

Safepipe 5000 Series

Quick Installation Guide

SAFEPIPE™ 5000 Series Quick Installation Guide

Introduction	3
What is in the box?	4
Contents	
SAFEPIPE™ 5000 Series	
Quick Installation Guide	
Administrator's CD-ROM	
Administrator's Booklet	
Before You Start	5
Product Description	7
Hardware Description	
Initial Installation	9
Welcome to Safepipe's Browser-Based Management Interface	13
Getting started	14
You are now ready to begin configuration of Safepipe	16

Safepipe 5000 Series Quick Installation Guide

For New Installations

Introduction

Thank you for choosing Safepipe and welcome to the world of Virtual Private Networking with IPSec.

Correctly configured, your Safepipe will enable your communication to take place securely via VPN 'tunnels'. You are able to create such VPN tunnels in more than one way:

- between two Safepipes, for example the Safepipe on your network and one on a network belonging to a branch or business partner
- between a Safepipe and a workstation with VPN Client software. It is possible to create VPN tunnels between a Safepipe and up to 1000 such VPN Clients, depending on the Safepipe version.

With this Quick Installation Guide you will be able to install Safepipe onto your LAN and prepare the interface for further configuration. Actual tunnel and client configurations and general usage instructions are found in the Administrator's Guide.

What is in the box?

Contents:

One **Safepipe 5000 Series** VPN device, one Quick Installation Guide, one Administrator's CD-ROM, one Administrator's Guide, five VPN Client CD-ROMs, one power cable, two Ethernet cables, two rack mounting brackets, and eight screws.

If anything is missing, please contact your Eicon product distributor.

Safepipe 5000 Series

An all-in-one secure communication product that is a high performance VPN solution for large enterprises. With a 20Mbit throughput, it supports up to 200 LAN-to-LAN tunnels and 1000 remote users.

Quick Installation Guide

The guide helps you quickly install your Safepipe to the private LAN for the first time. It also introduces you to Safepipe's convenient browser-based management interface.

Administrator's CD-ROM,

An installation wizard to assist you in setting up your Safepipe as well as a guide that includes maintenance and troubleshooting topics. The Administrator's CD-ROM runs on the following Windows operating systems: 95/98, 2000, NT and ME.

Administrator's Guide

The booklet takes you through tunnel and VPN Client configurations. Tunnels are the basis of any VPN through which encrypted data travels securely over the Internet. During Safepipe's configuration and management, the term 'tunnel' refers to the connection between two LANs over an unsecure network. The term 'VPN Client' refers to a telecommuter's or mobile worker's remote workstation that needs access to one of the offices' LAN.

Before You Start:

- You must determine the LAN IP address and subnet mask that you wish Safepipe to use.
- The IP address must be permanently assigned to Safepipe and cannot be provided dynamically by DHCP.
- Safepipe and the administrator's PC (the one used to install and configure Safepipe) must be on the same LAN. This affects both the IP address and subnet.
 - For example: the LAN has the network number *192.168.2.xxx* and the administrator's PC has the IP address of *192.168.2.21*, then Safepipe could use the IP address *192.168.2.1*.
 - For example: The PC has subnet mask *255.255.255.0*, therefore Safepipe should also use the subnet mask *255.255.255.0*.

You can find out what the administrator PC's IP address and subnet mask are by clicking Start > Run, entering WINIPCFG (Windows 95/98/Me) or IPCONFIG (Windows NT/2000) and clicking OK. Click on the Ethernet/LAN adaptor from the pull-down menu.

- You must choose a secure password for the Safepipe configuration interface.

To get the most out of your security equipment, you should be careful to use passwords that are impossible to guess. Secure password usage allows Safepipe to function as intended.

Passwords should not be names of people and places the user knows, nor any easily recognisable word or phrase. A password should be a combination of upper and lower-case letters, numbers and typographic (% # &, etc..) characters. The longer and more senseless the combination is, the better. Sometimes it helps to use a mnemonic of a phrase to create a password - say "Shakespeare is a great writer!" could be the password: \$h%prSAGr8tW1tr!. If you do not choose a secure password, then your Safepipe may be vulnerable to attack.

Never save a password in an accessible place, including on your browser (for example: on a pop-up box that offers to save a password in a password list).

