

EN	<p>Dear Customer,</p> <p>Gigaset Communications GmbH is the legal successor to Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), which in turn continued the Gigaset business of Siemens AG. Any statements made by Siemens AG or SHC that are found in the user guides should therefore be understood as statements of Gigaset Communications GmbH.</p> <p>We hope you enjoy your Gigaset.</p>	DA	<p>Kære Kunde,</p> <p>Gigaset Communications GmbH er retlig efterfølger til Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), som fra deres side videreførte Siemens AGs Gigaset-forretninger. Siemens AGs eller SHCs eventuelle forklaringer i betjeningsvejledningerne skal derfor forstås som Gigaset Communications GmbHs forklaringer.</p> <p>Vi håber, du får meget glæde af din Gigaset.</p>
DE	<p>Sehr geehrte Kundin, sehr geehrter Kunde,</p> <p>die Gigaset Communications GmbH ist Rechtsnachfolgerin der Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), die ihrerseits das Gigaset-Geschäft der Siemens AG fortführte. Etwaige Erklärungen der Siemens AG oder der SHC in den Bedienungsanleitungen sind daher als Erklärungen der Gigaset Communications GmbH zu verstehen.</p> <p>Wir wünschen Ihnen viel Freude mit Ihrem Gigaset.</p>	FI	<p>Arvoisa asiakkaamme,</p> <p>Gigaset Communications GmbH on Siemens Home and Office Communication Devices GmbH & Co. KG (SHC)-yhtiksen oikeudenomistaja, joka jatkoi puolestaan Siemens AG:n Gigaset-liiketoimintaa. Käyttöoppaissa mahdollisesti esiintyvät Siemens AG:n tai SHC:n selosteet on tämän vuoksi ymmärrettävä Gigaset Communications GmbH:n selosteina.</p> <p>Toivotamme Teille paljon iloa Gigaset-laitteestanne.</p>
FR	<p>Chère Cliente, Cher Client,</p> <p>la société Gigaset Communications GmbH succède en droit à Siemens Home and Office Communication Devices GmbH & Co. KG (SHC) qui poursuivait elle-même les activités Gigaset de Siemens AG. Donc les éventuelles explications de Siemens AG ou de SHC figurant dans les modes d'emploi doivent être comprises comme des explications de Gigaset Communications GmbH.</p> <p>Nous vous souhaitons beaucoup d'agrément avec votre Gigaset.</p>	SV	<p>Kära kund,</p> <p>Gigaset Communications GmbH övertar rättigheterna från Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), som bedrev Gigaset-verksamheten efter Siemens AG. Alla förklaringar från Siemens AG eller SHC i användarhandboken gäller därför som förklaringar från Gigaset Communications GmbH.</p> <p>Vi önskar dig mycket nöje med din Gigaset.</p>
IT	<p>Gentile cliente,</p> <p>la Gigaset Communications GmbH è successore della Siemens Home and Office Communication Devices GmbH & Co. KG (SHC) che a sua volta ha proseguito l'attività della Siemens AG. Eventuali dichiarazioni della Siemens AG o della SHC nei manuali d'istruzione, vanno pertanto intese come dichiarazioni della Gigaset Communications GmbH. Le auguriamo tanta soddisfazione con il vostro Gigaset.</p>	NO	<p>Kjære kunde,</p> <p>Gigaset Communications GmbH er rettslig etterfølger etter Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), som i sin tur videreførte Gigaset-geskjeften i Siemens AG. Eventuelle meddelelser fra Siemens AG eller SHC i bruksanvisningene er derfor å forstå som meddelelser fra Gigaset Communications GmbH.</p> <p>Vi håper du får stor glede av din Gigaset-enhet.</p>
