
Copyright Notices

©eSoft, Inc. 2006. eSoft and InstaGate are registered trademarks and SoftPak and SoftPak Director are trademarks of eSoft, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Apple, Macintosh and Mac are registered trademarks of Apple Computer Inc. Adobe, the Adobe logo, and Acrobat are registered trademarks of Adobe Systems Inc. UNIX is a registered trademark of UNIX Systems Laboratories, Inc. All other brand and/or product names are the property of their respective holders.

Portions of InstaGate's software are covered under the GNU General Public License. You may freely obtain source code versions of the software covered by the GNU General Public License through the Internet at <http://www.redhat.com>. However, some applications remain the property of their owners, and require their permission to redistribute. For more information, access the eSoft web site at <http://www.esoft.com>.

Portions of InstaGate's software are Copyright © The Regents of the University of California. A complete copy of the copyright notice follows:

Copyright © The Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the University of California, Berkeley and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of InstaGate’s software are Copyright © The Apache Group. A complete copy of the copyright notice follows:

Copyright © 1995-1997 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”

4. The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission.

5. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”



Table of Contents

CHAPTER 1, Introduction.....	11
About InstaGate	11
Summary of Features	12
Familiarizing Yourself with the Controls and Connections.....	12
Front Pane of InstaGate EX2, PRO, xSPI	12
Back Panel of InstaGate EX2, PRO, xSP	13
Front Pane of InstaGate 404.....	14
Back Panel of InstaGate 404	14
Front Panes of InstaGate 604, 806l	15
Back Panel of InstaGate 604, 806	15
Accessing InstaGate’s Administrative Interface	17
Safety Information.....	17
CHAPTER 2, Client Computer Configuration	21
Client Configuration Overview.....	21
Configuring TCP/IP on Windows Clients.....	22
Using the TCP/IP Control Panel to Configure TCP/IP	23
Configuring TCP/IP on Linux Clients	24
Using netconfig to Configure TCP/IP.....	24
Using linuxconf to Configure TCP/IP.....	25
Using control-panel to Configure TCP/IP.....	25
Manually Editing Configuration Files to Configure TCP/IP	26
Checking For Required Packages.....	28
Installing Required Packages	28
Configuring your Browser to Use InstaGate’s Proxy Server.....	29
Manual Web Browser Proxy Server Configuration	29
.....	29
CHAPTER 3, User Management.....	31
Adding Users.....	31
Modifying Users.....	32
Deleting Users.....	34
Configuring Remote Authentication.....	34

CHAPTER 4, Email Management	39
Enabling Mail Relay.....	39
Configuring Advanced Mail Relay Options.....	40
Enabling Email Address Verification	42
Managing the Email Server Queue	44
CHAPTER 5, Server Configuration	45
Configuring the File and WINS Servers	45
Accessing the File Server from the LAN	47
CHAPTER 6, System Management.....	49
Using the Backup and Restore Utility.....	49
Configuring the Backup Settings.....	49
Manually Backing up Files	51
Restoring Backup Files	51
Specifying the Administrator Settings	52
Specifying Advanced System Administrator Settings	54
Enabling Global Management.....	54
Configuring the Local Options.....	55
Shutting Down or Restarting the System	56
Enabling the SNMP Agent	57
Customizing the SNMP Agent.....	57
CHAPTER 7, Firewall Management.....	59
Configuring IPSec Remote Office VPNs.....	59
Adding IPSec Remote Office VPNs	60
Configuring IKE Key Settings.....	64
Configuring IPSec Key Settings.....	65
IPSec Remote Office VPNs Advanced Options	66
Configuring IPSec Remote User VPN	66
Configuring PPTP VPN	68
Enabling PPTP VPN Forwarding.....	69
Configuring a Windows Client for PPTP.....	70
Configuring Firewall Policies.....	71
Adding Firewall Policies	72
Modifying Firewall Policies.....	75

Deleting Firewall Policies.....	75
Defining Custom Services	76
Enabling Global Firewall Options.....	78
CHAPTER 8, Network Configuration	79
Configuring the LAN Settings.....	79
Configuring the WAN Settings.....	81
DSL	81
Ethernet	85
Euro ISDN	87
Modem or External Modem.....	89
Synchronous Serial V.35/X.21 or T1/E1 CSU/DSU	90
Wireless 802.11B	93
Configuring the Internet Connection Settings.....	95
Defining an Internet Connection Schedule	96
Configuring Static Routes.....	98
Configuring the DMZ Settings	98
Connecting InstaGate to your DMZ Network.....	100
CHAPTER 9, Alerts and Reports	105
ThreatMonitor	105
Overview.....	105
System Monitor	106
Firewall Monitor.....	106
Reports & Graphs	107
ThreatMap	107
Configuring the System Alert Settings.....	108
Configuring the Daily Report Settings	110
Generating the Internet Connection Report.....	111
Generating the User Quota Report.....	111
Generating the System Security Report	111
Generating the PPTP VPN Report.....	112
CHAPTER 10, Support and Diagnostics.....	113
Viewing System Information.....	113
Running System Diagnostics	114

Running Connection Diagnostics	114
Viewing the Connection Log (InstaGate EX2, XSP and PRO)	115
Registering InstaGate	115
Enabling Remote Support	115
Viewing the System Logs	116
Sample System Log Entries	116
Contacting eSoft	117
Troubleshooting	118
Solving Client Configuration Problems	118
Solving Administrative Interface Problems	119
Solving Internet Connection Problems	120
CHAPTER 11, User Administration Interface	121
Accessing the User Administration Interface	121
Changing your Account Password	122
APPENDIX A, LCD Screen/Keypad	123
Changing the Network Configuration Settings	124
Configuring the DHCP Server	124
Enabling Remote Support	126
Shutting Down the System	126
Rebooting the System	127
Resetting the Administrative Password	127
Restoring Factory Default Settings	127
APPENDIX B, SoftPak Director	129
Subscribing to SoftPaks and ThreatPaks	129
Viewing SoftPak or ThreatPak Details	130
Viewing Enabled SoftPaks or ThreatPaks	131
APPENDIX C, Technical Specifications	133
Hardware	133
Operating System	133
Safety and Reliability	134

APPENDIX D, Serial Console	135
APPENDIX E, Warranty and License Agreement.....	137
Standard Warranty	137
EC Countries Standard Warranty.....	139
eSoft Complete Care (eCC).....	142
Software Care.....	142
Extended Hardware Care	142
Hardware Hot Swap.....	143
Phone/Email Care.....	143
Refund/Return Policy	143
Delivery Methods and Time Frame.....	144
End-User License Agreement.....	145
APPENDIX F, Regulatory Notices.....	161
Glossary	163
Index	175

This chapter contains introductory information about InstaGate. It covers the following topics:

- About InstaGate
- Summary of Features
- Familiarizing Yourself with the Controls and Connections
- Accessing InstaGate's Administrative Interface

About InstaGate

InstaGate is a next-generation firewall/VPN appliance that provides comprehensive Internet security on one extensible platform. Designed for the most demanding network environments, InstaGate is fortified by a stateful firewall, and makes large scale VPNs easy to deploy with centralized management.

Setup for InstaGate is completed in minutes. With remote authentication support, InstaGate easily integrates into network databases using RADIUS. Once installed, maintaining InstaGate is a breeze. The SNMP agent provides the ability to monitor system status. And with automatic software updates, the only maintenance needed is periodic mouse clicks to ensure the updates install at the time you want.

What differentiates InstaGate is its extensible design. Engineered with the future in mind, InstaGate not only meets the immediate firewall and VPN needs of your organization, but allows you to instantly add new services and applications as needed.

SoftPak applications are security and IT software modules that add functionality to InstaGate. SoftPaks eliminate the need to “grow out” your network with additional software and hardware platforms. Delivered via eSoft's patent-pending SoftPak Director technology, SoftPaks transform InstaGate into a comprehensive Internet security solution. A catalog of SoftPak applications that includes anti-virus, centralized VPN management, vulnerability scanning and more can be instantly enabled on your InstaGate appliance with the click of a mouse.

Summary of Features

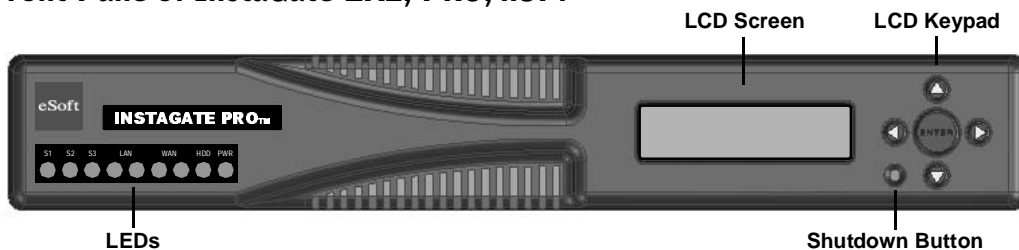
InstaGate provides multiple server capabilities in one unit to meet the needs of your entire network. It provides the following features:

- A built-in firewall to protect your network from unauthorized access
- PPTP and IPSec VPN servers to simulate a private network over the Internet
- An easy-to-use Web interface for managing InstaGate and the network
- Shared Internet access using a variety of communication options
- A large hard drive for file storage and backup
- Web access control to maintain an acceptable Internet use policy
- Web caching to reduce Internet access times
- A DHCP server to provide automatic IP address allocation for devices on your network
- Remote management

Familiarizing Yourself with the Controls and Connections

Before installing InstaGate, familiarize yourself with the appliance's controls and connections.

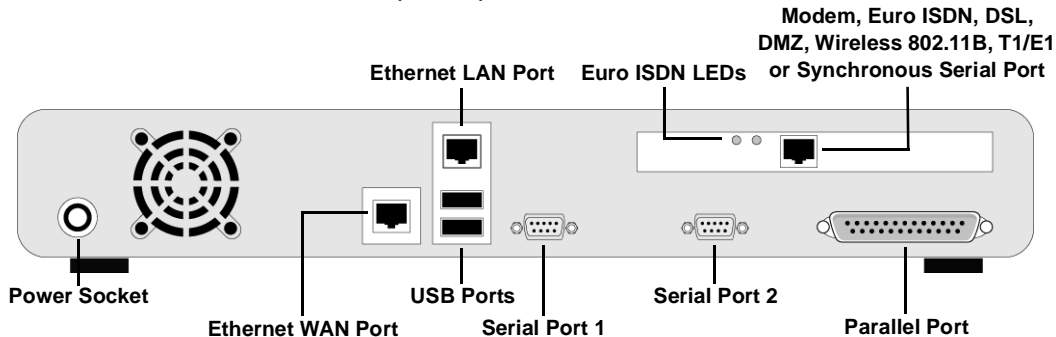
Front Pane of InstaGate EX2, PRO, xSPI



InstaGate's front panel contains the following features:

- **LEDs** — Display link and power status, as well as LAN, WAN, and hard drive activity.
- **LCD Screen** — Displays status and network information.
- **LCD Keypad** — Used to enter network configuration information and perform maintenance operations.
- **Shutdown Button** — Safely shuts down the system.

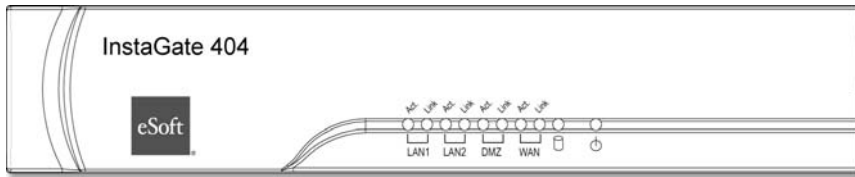
Back Panel of InstaGate EX2, PRO, xSP



InstaGate's back panel contains the following controls and connections:

- **Power Socket** — Connects the power connector from the power adapter.
- **Ethernet WAN Port** — Connects InstaGate to an external DSL modem, cable modem or WAN router.
- **Ethernet LAN Port** — Connects InstaGate to a hub or switch on your network.
- **USB Ports** — Reserved for future use.
- **Serial Port 1** — Allows dial in or dial out connections using an external modem.
- **Serial Port 2** — Allows dial in connections only (remote access).
- **Modem Port (optional)** — Connects InstaGate to an analog telephone line.
- **Euro ISDN Port (optional)** — Connects InstaGate to an ISDN telephone outlet or to an ISDN port.
- **DSL Modem Port (optional)** — Connects InstaGate to an analog telephone line.
- **Synchronous Serial Port (optional)** — Connects InstaGate to an external CSU/DSU.
- **T1/E1 CSU/DSU Port (optional)** — Connects InstaGate to a T1 or E1 line.
- **Wireless 802.11B Port (optional)** — Connects InstaGate to a wireless 802.11B WAN.
- **DMZ Port (optional)** — Connects InstaGate to a hub or switch on your DMZ network.
- **Euro ISDN Port LEDs** — Display activity on the ISDN adapter.
- **Parallel Port** — Connects a printer to InstaGate.

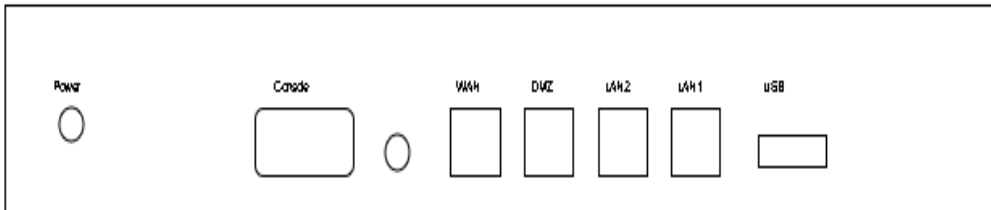
Front Pane of InstaGate 404



InstaGate's front panel contains the following features:

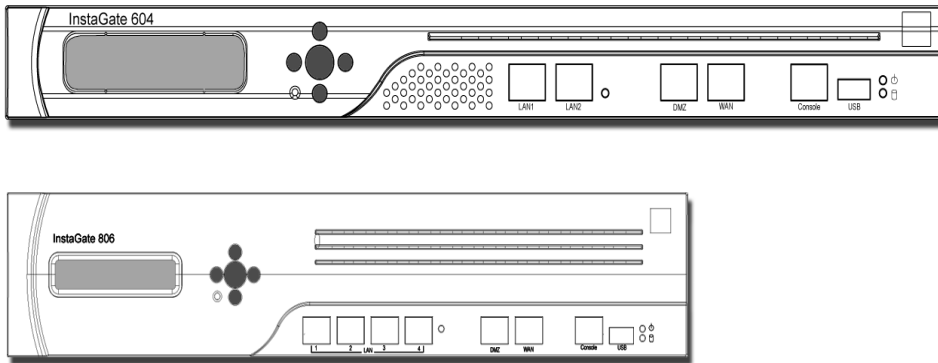
- **LEDs** — Display link and power status, as well as LAN, WAN, and hard drive activity.

Back Panel of InstaGate 404



- **Power Socket** — Connects the power connector from the power adapter.
- **Ethernet LAN ports** — There are two Ethernet LAN ports that are bridged together. These connect the InstaGate to a hub or switch on your network. The InstaGate 806 has four Ethernet LAN ports that are bridged together.
- **Ethernet WAN Port** — Connects InstaGate to an external DSL modem, cable modem or WAN router.
- **DMZ Port** — Connects InstaGate to a hub or switch on your DMZ network.
- **USB Port** — Used to connect USB devices, such as USB MODEMS and external mass storage.
- **Console Port** — Used to provide information about the unit, such as IP address.

Front Panes of InstaGate 604, 806



InstaGate's front panel contains the following features:

- **LEDs** — Display link and power status, as well as LAN, WAN, and hard drive activity.
- **LCD Screen** — Displays status and network information.
- **LCD Keypad** — Used to enter network configuration information and perform maintenance operations.
- **Shutdown Button** — Safely shuts down the system
- **Ethernet LAN ports** — The InstaGate 604 has two Ethernet LAN ports. These connect the InstaGate to a hub or switch on your network. The InstaGate 806 has four Ethernet LAN ports.
- **Ethernet WAN Port** — Connects InstaGate to an external DSL modem, cable modem or WAN router.
- **DMZ Port** — Connects InstaGate to a hub or switch on your DMZ network.
- **USB Port** — Used to connect USB devices, such as USB MODEMS and external mass storage.
- **Console Port** — Used to provide information about the unit, such as IP address.

Back Panel of InstaGate 604, 806

InstaGate's back panel contains the following controls and connections:

-
- **Power Socket** — Connects the power connector from the power adapter.

Accessing InstaGate's Administrative Interface

InstaGate's administrative interface makes it easy to set up Internet access and user accounts on InstaGate. You can access the administrative interface from any computer on your network provided the TCP/IP configuration is correctly set. For information about setting up the computers on your network, see "Client Computer Configuration" on page 21.

To access the administrative interface:

1. Open a Web browser (Firefox 1.5x, Internet Explorer 6.x or later) on a client computer connected to the network.
2. In the address box, enter the following URL:

https://<ip_address>:8001

(where <ip_address> is InstaGate's IP address)

3. The SSL Certificate used to encrypt connections to the administrative interface appears. You must accept the certificate to access the administrative interface.

The first time you access InstaGate, you are automatically launched into the Setup Wizard. The Setup Wizard guides you through the basic configuration steps necessary to use InstaGate on your LAN. For information about the Setup Wizard, refer to the online help.

Safety Information

The following instructions pertain to the risk of fire, electric shock, or bodily injury. Please read these instructions carefully.

- Follow all instructions and warnings marked on this product and included in this manual.
- Do not use this product on an unstable cart, stand or table. The product may fall, causing potentially serious damage to the product, and/or to personnel.
- Slots and openings in the cabinet and the back are provided for ventilation. These openings must not be blocked or covered to ensure reliable operation of your product, and to protect it from overheating. Do not use this product on a bed, rug, sofa, or other similar surface. This product should not be placed in a built-in installation unless proper ventilation is provided.
- Never push objects of any kind into the product through the cabinet openings, as they may touch dangerous voltage points or short out parts that could result in fire or electric shock. Never spill liquid of any kind on the product.

-
- Only connect this product to a power outlet that matches the power requirements of this product. If you're not sure of the type of AC power available, consult your dealer or local power company.
 - Do not allow anything to rest on the power cord. Do not place this product where people may walk on the cord.
 - If you must use an extension cord with this product, make sure the total amperage rating of all equipment plugged into it does not exceed the amperage rating of the extension cord. Also, make sure that the total of all products plugged into the main AC power outlet does not exceed 15 amps.
 - Unplug your product from the main electrical power outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
 - Do not use this product near water.
 - Unplug this product from the main power outlet and call for service under any of the following conditions:

The power cord or plug is damaged or frayed.

Liquid has spilled into the product.

The product has been exposed to rain or water.

The product has been dropped or the cabinet has been damaged.

The product exhibits a distinct change in performance, indicating a need for service.

Note InstaGate's operating system is not designed to support multiple power cycles. If you're unsure of InstaGate's stability, please contact Technical Support for assistance.

Power Supply Warning

Do not open the power supply cover, as hazardous voltages may be present. There are no serviceable components inside.

Battery Warning

CAUTION There is danger of explosion if the battery is not replaced correctly. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to manufacturer's instructions.



Chapter 2

Client Computer Configuration

This chapter guides you through the process of configuring the client computers on your network to access InstaGate. It covers the following topics:

- Client Configuration Overview
- Configuring TCP/IP on Windows Clients
- Configuring TCP/IP on Linux Clients
- Configuring Your Web Browser

Client Configuration Overview

Before you can configure InstaGate, you must first set up a client computer on your network to access it. Initially, you should only set up the computer you intend to use to configure and manage InstaGate. Once you have set up this computer and used it to configure the system, you can then set up the remaining client computers on your network.

InstaGate uses TCP/IP for communicating with the computers on your LAN. If InstaGate's DHCP server is enabled, each client computer's TCP/IP parameters (IP address, default gateway, and DNS settings) can be configured automatically. If you choose to use an existing DHCP server (such as Windows NT) rather than InstaGate's DHCP server, you will need to configure the existing DHCP server to set up each client computer's TCP/IP configuration.

If you choose not to use DHCP at all (or a particular client on your network doesn't support DHCP) you must manually configure each client's TCP/IP parameters to use a static IP address.

InstaGate supports client computers running any of the following operating systems: Windows 98, Windows ME, Windows NT 4.x, Windows 2000, Windows XP, Mac OSX, and Linux.

Each client must also have TCP/IP software and a Web browser (FireFox 1.5x or later or Internet Explorer 6.x or later) installed in order to communicate with InstaGate.

Configuring TCP/IP on Windows Clients

To configure TCP/IP on a Windows computer so that it can communicate with InstaGate:

1. Right-click the *Network Neighborhood* icon on your desktop, and then click *Properties*.

Some versions of Windows may also require you to right-click *Local Area Connection*, and then click *Properties*.

2. Double-click *TCP/IP*.
3. Select one of the following options:

- **Obtain an IP address automatically** — If you have enabled InstaGate’s DHCP server, select this option to assign the client’s TCP/IP settings automatically (recommended).

DHCP allows InstaGate to automatically manage the TCP/IP configuration of all the computers on your LAN that support the DHCP protocol. When a computer on your LAN first starts, it broadcasts a message on the LAN requesting its TCP/IP parameters. InstaGate receives this message and replies with a message containing all the parameters the computer needs to access InstaGate.

Note InstaGate’s DHCP server configures a client’s IP address, default gateway and DNS settings. Therefore, if you select the Obtain an IP address automatically option, you must clear any existing gateways or DNS settings listed. If these fields are not cleared, they override the settings supplied by InstaGate.

- **Specify an IP address** — If you wish to assign a static IP address to the client computer, you must configure the client’s TCP/IP parameters by specifying the following settings:
 - a. Enter an *IP address* for the client that is consistent with the InstaGate subnet you are using, (for example, **192.168.1.211**).
 - b. Enter the *Subnet mask* for your network. The default is **255.255.255.0**.
 - c. Enter InstaGate’s IP address as the *Default gateway*. The default is **192.168.1.1**.
 - d. Enter InstaGate’s IP address as the *DNS server*.
 - e. Enter **internal** as the default *Domain* or *DNS suffix*.
4. Click *OK*, and then click *OK* again.

Using the TCP/IP Control Panel to Configure TCP/IP

If *TCP/IP* appears in the *Control Panels* submenu, use the TCP/IP control panel to configure TCP/IP.

1. From the *Apple* menu, choose *Control Panels*, and then *TCP/IP*. The TCP/IP control panel appears.
2. In the *Connect via:* pull down box, select *Ethernet*, then make the following selections:
 - **Configure** — Since Apple Open Transport supports DHCP for automatic IP address assignment, you can use InstaGate's DHCP server to automatically assign IP addresses to your Macintosh clients (highly recommended). If you wish to use automatic IP address assignment, choose *Using DHCP Server* in this menu.

If you do not wish to use InstaGate's DHCP server to automatically assign an IP address, select *Manually*. If you choose the manual option, you will need to assign a unique IP address to each Macintosh client.
 - **IP Address** — If you selected automatic IP address assignment in the *Configure* menu, leave this field blank. If you selected manual IP address assignment, enter an IP address for this Macintosh client in a range that is consistent with the InstaGate subnet you are using, (for example, **192.168.1.211**).
 - **Domain name** — In most cases you can leave this field blank. You do not need to enter a domain name in this field unless you have another local DNS server on your LAN (ask your network administrator).
 - **Subnet mask** — If you are using InstaGate's DHCP server, you can leave this field blank. Otherwise, enter the subnet mask for your network (the default is **255.255.255.0**).
 - **Router address** — Enter the IP address of InstaGate (the default is **192.168.1.1**). If you have changed InstaGate's IP address, enter the correct address in this field. This tells TCP/IP to use InstaGate as your router to resources on the Internet.
 - **Name server address** — Enter InstaGate's IP address (the default is **192.168.1.1**). If you have changed InstaGate's IP address, enter the correct address in this field.
3. Click the close box to exit the TCP/IP control panel.
4. Click *Save* to finish configuring TCP/IP.

Configuring TCP/IP on Linux Clients

The following steps outline how to configure TCP/IP on computers running Red Hat Linux. Four different methods of configuring TCP/IP are provided, including:

- Using netconfig
- Using linuxconf
- Using control-panel
- Manually editing configuration files

TCP/IP is automatically installed on every Red Hat Linux computer, so all that is needed is to configure it for your network.

Using netconfig to Configure TCP/IP

You must have the netconfig program installed to use this method, as well as either the DHCPD or PUMP Red Hat packages (does not apply to static IP configuration). These packages should be installed by default. If you are not sure what is installed, or if for some reason the configuration does not work, see “Checking For Required Packages” on page 28.

To configure TCP/IP using netconfig:

1. Log in as root to the computer you wish to configure.
2. At the command prompt, type:

```
netconfig
```

The prompt *Would you like to set up networking?* appears.

3. Select *Yes*.
4. Select *Use dynamic IP configuration*.

Note If you wish to use static IP configurations instead, do *not* select *Use dynamic IP configuration...* and enter the *IP Address*, *Subnet Mask*, *Gateway* and *DNS Server*.