- Select a PC running Windows 95/98/Me or Windows NT/2000 that you can disconnect from your LAN and use to temporarily connect directly to the Safepipe. You will only need to connect to Safepipe this way for a few minutes - most of the configuration will be performed through a browser with Safepipe connected to your LAN.
- The first installation phase takes place before Safepipe's encryption is activated; thus the administration password used at this time is vulnerable. We suggest that the first installation phase take place in an isolated work environment. You could connect the Ethernet cable directly from the PC to Safepipe, or make sure no other cable(s) are plugged into the hub or switch between the PC and Safepipe.

Questions?

Please do not hesitate to contact your Eicon Networks product distributor, should you have any questions regarding the use of your Safepipe. The Eicon Networks product distributors are there to help you get the most out of your Eicon Networks equipment.

Product Descriptions

Hardware Descriptions



The front panel on all Safepipes include:

1. Restart - pressing this button will reset the unit's hardware without putting it in service mode.
2. Service - pressing this button will reboot the unit to service mode
In service mode, the unit can be software upgraded and initially configured with the Administration Tool. The unit cannot receive upgrades if it is not in service mode.
3. WAN LEDs - are controlled by the ISDN circuit or the WAN card inserted in the PCI slot:
 - **Link:** status of WAN Hardware connection
Green: layer 1 is running ; *No light:* layer 1 is down
 - **Connection:** status of WAN Software connection
Yellow: off hook (layer 3 running) ; *No light:* on hook
 - **Activity:** status of traffic on connection
Yellow: activity on connection ; *No light:* no activity
4. Ethernet 1 LEDs :
 - **Link:** status of Ethernet link - *Green:* 10/100Mbit link ; *No light:* no link
 - **Activity:** status of Ethernet activity - *Yellow:* activity on link ; *No light:* no activity on link
5. Ethernet 2 LEDs : same as with Ethernet 1
6. LCD display - the screen showing the current set up of the unit: Ethernet/LAN 1 IP address,

Ethernet/LAN 2 IP address, IP Gateway address and Subnet Mask. It is used to give the administrator important and informational messages about current software operation/-status.



The rear panel on all Safepipes include:

1. Main power switch
2. External power connector, 100-240 VAC
3. Ethernet 2 connector (external network)
4. Ethernet 1 connector (internal network)
5. Optional connector (DMZ/WAN)
6. WAN expansion slot (optional)

Initial Installation:

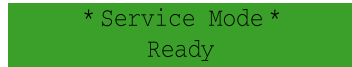
- 1 Connect Safepipe's Ethernet 1 port directly to the Ethernet port on the administrator's workstation, using one of the Ethernet cables provided. Then connect Safepipe to a power outlet with the power cable and switch 'on' the on/off button.



Rear-view of a unit, showing Ethernet ports, power outlet and on/off switch

Note: As Safepipe's secure connection is not yet activated, it is, at this time, recommended that the administrator's PC is isolated from the LAN.

- 2 The Ethernet 1 'LINK' light should now be lit on the front panel of Safepipe and you should see this display:



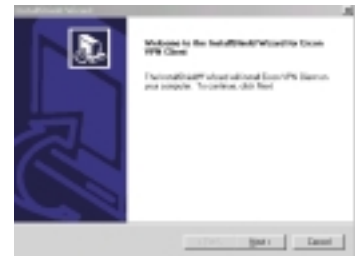
If you do not see the 'Service Mode' display on the front panel of the Safepipe, then you will need to use a paperclip to press the 'Service' button also located on the front-panel.

- 3 Insert the Administrator's CD-ROM in your CD-ROM drive. It should start automatically after a few seconds. Otherwise, click Start > Run > Browse to locate the *setup.exe* file on your CD-ROM drive.

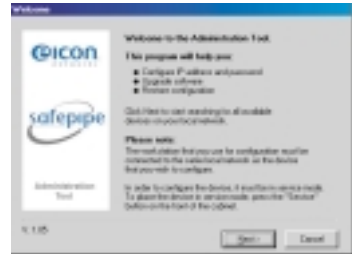


Select Installation, then Administration Tool to install the tool on your workstation.

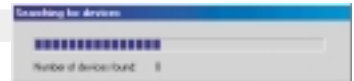
- 4 The InstallShield Wizard will take you through a few easy steps to install the Administration Tool. When installation is complete, exit the CD-ROM. Click Start > Programs > Eicon Networks > Eicon Administration Tool to use the Administration Tool to start configuration.



