transmission Unit (MTU) is a parameter that determines the largest datagram than can be transmitted by an IP interface (without it needing to be broken down into smaller units). The MTU should be larger than the largest datagram you wish to transmit un-fragmented. Note: This only prevents fragmentation locally. Some other link in the path may have a smaller MTU - the datagram will be fragmented at that point. Typical values are 1500 bytes for an Ethernet interface or 1452 for a PPP interface.

N

NAT

Network Address Translation (NAT) is the translation or mapping of an IP address to a different IP address. NAT can be used to map several internal IP addresses to a single IP address, thereby sharing a single IP address assigned by the ISP among several PCs.

Check Point FireWall-1's Stateful Inspection Network Address Translation (NAT) implementation supports hundreds of pre-defined applications, services, and protocols, more than any other firewall vendor.

NetBIOS

NetBIOS is the networking protocol used by DOS and Windows machines.

P

Packet

A packet is the basic unit of data that flows from one source on the Internet to another destination on the Internet. When any file (e-mail message, HTML file, GIF file etc.) is sent from one place to another on the Internet, the file is divided into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file at the receiving end.

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) enables connecting multiple computer users on an Ethernet local area network to a remote site or ISP, through common customer premises equipment (e.g. modem).

PPTP

The Point-to-Point Tunneling Protocol (PPTP) allows extending a local network by establishing private “tunnels” over the Internet. This protocol it is also used by some DSL providers as an alternative for PPPoE.

R

RJ-45

The RJ-45 is a connector for digital transmission over ordinary phone wire.

Router

A router is a device that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks.

S

Server

A server is a program (or host) that awaits and requests from client programs across the network. For example, a Web server is the computer program, running on a specific host, that serves requested HTML pages or files. Your browser is the client program, in this case.

Stateful Inspection

Stateful Inspection was invented by Check Point to provide the highest level of security by examining every layer within a packet, unlike other systems of inspection. Stateful Inspection extracts information required for security decisions from all application layers and retains this information in dynamic state tables for evaluating subsequent connection attempts. In other words, it learns!

Subnet Mask

A 32-bit identifier indicating how the network is split into subnets. The subnet mask indicates which part of the IP address is the host ID and which indicates the subnet.

T

TCP

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

For example, when an HTML file is sent to you from a Web server, the Transmission Control Protocol (TCP) program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network.

At the other end (the client program in your computer), TCP reassembles the individual packets and waits until they have arrived to forward them to you as a single file.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the underlying communication protocol of the Internet.

U

UDP

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end.

UDP is often used for applications such as streaming data.

URL

A URL (Uniform Resource Locator) is the address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol. On the Web (which uses the Hypertext Transfer Protocol), an example of a URL is 'http://www.sofaware.com'.

V

VPN

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

VPN tunnel

A secure connection between a Remote Access VPN Client and a Remote Access VPN Server.

W

WLAN

A WLAN is a wireless local area network protected by the Safe@Office appliance.

Index