5. Select *OK* to finish configuration.

Using linuxconf to Configure TCP/IP

You must have the linuxconf program installed to use this method, as well as either the DHCPDCD or PUMP Red Hat packages (does not apply to static IP configuration). These packages should be installed by default. If you are not sure what is installed, or if for some reason the configuration does not work, see “Checking For Required Packages” on page 28.

To configure TCP/IP using linuxconf:

1. Log in as root to the computer you wish to configure.
2. At the command prompt, type:

```
linuxconf
```
3. Open the menus *Config*, *Networking*, *Client Tasks*, and *Basic Host Information*.
4. Select *Adapter 1*.
5. Select *DHCP* for the config mode.

Note If you wish to use static IP configurations instead, select *Manual* for the config mode and enter the *IP Address* and *Subnet Mask*. DNS servers are found under the *Name Server* menu and gateways are found under the *Routing and Gateways/Default* menu.

6. Click *Accept*.
7. Click *Quit*, then *Activate Changes*.

Using control-panel to Configure TCP/IP

You must be running X to use this method. You must also have the Red Hat control-panel program installed, as well as either the DHCPDCD or PUMP Red Hat packages (does not apply to static IP configuration). These packages should be installed by default. If you are not sure what is installed, or if for some reason the configuration does not work, see “Checking For Required Packages” on page 28.

To configure TCP/IP using control-panel:

1. Log in as root to the computer you wish to configure.
2. If you are not running X, then start an X Window session by typing:

```
startx
```

-
3. Open an xterm window.
 4. At the xterm command prompt, type:

```
control-panel
```
 5. Click on *Network Configuration*.
 6. Click on *Interfaces*.
 7. Select *eth0* and click *Edit*.
 8. Select *DHCP* as the Interface configuration protocol.

Note If you wish to use static IP configurations instead, select *Static* as the configuration protocol and enter the *IP Address* and *Subnet Mask*. DNS servers are found under the *Names* menu and gateways are found under the *Routing* menu.

9. Click *Save*.
10. Click *Quit*.

Manually Editing Configuration Files to Configure TCP/IP

This method requires that you know how to use a text editor under Linux. You can replace “vi” in the following directions with the editor of your choice. You must also have either the DHCPD or PUMP Red Hat packages installed to use this method (does not apply to static IP configuration). These packages should be installed by default. If you are not sure what is installed, or if for some reason the configuration does not work, see “Checking For Required Packages” on page 28.

Using DHCP

To configure TCP/IP using DHCP by manually editing the configuration files:

1. Log in as root to the computer you wish to configure.
2. At the command prompt, type:

```
cd /etc/sysconfig/network-scripts
vi ifcfg-eth0
```
3. Set “BOOTPROTO=” to *dhcp*. Do not modify any of the other settings at this time.
4. Save and close the *ifcfg-eth0* file.
5. Restart networking by typing:

```
/etc/rc.d/init.d/network restart
```

Using Static IP Addresses

To configure TCP/IP using static IP addresses by manually editing the configuration files:

1. Log in as root to the computer you wish to configure.

2. At the command prompt, type:

```
cd /etc/sysconfig/network-scripts
vi ifcfg-eth0
```

3. Set “BOOTPROTO=” to *static*.
4. Set “IPADDR=” to the IP address for this linux client in a range that is consistent with the InstaGate subnet you are using, (for example, **192.168.1.211**).
5. Set “NETMASK=” to the subnet mask. The default is **255.255.255.0**.
6. Set “GATEWAY=” to the IP address for InstaGate. This tells TCP/IP to use InstaGate as your gateway to resources on the Internet. The default is **192.168.1.1**.
7. Save and close the ifcfg-eth0 file.

8. At the console, type:

```
cd /etc/sysconfig/
vi network
```

9. Set “GATEWAY=” to the IP address for InstaGate.

10. Set “GATEWAYDEV=” to *eth0*.

11. Save and close the network file.

12. To configure the DNS addresses, type:

```
vi /etc/resolv.conf
```

The first line should contain “search *DOMAIN NAME*”, where *DOMAIN NAME* is your domain. This allows commands like “ftp host1” to connect to host1.domainname.

The next line should contain “nameserver *DNS IP ADDRESS*”, where *DNS IP ADDRESS* is the address of the first DNS server.

The third line is optional and may contain “nameserver *DNS IP ADDRESS*”, where *DNS IP ADDRESS* is the address of a second DNS server.

13. Save and close the file.

14. Restart networking by typing:

```
/etc/rc.d/init.d/network restart
```

Checking For Required Packages

To check which packages are currently installed:

1. Log in as root to the computer you wish to check.
2. At the console or at an xterm window, type:

```
rpm -q pump
```

The command should print a line similar to: `pump-0.7.2-2`. The numbers indicate the package version and are not important at this point.

3. If instead the line “Package pump is not installed” appears, try looking for DHCPD by typing:

```
rpm -q dhcpd
```

You should see a line similar to: `dhcpd-1.3.17p15-2`. If instead the line “Package dhcpd is not installed” appears, you will need to install either PUMP or DHCPD.

Installing Required Packages

To install the required packages:

1. Log in as root.
2. Insert CD #1 of the Red Hat install CD's.
3. At the console or at an xterm window, type:

```
mount /mnt/cdrom  
cd /mnt/cdrom/RedHat/RPMS  
rpm -i pump [Tab]
```

4. If the previous command does not work, try the following:

At the console or at an xterm window, type:

```
rpm -i dhcpd [Tab]  
rpm -i linuxconf [Tab]  
rpm -i control-panel [Tab]  
rpm -i netcfg [Tab]
```

Configuring your Browser to Use InstaGate's Proxy Server

Normally your browser makes a direct connection to a Web, FTP, or other server on the Internet. In this mode, InstaGate acts as a router, relaying the command and data packets to complete the Web request. No individual Web browser configuration is required.

However, if you set InstaGate's Web Access Control to *Require Username and Password* authentication (see "To remove a site from the list, simply select the site and click Delete." on page 70), each client computer's Web browser must be configured to access InstaGate as a Web proxy server.

Manual Web Browser Proxy Server Configuration

Instructions for manually configuring the following Web browsers to use InstaGate's Web proxy server are provided:

- Internet Explorer 6.x

Internet Explorer 6.x

To configure Internet Explorer 5.x to access InstaGate as a Web proxy server:

1. From the *Tools* menu, select *Internet Options...* to open the options dialog box.
2. Click on the *Connections* tab.
3. Click on the *LAN Settings* button to open the Local Area Network (LAN) Settings dialog box.
4. Enter the following information into the *Proxy server* section in the middle of this dialog box:
 - **Use Proxy server** — Check this box
 - **Address** — `Instagate` or the `<IPaddress-of-InstaGate>`
 - **Port** — `8080`
 - **Bypass proxy server for local addresses** — Check this box
5. Click *OK* in the Local Area Network (LAN) Settings dialog box.
6. Click *OK* in the Internet Options dialog box to save your new settings.
7. Exit and restart Internet Explorer to start using InstaGate's proxy server.

This chapter describes how to create and manage the individual users on InstaGate. It covers the following topics:

- Adding Users
- Modifying Users
- Deleting Users
- Configuring Remote Authentication

Adding Users

The Add Users page allows you to set up new users on InstaGate and establish their access privileges.

Each user account has a *Full Name*, *Account Name* and *Password* associated with it. The account name and password are used to access all of InstaGate's applications.

It is a good idea to make the InstaGate account name match the user's Windows login name. If the Windows login name and the InstaGate account name do not match, the user will not be able to access InstaGate via Windows networking.

To add a new user:

1. Select *Add Users* from the *Users* menu.

Users: Add Users

Number of users currently on system: 3 User License Limit: Unlimited

#	Full Name	Account Name	Password	Verify Password
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Another...

Add All Users with the Following Access Information

Email Access Receive System Alerts

Remote Access (VPN) Receive System Reports

Quota:

Web Access Group

All Users WebAccessFull

Apply Cancel

2. Type the user's *Full Name* (for example, **John Smith**). The user's full name may consist of any characters except colons (:) or quotation marks ("). This field may not be left blank.
3. Type the user's *Account Name*. The user's account name must start with a lowercase letter. The remaining characters in the account name may consist of lowercase letters, numbers, periods (.), underscores (_), and dashes (-). This field may not be left blank.
4. Type and verify the user's *Password*. The user's password may consist of any characters except colons (:) or blank spaces, and may be up to 13 characters long. This field may not be left blank.
5. Select the *Remote Access (VPN)* check box to provide the user with remote VPN access through PPTP and IPsec, as well as remote dial in access.
6. Specify the maximum amount of disk space available to the user from the *Quota* drop down box.
7. Specify the user's *Web Access* privileges. This field is only available if you selected to require username and password authentication in the Web Access Control page.
8. To enter multiple users with the same access information, click *Another...* and repeat steps 2 through 4.
9. Click *Apply* to add the new user(s), or *Cancel* to exit without adding.

Modifying Users

To modify a user account:

1. Select *Modify & Delete Users* from the *Users* menu.
2. Click the radio button next to the user you wish to modify.

-
3. Click *Modify*.

Users: Modify & Delete Users: Modify

User Account

Full Name: user

Account Name: user

Password: ***

Verify Password: ***

Use Remote Password

Access Information

Email Access Receive System Alerts

Remote Access (VPN) Receive System Reports

Quota: 10 MB | Current disk usage: 0.06Mb

Web Access Group

All Users WebAccessFull

Apply Cancel

4. Change the user's *Full Name* or *Password* as desired.
5. If you have enabled remote authentication (see “Configuring Remote Authentication” on page 34), select the *Use Remote Password* check box to use the user's remote password rather than their InstaGate password to access InstaGate's applications (such as, RAS, PPTP, and Web proxy access).
6. Make any necessary changes to the user's *Access Information*.
7. Click *Apply* to save your changes, or *Cancel* to exit without saving.

Note To change a user's account name, you must first delete the user, then add the new account name.

Deleting Users

To delete a user account:

1. Select *Modify & Delete Users* from the *Users* menu.
2. Click the radio button next to the user you wish to delete.
3. Click *Delete*.
4. Click *Delete* again to delete the user account, or *Cancel* to exit without deleting.

Configuring Remote Authentication

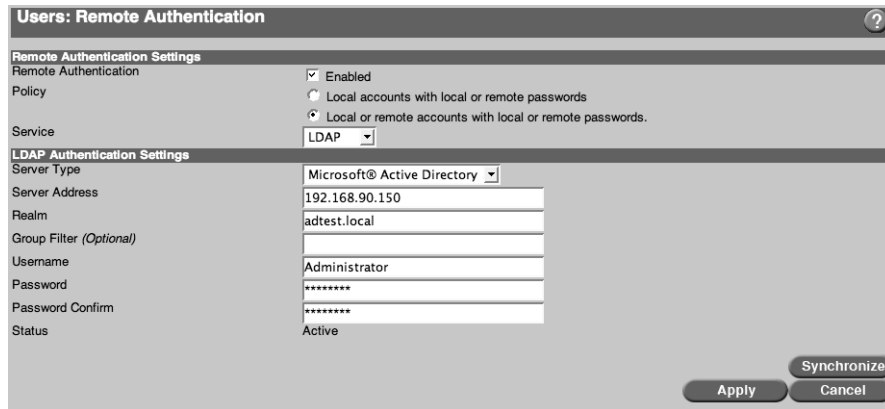
The system supports Remote Authentication Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP) and Mail Server (SMTP) Authentication.

RADIUS is a client-server system that stores authentication information for users in a central database, providing authentication for the entire network from one location. If you have a RADIUS server, the system can act as a RADIUS client and authenticate users using the existing server.

LDAP is a protocol used to access information directories, such as usernames and passwords. If you are using an LDAP server, the system can authenticate incoming requests using account information stored on the LDAP server.

Using the Active Directory type of LDAP, you can configure your Windows clients to "transparently" authenticate using web proxy using the credentials provided by users when they log into their clients.

SMTP is a protocol primarily used to transfer mail between clients and servers. Extension to the SMTP protocol support authenticating users and can be used by the system to pass authentication information through for a truly transparent configuration.



To configure remote authentication:

1. Select Remote Authentication from the Users and Groups menu.
2. Select the Remote Authentication Enabled check box.
3. Select one of the following remote authentication options:
 - a. Local accounts with local or remote passwords -The remote authentication server only stores and authenticates user passwords. All users must have a local account to access network resources through the system.
 - b. Local or remote accounts with local or remote passwords -The remote authentication server stores and authenticates both user names and passwords. Remote users do not have to have a local account to access most network resources through the system. Services that require information to be stored locally (such as the Complete Mail Server) still require a local account.
4. Select one of the following Remote Authentication Services:
 - LDAP, Active Directory - Use a Windows Server .
 - a. For LDAP Server Type select Microsoft Active Directory.
 - b. For Server Address, specify the IP address of the Windows server.
 - c. For Realm, specify the Active Directory realm name in domain name notation such as company.local.
 - d. You may optionally define a Group Filter. If specified, only groups with a name that

contains the specified filter (case insensitive) will be synchronized. For example, a filter of company would get groups such as Company Users, Company Executives and not Domain Users. This can greatly reduce the number of groups that will appear under user group management.

- e. For Username and Password fields, specify the username and password required to query the Active Directory server. You must have an account with sufficient access to work correctly.
 - LDAP - Generic Server.
 - a. For LDAP Server Type select Generic LDAP Server.
 - b. Specify the IP address of the LDAP Server.
 - c. Specify the port number used for LDAP authentication.
 - d. Enter the Workgroup of the Active Directory Domain. example: WORKGROUP
 - e. Enter the domain portion of the Active Directory Domain example: domain.com
 - f. Enter the LDAP Base DN. For example, if your domain name is domain.com, your LDAP base DN might be dc=domain,dc=com.
 - g. Enter the Admin DN (Distinguished Name) of the Active Directory domain. example: cn=Administrator,cn=Users,dc=domain,dc=com
 - h. If the LDAP server requires authentication, enter the LDAP Username and Password. Typically, Windows NT4 servers without Active Directory do not require authenticated access. Servers with Active Directory, however, usually require a user name and password to access information.
 - RADIUS - Use an external RADIUS server.
 - a. For Authentication Server Address and Port, specify the appropriate IP address and port values. Typically the port is 1812.
 - b. For Accounting Server Address and Port, specify the appropriate IP address and port values. Typically the port is 1813.
 - c. Specify the value of the secret shared between system and the RADIUS server in the RADIUS Secret text box.
 - SMTP - Configure the system to authenticate using the mail server defined in EmailServer Settings
5. Click Apply to save your settings, or Cancel to exit without saving.

If using LDAP, Active Directory, clicking Apply will attempt to contact and query the Active Directory Server. If there are any problems they will be shown so you can correct them and try again. Once you've successfully configured it, the Status field will show either Active or Disabled, depending on whether the Active Directory server is reachable.

Finally, if you're using LDAP, Active Directory, the Synchronize button will synchronize information between the servers. The system will automatically synchronize every day around midnight.



This chapter describes how to manage email using InstaGate. It covers the following topics:

- Enabling Mail Relay
- Managing the Outgoing Mail Queue

Enabling Mail Relay

Enabling mail relay allows InstaGate to act as an Internet mail gateway, automatically forwarding all incoming email to an SMTP mail server on your LAN.

To enable mail relay:

1. Select *Settings* from the *Email* menu.

Email: Settings

Mail Relay Settings

Server Enabled

Domain Name

Trusted Networks
Only clients on listed networks are allowed to send mail without authentication.

Automatic
 Custom (192.168.1.0/24)

Send Incoming Email To

Mail Server Address

Mail Server Requires Authentication

Send Outgoing Email To Relay Server (optional)
Enter server address only if you want all outbound mail directed to a single relay server.

Relay Server Address

Relay Server Requires Authentication

Advanced
Apply Cancel

2. Click the *Server Enabled* check box.
3. Enter your *Domain Name* (for example, **example.com**).
4. The product provides an anti-forwarding feature to prevent the misuse of your mail server by unauthorized connections. Any address or network not in this list that attempts to relay mail

will be rejected if your *Domain Name* or system IP address is used in the HELO string during the connection. If you wish to allow specific trusted hosts or networking to relay specify those in *Trusted Networks*. For example:

10.10.1.2 (single IP address)

10.10.1.0/24 (class C network beginning at 10.10.1.0)

To allow relaying from all hosts (disable SMTP authentication) enter *. This setting is not recommended, however, as it may lead to spam being forwarded through your mail server.

5. If you are using the mail server in relay mode, enter the *Mail Server Address* of your local SMTP mail server.

If your local SMTP server requires authentication, select the *Mail Server Requires Authentication* check box, and enter the *Login Name* and *Password*.

6. Enter the *Relay Server Address* of your ISP's outgoing (SMTP) server, if applicable. The outgoing SMTP server is used to send mail to the Internet.

If your ISP's outgoing SMTP server requires authentication, select the *Relay Server Requires Authentication* check box, and enter the *Login Name* and *Password* provided by your ISP.

7. If your email server requires any advanced configuration settings (such as, specifying the maximum message size accepted by the server or disabling client SMTP authentication) click [Advanced](#).
8. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring Advanced Mail Relay Options

Email: Settings: Advanced

Server Settings

- Forward copies of undeliverable messages to administrator.
- Allow Client Authentication.
- Allow Non-standard HELO Names.
- Check for duplicate messages due to remote server timeouts.

Maximum Message Size: 10 MB

Maximum Connections Per Host: 5

SMTP Timeouts

TCP Connect: 5 minutes

Command Inactivity: 5 minutes

Data Block Transmission: 5 minutes

Message Termination: 10 minutes

Apply Cancel

To complete the Advanced Options page:

1. If you want the remote system administrator to receive copies of undeliverable mail messages (error or warning messages from the email server) select the *Forward copies of undeliverable messages to administrator* check box.
2. Select the Allow Client Authentication check box to allow remote clients to connect to the SMTP server and relay mail. The clients must authenticate using a valid product account.
3. Select the Non-standard HELO names to allow to accept messages from servers that are behind the product and are configured with underscores in their domain name.
4. Enter the *Maximum Message Size (MB)* for the SMTP server. If you do not wish to limit the size of messages accepted by the server, type **unlimited**.
5. Enter the *Maximum Connections Per Host*. This number specifies the maximum number of simultaneous connections to the SMTP server allowed per host. If you do not wish to limit the number of connections, type **unlimited**.
6. Mail clients such as Outlook or Outlook Express that default to server timeouts of only one minute, when the RFC 2822 recommended default is 10 minutes. These clients do not check to see if mail has been processed successfully and result in duplicate messages. Check this if you are using one of the above mentioned mail clients to prevent duplicate messages due to client timeouts.
7. Select the *Allow Off-site access to POP and IMAP Servers* check box to allow remote users to access the email server and download their mail. ***This feature is only available for the Insta-Gate product.***
8. Enter the SMTP TCP Connect Timeout. This sets a timeout for the connect function, which sets up a TCP/IP call to the remote host.
9. Enter the SMTP Command Inactivity Timeout. This sets a timeout for receiving a response to an SMTP command that has been sent out. It is also used when waiting for the initial banner line from the remote host.
10. Enter the SMTP Data Block Transmission Timeout. This sets a timeout for the transmission of each block in the data portion of a message. As a result, the overall timeout for a message depends on the size of the message.
11. Enter the SMTP Message Termination Timeout. This is the timeout that applies while waiting for the response to the final line that terminates a message.

This applies to multi-drop and mirrored systems. Enter the Maximum messages to retrieve per session. This controls the number of messages to retrieve per retrieval "session". Under most circumstances the default value of unlimited is fine but issues with certain ISPs may require you to set the value to a non-unlimited number like 10.

12. Click *Apply* to save your settings and return to EMail Server Settings page.

13. Click *Apply* to save your settings and return to the Email Relay page.

Enabling Email Address Verification

The product provides several options for verifying incoming email addresses. The options available vary depending on how you have configured the product's [Email Server Settings](#).

To configure the email address verification settings:

1. Select *Verify Sender Using Local Domain Exists* to validate Email claiming to come from a local user matches a user you defined on the system. This option is useful in reducing techniques used to trick users into opening Email that appears to come from someone inside the company.
2. Select *Verify Sender Email Account Exists* to validate the sender's Email address of all incoming messages (local and external) by contacting the sending host (mail server). The product contacts the sender's specified domain Email server to verify it accepts Email for the sender. Like the above option this is useful in reducing email that appears to come from someone inside the company.
3. Select the *Enable SPF* check box to enable SPF checking on mail received by the mail server.
 - a. Select *Ignore Authenticated Clients, Trusted Network and my MX Servers* to bypass SPF checks on Email coming from clients that authenticated or servers on a trusted network or defined by your DNS MX records. This option is useful when Email is queued on secondary MX server then delivered to the product and when remote users using defined domains send mail through the product.
4. Select the *Deny Email with Invalid Headers* check box to verify that incoming message headers (*Sender:*, *From:*, *Reply-To:*, *To:*, *Cc:*, and *Bcc:*) are formatted correctly. This is a syntax check only. However, a common spamming ploy is to send syntactically invalid headers.
5. If you are using the mail server in relay mode, select the *Verify Recipient Email Account Exists Using Incoming SMTP Server* check box to validate the recipient address of incoming messages by contacting the local SMTP mail server specified in the [Server Settings](#) page.

This option is typically preferable to LDAP verification (see step 6) in that it provides real-time access without the complexity that configuring the LDAP client can entail. The only time this method is undesirable, is if the internal server accepts all incoming messages instead of rejecting invalid users.

6. If you are using the mail server in relay mode, select the *Verify Recipient Email Account Exists Using LDAP* check box to validate the recipient address of incoming messages using a list of email addresses defined on an LDAP server.

-
- a. Enter the *Domain* of the LDAP server.
 - b. If the LDAP server requires authentication, select the *Authentication Required Enabled* check box and enter the authentication *Login Name* and *Password*.

Typically, Windows NT4 servers without Active Directory do not require authenticated access. Servers with Active Directory, however, usually require a user name and password to access information.

- c. Select how frequently to contact the LDAP server for address updates from the *Refresh interval* drop-down list. To update the list immediately, click *Update Now*.
7. If you are using the mail server in relay mode, you can also create a list of valid email addresses manually by entering the addresses in the *Email Addresses on Internal Server* text box.
 8. If you have installed the Mail Server SoftPak and are using the server in stand-alone mode, select one of the following methods for handling unaddressable mail (mail that is not destined for a specific user, alias, or distribution list) from the *Send unaddressable mail* drop-down list:
 - a. **Reject** ? Immediately rejects the email causing the remote email client or server to generate a bounce message.
 - b. **User** ? Sends the email to a selected user with email access.
 9. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Managing the Email Server Queue

The mail server queue allows you to view and manage undelivered messages.

To access the mail queue:

1. Select *Messages in Queue* from the *Email Server* menu. The mail queue displays all messages waiting to be delivered, as well as held and undeliverable mail.
2. To sort the messages, simply click the appropriate column heading (*Message ID*, *Date*, or *From*).
3. To view a message, click the *Message ID* (blue-highlighted text). The message in its entirety appears in a separate window.
4. To delete messages in the mail queue, select the messages you wish to delete, and click *Delete*.

To notify the original sender of a deleted message that the email could not be delivered to the intended recipient, click the *On Delete, generate bounce messages Enabled* check box.

5. To release and deliver held messages, select the messages you wish to release, and click *Release*.
6. To hold messages from being delivered, select the messages you wish to hold, and click *Hold*. Held messages are displayed in the mail queue highlighted in yellow.
7. To delete all messages in the mail queue, click *Purge*.
8. Click *Done* to exit the mail queue.

This chapter describes how to enable and configure the InstaGate servers. It covers the following topic:

- Configuring the File and WINS Servers
- Configuring the Dial In Server

Configuring the File and WINS Servers

InstaGate's File Server allows local administrators to access the *Admin* folder from Windows and Macintosh clients on the LAN. The *Admin* folder contains InstaGate's system logs.

InstaGate also provides a Windows Internet Naming Service (WINS) Server. WINS is an optional TCP/IP services component that automates the assignment of NetBIOS computer names to IP addresses for Windows networks. Rather than requiring you to maintain a static list of computer names, the WINS server provides dynamic name resolution to WINS clients. As each client makes its initial access to the WINS server, it registers itself. It repeats this registration periodically.

InstaGate can be configured as a WINS server or to do WINS resolution through a user-defined WINS server.

To configure the File and WINS Servers:

1. Select *File Server* from the *Servers* menu.

-
2. Select the *File Server Enabled* check box.



3. Type the Windows *Workgroup Name* for your LAN. The workgroup name should match the workgroup name configured on all the Windows workstations on your LAN.

To determine your workgroup name: From the *Start* button, select *Settings, Control Panel*. Double-click on the *Network* icon (or the *System* icon in certain versions of Windows) to open the Network properties form, and select the *Identification* tab. The Windows network Workgroup name is listed in the *Workgroup:* field.