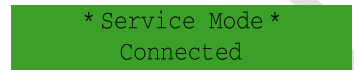
5 The following window will appear:



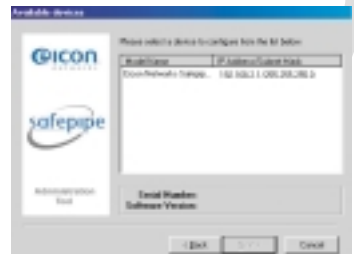
6 Click 'Next'. You will see the following progress indicator:



7 If the Administration Tool is able to connect to Safepipe then the display on the front of Safepipe will change to:



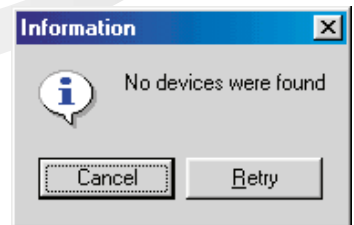
On the PC's screen, the details of the Safepipe device you are connected to are shown:



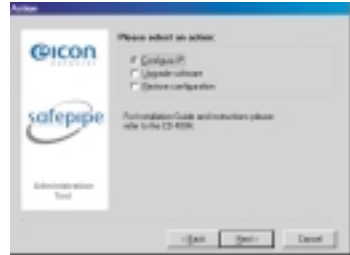
8 If the Administration Tool is not able to connect to Safepipe then you will see the following window:

- In this case, check that the Ethernet cable is correctly connected (is the Ethernet 1 'LINK' light lit?)
- Check that Safepipe is in 'Service mode' - if not, press the Service button on the front panel.

If you still cannot connect to Safepipe, restart your PC and try again. Once you have found the device, Click 'Next' to continue.

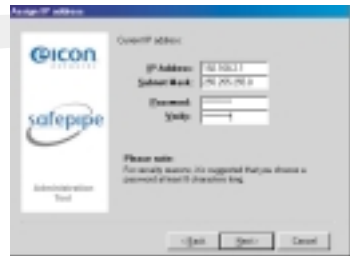


9 Select 'Configure IP' and click 'Next'.

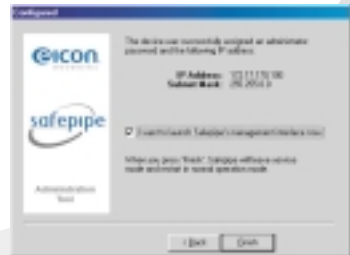


10 Assign an IP address and enter the subnet mask for Safepipe (both within the same range as the administrator's workstation).

Specify a password for use when accessing Safepipe. Remember to use a secure password. Click 'Next'.



11 To save your changes, the Administration Tool restarts Safepipe once you click 'Finish', and launches the management interface by default. If you do not want to launch the management interface now, uncheck the box 'I want to launch Safepipe's management interface now'.



You should now:

- a) Disconnect your PC from the Ethernet 1 connection on the Safepipe.
- b) Reconnect the PC to your LAN.
- c) Switch 'off' the on/off button.
- d) Mount Safepipe on a 19" rack.
- e) Connect Safepipe to the LAN via the Ethernet 1 port.
- f) Switch 'on' the on/off button.



- 12 During restart, Safepipe will begin its normal mode of operation, displaying the time and configuration information on the front panel. If your browser does not automatically launch and connect to Safepipe's management interface, open your browser and enter the IP address you specified in Step 10.

Welcome to Safepipe's Browser-based Management Interface:

- 1 From Safepipe's Welcome Page you will see that your browser must support encryption. Check your browser's 'About' window for verification (Microsoft Internet Explorer and Netscape Navigator ship with at least 40-bit strength encryption). If upgrading, follow the manufacturer's instructions - the end result is a Certificate of Authenticity.

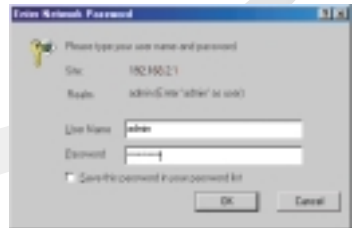


Read the Welcome Page and click 'Continue' at the bottom. Accept all alerts and warnings.

There may be an alert regarding a discrepancy in certificate names. This appears because Safepipe's IP address is dynamic, and certificates are created with fixed sites. A secure connection is still produced, however a warning results.