The workgroup name appears in Network Neighborhood on a Windows client machine. The default is **WORKGROUP**.

4. Select *WINS Disabled* to disable the WINS Server. WINS is a method of providing cross-network servers for NetBIOS name resolution. If your Windows network spans more than one TCP/IP subnet, you must use a WINS server. If your network only has one subnet, however, the standard “broadcast” name resolution will suffice. You will also want to disable the WINS server if you already have a Windows NT server on your network performing the same task.
5. Select *This System Acts as WINS Master Server* to configure InstaGate as a WINS server. If InstaGate is set up to work as a WINS server, the DHCP server will pass that information to the various windows clients when assigning their IP addresses. Once this is done, the clients will use InstaGate to resolve names in the Microsoft Networking (SMB) environment.
6. Select *Use Other System as WINS Master Server* and enter the *IP Address of the WINS Master Server* if you already have a WINS Server connected to your network.
7. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Accessing the File Server from the LAN

Local system administrators can access the file server using any of the following methods:

- **Windows Network Neighborhood** — To access the file server, your Windows username must be the same as your InstaGate account name, and you must be set up as a local system administrator. See “Specifying the Administrator Settings” on page 52 for more information.

Once you are logged into Windows correctly, you can access the file server as follows:

- a. Open *Windows Explorer*.
 - b. Click *Network Neighborhood*.
 - c. Select your InstaGate’s *Host Name* from the list of network entries.
 - d. Select the *Admin* folder.
- **Finder** — To access the file server from a Macintosh OS X client, you must use the smb utilities included in OS X
 - a. Select *Finder*
 - b. Select the *Network* icon.
 - c. Select your InstaGate’s *Workgroup* from the list of network entries.
 - d. Select *InstaGate* from the list.
 - e. Click *Authenticate* and enter your InstaGate account *Name* and *Password*. You must be set up as a local system administrator to access the file server.
 - f. Click *OK*.
 - g. Double-click the *Admin* volume. The volume appears as an icon on your desktop.



This chapter describes the various system administration utilities necessary for effective system management. It covers the following topics:

- Using the Backup and Restore Utility
- Specifying the Administrator Settings
- Enabling Global Management
- Configuring the Local Options
- Shutting Down or Restarting the System
- Enabling the SNMP Agent

Using the Backup and Restore Utility

InstaGate includes a backup and restore utility to prevent the loss of configuration settings and data due to system failure. Backups can be performed manually, or automatically according to a set schedule. In order to use either backup option, however, you must first configure your backup settings.

Configuring the Backup Settings

To configure InstaGate's backup settings:

1. Select *Backup & Restore* from the *System* menu. The current backup settings are displayed.

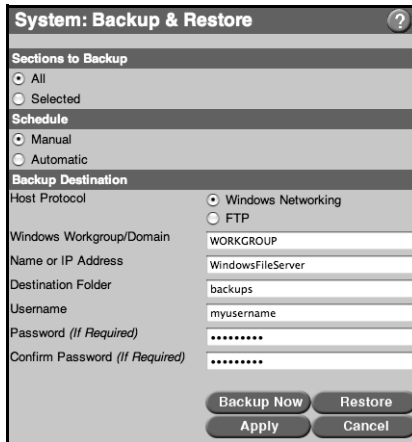


2. Specify the *Sections to Backup* by selecting the appropriate check boxes.
3. To back up your files manually, select the *Manually* radio button. To schedule regular automatic backups, select the frequency of the backups. Automatic backups can be performed *Daily*, *Weekly*, or *Monthly*.
4. Select the *Backup Time*. This field is only available for automatic backups.
5. Select the *Backup Day*. This field is only available for weekly or monthly automatic backups.
6. Type the *Number of Backups to Retain* in the backup directory. After completing a backup, the system will automatically remove any backup files (.tgz) from the backup location beyond the specified limit. Files are removed from oldest to newest.
7. Select the backup connect protocol. Files can be transferred to the backup location using *Windows Networking* or *FTP*.
8. Enter *Windows Workgroup/Domain* if you select *Windows Networking*.
9. Type a valid *Username* and *Password* on the backup server. The username and password are used to login to the server prior to transferring files.
10. Type the *Name or IP Address* of the backup server (for example, **10.10.1.2** or **ftp.server.com**).
11. Type the share or directory used to store backup files in the *Windows Networking Share or FTP Directory* text box. Make sure the target location has enough disk space to hold the backup archives.
12. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Manually Backing up Files

To manually back up InstaGate's configuration settings and user data:

1. Select *Backup & Restore* from the *System* menu. The current backup settings are displayed.



2. To start the backup process immediately according to the specified backup settings, click *Backup Now*.
3. To restore previously saved backup files, click *Restore*. See “Restoring Backup Files” on page 51 for more information.

Note Make sure the target location is turned on and available and has enough disk space to hold the backup archive. Failure to do this may result in zero-length or truncated archives.

Restoring Backup Files

The restore feature allows you to restore groups of files or specific files from any backup archive found in the network backup location.

To restore InstaGate backup files:

1. Select *Backup & Restore* from the *System* menu. The current backup settings are displayed.
2. Click *Restore*.



3. Select the backup file to restore from the drop-down list. All .tgz files in the designated backup location are listed.
4. Select the groups of *Files to Restore* by clicking the appropriate check boxes.
5. To restore specific files, select the *Custom* check box and click the files you wish to restore. Use the *Ctrl* key to select multiple files.
6. Click *Apply* to restore the selected files, or *Cancel* to exit without restoring.

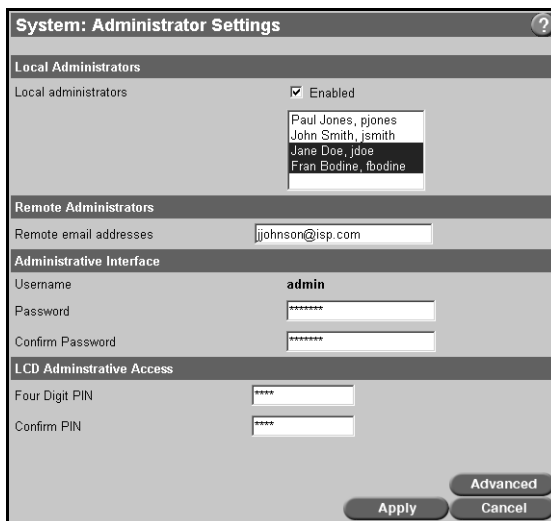
Specifying the Administrator Settings

Every organization should identify one or more individuals to act as the InstaGate administrator. The administrator should be the only person with the administrative password, and thus the only person who can access InstaGate's administrative interface. A good administrative password (and keeping it a secret) is your best line of defense against a compromise of security that originates from within your LAN.

Additionally, InstaGate allows the administrator to specify one or more system administrators. System administrators receive email warning and error messages, system alert messages, daily summary reports, and Windows networking access to InstaGate's backup and system log files

To specify the administrator settings:

1. Select *Administrator Settings* from the *System* menu.



2. To specify a local administrator, click the *Local administrators Enabled* check box and select the administrator from the list of InstaGate users. Use the *Ctrl* key to specify more than one local administrator. Only local system administrators have Windows networking access to InstaGate’s system log files.
3. Enter the system administrator’s *Remote email address*. To specify more than one remote administrator, separate each email address with a comma. Remote system administrators receive email warning and error messages, system alert messages, and daily summary reports.
4. Enter and confirm the *Password* used to access the InstaGate administrative interface. The username is always **admin**.
5. To control access to the LCD interface (see “LCD Screen/Keypad” on page 123), enter and confirm a *Four Digit PIN* (numbers only). Once specified, administrators must enter the PIN using the arrow buttons on the LCD keypad in order to access the LCD menu.
6. To specify the domain used when sending system generated mail (daily reports, SoftPak renewal notices, etc.) or to enable and disable administrative security features, click *Advanced*. See “Specifying Advanced System Administrator Settings” on page 54 for more information.
7. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Note If you forget the administrative password, you can reset the password to **admin** using the LCD keypad. See “Resetting the Administrative Password” on page 127 for more information.

Specifying Advanced System Administrator Settings

To specify the domain used when sending system generated mail (daily reports, SoftPak renewal notices, etc.):

1. Click *Advanced* in the Administrator Settings page.
2. Click *Use Default* to use the domain name specified in the Email Server/Relay Settings page. If you have not specified a mail domain name, InstaGate's WAN IP address is used enclosed in brackets (for example, InstaGate@[199.54.137.6]).
3. Click *Use Specified* to enter a domain name or IP address of your choice. Any IP addresses specified are enclosed in brackets in the message header (for example, InstaGate@[199.54.137.6]).
4. Click *Apply* to save your settings, or *Cancel* to exit without saving.

To change the settings for the administrator interface:

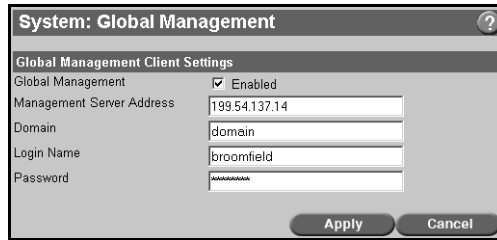
1. Click *Referrer Check Enabled* to enforce checks that help prevent cross-site scripting attempts. In most cases it is advised to leave this setting enabled to improve InstaGate security.
2. If you access your InstaGate through a domain name or through a redirected/NAT environment, you may need to add that host name to this list. To add additional hosts to the referrer check, enter the host names in the *Allowed Referrer Hosts* text box.
3. To increase or decrease the time until InstaGate performs an *auto logout* of the administrator, enter the time in minutes. To disable auto-logout enter zero in this field.
4. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Enabling Global Management

eSoft's Global Management technology allows a central administrator to configure and manage network security and access policies for multiple InstaGate devices. Participating InstaGates use global management clients to connect to a global management server (such as, *VPN Manager*). Once connected, a device continually exchanges configuration information with the management server and reconfigures as necessary.

To enable Global Management:

1. Select *Global Management* from the *System* menu.



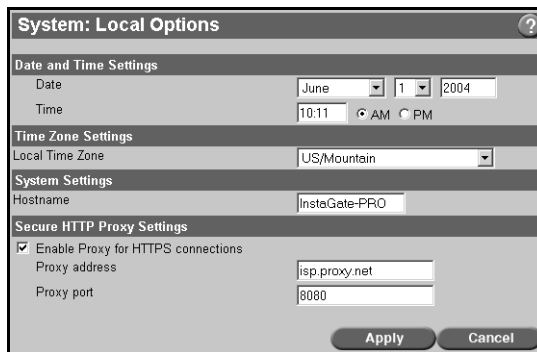
2. Select the *Global Management Enabled* check box. This enables InstaGate’s global management client, allowing it to connect to a global management server.
3. Enter the IP address or host name of the *Management Server*.
If InstaGate itself is the management server, click the *Self* radio button. This option is only available if you have installed a global management server SoftPak (such as, *VPN Manager*).
4. Enter the *Domain* for management. The domain name is used to identify and group the clients managed by the global management server.
5. Enter a *Login Name* and *Password* for the client. The name and password specified are used to authenticate (or register) the client when connecting to the global management server.
6. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring the Local Options

The Local Options page allows you to set your system date and time and specify your system host name.

To configure the local options:

1. Select *Local Options* from the *System* menu.



-
2. Specify the current *Date*.
 3. Enter the current *Time* in the form HH:MM, and select *AM* or *PM*.
 4. Select your *Local Time Zone* from the drop-down list.
 5. Enter a unique *Host Name* for your system. The host name is used to identify InstaGate in Windows networking and appears in the LCD screen.
 6. Some ISP's require that all HTTPS connection requests be passed to a dedicated proxy server located at the ISP. InstaGate uses HTTPS to contact the SoftPak Director for product updates and registration. Therefore, if required by your ISP, you must select the *Enable Proxy for HTTPS connections* check box in order to contact the SoftPak Director. You must also enter the proxy server's *Proxy Address* and *Proxy Port* (which can be obtained from your ISP).
 7. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Shutting Down or Restarting the System

Before turning off InstaGate's power it is important that you shut down the system properly. The Shutdown & Restart page allows you to safely shut down or restart InstaGate.

Note You can also safely shut down InstaGate by pushing a paper clip or similar implement into the recessed *Shutdown Button* located on the front panel of the appliance, or by using the LCD keypad. See "Shutting Down the System" on page 126 for more information.

To shut down or restart InstaGate:

1. Select *Shutdown & Restart* from the *System* menu.
2. To shut down InstaGate, click *Shutdown*. To restart InstaGate, click *Restart*.

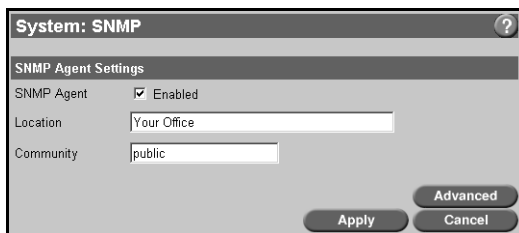
Note After the system has successfully shut down, the light in the LCD display turns off. You can then shut off the appliance's power by disconnecting the power source.

Enabling the SNMP Agent

SNMP allows an administrator to manage multiple network devices through a single network management console or client. The “server” portion that resides on each network device is called an SNMP *agent*. To access each agent, the client uses an identifier called a *community*. A community can be managed using any name the administrator chooses. The default community name for the InstaGate’s SNMP agent is *public*.

To enable the SNMP agent:

1. Select *SNMP* from the *System* menu.



2. Select the *SNMP Agent Enabled* check box to enable InstaGate’s SNMP agent. To maximize security, only enable SNMP in cases where it is used.
3. Enter the physical *Location* of your InstaGate. This field is for identification purposes only and can consist of any combination of letters, numbers, spaces, or special characters.
4. Enter the *Community* name used to access the agent. The default community name is **public**, but should be changed as soon as possible.
5. To customize the InstaGate’s SNMP agent, click *Advanced*. See “Customizing the SNMP Agent” on page 57 for more information.
6. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Customizing the SNMP Agent

The SNMP Advanced page allows you to enter commands to customize InstaGate’s SNMP agent.

To customize the SNMP agent:

1. Click *Advanced* in the SNMP configuration page.
2. Enter the SNMP configuration commands. Be sure to include a line break after each command.
3. Click *Apply* to save your settings, or *Cancel* to exit without saving.

This chapter describes how to modify InstaGate's firewall to control Internet access to and from your LAN. It covers the following topics:

- Configuring IPSec Remote Office VPNs
- Configuring IPSec Remote User VPN
- Configuring PPTP VPN
- Configuring Firewall Policies
- Defining Custom Services
- Enabling Global Firewall Options

Configuring IPSec Remote Office VPNs

A virtual private network (VPN) allows an organization to use the Internet's backbone to build a secure wide area network (WAN). This enables data to be transmitted and received through a secure tunnel. For companies with branch offices, a virtual private network using IPSec technology is an ideal solution for secure data communications, email, and client/server applications between offices.

IPSec support is primarily intended to provide secure site-to-site communications by using a VPN gateway (InstaGate appliance) at each site. The VPN Server authenticates the incoming request before establishing a secure tunnel for data transmission. Security sensitive information retrieved through VPN is encrypted before sending it through the tunnel and decrypted when it reaches the end of the tunnel.

Note IPSec may not function correctly if InstaGate is configured to use a dynamic (constantly changing) IP address.

To configure remote office VPNs:

1. Select *Remote Office VPNs* from the *Firewall* menu. A list of the IPSec VPNs currently defined on your system appears. If you have defined more than one type of VPN, the *Network* drop-down list allows you to specify the type(s) you wish to view.
2. To add a new IPSec VPN, click *Add*. See “Adding IPSec Remote Office VPNs” on page 60 for more information.
3. To modify an existing IPSec VPN, select the VPN you wish to modify and click *Modify*.
4. To create a copy of an existing VPN, select the VPN you wish to copy and click *Copy*. The Add screen appears pre-filled with the values of the selected VPN.
5. To delete a VPN, select the VPN you wish to delete and click *Delete*.
6. If you are experiencing difficulty with an existing VPN connection, click *Advanced* to enable advanced troubleshooting options. See “IPSec Remote Office VPNs Advanced Options” on page 66 for more information.
7. Click *Done* when you have finished configuring IPSec VPNs.

Adding IPSec Remote Office VPNs

The screenshot shows a dialog box titled "Firewall: IPSec VPNs: Add". It is divided into several sections:

- IPSec VPN**:
 - Name: RemoteOffice
 - Available: Enabled
 - Network: Local Network to Remote Network
 - Key Management: Automatic (Shared Secret)
- Network Settings**:
 - Local Host IP Address: WAN Interface
 - Local Network: 192.168.1.0 / 255.255.255.0
 - Remote Gateway IP Address: 199.54.137.15
 - Remote Network: 10.10.10.0 / 255.255.255.0
- Key Management Settings**:
 - Shared Secret: IPSecSharedSecret

At the bottom right, there are three buttons: "Advanced", "Apply", and "Cancel".

To add a new IPSec remote office VPN:

1. Enter a *Name* to identify the VPN.
2. To make the VPN available for use, click the *Available* check box.
3. Select the type of IPSec VPN you wish to add from the *Network* drop-down list. The type you

select changes the VPN configuration options displayed on the screen. The following VPN types are available:

- **Local Network to Remote Network** — Allows two networks to connect to each other.
 - **Local Network to Remote Host** — Allows a remote IPSec client (for example, Windows XP or a remote InstaGate) to connect to your local network.
 - **Local Host to Remote Host** — Allows a remote IPSec client to connect to your local InstaGate (for example, to transfer mail), but not to your local network.
 - **Local Host to Remote Network** — Allows a remote network to connect to your local InstaGate, but not to your local network.
4. If you are connecting your local network to a remote network or host, and the remote gateway has a dynamic IP address or uses a failover Internet connection, select the *Dynamic Remote Enabled* check box.
 5. Select how the two ends of the VPN link authenticate each other during key exchange from the *Key Management* drop-down list. Settings for the selected key management method (*Automatic* or *Manual*) are specified at the bottom of the page

Note The Key Management setting must be the same at both ends of the VPN link. If you selected the *Dynamic Remote Enabled* check box, both ends of the VPN must use *Automatic (Shared Secret)* key management.

6. Select the local network interface which uses the VPN from the *Local Host IP Address* drop-down list (either the *WAN Interface* or the *DMZ Interface*). This field only appears if you have enabled the DMZ interface without NAT protection.
7. To create an IPSec connection to a *Local Network* (for example, your LAN or DMZ network), enter the network's IP address and subnet mask. Entering the *WAN* address with a 255.255.255.255 netmask will allow the InstaGate to send all NAT traffic matching the remote network through the tunnel.
8. To create an IPSec connection to a remote host (for example, a Windows XP client or a remote InstaGate), enter the client's IP address in the *Remote Host IP Address* text box.

Note If you selected the *Dynamic Remote Enabled* check box, the configuration options change, requiring you to specify *Local* and *Remote Identifiers* rather than the *Remote Host* or *Remote Gateway IP Address*. To do this, first select the *Local Identifier Type* (IP Address or Domain Name) and enter the address (must be the IP Address of the WAN Interface) or name of the local *Identifier*. The local identifier settings specified here must match the remote identifier settings specified on the remote gateway. Then select the *Remote Identifier Type* (IP Address, Domain Name or Email Address) and enter the address or name of the remote *Identifier*. The remote identifier settings specified here must match the local identifier settings specified on the remote gateway.

9. To create an IPSec connection to a remote network, enter the *Remote Gateway IP Address* that should be used to deliver packets destined for the remote network. If the remote network is protected by a firewall, the gateway address should be that of the remote firewall's external (WAN) interface.

You must also specify the IP address and subnet mask of the *Remote Network*.

10. Enter the *Key Management Settings* for your VPN connection. The configuration options vary depending on the Key Management method selected at the top of the page.

- **Automatic (Shared Secret)** — To configure automatic key negotiation:
 - a. Enter the text that is to be shared between the two ends of the VPN link in the *Shared Secret* text box.

All automatic key management VPNs on the same remote host or gateway IP address must use the same shared secret. Therefore, if you are adding a new VPN with the same remote IP address as a VPN that already exists, the shared secret field is automatically completed as soon as you specify the remote address.

- b. Click *IKE* to specify the Internet Key Exchange (IKE) key settings for automatic key negotiation. The IKE page also allows you to specify the local and remote identifier settings if you are using a dynamic or failover Internet connection. See “Configuring IKE Key Settings” on page 64 for more information.
- c. Click *IPSec* to specify the IPSec key settings for automatic key negotiation. See “Configuring IPSec Key Settings” on page 65 for more information.

-
- **Manual** — To configure manual key negotiation:
 - a. Enter the *Outbound and Inbound SPI* (Security Parameters Index) numbers. The SPI is a unique identifier for a manual keyed connection. The SPI number must be of the form *0xhex*, where hex is one or more hexadecimal digit. It is generally necessary to make SPI at least 0x100 to be acceptable to KLIPS.
 - b. Select the algorithms used for encryption and authentication from the *Transforms* drop-down list. The following options are available:
 - **3DES Encryption, MD5 Authentication** — ESP with 3DES and HMAC-MD5-96
 - **3DES Encryption, SHA-1 Authentication** — ESP with 3DES and HMAC-SHA-1-96
 - **No Encryption, MD5 Authentication** — AH with HMAC-MD5-96
 - **No Encryption, SHA-1 Authentication** — AH with HMAC-SHA-1-96
 - **AES 128-bit Encryption, MD5 Authentication** — ESP with AES-128 and HMAC-MD5-96
 - **AES 128-bit Encryption, SHA-1 Authentication** — ESP with AES-128 and HMAC-SHA-1-96
 - **AES 192-bit Encryption, MD5 Authentication** — ESP with AES-192 and HMAC-MD5-96
 - **AES 192-bit Encryption, SHA-1 Authentication** — ESP with AES-192 and HMAC-SHA-1-96
 - **AES 256-bit Encryption, MD5 Authentication** — ESP with AES-256 and HMAC-MD5-96
 - **AES 256-bit Encryption, SHA-1 Authentication** — ESP with AES-256 and HMAC-SHA-1-96
 - **DES Encryption, MD5 Authentication** — ESP with DES and HMAC-MD5-96
 - **DES Encryption, SHA-1 Authentication** — ESP with DES and HMAC-SHA-1-96
 - c. Enter the *Encryption Key* and *Authentication Key*. To automatically generate random keys, click the *Create Keys* button. The encryption key and authentication key settings must be the same at both ends of the VPN link.

11. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring IKE Key Settings

IPSec mainly consists of two components — IPSec Packet Processing and Internet Key Exchange (IKE). The IPSec Packet Processing component secures IP packets by encrypting and authenticating them (see “Configuring IPSec Key Settings” on page 65). The IKE component negotiates security proposals between two entities and generates the key material. IKE uses digital certificates and pre-shared keys to authenticate the peers, and the Diffie-Hellman algorithm to create shared keys.

To configure the IKE key settings:

1. Specify how frequently to change encryption keys in the *Key Refresh* fields. Keys are automatically refreshed when the specified amount of time expires or the specified amount of data (in *Kilobytes*) passes through the VPN.
2. Select the *Strict PFS Enabled* check box to automatically delete the phase 1 security association after the phase 2 security association has been established. Strict PFS (Perfect Forward Secrecy) ensures new keying material is negotiated when the phase 2 security association expires.
3. If your external IP address (WAN interface) is dynamic, or you have a failover WAN connection, select the *Aggressive Mode Enabled* check box. You must then specify the local and remote identifier settings for the VPN.
 - a. Select the *Local Identifier Type* (IP Address or Domain Name) and enter the address (must be the IP Address of the WAN Interface) or name of the local *Identifier*. The local identifier settings specified here must match the remote identifier settings specified on the remote gateway.
 - b. Select the *Remote Identifier Type* (IP Address, Domain Name or Email Address) and enter the address or name of the remote *Identifier*. The remote identifier settings specified here must match the local identifier settings specified on the remote gateway.
4. Select the IKE *Proposals* for the VPN.

IPSec VPNs use proposals to negotiate a connection. A proposal is a set of encryption and authentication algorithms. The endpoints of a VPN must use the same authentication and encryption algorithms to establish communication.

The following predefined proposal configurations are provided:

- **High Security** — 3DES Enc, SHA-1 Auth, DH 2; 3DES Enc, MD5 Auth, DH 2
- **High Performance** — AES 128-bit Enc, MD5 Auth, DH 2; AES 128-bit Enc, SHA-1 Auth, DH 2

During negotiation, the endpoints present these proposals to each other in the order listed and use the first one that is common to both.

To set up a custom proposal configuration, select *Custom* from the *Proposal* drop-down box. Click the *Add* button to specify the proposals you wish to include. Use the *Up* and *Down* buttons to specify the order in which the proposals are presented.

5. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring IPsec Key Settings

IPsec mainly consists of two components – IPsec Packet Processing and Internet Key Exchange (IKE). The IPsec Packet Processing component secures IP packets by encrypting and authenticating them. IPsec uses DES, 3DES and AES to provide confidentiality, and HMAC-MD5 and HMAC-SHA1 to provide integrity and authenticity of the data.

To configure the IPsec key settings:

1. Specify how frequently to change encryption keys in the *Key Refresh* fields. Keys are automatically refreshed when the specified amount of time expires or the specified amount of data (in *Kilobytes*) passes through the VPN.
2. Select *Group 1* or *Group 2* from the *PFS* drop-down list if the IPsec-compliant device on the remote end of the VPN link also supports Perfect Forward Secrecy (PFS). PFS prevents the compromise of a session key from permitting access to data encrypted in a previous session. The PFS setting must be the same at both ends of the VPN link.
3. Select the IPsec *Proposals* for the VPN.

IPsec VPNs use proposals to negotiate a connection. A proposal is a set of encryption and authentication algorithms. The endpoints of a VPN must use the same authentication and encryption algorithms to establish communication.

The following predefined proposal configurations are provided:

- **High Security** — 3DES Enc, SHA-1 Auth, DH 2; 3DES Enc, MD5 Auth, DH 2
- **High Performance** — AES 128-bit Enc, MD5 Auth, DH 2; AES 128-bit Enc, SHA-1 Auth, DH 2

During negotiation, the endpoints present these proposals to each other in the order listed and use the first one that is common to both.

To set up a custom proposal configuration, select *Custom* from the *Proposal* drop-down box. Click the *Add* button to specify the proposals you wish to include. Use the *Up* and *Down* buttons to specify the order in which the proposals are presented.

4. Click *Apply* to save your settings, or *Cancel* to exit without saving.

IPSec Remote Office VPNs Advanced Options

The Remote Office VPNs Advanced page provides options to help troubleshoot problems with your VPN connection.

To enable the advanced options:

1. Select *Remote Office VPNs* from the *Firewall* menu.
2. Click *Advanced*.
3. Select the *IPSec Debugging Enabled* check box to write detailed technical information concerning your VPN to the General System EVERYTHING.log (see “Viewing the System Logs” on page 116). This feature should only be enabled while troubleshooting to avoid burdening your system with log data.
4. Select the *Copy ‘Don’t Fragment’ bit into IPSec packets Enabled* check box if your network environment has difficulty with packet fragments. This option prevents InstaGate from fragmenting IPSec packets.
5. Click *Apply* to save your settings or *Cancel* to exit without saving.

Configuring IPSec Remote User VPN

Using Internet Protocol Security (IPSec) technology, InstaGate’s Remote User VPN allows mobile remote users to securely retrieve information from the local LAN over the Internet.

Note In order to connect to the VPN, remote users must have a valid InstaGate account with remote access privileges (see “Adding Users” on page 31). If you do not want to create an account for each user, you can use a RADIUS server for remote authentication (see “Configuring Remote Authentication” on page 34).

To enable IPsec Remote User VPN:

1. Select *Remote User VPN* from the *Firewall* menu.

The screenshot shows the 'Firewall: Remote User VPN' configuration window. It is divided into three sections: 'Remote Users Settings', 'Local Identifier', and 'Remote Identifier'. In the 'Remote Users Settings' section, the 'Allow Remote User VPN Clients' checkbox is checked and labeled 'Enabled'. The 'IP Address Pool' is set to '10.10.1.0 / 255.255.255.192'. The 'Local Network' is set to '192.168.100.0 / 255.255.255.0'. The 'Shared Secret' is 'a304061172da1bb292095b96c47b26f3'. In the 'Local Identifier' section, the 'Type' is 'Domain Name' and the 'Identifier' is 'mainoffice.domain.com'. In the 'Remote Identifier' section, the 'Type' is 'Domain Name' and the 'Identifier' is 'client.domain.com'. At the bottom, there is a 'Block Internet Activity' checkbox which is unchecked and labeled 'Enabled'. 'Apply' and 'Cancel' buttons are at the bottom right.

2. Select the *Enabled* check box to allow remote user VPN clients.
3. Enter a network IP address and subnet mask in the *IP Address Pool* fields. Addresses from this pool are dynamically allocated to clients that connect to the VPN. The addresses specified cannot be included in any static routes or other networks defined on InstaGate.
4. Enter a *Local Network* IP address and subnet mask. Remote clients can only access this network through the VPN.
5. Enter the text that is to be shared between the two ends of the VPN tunnel in the *Shared Secret* text box. The text specified must be the same at both ends of the tunnel. The shared secret is used by both InstaGate and the remote client to encrypt and decrypt data passed through the tunnel.
6. Select the *Local Identifier Type* (IP Address or Domain Name) and enter the address (must be the IP Address of the WAN Interface) or name of the *Identifier*. The local identifier settings specified here must match the remote ID settings specified on the remote client.
7. Select the *Remote Identifier Type* (IP Address, Domain Name or Email Address) and enter the address or name of the *Identifier*. The remote identifier settings specified here must match the local ID settings specified on the remote client. You may add multiple remote identifiers by separating each entry by a comma.
8. Select the *Block Internet Activity Enabled* check box to prevent users from accessing the Internet while connected to the VPN.
9. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring PPTP VPN

Virtual Private Networking enables multiple remote users to simultaneously access your LAN from virtually anywhere in the world using the Internet. VPN technology is a low-cost alternative to LAN Remote Access Service (RAS) servers and their associated long-distance phone charges and equipment costs. In some situations, it can also let companies avoid leasing expensive private data lines when establishing wide area networks (WANs).

InstaGate provides a built in server as well as pass-through support for secure remote VPN access through the Point-to-Point Tunneling Protocol (PPTP).

With PPTP users with remote access privileges (specified in the *Add Users* page) can take advantage of the benefits of VPN communication to gain secure, transparent access to the corporate network from anywhere in the world, without the need for additional software for their client PCs. Windows 98, Windows NT, and Windows 2000 all come bundled with VPN clients based on PPTP. VPN client software is also included in Microsoft's free upgrade to the Windows 95 dial-up networking package (DUN 1.3). Commercial third-party implementations of PPTP are available for Macintosh clients.

With PPTP client software installed on a mobile or home PC, a user can dial up an Internet Service Provider of their choice and establish an encrypted tunnel, through InstaGate, into the corporate network across the Internet. The user then has full access to all the resources of the internal network, just as if the PC were directly attached to the LAN. InstaGate authenticates all users attempting to establish such tunnels.

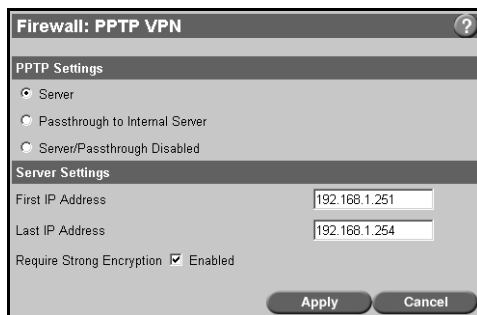
PPTP is not available if InstaGate is configured to use a dynamic IP address.

To enable the PPTP VPN Server:

1. Select *PPTP VPN* from the *Firewall* menu.
2. Select *Server* to enable InstaGate's PPTP VPN Server.

If PPTP VPN support is not a necessary requirement for your business, select *Server/Passthrough Disabled* to reduce system load.

To forward PPTP VPN sessions to another VPN server on your LAN, select *Passthrough to Internal Server*. See "Enabling PPTP VPN Forwarding" on page 69 for more information.



3. Specify the range of IP addresses that are available for assignment to PPTP client sessions in the *First* and *Last IP Address* fields. Addresses in this range should not be used by any other devices on the network or overlap any range of addresses that could be dynamically assigned by a DHCP server.
4. Select the *Require Strong Encryption* check box to require that PPTP sessions initiated by Windows clients employ 128-bit encryption. In order to employ strong encryption, Windows clients must use MS CHAP version 2.0 and 128-bit encryption.

Leave this box unchecked to support both 128-bit and 40-bit encryption keys. In this mode the PPTP VPN server will always attempt to negotiate use of 128-bit keys, and fall back to 40-bit keys only if the client does not support the longer key length.
5. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Enabling PPTP VPN Forwarding

InstaGate provides passthrough support for secure remote VPN access through the Point-to-Point Tunneling Protocol (PPTP). In this mode, InstaGate simply becomes an address translating router for PPTP packets.

To forward PPTP sessions to a designated VPN server on the LAN:

1. Select *PPTP VPN* from the *Firewall* menu.
2. Select the *Passthrough to Internal Server* radio button.
3. Enter the internal VPN *Server IP Address* to which PPTP sessions should be forwarded.
4. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring a Windows Client for PPTP

Remote users may need to make some changes to their system settings before they can use PPTP from their Windows 95, Windows 98, Windows NT, or Windows 2000 machines.

To set up a Windows 95 client machine, you must have Microsoft's Dial-Up Networking Client version 1.3 for Windows installed.

To configure a remote user for PPTP:

1. Select *My Computer*.
2. Select *Dial-Up Networking*.
3. In Windows 95/98, select *Make New Connection*, select *Microsoft VPN Adapter* as the device, and click *Next*.

In Windows NT/2000, select the *I know all about phone book entries* check box and click *Finish*.

4. In Windows 95/98, enter the *IP Address* of InstaGate, click *Next*, and then click *Finish*.

In Windows NT/2000, enter the IP address of InstaGate in the *Phone Number* field, set *Dial Using* to *RAS VPN*, and click *OK*.

To create a virtual private network connection across the Internet, you must also create a Dial-Up Networking connection to your Internet Service Provider. Once connected to your ISP, use the phone book entry created in step 3 to initiate the VPN connection. You will be prompted for a user name and password. Enter your InstaGate account name and password. When the dialog disappears, you are securely connected to the network behind the firewall.

Note To remove a site from the list, simply select the site and click *Delete*.

Configuring Firewall Policies

A firewall policy is a set of parameters that define which services are available to your users and hosts. Use firewall policies to allow or deny communication in either direction between InstaGate and any or all IP addresses.

When an IP packet arrives, InstaGate checks the list of policies from top to bottom and uses the first policy it finds whose parameters match the IP packet. The IP packet must match the following parameters:

- Service being requested (SMTP, HTTP, etc.)
- Source address of the IP packet
- Destination address of the IP packet (optional)

Once a policy is chosen, InstaGate checks the *Action* field to determine how the IP packet should be handled. If the Action field is set to *Accept*, the packet is allowed. If the Action field is set to *Deny*, the packet is immediately dropped before any data is transferred. If the Action field is set to *Redirect*, the packet is accepted and passed to a specified destination. If the Action field is set to *Web Access Control*, the packet is accepted and passed to InstaGate's Web Proxy Server.

You will probably need to create several different policies to meet your organization's requirements.

To configure firewall policies:

1. Select *Policies* from the *Firewall* menu. A list of the policies currently defined on your system appears. You can view the policies which apply to the *LAN* interface, the *WAN* interface, the *DMZ* interface, or *All* policies.
2. To add a new firewall policy, click *Add*. See "Adding Firewall Policies" on page 72 for more information.

Note Any changes made to firewall policies (adding, modifying or deleting) are logged in the EVERYTHING.log file. To view the EVERYTHING.log file, select *System Logs* from the *Support and Diagnostics* menu, and select *General System* from the *Areas* drop-down list.

3. To modify an existing firewall policy, select the policy you wish to modify, and click *Modify*. See "Modifying Firewall Policies" on page 75 for more information.

-
4. To change the order of your firewall policies, "Click and drag" the policy to desired location and drop in that location. When you are finished, use the Apply button to commit your changes. Alternatively, you may select the policy you want to move, and click *Up* or *Down*.

When an IP packet arrives, InstaGate checks your policies list from top to bottom and selects the first policy that matches the source address and service requested. It is important, therefore, to list your policies in the correct order to prevent the wrong policy from being applied.

5. To remove an existing firewall policy, select the policy you want to remove, and click *Delete*. See "Deleting Firewall Policies" on page 75 for more information.
6. To create a copy of an existing firewall policy, select the policy you want to copy, and click *Copy*.

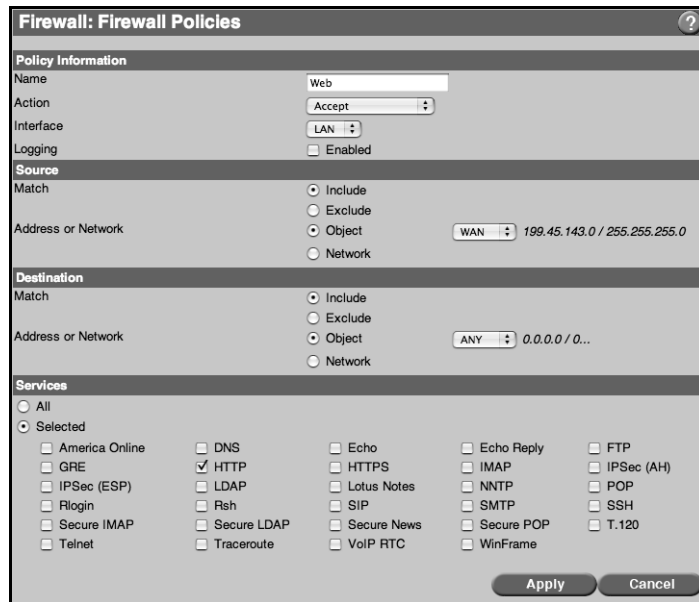
A copy of the selected policy is created with a unique name based on the name of the original. In order to preserve uniqueness, the word "copy" is appended to the name of the policy. If a policy with such a name already exists, a number is appended. That number is incremented until no matching policies are found. For example, if you try to copy a policy named "Block FTP", and policies named "Block FTP copy" and "Block FTP copy 1" already exist, the new copy is named "Block FTP copy 2".

7. Click *Done* when you have finished configuring firewall policies.

Adding Firewall Policies

To add a new firewall policy:

1. Select *Policies* from the *Firewall* menu. A list of the policies currently defined on your system appears.
2. Click *Add*.



3. Enter a *Name* for the policy.
4. Select the *Action* to take when an IP packet arrives matching the policy:
 - a. **Accept** - Allows the packet.
 - b. **Deny** - Rejects the packet.
 - c. **Redirect (DNAT)** - Accepts the packet and passes it to a specified destination, usually on the LAN, by modifying the destination IP address on the incoming packet.
 - d. **Source NAT (SNAT)** - Accepts the packet and passes it to the specified destination, but modifies the source IP address of the packet to the specified Public Source IP address.
 - e. **Application Proxy** - Accepts the packet and passes it to InstaGate's HTTP/HTTPS web caching proxy server.
5. Select the *Interface* the policy applies to. To control access to the Internet by internal users, select *LAN*. To control access to your network by external users, select *WAN*. Select *DMZ* to control access to the LAN or WAN from servers on the DMZ network.
6. Select the *Logging Enabled* check box to log all connection attempts matching the policy. If you have *Application Proxy* selected in the *Action* field, logging is automatically enabled.
7. All Actions allow you to configure values to match on the *Source (or Private Source)* of pack-

ets passing through the *InstaGate*. To configure the values you need to perform the following:

- a. Select *Include* or *Exclude* from the *Match* parameter. This setting allows you to specify whether packets matching the source address will be included or excluded in the firewall policy.
- a. Enter the *Address* or *Network* to match in the policy. Use *Object* to select from a list of pre-defined values or *Network* to manually enter the address and subnet mask of the source host or network.

Note The predefined *objects* are useful when you change the IP address of the LAN, WAN, DMZ or secondary WAN addresses. *InstaGate* will automatically update the firewall rule to the new IP address when the IP Address changes in any of the objects

8. The *Source NAT (SNAT) Action* requires you specify the *Public Source* used in the firewall policy. The value used in this section replaces the original source IP address of the packet exiting *InstaGate*. To specify the address choose the *Object* from the list or specify the IP address manually by selecting IP Address and entering the IP address in the text box.
9. All *Actions* allow you to configure values to match on the *Destination (or Public Destination)* of packets passing to or through the *InstaGate*. To restrict the policy to IP packets destined for a specific host or network perform the following steps:
 - a. Select *Include* or *Exclude* from the *Match* parameter. This setting allows you to specify whether packets matching the destination address will be included or excluded in the firewall policy.
 - a. Enter the *Address* or *Network* to match in the policy. Use *Object* to select from a list of pre-defined values or *Network* to manually enter the address and subnet mask of the destination host or network.
10. The *Redirect (DNAT) Action* requires you to specify the *Private Destination* where *InstaGate* will redirect or send the packets. The value replaces the original destination IP address of the packets with the value specified when the packet exits *InstaGate*. For example, to redirect Internet service requests like Web (HTTP) or mail (SMTP) to a computer resource on your LAN, enter *InstaGate's* WAN IP address (192.168.1.1) in the *Public Destination* address field, and the IP address of the computer resource on your LAN that the request from the Internet should be forwarded to in the *Private Destination* address field.

The port and protocol for the destination IP addresses are determined by the *Service* selected.

11. The *Redirect (DNAT) Action* gives you an additional option called *Redirect Source Address* to automatically create a *Source NAT* rule for traffic from the *Private Destination* to be mapped

to the *Public Destination*. This is useful when you *Redirect* packets from a secondary address and you want all packets that originate from the private address to use that same IP address.

12. Select the *Services* affected by the policy. If the policy applies to all services, select the *All services* radio button. If the policy only applies to certain services, select the *Select services* radio button, and specify the services affected.
13. Click *Apply* to save the firewall policy, or *Cancel* to exit without saving.

Modifying Firewall Policies

To modify a firewall policy:

1. Select *Policies* from the *Firewall* menu. A list of the policies currently defined on your system appears.
2. Select the policy you wish to modify, and click *Modify*.
3. Make any necessary changes to the policy.
4. Click *Modify* to save your changes.

Deleting Firewall Policies

To delete a firewall policy:

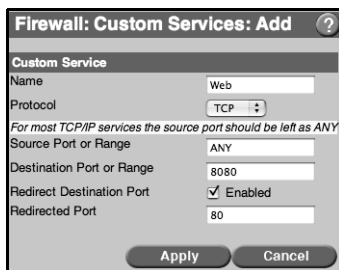
1. Select *Policies* from the *Firewall* menu. A list of the policies currently defined on your system appears.
2. Select the policy you wish to delete, and click *Delete*.
3. Click *Delete* again to delete the firewall policy.

Defining Custom Services

InstaGate allows you to define custom Internet services. Access to these services can then be controlled through firewall policies.

To add a custom service:

1. Select *Custom Services* from the *Firewall* menu. A list of the services currently defined on your system appears. InstaGate automatically defines some of the more popular Internet services (AOL, IMAP, Lotus Notes, etc.)
2. Click *Add*.



3. Enter a *Name* for the service.
4. Select the *Protocol* of the service. A protocol is a standardized form of communication between network devices.

To specify a protocol that does not appear in the Protocol list, select *Other* and enter the *Protocol Number* (for example, **2** for *igmp*, **89** for *ospf*, or **94** for *ipip*).

5. If you selected *TCP* or *UDP* in the Protocol field, enter the network port number or the range of network port numbers to which requests for the service will connect. You can specify the *Source Port* number, the *Destination Port* number, or both. Enter port ranges in “x-y” format (for example, 23-25 or 8500-8599). The manufacturer of the software for which you are creating the custom service should be able to provide you with the port number the software uses.

If you selected *ICMP* in the Protocol field, enter the *Service number* for the custom service.

This field does not appear if you have *GRE*, *AH*, or *ESP* selected in the Protocol field.

Note For a list of common service ports and their protocols, as well as common ICMP messages and their service numbers, refer to the online help.

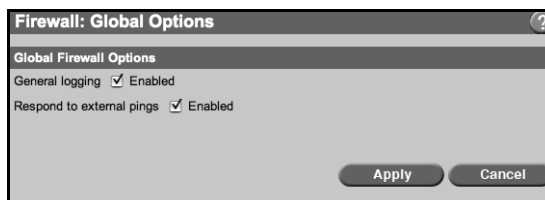
-
6. If you selected TCP or UDP in the *Protocol* field, you may optionally specify a different destination port. The *Redirect Destination Port* allows you to specify a different destination port when used in conjunction with a *Redirect (DNAT)* firewall policy. For example, you could have an internet Web server running on TCP 80, but have InstaGate redirect traffic from another TCP port you specify, such as port 8080.
 7. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Enabling Global Firewall Options

The Global Options page allows you to enable general firewall logging and pings on the WAN interface.

To enable the global firewall options:

1. Select *Global Options* from the *Firewall* menu.



2. Select the *General logging Enabled* check box to automatically log all blocked, failed or unauthorized connection attempts that may pose security concerns.
3. Select the *Respond to external pings Enabled* check box to allow machines on the Internet to ping the WAN interface (or to allow machines on the DMZ network to ping the DMZ interface).

Ping is a diagnostic tool used for testing connectivity between two machines on a TCP/IP network. Occasionally, it may be necessary for the InstaGate to respond to external pings in order for third party network services to work. Due to potential security concerns, however, this feature should only be enabled while troubleshooting.

4. Click *Apply* to save your settings, or *Cancel* to exit without saving.

This chapter provides detailed information on how to modify and manage your LAN, WAN and DMZ configuration settings. It covers the following topics:

- Configuring the LAN Settings
- Configuring the WAN Settings
- Configuring the Internet Connection Settings
- Configuring Static Routes
- Configuring the DMZ Settings
- Configuring Failover Support

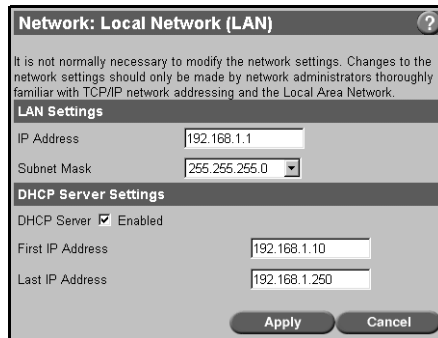
Configuring the LAN Settings

Once configured, it is not normally necessary to modify the network settings. Changes to the network settings should only be made by network administrators thoroughly familiar with TCP/IP network addressing and your LAN.

If you do change InstaGate's default network configuration be sure to read the warnings that go along with each network configuration parameter. Improper configuration of some of the network configuration parameters may make InstaGate unreachable or parts of your LAN inoperable.

To modify the local network configuration settings:

1. Select *Local Network (LAN)* from the *Network* menu.



2. Type InstaGate's LAN Ethernet *IP Address*. The default is **192.168.1.1**.

Changing InstaGate's IP address will make the server and the Internet temporarily unreachable for the computers on your LAN. If the computers on your LAN are already configured to use InstaGate, and you change the server's IP address, the computers will need to be reconfigured.

- If you are using InstaGate's DHCP server, simply restart all of the computers on your LAN.
 - If you are using another DHCP server or static TCP/IP configuration for the computers on your LAN, you will need to change the DHCP server/static client configuration settings to reflect InstaGate's new network configuration. After changing the settings, either restart the client computers or run the `windowsipcfg` program from the DOS Prompt and click *Release All* and then *Renew All*.
3. Select the *Subnet Mask* used on your network (default **255.255.255.0**). A subnet mask is a number used in conjunction with an IP address to define the set of local addresses on a LAN.
 4. Select the *DHCP Server Enabled* check box to activate InstaGate's DHCP Server.

By enabling InstaGate's DHCP server, each client computer's IP address, default gateway (router), and DNS settings can be configured automatically. All of these TCP/IP parameters are necessary for optimal use of InstaGate's resources. If you choose to use an existing DHCP server (such as Windows NT) rather than InstaGate's DHCP server, you will need to configure the existing DHCP server to properly set up each client computer's TCP/IP configuration (or configure each client manually).
 5. Type the *First* and *Last IP Address* in the range of addresses to be assigned to DHCP clients. The default starting IP address is **192.168.1.10** and the default ending IP address is **192.168.1.250**.
 6. Click *Apply* to save your changes, or *Cancel* to exit without saving.

Note InstaGate uses Network Address Translation (NAT) to hide the internal IP addresses of clients and servers on your network from the Internet. NAT is permanently enabled on InstaGate.

Configuring the WAN Settings

The configuration parameters specified in the ISP Settings page allow InstaGate to connect to your Internet Service Provider (ISP) and access its resources.

To modify the WAN configuration settings:

1. Select *ISP Settings (WAN)* from the *Network* menu.
2. Select the WAN connection *Device Type* from the drop-down list. This determines which port is used to connect to the Internet, and alters the screen accordingly. **The InstaGate 404, 604, and 806 only have the Ethernet in the drop-down list.**
3. Complete the remainder of the form using the information provided for your selected device type. See “DSL” on page 81, “Ethernet” on page 85, “Euro ISDN” on page 87, “Modem or External Modem” on page 89, “Synchronous Serial V.35/X.21 or T1/E1 CSU/DSU” on page 90, or “Wireless 802.11B” on page 93. **These options are for InstaGate EX2, PRO, xSP.**

DSL

If you are using InstaGate’s internal DSL modem as your Internet gateway, you need to configure the IP parameters for the link.