- 2 When prompted, type in the following:
Username: *admin*
Password: *[the same password as in Step 10]*

Note: To ensure high security, do not save the password.




Click OK and you will be connected to Safepipe's management interface:




Safepipe's main menu page.

Getting Started:

- 1 While still on the Main Menu page, click on the 'Site Map' button located in the middle of the page. 

The Site Map gives you an overview of Safepipe's entire interface. Browse through the various sections, but before you can edit any of the default settings (if necessary), you must configure your network on Safepipe.

To set-up your network:

Click 'IP'  under the 'Network' section.

On this page, Safepipe's Private Interface (Ethernet 1) IP address and subnet mask are shown.

You must set-up the connection between Safepipe and the Internet (Public Interface/ Ethernet 2). The IP address and Subnet Mask are assigned to you by your ISP. The Gateway IP address is the ISP's IP address.

Remember to click 'Apply Changes' after entering the fields. 



Private Interface (Ethernet 1)	
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0
Public Interface (Ethernet 2)	
IP Address:	213.120.33.143
Subnet Mask:	255.255.0.0.0
Gateway IP:	213.120.14.333

- 2 Next, verify Safepipe's date and time. The system log, which helps you diagnose any eventual problems, date stamps events so it is best to keep this as accurate as possible.

Click 'System'  > 'Access'  > 'Date & Time' tab.

Check that the information shown is correct. If it is, do nothing. If it is not as it should be, overwrite the relevant field(s) and click 'Apply Changes'.



Date is recorded as *MMM/DD/YYYY*, where the *month* is the first three letters in the English month, the *day* is two digits and the *year* is 4 digits. Example: February 6, 2001 is recorded in Safepipe as Feb 06 2001.

Time is based on the 24-hour clock and is recorded as *HH:MM*, where the *hour* is two digits and the *minutes* are two digits. Example: 4:19 in the morning is recorded as 04:19, 4:19 in the afternoon is recorded as 16:19.



You are now ready to begin configuration of Safepipe

After this initial installation, Safepipe must be configured to allow for VPN tunnel and Client connections. For configuration and general usage instructions, refer to the Administrator's Guide.


In this Quick Installation Guide you utilised a number of tools and interfaces which can be used again in the future.

Some of the tasks you have accomplished and the tools you have used are:

1. Installed Safepipe's Administration Tool onto your desktop. The Administration Tool can be used in the future when Safepipe is in service mode (push the 'Service' button on the unit's front panel). The Administration Tool can be used to:
 - Reconfigure the IP address and subnet mask
 - Set the administration password
 - Update software
 - Restore factory settings or restore a previously saved configuration
2. Connected Safepipe to the company's private LAN by following this Quick Installation Guide and perhaps using the Administrator's CD-ROM for troubleshooting problems during installation.
3. Securely connected via your browser to Safepipe's browser-based management interface. Safepipe's interface uses up to 128-bit encryption strength based on SSL. To connect with Safepipe in the future, you can use http within SSL which is specified by the URL '*https://xxx.xxx.xxx.xxx*' ('x' represents Safepipe's private IP address).
4. Started network configuration via Safepipe's browser-based management interface. By configuring Safepipe's Private and Public Interfaces, you have made it accessible both to and from the company's LAN and to the Internet. Updating Safepipe's Date and Time function makes it possible to immediately keep logical logs and status reports (built-in features).

5. Become familiar with the Safepipe interface site map. From here you can navigate your way to the various management pages in order to configure and edit Safepipe settings to meet your network's conditions and requirements.
 - Safepipe's browser-based management interface includes a built-in help system that can assist you in further configuring and managing your Safepipe.



Simply click the 'Help' icon  at the top of each configuration page if you need explanations or hints on how to fill-in the particular fields. Alternatively, you can use the Help Index located on the site map for a complete index of all the topics covered throughout the site.

CE approvals: Safepipe is CE approved. Please refer to www.eicon.com for more information.

Other approvals: Safepipe has been approved by relevant authorities with regard to safety and EMC regulations. Please contact your product distributor for further information.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: (1) Reorient or relocate the receiving antenna. (2) Increase the separation between the equipment and receiver. (3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. (4) Consult the dealer or an experienced radio/TV technician for help.

Caution: Changes or modifications not expressly approved by Eicon Networks A/S could void the user's authority to operate this equipment according to part 15 of the FCC rules.

Safepipe is a trademark of Eicon Networks Research A/S.