Note: This feature is available on the InstaGate EX, PRO, and xSP.

To set up your DSL connection:

1. Select the encapsulation *Mode* supported by your ISP. The following options are available: *Classic*, *PPPoA*, and *Bridged*.
2. Complete the remainder of the form using the information provided for the selected mode. See “Classic Mode” on page 82, “PPPoA Mode” on page 82, or “Bridged Mode” on page 83.

Network: ISP Settings (WAN)

WAN Connection Device

Device Type: DSL

Mode

Classic
 PPPoA
 Bridged

IP Address Settings

Assign a Static IP Address

IP Address: 199.54.137.1
Subnet Mask: 255.255.255.0
Gateway IP Address: 199.54.137.14

DNS Resolver Settings

Primary DNS IP Address: 199.54.137.14
Secondary DNS IP Address (optional):

Advanced Addresses
Apply Cancel

Classic Mode

To configure your DSL connection to use classical IP encapsulation:

1. Enter the *IP Address* of the DSL interface. This address is provided by your ISP and used by InstaGate as its Internet address.
2. Select the *Subnet Mask* for the DSL interface. The default is **255.255.255.0**.
3. Enter the *Gateway IP Address*. This is the address of your ISP's router.
4. Enter your ISP's *Primary DNS IP Address* and *Secondary DNS IP Address*. If your ISP does not have a secondary (or backup) DNS server, leave this field blank.
5. To specify the VPI/VCI values your ISP is using for your DSL connection, click *Advanced*. See "DSL Advanced Options" on page 84 for more information.
6. To add secondary IP addresses to the WAN interface, click *Addresses*. See "Secondary IP Addresses" on page 85 for more information.
7. Click *Apply* to save your settings, or *Cancel* to exit without saving.

PPPoA Mode

To configure your DSL connection to use PPPoA encapsulation:

1. Select the encapsulation mode supported by your ISP (*VC Mode* or *LLC Mode*).
2. Select the authentication protocol used by your ISP (*PAP* or *CHAP*).

-
3. Type your login name in the ISP *Username* text box.
 4. Type your login password in the ISP *Password* text box.
 5. If your ISP requires CHAP authentication, enter the name of your *ISP's CHAP Server*. If you don't know the name of your ISP's CHAP server, entering * in this field will work in almost all instances.
 6. Set the IP address for the connection:
 - If your ISP allocates your IP address on connection, click the *Obtain a Dynamic IP Address* radio button.
 - If your ISP has provided you with a static (permanent) IP address, click the *Assign a Static IP Address* radio button and enter the *IP Address* in the text box.
 7. Enter your ISP's *Primary DNS IP Address* and *Secondary DNS IP Address*. If your ISP does not have a secondary (or backup) DNS server, leave this field blank.
 8. To specify the VPI/VCI values your ISP is using for your DSL connection, click *Advanced*. See "DSL Advanced Options" on page 84 for more information.
 9. To add secondary IP addresses to the WAN interface, click *Addresses*. See "Secondary IP Addresses" on page 85 for more information. This option is only available if you have a static Internet connection.
 10. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Bridged Mode

To configure your DSL connection to use bridged encapsulation:

1. Select the *Protocol* supported by your ISP.
 - If your ISP uses the standard line protocol, click *None*.
 - If your ISP requires the use of PPPoE, click *PPPoE* and specify the following authentication settings:
 - a. Type your login name in the ISP *Username* text box.
 - b. Type your login password in the ISP *Password* text box.
 - c. If your ISP requires CHAP authentication, enter the name of your *ISP's CHAP Server*. If you don't know the name of your ISP's CHAP server, entering * in this field will work in almost all instances.

2. Set the IP address for the connection:

- If your ISP allocates your IP address on connection, click *Obtain a Dynamic IP Address* to automatically configure your IP settings.

Some ISP's may require you to specify a *DHCP Client Hostname*. Contact your ISP to determine if a DHCP Client Hostname is required.

- If your ISP has provided you with a static (permanent) IP address, click *Assign a Static IP Address* and enter the following IP parameters:
 - a. Enter the *IP Address* of the DSL interface. This address is provided by your ISP and used by InstaGate as its Internet address. The address you use must be in the same subnet as your Internet gateway.
 - b. Select the *Subnet Mask* for the DSL interface. The default is **255.255.255.0**. This setting is not required for connections using PPPoE.
 - c. Type the *Gateway IP Address*. This is the address of your ISP's router. It is not required for connections using PPPoE.
3. Enter your ISP's *Primary DNS IP Address* and *Secondary DNS IP Address*. If your ISP does not have a secondary (or backup) DNS server, leave this field blank.
4. To specify the VPI/VCI values your ISP is using for your DSL connection, click *Advanced*. See "DSL Advanced Options" on page 84 for more information.
5. To add secondary IP addresses to the WAN interface, click *Addresses*. See "Secondary IP Addresses" on page 85 for more information. This option is only available if you have a static Internet connection.
6. Click *Apply* to save your settings, or *Cancel* to exit without saving.

DSL Advanced Options

In some circumstances, InstaGate may be unable to automatically detect the virtual path identifier/virtual circuit identifier (VPI/VCI) values your ISP is using for your DSL connection. The DSL Advanced Options page allows you to manually specify the VPI/VCI settings.

Note: This feature is available on the InstaGate EX, PRO, and xSP.

To manually specify the VPI/VCI settings:

1. Select the *Manually specify* radio button.
2. Enter the *VPI* value provided by your ISP. For example, **8**.
3. Enter the *VCI* value provided by your ISP. For example, **35**.

-
- Click *Apply* to save your settings and return to the ISP Settings page.

Secondary IP Addresses

By adding secondary IP addresses to the WAN interface, multiple machines on the LAN can be accessed on the same IP port using firewall passthrough rules. For example, secondary IP addresses allow an organization to set up multiple Web servers, with several machines on the LAN serving Web pages over IP Port 80.

This option is only available if you are using a static DSL connection.

To add a secondary Internet IP address:

- Enter the secondary Internet *IP Address* and click *Add*. The IP address specified cannot be an address on the LAN or (if you have the DMZ SoftPak installed) the DMZ network, and it cannot be the same as your gateway/remote IP address.
- Click *Apply* to save your settings, or *Cancel* to exit without saving.

Ethernet

If you are using the Ethernet WAN port to communicate with your ISP (for example, an external DSL modem, a cable modem, or a WAN router), you need to configure the IP parameters for the link.

The screenshot shows a configuration window titled "WAN Connection Device". The "Device Type" is set to "Ethernet". Under "Protocol", "None" is selected. The "IP Address Settings" section has "Assign a Static IP Address" selected, with the IP Address field containing "199.45.143.210", the Subnet Mask field containing "255.255.255.0", and the Gateway IP Address field containing "199.45.143.1". The "Network Address Translation" section has "Use Network Address Translation (NAT) (Recommended)" checked. The "DNS Resolver Settings" section has empty fields for "Primary DNS IP Address" and "Secondary DNS IP Address (optional)". At the bottom right, there are "Apply", "Cancel", and "Addresses" buttons.

To set up your Ethernet connection:

1. Select the Ethernet *Protocol* supported by your ISP.
 - If your ISP uses the standard line protocol, click *None*.
 - If your ISP requires the use of PPPoE, click *PPPoE* and specify the following authentication settings:
 - a. Type your login name in the ISP *Username* text box.
 - b. Type your login password in the ISP *Password* text box.
 - c. If your ISP requires CHAP authentication, enter the name of your *ISP's CHAP Server*. If you don't know the name of your ISP's CHAP server, entering * in this field will work in almost all instances.
2. Set the IP address for the connection:
 - If your ISP allocates your IP address on connection, click *Obtain a Dynamic IP Address* to automatically configure your IP settings.

If you are using a cable modem to connect to the Internet, your cable modem service provider may require a *DHCP Client Hostname*. Contact your ISP to determine if a DHCP Client Hostname is required.
 - If your ISP has provided you with a static (permanent) IP address, click *Assign a Static IP Address* and enter the following IP parameters:
 - a. Type the *IP Address* of the Internet Ethernet interface. This address is provided by your ISP and used by InstaGate as its Internet address. The address you use must be in the same subnet as your Internet gateway.
 - b. Select the *Subnet Mask* for the Internet Ethernet interface. The default is **255.255.255.0**. This setting is not required for connections using PPPoE.
 - c. Type the *Gateway IP Address* of the Internet Ethernet interface. This is the address of your ISP's router. It is not required for connections using PPPoE.
3. If you need to disable NAT, uncheck Use Network Translation. Your ISP will need to route your LAN IP addresses to and from the Internet.
4. Enter your ISP's *Primary DNS IP Address* and *Secondary DNS IP Address*. If your ISP does not have a secondary (or backup) DNS server, leave this field blank.
5. To add secondary IP addresses to the WAN interface, click *Addresses*. See "Secondary IP Addresses" on page 87 for more information. This option is only available if you have a static Ethernet connection.
6. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Secondary IP Addresses

By adding secondary IP addresses to the WAN interface, multiple machines on the LAN can be accessed on the same IP port using firewall policies. For example, secondary IP addresses allow an organization to set up multiple Web servers, with several machines on the LAN serving Web pages over IP Port 80.

This option is only available if you are using a static Ethernet connection.

To add a secondary Internet IP address:

1. Enter the secondary Internet *IP Address* and click *Add*. The IP address specified cannot be an address on the LAN or DMZ network, and it cannot be the same as your gateway/remote IP address.
2. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Euro ISDN

Note: This feature is available on the InstaGate EX, PRO, and xSP.

If you are using InstaGate's internal Euro ISDN adapter to connect to the Internet, you need to provide the login details for your ISP.

Network: ISP Settings (WAN)

WAN Connection Device

Device Type: Euro-ISDN

ISP Connection Settings

Username: jsmith

Password: *****

ISP's CHAP Server (optional): *

Phone Number: 303-555-1212

ISDN Connection Settings

PPP Communication: Asynchronous 64K - HDLC

Switch type: Euro-ISDN (EDSS1)

MSN (for Euro-ISDN) or EAZ (for German 1TR6): 30355512120101

DNS Resolver Settings

Primary DNS IP Address: 192.168.2.254

Secondary DNS IP Address (optional):

Advanced

Apply Cancel

To set up your ISDN connection:

1. Type your login name in the ISP *Username* text box.
2. Type your login password in the ISP *Password* text box.
3. If your ISP requires CHAP authentication, enter the name of your *ISP's CHAP Server*. If you don't know the name of your ISP's CHAP server, entering * in this field will work in almost all instances.
4. Type the dial in ISDN number in the ISP's *Phone Number* text box.
5. Select the *PPP Communication* type. For a description of each of the PPP communication types, refer to the online help.
6. Select the telephone company's *ISDN Switch Type*. InstaGate's Europe ISDN adapters support the Euro ISDN (EDSS1) or the German ISDN (ITR6) switch types. Check with your telephone company when you order your ISDN line to determine which switch type to select.
7. Unlike an analog phone line, an ISDN phone line can have several phone numbers associated with it. These numbers have an *MSN* (Euro ISDN EDSS1) or *EAZ* (German ISDN ITR6), which InstaGate uses to distinguish among phone numbers on an ISDN line.

Your telephone company will tell you your MSNs or EAZs. In most cases the MSN is the ISDN phone number and the EAZ is the last number in the phone number (except as noted below). If you are connected to a PBX that uses ISDN, then your MSN is the extension where InstaGate is connected.

Exceptions:

- **Austria** — The MSN is always 0
 - **Switzerland** — The MSN is the last number of your phone number
 - **Germany** — You can use any available EAZ, except for 0 and 9
8. Enter your ISP's *Primary DNS IP Address* and *Secondary DNS IP Address*. If your ISP does not have a secondary (or backup) DNS server, leave this field blank.
 9. If your ISP requires any advanced configuration settings, click *Advanced*. See "Euro ISDN Advanced Options" on page 89 for more details.
 10. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Euro ISDN Advanced Options

To complete the Advanced Options form:

1. Some ISPs use a terminal-type login to access the Internet. If your ISP requires a terminal-type login, select the *Use terminal-type ISP login* check box.
2. If your ISP requires a custom dialer connect script, click the *Edit Script* button.
 - a. Click the *Custom Script Enabled* check box.
 - b. Type the expect-response strings (modem AT commands) for the dialer connect script. A default dialer connect script is provided. Edit the default script by adding your ISP information to it.
 - c. Click *Apply* to save your settings and return to the Advanced Options page.
3. Set the IP address for the connection:
 - If your ISP allocates your IP address on connection, click the *Obtain a Dynamic IP Address via ISP* radio button.
 - If your ISP has provided you with a static (permanent) IP address, click the *Assign a Static IP Address* radio button and enter the IP address in the text box.
4. Click *Apply* to save your settings and return to the Euro ISDN Configuration page.

Modem or External Modem

Note: This feature is available on the InstaGate EX, PRO, and xSP.

If you are using InstaGate's internal modem port or an external modem connected to Serial Port 1 as your Internet gateway, you need to provide the login details for your ISP.

The screenshot shows a configuration window titled "Network: ISP Settings (WAN)". It is divided into three main sections:

- WAN Connection Device:** A dropdown menu for "Device Type" is set to "Modem".
- ISP Connection Settings:** Includes fields for "Username" (containing "jsmith"), "Password" (masked with asterisks), "ISP's CHAP Server (optional)" (containing "*"), and "Phone Number" (containing "303-555-1212").
- DNS Resolver Settings:** Includes fields for "Primary DNS IP Address" (containing "192.168.2.254") and "Secondary DNS IP Address (optional)" (empty).

At the bottom right, there are three buttons: "Advanced", "Apply", and "Cancel".

To set up your modem connection:

1. Type your login name in the ISP *Username* text box.
2. Type your login password in the ISP *Password* text box.
3. If your ISP requires CHAP authentication, enter the name of your *ISP's CHAP Server*. If you don't know the name of your ISP's CHAP server, entering * in this field will work in almost all instances.
4. Type the dial in phone number in the ISP's *Phone Number* text box.
5. Enter your ISP's *Primary DNS IP Address* and *Secondary DNS IP Address*. If your ISP does not have a secondary (or backup) DNS server, leave this field blank.
6. If your ISP requires any advanced configuration settings, click *Advanced*. See "Modem or External Modem Advanced Options" on page 90 for more details.
7. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Modem or External Modem Advanced Options

To complete the Advanced Options form:

1. Some ISPs use a terminal-type login to access the Internet. If your ISP requires a terminal-type login, select the *Use terminal-type ISP login* check box.
2. If your ISP requires a custom dialer connect script, click the *Edit Script* button.
 - a. Click the *Custom Script Enabled* check box.
 - b. Type the expect-response strings (modem AT commands) for the dialer connect script. A default dialer connect script is provided. Edit the default script by adding your ISP information to it.
 - c. Click *Apply* to save your settings and return to the Advanced Options page.
3. Set the IP address for the connection:
 - If your ISP allocates your IP address on connection, click the *Obtain a Dynamic IP Address via ISP* radio button.
 - If your ISP has provided you with a static (permanent) IP address, click the *Assign a Static IP Address* radio button and enter the IP address in the text box.
4. Click *Apply* to save your settings and return to the Modem Configuration page.

Synchronous Serial V.35/X.21 or T1/E1 CSU/DSU

Note: This feature is available on the InstaGate EX, PRO, and xSP.

If you are using InstaGate’s synchronous serial (DB-37) or T1/E1 port to communicate with your ISP, you need to configure the IP parameters for the link.

The screenshot shows the 'Network: ISP Settings (WAN)' configuration window. It is divided into several sections:

- WAN Connection Device:** Device Type is set to 'Synchronous V.35/X.21 or T1/E1 CSU/DSU'.
- CSU/DSU Settings:** 'External' is selected. Under 'T1', 'Decoding' is 'B8ZS', 'Framing' is 'ESF', 'LBO' is 'CSU: 0db', and 'Active Channels' is 'All'.
- Synchronous Serial Protocol:** 'Frame Relay' is selected.
- Frame Relay Settings:** 'Protocol' is 'ANSI' and 'DLCI' is '16'.
- IP Address Settings:** 'Local IP Address' is '192.168.2.1' and 'Remote IP Address' is '199.174.1.54'.
- DNS Resolver Settings:** 'Primary DNS IP Address' is '192.168.2.14' and 'Secondary DNS IP Address (optional)' is empty.

Buttons at the bottom right include 'Addresses', 'Apply', and 'Cancel'.

To set up your WAN connection:

1. Select the appropriate CSU/DSU setting for your connection:
 - **External** — Select this option if you are connecting InstaGate’s synchronous serial port to an external CSU/DSU.
 - **T1** — Select this option if you are connecting InstaGate’s internal T1/E1 CSU/DSU port to a T1 line. The CSU/DSU configuration settings (*Decoding*, *Framing*, *LBO*, and *Active Channels*) must be obtained from the T1 provider.
 - **E1** — Select this option if you are connecting InstaGate’s internal T1/E1 CSU/DSU port to an E1 line. The CSU/DSU configuration settings (*Decoding*, *Framing*, and *Active Channels*) must be obtained from the E1 provider.
2. Select the *Synchronous Serial Protocol* supported by your ISP. The following options are available: *PPP*, *Cisco HDLC*, and *Frame Relay*.
3. Complete the remainder of the form using the information provided for the selected synchronous serial protocol. See “PPP Serial Protocol” on page 92, “Cisco HDLC Serial Protocol” on page 92, or “Frame Relay Serial Protocol” on page 93.

PPP Serial Protocol

Note: This feature is available on the InstaGate EX, PRO, and xSP.

To configure the PPP settings for your Synchronous Serial V.35/X.21 or T1/E1 connection:

1. Select the *PPP Authentication Type* used by your ISP (*PAP* or *CHAP*). If your ISP does not require authentication to establish a PPP link, select *None*.
2. If your ISP requires PAP or CHAP authentication, enter your ISP *Username* (login name) and *Password*.
3. If your ISP requires CHAP authentication, enter the *Remote (CHAP) Server Name*. If you don't know the name of your ISP's CHAP server, entering * in this field will work in almost all instances.
4. Enter the *Local IP Address* of the PPP interface. This address is provided by your ISP and used by InstaGate as its Internet address.
5. Enter the *Remote IP Address* of the PPP interface. This is the address of your ISP's router.
6. Enter your ISP's *Primary DNS IP Address* and *Secondary DNS IP Address*. If your ISP does not have a secondary (or backup) DNS server, leave this field blank.
7. To add secondary IP addresses to the WAN interface, click *Addresses*. See "Secondary IP Addresses" on page 93 for more information.
8. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Cisco HDLC Serial Protocol

Note: This feature is available on the InstaGate EX, PRO, and xSP.

To configure the Cisco HDLC settings for your Synchronous Serial V.35/X.21 or T1/E1 connection:

1. Enter the *Local IP Address* of the Cisco HDLC interface. This address is provided by your ISP and used by InstaGate as its Internet address.
2. Enter the *Remote IP Address* of the Cisco HDLC interface. This is the address of your ISP's router.
3. Enter your ISP's *Primary DNS IP Address* and *Secondary DNS IP Address*. If your ISP does not have a secondary (or backup) DNS server, leave this field blank.
4. To add secondary IP addresses to the WAN interface, click *Addresses*. See "Secondary IP Addresses" on page 93 for more information.
5. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Frame Relay Serial Protocol

Note: This feature is available on the InstaGate EX, PRO, and xSP.

To configure the Frame Relay settings for your Synchronous Serial V.35/X.21 or T1/E1 connection:

1. Select the *Frame Relay Protocol* used by your ISP, *ANSI*, *LMI*, or *Q933*.
2. Enter the *Frame Relay DLCI* (Data Link Connection Identifier) provided by your ISP. The DLCI defines the logical channel between InstaGate and your ISP.
3. Enter the *Local IP Address* of the Frame Relay interface. This address is provided by your ISP and used by InstaGate as its Internet address.
4. Enter the *Remote IP Address* of the Frame Relay interface. This is the address of your ISP's router.
5. Enter your ISP's *Primary DNS IP Address* and *Secondary DNS IP Address*. If your ISP does not have a secondary (or backup) DNS server, leave this field blank.
6. To add secondary IP addresses to the WAN interface, click *Addresses*. See "Secondary IP Addresses" on page 93 for more information.
7. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Secondary IP Addresses

By adding secondary IP addresses to the WAN interface, multiple machines on the LAN can be accessed on the same IP port using firewall policies. For example, secondary IP addresses allow an organization to set up multiple Web servers, with several machines on the LAN serving Web pages over IP Port 80.

To add a secondary Internet IP address:

1. Enter the secondary Internet *IP Address* and click *Add*. The IP address specified cannot be an address on the LAN or (if you have the DMZ SoftPak installed) the DMZ network, and it cannot be the same as your remote IP address.
2. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Wireless 802.11B

Note: This feature is available on the InstaGate EX, PRO, and xSP.

If you are using InstaGate's Wireless 802.11B port to communicate with your ISP, you need to configure the IP parameters for the link.

The screenshot shows the 'Network: ISP Settings (WAN)' configuration window. It is divided into several sections:

- WAN Connection Device:** Device Type is set to 'Wireless 802.11B'.
- IP Address Settings:** Two radio buttons are present: 'Obtain a Dynamic IP Address via DHCP' (unselected) and 'Assign a static IP address' (selected).
- Static IP Address Settings:** IP Address is '199.54.137.21', Subnet Mask is '255.255.255.0', and Gateway IP Address is '199.54.137.14'.
- DNS Resolver Settings:** Primary DNS IP Address is '199.54.137.14' and Secondary DNS IP Address (optional) is blank.
- Wireless Network Settings:** ESS ID is 'eSoft'.

Buttons at the bottom right include 'Addresses', 'Security', 'Apply', and 'Cancel'.

To set up your Wireless 802.11B connection:

1. Set the IP address for the connection:
 - If your ISP allocates your IP address on connection, click *Obtain a Dynamic IP Address* to automatically configure your IP settings.

Some ISP's may require you to specify a *DHCP Client Hostname*. Contact your ISP to determine if a DHCP Client Hostname is required.
 - If your ISP has provided you with a static (permanent) IP address, click *Assign a Static IP Address* and enter the following IP parameters:
 - a. Type the *IP Address* of the wireless interface. This address is provided by your ISP and used by InstaGate as its Internet address. The address you use must be in the same subnet as your Internet gateway.
 - b. Select the *Subnet Mask* for the wireless interface. The default is **255.255.255.0**.
 - c. Type the *Gateway IP Address*. This is the address of your ISP's router.
2. Enter your ISP's *Primary DNS IP Address* and *Secondary DNS IP Address*. If your ISP does not have a secondary (or backup) DNS server, leave this field blank.
3. Enter the *ESS ID* for your WAN. The ESS ID is a unique name shared among all points in a wireless network. The ESS ID is case sensitive and must be identical for all points in the network.

-
4. Select the *WEP Encryption Enabled* check box to enable WEP encryption on the WAN interface.

WEP (Wired Equivalent Privacy) is a data privacy mechanism based on a 40 bit shared key algorithm. In order to utilize WEP encryption, all points in your wireless network must have WEP enabled and be set to the same encryption key settings.
 5. Select the default key used to access your wireless WAN via WEP encryption from the *Active Key* drop-down box. Make sure that the Active Key setting is the same for each point on your wireless network.
 6. Enter four unique WEP encryption keys for your wireless WAN. Typically, the encryption keys for your network are generated by your wireless network access point, and must then be copied into this form.
 7. To add secondary IP addresses to the WAN interface, click *Addresses*. See “Secondary IP Addresses” on page 95 for more information. This option is only available if you have a static Internet connection.
 8. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Secondary IP Addresses

By adding secondary IP addresses to the WAN interface, multiple machines on the LAN can be accessed on the same IP port using firewall passthrough rules. For example, secondary IP addresses allow an organization to set up multiple Web servers, with several machines on the LAN serving Web pages over IP Port 80.

This option is only available if you are using a static Ethernet connection.

To add a secondary Internet IP address:

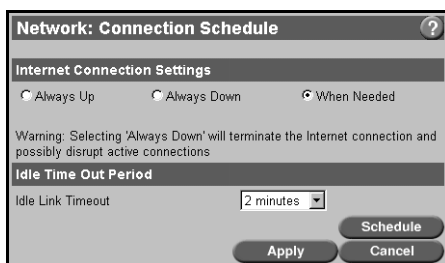
1. Enter the secondary Internet *IP Address* and click *Add*. The IP address specified cannot be an address on the LAN or (if you have the DMZ SoftPak installed) the DMZ network, and it cannot be the same as your gateway/remote IP address.
2. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Configuring the Internet Connection Settings

The Connection Schedule page (not available on InstaGate 404, 604 and 806) allows you to enable or disable InstaGate’s Internet connection. If you are using a dial-up communication device (modem or ISDN), you can also specify how long InstaGate remains connected to the Internet during periods of inactivity.

To specify your Internet connection settings:

1. Select *Connection Schedule* from the *Network* menu.



2. Select one of the following connectivity options:
 - **Always Up** — System is always connected to the Internet.
 - **Always Down** — System is never connected to the Internet.
 - **When Needed** — System connects to the Internet automatically, and disconnects after a specified inactivity period. This option is only available when using a dial-up WAN device (modem or ISDN).
3. If you selected to connect to the Internet automatically and disconnect after a specified inactivity period, select the *Idle Link Timeout* period from the drop-down list.

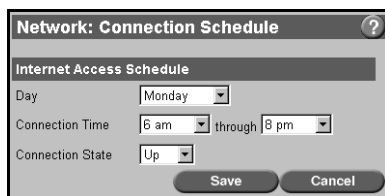
Reducing the timeout period will shut down InstaGate’s Internet connection more quickly after Internet activity has stopped, reducing connect time to the ISP. Increasing the timeout period will keep InstaGate connected to the Internet longer after inactivity, reducing the possibility that the server will have to re-dial the ISP to access the Internet.
4. To specify times that InstaGate should remain connected to the Internet and times that InstaGate should disconnect from the Internet, regardless of traffic on the LAN, click *Schedule* (see “Defining an Internet Connection Schedule” on page 96). This option is only available when using a dial-up WAN device (modem or ISDN).
5. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Defining an Internet Connection Schedule

The Internet connection scheduling option allows you to specify times that InstaGate should remain connected to the Internet and times that InstaGate should disconnect from the Internet, regardless of traffic on the LAN. This option is only available when using a dial-up WAN device (modem or ISDN).

To define your Internet connection schedule:

-
1. Select *Connection Schedule* from the *Network* menu.
 2. Click *Schedule*.
 3. Click *Add*.



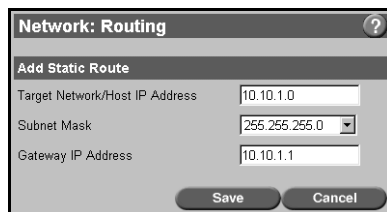
4. Select the *Day* of the week you wish to schedule.
5. Select the *Connection Time* period during the day you wish to schedule.
6. Select the *Connection State* for the selected time period, either *Up* or *Down*.
7. Click *Save* to save the connection rule, or *Cancel* to exit without saving.
8. Repeat steps 3 through 7 until you have finished defining your Internet connection schedule.

Configuring Static Routes

Define static routes to connect your network to other networks through InstaGate.

To set up static routes:

1. Select *Routing* from the *Network* menu.
2. Click *Add*.



The screenshot shows a dialog box titled "Network: Routing" with a question mark icon in the top right corner. Below the title bar is a section labeled "Add Static Route". This section contains three input fields: "Target Network/Host IP Address" with the value "10.10.1.0", "Subnet Mask" with a dropdown menu showing "255.255.255.0", and "Gateway IP Address" with the value "10.10.1.1". At the bottom of the dialog are two buttons: "Save" and "Cancel".

3. Type the IP address of the network or host you would like to add a route to in the *Target Network/Host IP Address* field.
4. Select the *Subnet Mask* for the target network.
5. Type the IP address of the computer resource that will act as the gateway to the target network in the *Gateway IP Address* field.
6. Click *Save* to add the new route, or *Cancel* to exit without saving.

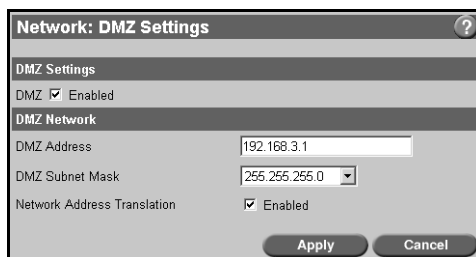
Configuring the DMZ Settings

DMZ adds a third network to InstaGate. The DMZ (De-Militarized Zone) network is used for servers and other systems that must be accessible from the Internet, such as Web or FTP servers. The DMZ sits between the LAN and the Internet (see “Connecting InstaGate to your DMZ Network” on page 100). While servers on the DMZ are publicly accessible, firewall protection can be enabled to protect the DMZ from Internet attacks. The LAN is always automatically protected from the DMZ.

Servers on the DMZ must have manually configured IP addresses, with the DMZ address as the default gateway.

To configure the DMZ settings:

1. Select *DMZ Settings* from the *Network* menu.
2. Click the *DMZ Enabled* check box.



3. Type the IP address of the DMZ interface in the *DMZ Address* text box. The DMZ interface can be on the same subnet as the WAN interface, or on a separate subnet. Configuring the DMZ interface on the same subnet as the WAN interface can be useful if the range of IP addresses assigned by your ISP is too small to divide into subnets.
4. Select the *DMZ Subnet Mask* used on the DMZ network (default **255.255.255.0**). The subnet mask is used in conjunction with the DMZ IP address to define the set of addresses available on the DMZ.
5. Select the *Network Address Translation Enabled* (NAT) check box to activate NAT (and the firewall) on the DMZ network. NAT translates multiple IP addresses on the DMZ to one public address that is sent out to the Internet. This adds a level of security since the address of a system connected to the DMZ is never transmitted on the Internet. Internet access to servers on the DMZ is provided through defined firewall policies. DMZ servers are only protected by the firewall if NAT is enabled.

NAT protects DMZ servers from Internet attacks and only requires a single WAN IP address. The disadvantages of enabling NAT, however, are that only one DMZ server can provide a particular service, and that some services do not work well with NAT. Examples include popular messaging programs such as IRC and ICQ, and games that use Battle.Net or DirectPlay.

With NAT disabled, each DMZ server must have a unique Internet IP address. This eliminates the problems some services have with NAT, and allows multiple servers to provide the same service. However, without NAT, the DMZ servers are not protected by the firewall.

6. Click *Apply* to save your changes, or *Cancel* to exit without saving.

Connecting InstaGate to your DMZ Network

InstaGate is connected to your DMZ network like any other computer. The Ethernet DMZ Port automatically sets itself to the speed of your DMZ network (10 Mbps or 100 Mbps).

To connect InstaGate to your DMZ network:

1. Connect one end of a straight through CAT5 Ethernet cable (either of the two gray Ethernet cables provided) to the Ethernet DMZ Port on the back of InstaGate.

Note If you are using a modem, Euro ISDN, serial, or synchronous serial V.35/X.21 port rather than the Ethernet WAN port to connect to the Internet, and you do not have an Ethernet DMZ port installed, use the Ethernet WAN port as the DMZ interface.

2. Connect the other end of the Ethernet cable to a 10BASE-T or 100BASE-TX hub or switch on your DMZ network. Be sure to connect the Ethernet cable to a regular port on the hub, not an uplink port.





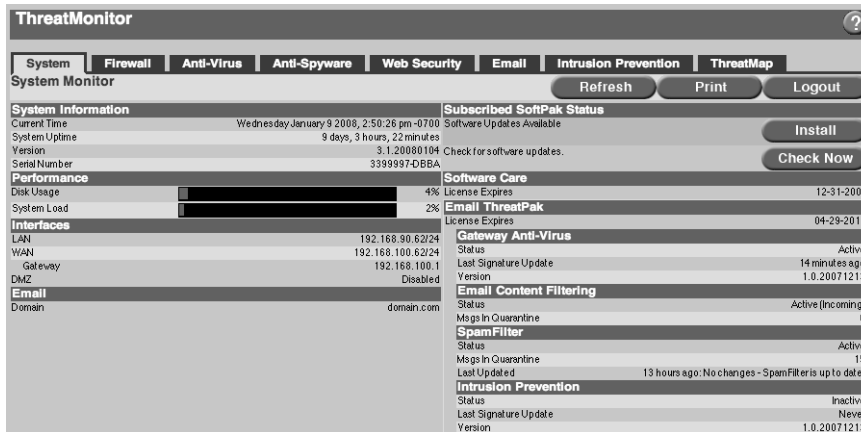
This chapter describes ThreatMonitor and how to configure and generate the various alerts and reports provided by InstaGate. It covers the following topics:

- Configuring the System Alert Settings
- Configuring the Daily Report Settings
- Generating the Internet Connection Report
- Generating the User Quota Report
- Generating the System Security Report
- Generating the PPTP VPN Report

ThreatMonitor

Overview

The ThreatMonitor system provides a status overview of the system by a textual and graphical representation. It consists of system-specific monitors that can be selected via a tabbed interface. The ThreatMonitor tabs represent the Softpaks that are either installed, or not yet subscribed. If the Softpak is not enabled, the monitor will display a form giving the user an option to enable the Softpak. For the un-subscribed Softpaks, the corresponding tab displays a sample report, and graph. By default each monitor will refresh every 5 minutes. The Refresh button is also available to force a refresh immediately. The Print button is available to print the graphs and reports.



System Monitor

The System monitor is the first tab and is always displayed. It is intended to show the most important information of the system, namely the subscribed Softpak status, software updates available for each Softpak, the version of the Softpak, and the license expiration date. It also displays system specific information such as the system up-time, the serial number, the disk usage, the system load, and information regarding the interfaces. The Software Updates section also has the "Check Now" button that checks for software updates. If there are software updates available for download, there is a "Install Now" button displayed instead of "Check Now". If there are no software updates available, the Software Updates section is not displayed. If the expiry date of any of the installed Softpaks is less than 60 days, you will see a yellow background in the section above the Softpak Status.

Firewall Monitor

The Firewall monitor is always present as the second tab. This monitor displays network traffic statistics on the eSoft appliance. It displays graphs and reports for different network traffic such as In-bound/Out-bound traffic, Protocol based profile, and accepted/blocked traffic.

Reports & Graphs

Each monitor consists of zero or more reports, each consisting of a graph and related data for the graph. The report could be detailed or summarized in nature. It can be created for various ranges: 24 hours, 1 week, 2 weeks, and 1 month. The different types of graphs that can be plotted for a particular data set selected are bar graph, line graph, pie graph, and health graph.

ThreatMap



ThreatMap will display the geographic location of each of the threats detected against your network. Depending on the Softpaks that are installed, the ThreatMap may include geographic source of viruses, intrusion attempts, spyware, spam, and more. Enabling ThreatMap will only send the threat data to eSoft's server, it will not send any other information/logs. Enabling ThreatMap, will let you explore the top threats to your network on an interactive world map.

ThreatMap only shows mappable IP addresses, this does not include threats from private IP addresses.

Not all threats retain IP address information such as spyware caught via email traffic. Spyware only shows caught files and not blocked addresses.

Threats are uploaded nightly, this could result in a delay before the threats appear on the map.

You might see a "403 Forbidden message" this could be due to cached requests by the browser. This message should disappear by refreshing the browser.

Configuring the System Alert Settings

System Alerts allow the InstaGate administrator to set system thresholds that when exceeded, send an email alert message to the remote system administrators. System thresholds that can be monitored include mail, connection time, data transfer and authentication attempts.

InstaGate monitors system alert thresholds every 10 minutes. Once an alert threshold is exceeded, a single alert message is sent. After the first alert message is sent, InstaGate generates additional alerts for the event once every four hours until the threshold value no longer exceeds the configured value for the event.

To activate system alerts:

1. Select *System Alert Settings* from the *Alerts & Reports* menu.



The screenshot shows a dialog box titled "Alerts & Reports: System Alert Settings". It has a help icon in the top right corner. The dialog is divided into several sections:

- Alert Recipients:** Alerts will be mailed to: jstephens@isp.com
- Connection Alerts:**
 - Daily connect time over: 1 hour
 - Weekly connect time over: 1 day
 - Monthly connect time over: 1 week
 - Stop connection on alert
- Data Transfer Alerts:**
 - Daily transfer over: 10 MB
 - Weekly transfer over: 30 MB
 - Monthly transfer over: 120 MB
 - Stop connection on alert
- Authentication Alerts:**
 - Failed FTP logins
 - Failed Windows Networking logins

At the bottom right, there are "Apply" and "Cancel" buttons.

2. Click the check boxes next to the alerts you wish to enable, and then select the threshold values for the alerts.

Note The *Stop connection on alert* setting automatically shuts down InstaGate's connection to your ISP whenever a specified alert threshold is exceeded. To connect to the ISP again once an alert has stopped the connection, you must clear this check box and then restart InstaGate.

3. Click *Apply* to activate the alerts, or *Cancel* to exit without activating.

Configuring the Daily Report Settings

The Daily Report Settings page allows the administrator to configure a set of reports to be mailed each day. Reports are generated and sent to the remote system administrators at midnight.

Note Reports are mailed in HTML format. If your mail program cannot properly format HTML messages, save the contents of the message (including all HTML tags) to a file and then open the file from your Web browser.

To set up report mailing:

1. Select *Daily Report Settings* from the *Alerts & Reports* menu.



The screenshot shows a dialog box titled "Alerts & Reports: Daily Report Settings". It has a "Report Settings" section with a "Report Name" field containing "Daily log summary from Instagate EX" and a "Report Recipients" field containing "jstephens@isp.com". Below this is a "Reports to Include" section with five checkboxes: "Internet Connection" (checked), "System Security" (unchecked), "Internet Access" (unchecked), "User Quotas" (checked), and "VPN" (unchecked). At the bottom are "Apply" and "Cancel" buttons.

2. Specify a *Report Name* to be printed in the subject field of the report message. The report name is useful if you receive reports from more than one InstaGate appliance.
3. Select which *Reports to Include* each day.
4. Click *Apply* to save your settings, or *Cancel* to exit without saving.

Generating the Internet Connection Report

The Internet Connection Report allows you to view statistics concerning InstaGate's connectivity for the current day. Statistics available include hours of connect time, megabytes transmitted, and megabytes received.

To run the Internet Connection Report:

1. Select *Internet Connection* from the *Alerts & Reports* menu. The report is automatically generated.
2. Click *Done* when you have finished viewing the report.

Generating the User Quota Report

The User Quota Report shows the amount of disk space currently in use, as well as the specified disk usage quota for each InstaGate user.

To run the User Quota Report:

1. Select *User Quota* from the *Alerts & Reports* menu. The report is automatically generated.
2. Click *Done* when you have finished viewing the report.

Generating the System Security Report

The System Security Report contains a log of failed login attempts discarded data packets.

Discarded packet entries can appear in your Security Report for a number of reasons. Discarded packets from the LAN interface are generally caused by configuration errors on the LAN. However, they can also be a sign of a computer on your LAN trying to attack another computer on the Internet.

Discarded packets from the Internet interface have many different causes. Among the most common benign reasons for discarded packets are configuration or routing errors from your ISP's equipment and typing errors from legitimate users. Malicious discarded packet logs include packets that are dropped because they have an invalid packet length, packets that have source routing enabled, and series of discarded packet entries with ascending destination application port numbers.

To run the System Security Report:

1. Select *System Security* from the *Alerts & Reports* menu.

-
2. Select the number of days to include in the report from the drop-down list. InstaGate keeps logs of failed logins and discarded packets for up to one week.
 3. To include failed login attempts in the report, select the *Failed Logins* check box.
 4. To include a list of discarded packet entries in the report, select the *Illegal Traffic* check box.
 5. Click *Run Report* to generate the report.

Generating the PPTP VPN Report

The PPTP VPN Report displays usage information for the PPTP VPN server. Statistics available include the amount of connect time per user, the number of megabytes transmitted, and the number of megabytes received.

To run the PPTP VPN Report:

1. Select *PPTP VPN* from the *Alerts & Reports* menu.
2. Select the number of days to include in the report from the drop-down list. InstaGate keeps logs of VPN usage for up to one week.
3. Click *Run Report* to generate the report.

This chapter provides information to help you diagnose and troubleshoot problems you encounter in setting up or using InstaGate. It covers the following topics:

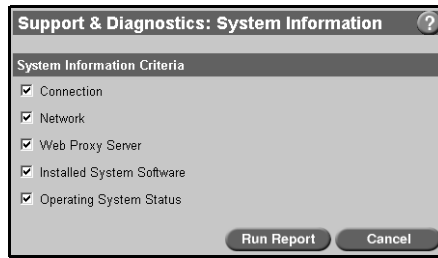
- Viewing System Information
- Running System Diagnostics
- Running Connection Diagnostics
- Viewing the Connection Log
- Registering InstaGate
- Enabling Remote Support
- Viewing the System Logs
- Contacting eSoft
- Troubleshooting

Viewing System Information

The System Information page provides essential data for monitoring system usage, performance, and configuration. The report collects your system configuration information and provides a menu for displaying the associated system topics. Support technicians require specific information about your system when they are troubleshooting your configuration. You can use the System Information page to quickly find the data they need to resolve your problem.

To display the System Information page:

1. Select *System Information* from the *Support & Diagnostics* menu.



2. Specify the system topics you wish to view by selecting the appropriate check boxes.
3. Click *Run Report* to display the system information, or *Cancel* to exit without viewing. It may take several minutes to complete the system information report.

Running System Diagnostics

System Diagnostics monitor the processes running on InstaGate, the condition of InstaGate's disk drive, and the network packet transmit and packet receive statistics. If a problem is detected, System Diagnostics will detail the problem and recommend that you restart InstaGate.

To run the System Diagnostics:

1. Select *System Diagnostics* from the *Support & Diagnostics* menu.
2. Click *Done* when you have finished viewing the diagnostics.

Running Connection Diagnostics

Connection Diagnostics test InstaGate's connection to your ISP. Use Connection Diagnostics to test new WAN configuration settings, and whenever you suspect problems with your Internet connection. When used with the Internet Connection Log, Connection Diagnostics is a powerful tool for determining problems with your Internet connection.

To run Connection Diagnostics:

1. Select *Connection Diagnostics* from the *Support & Diagnostics* menu.
2. Click *Done* when you have finished viewing the diagnostics.
3. If there is a problem with any of your WAN configuration settings, the diagnostics will display a *View Logs* button to help you diagnose the problem. Otherwise, a success message is displayed.

Viewing the Connection Log (InstaGate EX2, XSP and PRO)

The Internet Connection Log allows you to view a detailed summary of each Internet connection attempt InstaGate has made to your ISP for the current day. The Internet Connection Log, in conjunction with Connection Diagnostics, can help you diagnose problems with InstaGate connecting to your ISP.

The Connection Log is only available if InstaGate is configured for a dial-up communication device (modem or ISDN).

To view the Connection Log:

1. Select *Connection Log* from the *Support & Diagnostics* menu.
2. Click *Done* when you have finished viewing the Connection Log.

Registering InstaGate

The Registration page is used to enter and view InstaGate registration information. Registering is quick, easy and will keep you informed of the latest updates.

To register your InstaGate:

1. Select *Registration* from the *Support & Diagnostics* menu.
2. Enter your registration information and click *Send* to automatically register online.

Enabling Remote Support

Enabling remote support opens InstaGate's firewall and enables login access to the administrative interface. This allows technical support to access InstaGate for remote diagnostics and configuration. You will need to provide your administrative password. You should only enable remote support while on the phone with an authorized technical support engineer. Furthermore, to ensure that you are speaking with an authorized technical support engineer, it is very important that you initiate the telephone call. Never enable remote support or give out your administrative password to an individual that contacts you directly claiming to be an authorized technical support engineer or a member of any other organization. Failure to follow these instructions may seriously compromise the security of InstaGate and your network.

To enable remote support:

1. Select *Remote Support* from the *Support & Diagnostics* menu.
2. Click *Enable* to enable remote support. Remember to return to this page and click *Disable* once you have finished your technical support call.

Viewing the System Logs

InstaGate provides detailed technical logs of all InstaGate activity. Logs are available for system, firewall, email, ftp, Web server, file sharing, and Web access activities. If you are familiar with networking and TCP/IP, these logs can help you to optimize the use of your InstaGate and troubleshoot problems.

To view or download the system logs:

1. Select *System Logs* from the *Support & Diagnostics* menu.
2. Select the *Log Area* you wish to view from the drop-down list.
3. To view a log in your Web browser, click the name of the log you wish to view. To download a log, select the radio button next to the log you wish to download, and click *Download*.

Sample System Log Entries

InstaGate's System Logs provide information detailing all system activity. Sample entries from a few of the logs available are listed below. Key information in the selected log entries is displayed in **bold**.

Firewall — firewall.log

The following log entry describes a connection that has been denied by the firewall:

```
2003 Jun 5 11:31:20 InstaGate-xSP PF Global DROP: IN=eth0 OUT=
MAC=ff:ff:ff:ff:ff:00:10:a4:9a:07:ed:08:00 SRC=192.168.1.10 DST=192.168.1.255 LEN=96
TOS=0x00 PREC=0x00 TTL=128 ID=60802 PROTO=UDP SPT=137 DPT=137 LEN=76
```

The following log entry describes a connection that has been accepted by the firewall:

```
2003 Jun 5 15:32:37 InstaGate-xSP tcplog[c0f3d200]: Connection opened, 192.168.1.10:3903 ->
192.168.100.2:23
```

The following log entry describes an accepted connection that has been terminated by the user:

```
2003 Jun 5 15:32:49 InstaGate-xSP tcplog[c0f3d200]: Connection closed, sent 94, received 981
```

Administrator Web — secureaccess.log

The following log entry describes an attempt to access the administrative interface without a username or password:

```
192.168.1.10 - - [05/Jun/2003:15:36:32 -0600] "GET / HTTP/1.1" 401 409
```

The following log entry describes a successful attempt to access the administrative interface:

```
192.168.1.10 - admin [05/Jun/2003:15:37:07 -0600] "GET / HTTP/1.1" 200 1390
```

Administrator Web — secureerror.log

The following log entry describes a failed attempt to access the administrative interface due to an incorrect password:

```
[Thu Jun 5 15:36:37 2003] [error] [client 192.168.1.10] user admin: authentication failure for "/": password mismatch
```

The following log entry describes a failed attempt to access the administrative interface due to an incorrect username:

```
[Thu Jun 5 15:36:51 2003] [error] [client 192.168.1.10] user notanadmin not found: /
```

Web Access Control — access.log

The following log entry describes a user's attempt to access a specified Web site that has been denied:

```
192.168.1.10 - - [05/Jun/2003:15:39:16 -0600] "GET http://www.esoft.com/ HTTP/1.1" 0 235  
TCP_MISS:NONE
```

The following log entry describes a user's attempt to access a specified Web site that has been allowed:

```
192.168.1.10 - - [05/Jun/2003:15:38:45 -0600] "GET http://www.esoft.com/ HTTP/1.1" 200 22084  
TCP_MISS:DIRECT
```

Contacting eSoft

If you are having difficulty troubleshooting problems in the installation and use of InstaGate, contact technical support for assistance. Please have your InstaGate's serial number and software version available when you contact technical support.

You can find the serial number and software version of your InstaGate appliance as well as contact information for eSoft in the Contact Us page.

To access the Contact Us page:

1. Select *Contact Us* from the *Support & Diagnostics* menu.
2. The contact information is automatically displayed on the screen. Click *Done* to exit.

Troubleshooting

InstaGate has excellent troubleshooting capabilities to help you connect the computers on your LAN to the Internet.

Solving Client Configuration Problems

When I restart my computer it says a DHCP server could not be found. InstaGate is not receiving your computer's request for TCP/IP configuration. Check that:

- InstaGate is attached to your network.
- InstaGate and your computer are on the same LAN segment. InstaGate can only receive DHCP request messages from computers that are on the same LAN segment.
- InstaGate's DHCP server is enabled. See "Configuring the LAN Settings" on page 79. Run System Diagnostics to make sure DHCP is running and that there are no other problems with InstaGate.

When I try to access the Internet, I get a message from InstaGate that says my browser is not properly configured. InstaGate's Web Access Control is configured to require username and password authentication, but your Web browser is not configured to access InstaGate as a proxy server. See "Configuring your Browser to Use InstaGate's Proxy Server" on page 29.

Some/One of my computers cannot access the Internet, all of the other computers can. See if the problem computer can access InstaGate's administrative interface. If the problem computer cannot access the interface, then there is a problem with the computer's TCP/IP configuration or Web browser configuration.

If the problem computer can access the administrative interface, then the client computer's default gateway is not properly configured. If you are using DHCP to configure this computer, try running the `winiipcfg` program from the DOS Prompt and clicking *Release All* and then *Renew All* to force the computer to get new DHCP configuration information. If you still have problems reaching the Internet with this computer, you may need to enter the default gateway parameter manually. Consult the computer's TCP/IP networking documentation for details.

Whenever/sometimes I try to access the Internet from any/some/one of my computers, I get the message "the name server lookup for 'xyz.com' failed". Since InstaGate is configured to use your ISP's DNS servers, this error means that your computer did not receive a response from your ISP's servers.

- If this happens all the time from all of your computers, then the IP address you entered for your ISP's Primary DNS server is not correct. See "Configuring the WAN Settings" on page 81.

-
- If you suddenly get this message from all of your computers when they had worked previously, your ISP's DNS server is down or the DNS server for xyz.com is down.
 - If you always get this message from some/one of your computers, then the problem computer's DHCP configuration is not up to date. Try rebooting the problem computer. This will force the computer to get new DHCP configuration information.

Solving Administrative Interface Problems

When I try to access the administrative interface from my Web browser, I get a message from InstaGate that says my Web browser is not configured correctly. Your browser is configured to access InstaGate as a proxy server, but it does not exclude the server from proxy access. When using the administrative interface, your browser must communicate directly with InstaGate's Web server; not through InstaGate's proxy server. See "Configuring your Browser to Use InstaGate's Proxy Server" on page 29.

When I try to access the administrative interface from my Web browser I get the message "unknown host name". Make sure you entered the URL for the administrative interface correctly. If you are trying to access the administrative interface from a computer that does not use InstaGate as its DHCP server, then the computer's DNS configuration is probably wrong.

When I try to access the administrative interface from my Web browser I get the message "no route to host". Your computer's network configuration is not compatible with InstaGate's network configuration. Check the IP address and subnet mask of your computer with InstaGate's IP address and subnet mask. See "Configuring the LAN Settings" on page 79 for more information.

When I try to access the administrative interface from my Web browser I get the message "could not access InstaGate". Your computer did not receive a response from InstaGate's administrative interface. Make sure InstaGate is powered-on and connected to your network properly. Try pinging InstaGate with the computer's native ping program. For a Windows computer, from a DOS prompt, type `ping Instagate`.

If the ping fails, your computer and InstaGate cannot communicate over the network. Try pinging InstaGate and your computer from another computer on your network.

If the ping succeeds from another computer to InstaGate, then there is a problem with the network or network configuration of the problem computer. If the ping fails from the other computer to InstaGate, then InstaGate is not accessible on the LAN. Make sure the computers you ping from have proper TCP/IP configurations and that InstaGate is powered on and connected to the LAN.

Solving Internet Connection Problems

The Connection Diagnostics failed right after I ran InstaGate’s Setup Wizard for the first time. You may have made a mistake or input the wrong information in the Connectivity page, or there is a problem with your phone line or your ISP’s computer equipment. Click *View Logs* on the Connection Diagnostics page and look at the most recent connection attempt. The Connection Log will give you information about what happened.

Sometimes I have trouble accessing the Internet, other times it works just fine. You may be having intermittent problems connecting to the ISP. Check the Internet Connection Report (see “Generating the Internet Connection Report” on page 111). If your successful connection percentage is below 95% you may want to investigate what is causing the problems and discuss this with your phone company or ISP. To determine what is causing your connection problems, view the Connection Log (see “Viewing the Connection Log (InstaGate EX2, XSP and PRO)” on page 115).

This chapter describes InstaGate's User Administration interface. It covers the following topics:

- Accessing the User Administration Interface
- Changing your Account Password

Accessing the User Administration Interface

Only users with a valid InstaGate account have access to the User Administration interface.

To access the User Administration interface:

1. Enter one of the following URLs in the location field of your Internet browser:

`https://<IPAddress-of-Instagate>:8001/UserAdmin/`

`https://<Host_Name>:8001/UserAdmin/`

2. Enter your InstaGate *User Name* (account name) and *Password*.
3. Click *OK*.

Changing your Account Password

To change your InstaGate account password:

1. Select *Password* from the main menu.



John Smith
Set Password

Change Password:

Full Name

Account Name

Password

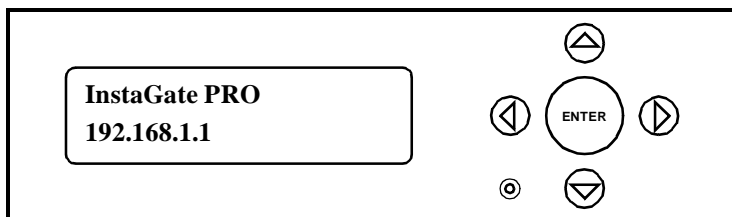
Verify Password

Note: After you change your password, you will need to re-enter the new password into your browser before proceeding.

2. Modify your *Full Name* and *Password* as necessary.
3. Click *Apply* to save your changes, or *Cancel* to exit without saving.

Note After changing your password, a prompt appears requiring you to log in using the password you just specified.

InstaGate features an LCD screen and keypad on the front panel. During startup, the LCD screen displays the status of the boot process. When the boot process is complete, the message *InstaGate PRO* or *InstaGate xSP* appears, along with the InstaGate's default IP address.



Once InstaGate is running, the LCD keypad allows you to perform a variety of tasks, including:

- changing the network configuration settings
- configuring the DHCP server
- enabling remote support
- shutting down the system
- rebooting the system
- resetting the administrative password
- restoring factory default settings

To access the LCD menu, press the *ENTER* button on the LCD keypad. If you have specified a PIN for the LCD interface (see “Specifying the Administrator Settings” on page 52) enter the four digit PIN using the arrow buttons, and press *ENTER*.

Use the up and down arrow buttons to navigate through the menu. To exit the LCD menu, press the down arrow button until the message *EXIT* appears, then press *ENTER*.

Changing the Network Configuration Settings

To reconfigure InstaGate's LAN interface:

1. Press the *ENTER* button on the LCD keypad. The LCD screen displays the message *SETUP NETWORK*.
2. Press *ENTER*.
3. Enter InstaGate's LAN Ethernet *IP ADDRESS* using the arrow buttons. The left and right arrow buttons move the cursor to the left or right. The up and down arrow buttons increase or decrease the value at the current cursor position.
4. Press *ENTER*.
5. Enter the *NETMASK* of the LAN Ethernet interface using the arrow buttons.
6. Press *ENTER*. The message *SAVE CHANGES?* appears.
7. Press *ENTER* to save the network configuration settings, or the up arrow button to cancel the configuration and return to the LCD menu.

Configuring the DHCP Server

By enabling InstaGate's DHCP server, each client computer's IP address, default gateway (router), and DNS settings can be configured automatically. All of these TCP/IP parameters are necessary for optimal use of InstaGate's resources. If you choose to use an existing DHCP server (such as Windows NT) rather than InstaGate's DHCP server, you will need to configure the existing DHCP server to properly set up each client computer's TCP/IP configuration (or configure each client manually).

To configure InstaGate's DHCP server:

1. Press the *ENTER* button on the LCD keypad. The LCD screen displays the message *SETUP NETWORK*.
2. Press the down arrow button. The message *SETUP DHCP SERVER* appears.
3. Press *ENTER*. The LCD screen displays the current status of the DHCP server, either *DHCP SERVER: DISABLED* or *DHCP SERVER: ENABLED*.
4. Use the arrow buttons to change the DHCP server's status and press *ENTER*.
5. If you selected to disable the DHCP server, the message *SAVE CHANGES?* appears. Press *ENTER* to disable the DHCP Server.

-
6. If you selected to enable the DHCP server, the message *FIRST ADDR* appears. Use the arrow buttons to specify the first address in the range of addresses to be assigned to DHCP clients. The default is **192.168.1.10**.
 7. Press *ENTER*. The message *LAST ADDR* appears. Use the arrow buttons to specify the last address in the range of addresses to be assigned to DHCP clients. The default is **192.168.1.250**.
 8. Press *ENTER*. The message *SAVE CHANGES?* appears.
 9. Press *ENTER* to save the DHCP configuration settings, or the up arrow button to cancel the configuration and return to the LCD menu.

DHCP Error Codes

If InstaGate detects any errors in your DHCP settings, an error message is displayed on the LCD screen, along with a number to help identify the error. The following table lists each DHCP error and its corresponding code number:

Code	Error
1	Invalid Last Address
2	Invalid First Address
3	First Address not on the LAN
4	Last Address not on the LAN
5	Range includes InstaGate's IP Address
6	Last Address is before the First Address
7	Range includes too many hosts

Enabling Remote Support

Enabling remote support allows login access to the administrative interface. This enables technical support to access InstaGate for remote diagnostics and configuration. You should only enable remote support while on the phone with an authorized technical support engineer. Furthermore, to ensure that you are speaking with an authorized technical support engineer, it is very important that you initiate the telephone call. Failure to follow these instructions may seriously compromise the security of InstaGate and your network.

To enable remote support:

1. Press the *ENTER* button on the LCD keypad. The LCD screen displays the message *SETUP NETWORK*.
2. Press the down arrow button twice. The message *ENABLE REMOTE SUPPORT* appears.
3. Press *ENTER*. The message *ENABLE SUPPORT MODE?* appears.
4. Press *ENTER* to enable remote support, or the up arrow button to return to the LCD menu without enabling remote support.

Shutting Down the System

Before turning off InstaGate's power it is important that you shut down the system properly.

To safely shut down InstaGate:

1. Press the *ENTER* button on the LCD keypad. The LCD screen displays the message *SETUP NETWORK*.
2. Press the down arrow button until the message *SYSTEM SHUTDOWN* appears.
3. Press *ENTER*. The message *SHUTDOWN SYSTEM?* appears.
4. Press *ENTER* to shut down the system, or the up arrow button to return to the LCD menu without shutting down.

Note After the system has successfully shut down, the light in the LCD display turns off. You can then shut off the appliance's power by disconnecting the power source.

Rebooting the System

To reboot InstaGate:

1. Press the *ENTER* button on the LCD keypad. The LCD screen displays the message *SETUP NETWORK*.
2. Press the down arrow button until the message *SYSTEM REBOOT* appears.
3. Press *ENTER*. The message *REBOOT SYSTEM?* appears.
4. Press *ENTER* to reboot the system, or the up arrow button to return to the LCD menu without rebooting.

Resetting the Administrative Password

Resetting the system administrative password resets the current administrative password to the default password **admin**. The administrative password is required to access InstaGate's administrative interface.

To reset the administrative password:

1. Press the *ENTER* button on the LCD keypad. The LCD screen displays the message *SETUP NETWORK*.
2. Press the down arrow button until the message *RESET SYSTEM ADMIN PASSWORD* appears.
3. Press *ENTER*. The message *RESET SYSTEM ADMIN PASSWORD?* appears.
4. Press *ENTER* to reset the password to **admin**, or the up arrow button to return to the LCD menu without resetting the password.

Restoring Factory Default Settings

Restoring defaults initializes a system to its shipped condition, automatically clearing all user accounts, connection settings, and server settings. All installed InstaGate SoftPaks are also removed.

To restore an InstaGate system to the factory default settings:

1. Press and hold both the left and right arrow buttons on the LCD keypad for 10 seconds. The LCD screen displays the message *RESTORE DEFAULTS?*.
2. Press *ENTER* to restore the factory default settings, or the up arrow button to return to the LCD status screen (*InstaGate PRO* or *InstaGate xSP*) without restoring.



Appendix B

SoftPak Director

SoftPak and ThreatPak applications are security and IT software modules that add functionality to your InstaGate appliance. SoftPaks and ThreatPaks are delivered via SoftPak Director. SoftPak Director allows you to perform the following functions:

- Subscribing to SoftPaks and ThreatPaks
- Viewing Enabled SoftPaks and ThreatPaks

Subscribing to SoftPaks and ThreatPaks

To subscribe to a SoftPak or ThreatPak:

1. Select *Catalog* from the *SoftPak Director* menu. A list of available SoftPaks and ThreatPaks are displayed along with a brief description and pricing information for each application.
2. Select the SoftPak or ThreatPak you wish to subscribe to, and click *Subscribe* (for certain SoftPaks you must also specify the number of user licenses you wish to purchase). A confirmation page appears listing the fees associated with the selected SoftPak or ThreatPak.

Note To view additional information about the selected SoftPak or ThreatPak, click *Details*. See “Viewing SoftPak or ThreatPak Details” on page 130 for more information.

3. Click *Yes*. The Billing Information page appears.
4. Enter your billing information, and click *Next*. A confirmation page appears listing the details of your order.
5. Click *Purchase* to subscribe to the SoftPak. If your order is processed successfully a receipt is displayed. Please print the receipt and keep it for your records.
6. Click *Download Now* to immediately download the SoftPak.

-
7. A status bar displays the progress of the download. When the download is complete, the Apply Updates page appears listing the system administrators who will be notified when the installation is complete. Click *Install* to install the SoftPak.

If you do not wish to install the software at this time, click *Cancel* to exit the SoftPak Director. The next time you access the administrative interface a message will appear instructing you to install the software. To install the software, click the *Install Now* button.

Note When you subscribe to a SoftPak or ThreatPak, a PDF file describing the configuration and use of the SoftPak is downloaded to InstaGate's file server and placed in the following directory:

```
\\<HostName>\Admin\SoftPaks\<SoftPakName>.
```

For example, \\InstaGate\Admin\SoftPaks\SpamFilter\SpamFilter SoftPak.pdf.

Viewing SoftPak or ThreatPak Details

The Details page provides a brief product description and pricing information for the selected SoftPak or ThreatPak. To exit the Details page, click *Done*.

If you have already subscribed, the Details page may provide a *Renew* button so that you can quickly renew your SoftPak subscription.

If you have not subscribed, a *Subscribe* button is provided.

Note You can also download a PDF version of the selected SoftPak's User Guide from this page. The User Guide provides detailed information about all of the SoftPak's features and services.

Viewing Enabled SoftPaks or ThreatPaks

The SoftPak Director Enabled page lists the SoftPaks to which you are currently subscribed. You can also check for software updates, renew SoftPak subscriptions and upgrade user license levels on this page.

To view enabled SoftPaks and ThreatPak:

1. Select *Enabled* from the *SoftPak Director* menu. A list of SoftPaks and ThreatPaks you are currently subscribed to appears, along with the expiration date for each (if applicable).
2. InstaGate automatically contacts the SoftPak Director every week to see if new software is available. To force an immediate check for updates, click *Check Now*.
3. Some SoftPaks require you to purchase subscriptions based on the number of users you wish to support. You can quickly upgrade the user license for a SoftPak, however, by selecting the SoftPak, specifying the number of users you wish to support, and clicking *Upgrade*. A confirmation page appears listing the fees associated with the selected upgrade. Click *Yes* to upgrade the user license.
4. To view additional information about an enabled SoftPak, click *Details*. See “Viewing SoftPak or ThreatPak Details” on page 130 for more information.
5. To renew your subscription to a SoftPak, select the SoftPak and click *Renew*. A confirmation page appears listing the fees associated with the selected SoftPak. Click *Yes* to renew your subscription.

Hardware

- 1U height - 9.25 x 11.5 x 1.7" / 23 x 29 x 4.3 cm
- 5 lbs / 2.3 kg
- 100-240V AC, 47-63Hz, 60W supply
- 566 MHz to 850 MHz Intel® processor
- 64 MB to 256 MB RAM
- 20 GB to 40 GB HDD
- LCD and keypad
- 3 10/100 ethernet ports (LAN, WAN, DMZ)
- 56K v.90 Modem (optional)
- Euro ISDN adapter (optional)
- DB-37 synchronous serial port (optional)
- 2 DB-9 RS-232 serial ports
- DB-25 parallel port

Operating System

- Red Hat 6.2
- Linux 2.4 kernel

Safety and Reliability

- Operating Environment: -10C to +45C, 5-95% R.H. non-condensing
- Storage Environment: -40C to +70C, 0-95% R.H. non-condensing
- MTBF: >50,000 POH
- MTTR: <30 Minutes
- Uptime: >99.999%
- Agency Marks: FCC Part 15 Class A, UL (U.S. & Canada),
- VCCI Class A, CE, TUV-GS
- Units manufactured in an ISO-9002 approved facility

Serial Console (404, 604, 806 only)

The serial console interface provides basic system information. To use this functionality you must connect the InstaGate and the management station with a null-modem serial cable. The 404 uses a standard DB9-DB9 Null Modem cable and the 604 and 806 uses a DB9-RJ45 null modem cable. Both cables are available from eSoft. You also have to run Hyper Terminal or another VT100 terminal emulator on the management system.

The following starts are the guideline for connecting the InstaGate and the management station:

1. Connect the serial cable from the management station to the console port on the InstaGate
2. Start Hyper Terminal or the terminal emulator on the management station.
3. To create a new connection in Hyper Terminal, type the name and select an icon, and then select OK.
4. Select the serial port to which the serial cable is connected to the management station (usually COM1 or COM2) and select OK.
5. The COM1 (or COM2) Properties dialog box appears
6. Configure the port settings as follows and then select OK
 - a. 115200 bps
 - b. 8 bit
 - c. no parity
 - d. 1 stop bit
 - e. no flow control
7. Press the ENTER key to start terminal



Appendix E

Warranty and License Agreement

Standard Warranty

Hardware Warranty

eSoft warrants that, for the period of one year from purchase date, the product will be free from defects in material and workmanship, and that the system will extensively comply with the published specifications of the purchased product.

The following service and support is provided by eSoft to each registered user of eSoft InstaGate products. Use of the term InstaGate refers to and includes all versions of the InstaGate product such as the InstaGate 404, InstaGate 604, InstaGate 806 and any other subsequent InstaGate products.

- One-year hardware repair/replacement
- 90 days free telephone technical support (877-754-2986) or (303-469-3846)
- Unlimited access to the on-line knowledge base (<http://support.esoft.com>)
- Expedited product replacement during first 30 days of ownership if required

You must complete and submit the on-line registration form included in the InstaGate software to register and activate your initial warranty/support coverage.

eSoft makes no warranty or representation that its products will work in combination with any hardware or application software products provided by third parties, that the operation of the products will be uninterrupted or error free, or that all defects in the products will be corrected. For any third party products listed in the InstaGate product documentation or specifications as being compatible, eSoft will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a “bug” or defect in the third party’s product.

Warranty Claims

eSoft shall incur no liability under this warranty if the Customer fails to provide eSoft with notice of the alleged defect during the applicable Warranty Period.

eSoft shall incur no liability under this warranty if eSoft's tests disclose that the alleged defect does not exist or is due to causes not within eSoft's reasonable control, including misuse, neglect, improper installation or testing, unauthorized attempts to repair or modify, or any other cause beyond the range of intended use, by accident, fire, lightning, or other hazard. If a returned product is determined not to be defective or to have a defect due to causes not within eSoft's reasonable control, eSoft's then current processing charge will apply.

Standard Warranty Service

If a product does not operate as warranted above during the applicable Warranty Period, eSoft shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of eSoft. Replacement products may be new or reconditioned.

Standard warranty service for hardware products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to eSoft during the applicable Warranty Period. Products returned to eSoft must be pre-authorized by eSoft with a Return Merchandise Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment.

During the first 30 days of the Warranty Period, eSoft will ship a replacement for defective product hardware covered under warranty. The Customer shall provide a valid credit card number as security deposit for cross-shipment of replacement unit(s). The Customer must return the defective product to eSoft within fourteen (14) days (30 days for international customers) after the request for replacement. If the defective product is not returned to eSoft within this time period, eSoft will bill the Customer for the product at list price. eSoft will repair or replace defective product hardware within the 1-year warranty period, and return the repaired or replaced product to the Customer via surface freight. Expedited freight is at Customer's expense.

Any hardware repaired or replaced within the Warranty Period shall be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer.

Out-of-Warranty Service

eSoft will either repair or, at its option, replace defective Product not covered under warranty. Repair or replacement charges are available from eSoft upon request. The warranty on a serviced product is thirty (30) days from date of shipment of the serviced unit.

eSoft's Liability

eSoft's liability, and Customer's sole and exclusive remedy, shall be limited to the express remedies set forth in this InstaGate Product Warranty.

Disclaimer of Warranties

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ESOFTE MAKES NO OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, REGARDING PRODUCTS. ALL OTHER WARRANTIES AS TO THE QUALITY, CONDITION, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT ARE EXPRESSLY DISCLAIMED.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ESOFTE SHALL NOT BE RESPONSIBLE FOR DIRECT DAMAGES IN EXCESS OF THE PURCHASE PRICE PAID BY THE END USER OR FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGE, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR DAMAGES TO BUSINESS OR BUSINESS RELATIONS, WHETHER OR NOT ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING LIMITATIONS SHALL APPLY NOTWITHSTANDING THE FAILURE OF ANY EXCLUSIVE REMEDIES.

EC Countries Standard Warranty

The EC Standard Warranty applies to the following countries:

- Belgium
- Germany
- Spain
- France
- Ireland
- Italy
- Luxembourg
- The Netherlands
- Denmark
- Austria
- Portugal

-
- Finland
 - Sweden
 - United Kingdom
 - Greece

Hardware Warranty

eSoft warrants that, for the period of two years from purchase date, the product will be free from defects in material and workmanship, and that the system will extensively comply with the published specifications of the purchased product.

The following service and support is provided by eSoft to each registered user of eSoft InstaGate products. Use of the term InstaGate refers to and includes all versions of the InstaGate product such as the InstaGate EX, InstaGate EX2, InstaGate PRO, and any other subsequent InstaGate products.

- Two-year hardware repair/replacement
- 90 days free telephone technical support (877-754-2986) or (303-469-3846)
- Unlimited access to the on-line knowledge base (<http://support.esoft.com>)
- Expedited product replacement during first 30 days of ownership if required

You must complete and submit the on-line registration form included in the InstaGate software to register and activate your initial warranty/support coverage.

eSoft makes no warranty or representation that its products will work in combination with any hardware or application software products provided by third parties, that the operation of the products will be uninterrupted or error free, or that all defects in the products will be corrected. For any third party products listed in the InstaGate product documentation or specifications as being compatible, eSoft will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a “bug” or defect in the third party’s product.

Warranty Claims

eSoft shall incur no liability under this warranty if the Customer fails to provide eSoft with notice of the alleged defect during the applicable Warranty Period.

eSoft shall incur no liability under this warranty if eSoft's tests disclose that the alleged defect does not exist or is due to causes not within eSoft's reasonable control, including misuse, neglect, improper installation or testing, unauthorized attempts to repair or modify, or any other cause beyond the range of intended use, by accident, fire, lightning, or other hazard. If a returned product is determined not to be defective or to have a defect due to causes not within eSoft's reasonable control, eSoft's then current processing charge will apply.

Standard Warranty Service

If a product does not operate as warranted above during the applicable Warranty Period, eSoft shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of eSoft. Replacement products may be new or reconditioned.

Standard warranty service for hardware products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to eSoft during the applicable Warranty Period. Products returned to eSoft must be pre-authorized by eSoft with a Return Merchandise Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment.

During the first 30 days of the Warranty Period, eSoft will ship a replacement for defective product hardware covered under warranty. The Customer shall provide a valid credit card number as security deposit for cross-shipment of replacement unit(s). The Customer must return the defective product to eSoft within thirty (30) days after the request for replacement. If the defective product is not returned to eSoft within this time period, eSoft will bill the Customer for the product at list price. eSoft will repair or replace defective product hardware within the 2-year warranty period, and return the repaired or replaced product to the Customer via surface freight. Expedited freight is at Customer's expense.

Any hardware repaired or replaced within the Warranty Period shall be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer.

Out-of-Warranty Service

eSoft will either repair or, at its option, replace defective Product not covered under warranty. Repair or replacement charges are available from eSoft upon request. The warranty on a serviced product is thirty (30) days from date of shipment of the serviced unit.

eSoft's Liability

eSoft's liability, and Customer's sole and exclusive remedy, shall be limited to the express remedies set forth in this InstaGate Product Warranty.

Disclaimer of Warranties

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ESOFTE MAKES NO OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, REGARDING PRODUCTS. ALL OTHER WARRANTIES AS TO THE QUALITY, CONDITION, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT ARE EXPRESSLY DISCLAIMED.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ESOFTE SHALL NOT BE RESPONSIBLE FOR DIRECT DAMAGES IN EXCESS OF THE PURCHASE PRICE PAID BY THE END USER OR FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGE, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR DAMAGES TO BUSINESS OR BUSINESS RELATIONS, WHETHER OR NOT ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING LIMITATIONS SHALL APPLY NOTWITHSTANDING THE FAILURE OF ANY EXCLUSIVE REMEDIES.

eSoft Complete Care (eCC)

Software Care

The Software Care module gives you access to the latest feature enhancements, software upgrades and security patches for your InstaGate appliance. Use of the term InstaGate refers to and includes all versions of the InstaGate product such as the InstaGate EX, InstaGate EX2, InstaGate PRO, and any other subsequent InstaGate products. Any updates are automatically delivered to your eSoft appliance on a weekly basis and installed at the time you want with the click of a mouse. The Software Care module is required for InstaGate users wanting to download and use SoftPak applications.

Extended Hardware Care

The Extended Hardware Care module extends your standard warranty for hardware repair and unlimited on-line technical support. This support enables you to additionally purchase next working day product replacement (Hardware Hot Swap) for the life of the agreement (non-U.S. allow two to four working days) ensuring a speedy recovery to any breakdown in your business critical Internet security and communication.

Hardware Hot Swap

Provides next day hardware replacement and one-way shipping costs for InstaGate appliances. Customers must be covered by original (one-year for standard, two-year for EC countries) product warranty or Extended Hardware Care agreement to qualify for purchase.

Products returned to eSoft must be pre-authorized by eSoft with a Return Merchandise Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment.

The Customer shall provide a valid credit card number as security deposit for cross-shipment of replacement unit(s). The Customer must return the defective product to eSoft within fourteen (14) days (30 days for international customers) after the request for replacement. If the defective product is not returned to eSoft within this time period, eSoft will bill the Customer for the product at list price.

Phone/Email Care

The Phone/Email Care module provides telephone and email technical support 24-hours a day, seven days a week (major holidays excluded). Available per incident, in a three-pack bundle, or on an unlimited basis, the Phone/Email Care module provides priority customer support when you need it.

Refund/Return Policy

All products are sold with a 30-day Return Policy for any failure to perform to published specifications.

If eSoft's hardware does not perform to published specifications, the customer may return the unit within 30 days of original purchase date for a full refund less shipping costs.

Returned products will not be accepted without a Return Merchandise Authorization (RMA) number issued by eSoft Inc.

All RMA requests must be submitted in writing (Attention: RMA Department) via fax, email or by US mail stating the reasons for return and must be received on or before the 30th day, commencing from the date of receipt.

Any addendums or changes to these terms must either be authorized at the time of purchase or requested and approved in writing prior to the expiration of the 30 days.

SoftPaks

SoftPak subscriptions are non-refundable, unless part of a unit authorized for return due to not performing to published specifications.

eSoft Complete Care (eCC) Agreements

Software Care (SWC) Agreements are non-refundable, unless part of a unit authorized for return due to not performing to published specifications.

Extended Hardware Care (EHC) Agreements are non-refundable, unless part of a unit authorized for return due to not performing to published specifications.

Phone/Email Care (PEC) Agreements are non-refundable, unless part of a unit authorized for return due to not performing to published specifications.

Delivery Methods and Time Frame

Hardware

eSoft uses multiple shippers to ensure that all of our shipments are delivered in a timely manner. Typically, orders are shipped same day if the order is received by 11am MST. Orders received after 11am MST will typically be shipped the next day. Normal method for domestic orders is UPS Ground unless otherwise specified.

International orders generally ship within 2-3 days. Normal method for international shipments is DHL unless otherwise specified. UPS is occasionally used for shipments to Canada and Mexico.

SoftPaks

SoftPaks are downloadable directly from your eSoft hardware unit. Receipt of a SoftPak application is instantaneous upon completion of the download process.

Service Agreements

Phone/Email Care agreements are immediately in effect at the time of purchase.

End-User License Agreement

IMPORTANT, READ CAREFULLY: THIS ESOFT END-USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND ESOFT, INC. ("ESOFT") FOR THE INSTAGATE ADMINISTRATION UTILITY AND OTHER PROPRIETARY SOFTWARE REQUIRED FOR THE PROPER OPERATION OF THE INSTAGATE HARDWARE (COLLECTIVELY THE "ESOFT SOFTWARE"), WHICH INCLUDES COMPUTER SOFTWARE AND ASSOCIATED MEDIA AND PRINTED MATERIALS (IF ANY), AND MAY INCLUDE ONLINE OR ELECTRONIC DOCUMENTATION. ESOFT IS WILLING TO GRANT YOU THE FOLLOWING LICENSE TO USE THE ESOFT SOFTWARE ACCORDING TO THIS AGREEMENT ONLY ON THE CONDITION THAT YOU ACCEPT ALL TERMS IN THIS AGREEMENT.

BY CLICKING ON THE "ACCEPT" BUTTON BELOW YOU ACKNOWLEDGE THAT YOU HAVE READ THIS EULA AND THAT YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, ESOFT IS NOT WILLING TO LICENSE THIS ESOFT SOFTWARE TO YOU AND YOU ARE NOT AUTHORIZED TO USE THE ESOFT SOFTWARE. IN SUCH CASE, YOU MAY RETURN THE ESOFT SOFTWARE WITH THE PRODUCT IN ITS ORIGINAL PACKAGING FOR A FULL REFUND.

The eSoft Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Unauthorized reproduction or distribution is subject to civil and criminal penalties.

1. GRANT OF LICENSE. eSoft grants You the right to use the eSoft Software only in conjunction with validly serialized eSoft InstaGate hardware. eSoft provides additional services and applications called SoftPaks that may be downloaded by You from the InstaGate SoftPak Director. These SoftPaks are described on the SoftPak Director menu and on Our web site at www.esoft.com and are licensed under the terms and conditions as set forth herein for the eSoft Software and during the InstaGate registration process. Use of the term InstaGate refers to and includes all versions of the InstaGate product such as the InstaGate 404, InstaGate 404e, InstaGate 604, InstaGate 806, InstaGate EX, InstaGate EX2, InstaGate PRO, InstaGate xSP, InstaGate xSP Branch Office, InstaGate xSP Business, and any other subsequent InstaGate products.

2. RESTRICTIONS. You may not use, copy, modify, or transfer the eSoft Software, or any copy thereof, in whole or in part, except as expressly provided in this EULA. You may not reverse engineer, disassemble, decompile, or translate the eSoft Software, or otherwise attempt to derive the source code of the eSoft Software, or authorize any third party to do any of the foregoing, except to

the extent allowed under any applicable law. Except as expressly permitted in the previous sentence, any attempt to transfer any of the rights, duties or obligations hereunder is void. You may not rent, lease, loan, resell for profit, or distribute the eSoft Software, or any part thereof. You agree to comply with all applicable laws regarding the use of the eSoft Software.

3. YOUR RESTRICTIONS.

You agree:

3.1. to make all payments due to eSoft or the authorized eSoft reseller in a timely fashion;

3.2. to notify Us promptly by email at support@esoft.com if You suspect unauthorized use of the InstaGate, eSoft Software or SoftPaks and that You remain responsible for such unauthorized use;

3.3. not to assign, transfer, or delegate this Agreement or Your rights or obligations under it without the prior written consent of eSoft and that any attempt to do such an assignment without prior written consent is void;

3.4. that You are responsible for the results obtained from Your use of the eSoft Software and InstaGate;

3.5. to comply with all applicable laws, regulations, or conventions, including, but not limited to, those related to child pornography, gambling or gaming, obscenity, securities, intellectual property rights, data privacy, import/export of data and taxes, or misleading or deceptive conduct;

3.6. that You are not a specifically designated individual or entity under any U.S. (or other) embargo or otherwise the subject, either directly or indirectly, to any order issued by any agency of the U.S. Government (or any other government) limiting, barring, revoking or denying, in whole or in part, Your export privileges and that You will notify Us immediately in the event You become subject to any such order;

3.7. that You are solely responsible for complying with applicable Internet acceptable use policies;

3.8. that You are responsible to maintain a backup copy of Your data and files;

3.9. not to alter the InstaGate hardware and not to install any software on the InstaGate other than that provided by Us;

3.10. that it is Your responsibility to provide appropriate client hardware and LAN connection at Your location;

3.11. that it is Your responsibility to provide a PC as an administrative machine;

3.12. to pay all shipping charges (including taxes, tariffs, and insurance) including, if a return is authorized, labor for packing and unpacking incurred for the return shipment of the InstaGate hardware to Us unless we specify otherwise;

3.13. that You are responsible for subscribing to an Internet Service Provider ("ISP") and complying with the agreement, including any payment terms, provided to You by such ISP. You are solely responsible for ensuring that attaching the InstaGate hardware does not violate the terms of the agreement between You and Your ISP;

3.14. that You will contact Your ISP when ISP-related support issues arise including, but not limited to, bandwidth and connection issues;

3.15. that You are responsible for providing an available port to connect the InstaGate hardware to your local network;

3.16. for all connectivity options supported, that You are responsible for ensuring Your ISP provides the proper IP address;

3.17. for analog connectivity option, that actual speeds may vary depending on a number of factors such as equipment or software used;

3.18. for analog and ISDN options, that You are responsible for specifying the way the InstaGate dials outside calls from Your premises. For example, dialing 9, 1, an area code or other prefixes before the POP number;

3.19. for the analog and ISDN connectivity options, that You are responsible for any charges You incur from Your local telephone service provider, including line installation, monthly, toll, long distance, and/or per minute charges;

3.20. for the DSL and cable options, that You are responsible for paying the installation, equipment, monthly charges and monthly local loop charges;

3.21. for the DSL and cable options, that You are responsible for ensuring that the equipment provides an Ethernet connection to the InstaGate hardware.

3.22. to provide eSoft with all information required for products and services that send data to eSoft as indicated in the User Guide. You agree to disable such services if You do not wish to submit the information.

4. Charges and Payments

4.1. You agree to pay any fees, taxes, including personal property taxes or sales and use taxes, resulting from Your purchases and Your use of the eSoft Software, SoftPaks and InstaGate hardware.

4.2 All charges You incur will be invoiced to You or the authorized eSoft reseller. Other charges (and applicable taxes) for any other services or SoftPaks ordered hereunder will be charged as they are incurred. If We do not receive payment from You or the eSoft authorized reseller, You agree to pay to Us all amounts due upon demand. You agree to pay all attorneys' and collection fees arising from Our efforts to collect any past due amounts from You to the extent permitted by law. We may charge You a late payment fee equal to the lesser of 1.5% per month or the maximum rate permitted by law on all outstanding balances. We reserve the right to assign Our accounts receivable and delegate the servicing and administration of charges and payments to a third party of Our choosing. You agree not to assert against any assignees of Us any claim, defense, or setoff You may have against Us. You acknowledge that We may disable the InstaGate hardware, eSoft Software and SoftPaks if payment is not received on the due date, and that such an act by Us does not remove Your obligation to make complete payments on any amounts due and owing to Us.

5. Changes, Notifications and Upgrades

5.1. Changes to the eSoft Software and SoftPaks will be provided to You through the InstaGate system administration menu and the email address you provide during the registration process.

5.2. If We need to contact You, We may do so by telephone, postal mail or email. If You need to contact Us concerning the InstaGate, eSoft Software or SoftPaks, You will do so by sending an email to support@esoft.com or by calling us on our technical support phone number.

6. Renewal and Termination

6.1. We may at any time modify or discontinue any or all aspects of the eSoft Software or SoftPaks or terminate this Agreement, or terminate, withdraw or restrict Your use of the eSoft Software or SoftPaks (in whole or in part) without notice, if We, in our sole judgment, determine or receive information that: a) You have violated the terms of this Agreement; b) doing so is necessary for security reasons or for proper continued operation of the InstaGate; c) Your use of the eSoft Software, InstaGate or SoftPaks is disruptive or causes a malfunction of the eSoft Software, InstaGate or SoftPaks; d) Your use of the eSoft Software, InstaGate or SoftPaks (or any part thereof) may violate the privacy, publicity, copyright or other intellectual property rights of Ours or a third party or may violate any other applicable laws and regulations; e) We do not receive timely payment; or f) We receive an order from a governmental body or a court of competent jurisdiction requiring Us to do so.

6.2. Without prejudice to any other rights, this EULA will terminate immediately without notice if you fail to comply with the terms and conditions of this EULA. Upon notice of termination, you agree to destroy all copies of the eSoft Software.

7. OWNERSHIP. The eSoft Software is licensed, not sold, to you for use only under the terms of this EULA, and eSoft reserves all rights not expressly granted to you. As between the parties, all title and copyrights in and to the eSoft Software and any copies thereof are owned by eSoft or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the eSoft Software is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content.

8. CONNECTIVITY CHARGES. You acknowledge that you are responsible for all charges relating to connecting to the Internet including, but not limited to, installation, use, and toll charges. This can include ISP charges as well as any charges you incur from your telephone, ISDN, DSL, cable or other service provider. YOU UNDERSTAND THAT THE ESOFT SOFTWARE WILL CAUSE THE DEVICE TO AUTOMATICALLY CONNECT TO THE INTERNET BASED UPON CONFIGURED SETTINGS AND NETWORK USAGE. YOU ALSO UNDERSTAND THAT THOSE CONNECTIONS CAN BE FOR EXTENDED PERIODS OF TIME BASED UPON NETWORK USAGE AND OTHER PARAMETERS CONFIGURED BY YOU. THESE CONNECTIONS CAN GENERATE TELEPHONE CHARGES AMOUNTING TO SEVERAL THOUSAND DOLLARS PER MONTH IF NETWORK TRAFFIC IS HIGH OR THE ESOFT SOFTWARE IS INCORRECTLY CONFIGURED BY YOU. YOU ARE ADVISED TO CLOSELY MONITOR CONNECTIONS TO THE INTERNET IN ORDER TO PROPERLY CONFIGURE THE ESOFT SOFTWARE FOR OPTIMAL OPERATION IN YOUR NETWORK ENVIRONMENT.

9. U.S. GOVERNMENT RESTRICTED RIGHTS. The eSoft Software is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is eSoft, Inc., 295 Interlocken Blvd., Suite 500, Broomfield, CO 80021.

10. EXPORT RESTRICTIONS. You agree that you will not export or re-export the eSoft Software to any country, person, entity or end user subject to U.S.A. export restrictions. Restricted countries currently include, but are not necessarily limited to Cuba, Iran, Iraq, Libya, North Korea, Syria, and the Federal Republic of Yugoslavia. You warrant and represent that neither the U.S.A. Bureau of Export Administration nor any other federal agency has suspended, revoked or denied your export privileges.

11. NOTE ON JAVA SUPPORT. THE ESOFT SOFTWARE MAY CONTAIN SUPPORT FOR PROGRAMS WRITTEN IN JAVA. JAVA TECHNOLOGY IS NOT FAULT TOLERANT AND IS NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE OR RESALE AS ON-LINE CONTROL EQUIPMENT IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, DIRECT LIFE SUPPORT MACHINES, OR WEAPON SYSTEMS, IN WHICH THE FAILURE OF JAVA TECHNOLOGY COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES").

12. NO WARRANTY. THE ESOFT SOFTWARE IS PROVIDED TO YOU "AS IS" AND ANY USE OF THE ESOFT SOFTWARE IS AT YOUR OWN RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ESOFT AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

13. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ESOFT OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE ESOFT SOFTWARE PRODUCT, EVEN IF ESOFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

14. LIMITATION OF LIABILITY. ESOFT'S ENTIRE LIABILITY AND YOUR EXCLUSIVE REMEDY UNDER THIS EULA SHALL NOT EXCEED THE AMOUNT RECEIVED BY ESOFT FROM YOU UNDER THIS AGREEMENT.

15. MISCELLANEOUS. This EULA is governed by the laws of the State of Colorado, in the United States of America, without regard to or application of conflicts of law rules or principles. The Federal and State Courts located in Broomfield County shall have sole jurisdiction over any disputes arising hereunder and the parties hereby submit to the personal jurisdiction of such courts. If any provision of this EULA is held to be unenforceable, that provision will be removed to the minimum extent necessary and the remaining provisions will remain in full force. In the event any proceeding or lawsuit is brought by eSoft or you in connection with this EULA, the prevailing party in such proceeding or lawsuit shall be entitled to receive its costs, expert witness fees and reasonable attorney's fees, including costs and fees on appeal. The failure of either party to require performance by the other party of any provision hereof shall not affect the full right to require such

performance at any time thereafter; nor shall the waiver by either party of a breach of any provision hereof be taken or held to be a waiver of the provision itself. Neither this EULA nor any rights or obligations of you hereunder may be assigned by you in whole or in part without the prior written approval of eSoft. Any assignment in derogation of the foregoing shall be null and void. This EULA is the complete and exclusive statement of the agreement between eSoft and you which supersedes any proposal or prior agreement, oral or written, and any other communications between the parties in relation to the subject matter of this EULA. This EULA shall not be modified except by a subsequently dated written amendment or exhibit signed by both parties by their duly authorized representatives. Should you have any questions concerning this EULA, or if you desire to contact eSoft for any reason, please write: eSoft, Inc., 295 Interlocken Blvd., Suite 500, Broomfield, CO 80021.

Privacy Policy The eSoft Privacy Policy can be found on the eSoft web site at <http://www.esoft.com>.

InstaGate software contains software covered under the GNU General Public License. You may freely obtain source code versions of the software covered by the GNU General Public License through the Internet at <http://ftp.esoft.com>. However, some applications remain the property of their owners, and require their permission to redistribute. For more information, access the eSoft web site at <http://www.esoft.com>.

Portions of InstaGate are free software. You can redistribute the free software contained in this product ("Free Software") and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. **ALL OTHER SOFTWARE PROVIDED TO YOU IS NOT FREE SOFTWARE AND IS SUBJECT TO THE TERMS OF YOUR AGREEMENT WITH eSoft, Inc.**

The Free Software is distributed **WITHOUT ANY WARRANTY; INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.** Please refer to the GNU General Public License for more details.

Permission to use, copy, modify, and distribute the Free Software and its documentation for **NON-COMMERCIAL** or **COMMERCIAL** purposes and without fee is hereby granted, provided that this copyright notice is kept intact and the terms of the GNU General Public License are otherwise observed. The GNU General Public License can be viewed below or at <http://www.gnu.org/licenses/gpl-2.0.txt>.

Portions of eSoft Software are protected by U.S. Patent 6,961,773 B2 as well as copyright and trademark laws.

Copyright 2006, eSoft, Inc. All Rights Reserved.

InstaGate, InstaGate 404, InstaGate 404e, InstaGate 404e, InstaGate 604, InstaGate 806, InstaGate EX, InstaGate EX2, InstaGate PRO, InstaGate xSP, InstaGate xSP Branch Office, InstaGate xSP Business, SoftPak, and SoftPak Director are trademarks of eSoft, Inc.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc.,

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w` and `show c` should show the appropriate parts of the General Public License. Of course, the commands you use maybe called something other than `show w` and `show c`; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, “Digital Apparatus,” ICES- 003. 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 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:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.
- Consult the dealer or an experienced radio/television technician for help.

Canadian Users

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the radio interference regulations of Industry Canada.

Le présent appareil numérique n’émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de Classe A prescrites dans le règlement sur le brouillage radioélectrique édicté par Industrie Canada.

European Users

This Information Technology Equipment has been tested and found to comply with the following European directives:

- EMC Directive
 - EN 55022:1998 Class A
 - EN 61000-3-2:1995 or EN 60555-2:1987
 - EN 61000-3-3:1995 or EN 60555-3:1987
 - EN 55024:1998 according to
 - EN 61000-4-2:1995 or IEC 801-2:1984
 - EN 61000-4-3:1996 or IEC 801-3:1984
 - EN 61000-4-4:1995 or IEC 801-4:1988
 - EN 61000-4-5:1995 or IEC 801-5:1995
 - EN 61000-4-6:1996 or IEC 801-6:1996
 - EN 61000-4-8:1994 or IEC 801-8:1993
 - EN 61000-4-11:1994 or IEC 801-11:1994
- Low Voltage Directive (Safety) 73/23/EEC as per EN 60950:1992(A1/A2/A3/A4/A11)

VCCI Statement

電波障害自主規制 届出装置の記述

<p>この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。</p> <p>従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。</p> <p>取扱説明書に従って正しい取り扱いをしてください。</p>

Information To The User

The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

account name

The part of a user's email address before the @domain.com of their Internet mail address.

administrator

Person responsible for system management. Aside from managing a system's configuration and user accounts, administrators also receive email warning and error messages, system alert messages, and daily summary reports.

administrative interface

HTML-based user interface for system set up and configuration. Access to the interface is password controlled.

alert

An email message sent to the system administrator when an established system threshold is exceeded.

Asynchronous Transfer Mode (ATM)

See *ATM*.

ATM

Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays.

authentication

The process of verifying that a user is who he claims to be.

backup

Maintenance function that copies a system's essential data to a secondary storage device, such as an FTP directory on another network computer or a magnetic tape drive.

bandwidth

The amount of data that can be sent through a given communications circuit per second.

browser

A program that allows a user to select and display Internet sites.

Challenge Handshake Authentication Protocol (CHAP)

See *CHAP*.

CHAP

Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access.

classical IP over ATM

Specification for running IP over ATM in a manner that takes full advantage of the features of ATM.

client

A workstation attached to a network.

configuration

System settings and parameters that determine how a system (or various components of a system) function.

connect time

Period of time in which the system is connected to the Internet.

Data-link Connection Identifier (DLCI)

See *DLCI*.

data transfer

The transmitting and receiving of data through the appliance to an ISP.

DHCP

Dynamic Host Configuration Protocol. Method whereby a server can automatically assign network configuration information to individual computers as they power up and connect to the network.

diagnostics

Tools used to diagnose and troubleshoot problems encountered in setting up or using a system.

Digital Subscriber Line (DSL)

See *DSL*.

directory

A simulated file folder on disk.

DLCI

Data-link Connection Identifier. Value that specifies a PVC or an SVC in a Frame Relay network.

DNS

Domain Name Service. An Internet service that translates a domain name or host name into a numeric IP address for connection to a particular site.

domain name

A location name on the Internet.

Domain Name Service (DNS)

See *DNS*.

DSL

Digital Subscriber Line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances.

Dynamic Host Configuration Protocol (DHCP)

See *DHCP*.

dynamic IP address

An address that is continually updated by the ISP each time an Internet connection is made (this may or may not be the same address each time).

encryption

The process of disguising a message in such a way as to hide its substance.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.

file sharing

The public (over the WAN) or private (over the LAN) sharing of computer data or space in a network with various levels of access privilege.

File Transfer Protocol (FTP)

See *FTP*.

firewall

A sub-system of computer software and hardware that intercepts data packets before allowing them into or out of a local area network.

forwarding

Routing email from one mail address to another.

FTP

File Transfer Protocol. Protocol that allows for the direct transfer of files from one host on a network to another.

full name

Typically a person's whole name (last name, first name, and middle initial).

gateway

The entrance and exit into a computer network.

Integrated Services Digital Network (ISDN)

See *ISDN*.

Internet Protocol (IP)

See *IP*.

Internet Protocol address (IP address)

See *IP address*.

Internet Service Provider (ISP)

See *ISP*.

IP

Internet Protocol. A layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices.

IP address

Internet Protocol address. A unique address used by ISP's, companies, and individuals to identify computers and peripherals on LANs, WANs, and the Internet.

ISDN

Integrated Services Digital Network. A dedicated telephone line connection that transmits digital data at the rate of 56Kbps.

ISP

Internet Service Provider. A company that sells direct access to the Internet.

LAN

Local Area Network. A collection of computers connected to one another over high-speed cable for sharing data and resources.

Local Area Network (LAN)

See *LAN*.

modem

A piece of hardware used to send data signals over standard telephone lines. Since standard telephone lines send and receive analog signals and computer systems send and receive digital signals, the modem converts signals from analog to digital and vice versa.

NAT

Network Address Translation. This translation occurs at the firewall to hide internal source or destination IP addresses from the external Internet user.

network

A group of computers linked together to share information and resources.

Network Address Translation (NAT)

See *NAT*.

password

A word or string of characters that allows a user to access an internal network or a specific server on a network.

Point-to-Point Protocol (PPP)

See *PPP*.

Point-to-Point Protocol over Ethernet (PPPoE)

See *PPPoE*.

Point-to-Point Protocol over ATM (PPPoA)

See *PPPoA*.

Point-to-Point Tunneling Protocol (PPTP)

See *PPTP*.

port

A connection or socket for connecting devices to a computer.

PPP

Point-to-Point Protocol. A protocol that allows a computer to connect to the Internet with a standard telephone line connected to a high speed modem.

PPPoE

Point-to-Point Protocol over Ethernet. A method for running the PPP protocol, commonly used for dial-up Internet connections, over Ethernet. Used by DSL and cable modem providers, PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet.

PPPoA

Point-to-Point Protocol over ATM. A protocol for transmitting packets over an ATM network.

PPTP

Point-to-Point Tunneling Protocol. A protocol used to establish an encrypted tunnel (VPN) from a client workstation into a network across the Internet.

protocol

A specific set of rules, procedures, and conventions that governs the relation and timing of data transmission between two devices.

proxy cache size

Setting that controls the amount of data that can be stored on the caching proxy server.

proxy server

Server component that enhances web access performance by caching most frequently accessed web data.

queue

Email messages lined up and waiting to be sent or retrieved.

RADIUS

Remote Authentication Dial-In User Service. An access control protocol that uses a challenge/response method for authentication.

Remote Authentication Dial-In User Service (RADIUS)

See *RADIUS*.

remote support

Maintenance option that allows an off-site administrator to connect to the appliance and access the administration utility.

restart

The process of shutting down the system and starting it again.

restore

Maintenance function that downloads a saved backup file from a secondary storage device to recover lost data or configuration settings.

route

A path for transmitting data.

script

A program used by certain computer languages and operating systems that provides a sequence of instructions to guide a computer through a sequence of actions.

Secure Sockets Layer (SSL)

See *SSL*.

server

A shared computer connected to other computers or peripheral devices on a LAN or WAN.

shutdown

The process of powering down the system.

Simple Mail Transfer Protocol (SMTP)

See *SMTP*.

Simple Network Management Protocol (SNMP)

See *SNMP*.

SMTP

Simple Mail Transfer Protocol. A protocol used in TCP/IP networks to transfer email messages between computers.

SNMP

Simple Network Management Protocol. A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network.

spam

Unwanted, bulk email advertisements and messages.

SSL

Secure Sockets Layer. A Netscape Communications encryption protocol that provides communications privacy over the Internet.

static IP address

A pre-assigned fixed address that is stored on the server and used every time an Internet connection is made.

static route

A fixed path for transmitting data between two networks.