NL	<p>Geachte klant,</p> <p>Gigaset Communications GmbH is de rechtsopvolger van Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), de onderneming die de Gigaset-activiteiten van Siemens AG heeft overgenomen. Eventuele uitspraken of mededelingen van Siemens AG of SHC in de gebruiksaanwijzingen dienen daarom als mededelingen van Gigaset Communications GmbH te worden gezien.</p> <p>Wij wensen u veel plezier met uw Gigaset.</p>	EL	<p>Αγαπητή πελάτισσα, αγαπητέ πελάτη,</p> <p>η Gigaset Communications GmbH είναι η νομική διάδοχος της Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), η οποία έχει αναλάβει την εμπορική δραστηριότητα Gigaset της Siemens AG. Οι δηλώσεις της Siemens AG ή της SHC στις οδηγίες χρήσης αποτελούν επομένως δηλώσεις της Gigaset Communications GmbH.</p> <p>Σας ευχόμαστε καλή διασκέδαση με τη συσκευή σας Gigaset.</p>
ES	<p>Estimado cliente,</p> <p>la Gigaset Communications GmbH es derechohabiente de la Siemens Home and Office Communication Devices GmbH & Co. KG (SHC) que por su parte continuó el negocio Gigaset de la Siemens AG. Las posibles declaraciones de la Siemens AG o de la SHC en las instrucciones de uso se deben entender por lo tanto como declaraciones de la Gigaset Communications GmbH.</p> <p>Le deseamos que disfrute con su Gigaset.</p>	HR	<p>Poštovani korisnici,</p> <p>Gigaset Communications GmbH pravni je sljednik tvrtke Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), koji je nastavio Gigaset poslovanje tvrtke Siemens AG. Zato sve izjave tvrtke Siemens AG ili SHC koje se nalaze u uputama za upotrebu treba tumačiti kao izjave tvrtke Gigaset Communications GmbH.</p> <p>Nadamo se da sa zadovoljstvom koristite svoj Gigaset uređaj.</p>
PT	<p>SCaros clientes,</p> <p>Gigaset Communications GmbH é a sucessora legal da Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), que, por sua vez, deu continuidade ao sector de negócios Gigaset, da Siemens AG. Quaisquer declarações por parte da Siemens AG ou da SHC encontradas nos manuais de utilização deverão, portanto, ser consideradas como declarações da Gigaset Communications GmbH.</p> <p>Desejamos que tenham bons momentos com o seu Gigaset.</p>	SL	<p>Spoštovani kupec!</p> <p>Podjetje Gigaset Communications GmbH je pravni naslednik podjetja Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), ki nadaljuje dejavnost znamke Gigaset podjetja Siemens AG. Vse izjave podjetja Siemens AG ali SHC v priročnikih za uporabnike torej veljajo kot izjave podjetja Gigaset Communications GmbH.</p> <p>Želimo vam veliko užitkov ob uporabi naprave Gigaset.</p>

CS	Vážení zákazníci, společnost Gigaset Communications GmbH je právním nástupcem společnosti Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), která dále přejala segment produktů Gigaset společnosti Siemens AG. Jakékoli prohlášení společnosti Siemens AG nebo SHC, které naleznete v uživatelských příručkách, je třeba považovat za prohlášení společnosti Gigaset Communications GmbH. Doufáme, že jste s produkty Gigaset spokojeni.	PL	Szanowny Kliencie, Firma Gigaset Communications GmbH jest spadkobiercą prawnym firmy Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), która z kolei przejęła segment produktów Gigaset od firmy Siemens AG. Wszelkie oświadczenia firm Siemens AG i SHC, które można znaleźć w instrukcjach obsługi, należy traktować jako oświadczenia firmy Gigaset Communications GmbH. Życzymy wiele przyjemności z korzystania z produktów Gigaset.
SK	Vážený zákazník, Spoločnosť Gigaset Communications GmbH je právnym nástupcom spoločnosti Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), ktorá zasa pokračovala v činnosti divízie Gigaset spoločnosti Siemens AG. Z tohto dôvodu je potrebné všetky vyhlásenia spoločnosti Siemens AG alebo SHC, ktoré sa nachádzajú v používateľských príručkách, chápať ako vyhlásenia spoločnosti Gigaset Communications GmbH. Veríme, že budete so zariadením Gigaset spokojní.	TR	Sayın Müşterimiz, Gigaset Communications GmbH, Siemens AG'nin Gigaset işletmesini yürüten Siemens Home and Office Communication Devices GmbH & Co. KG (SHC)'nin yasal halefidir. Kullanma kılavuzlarında bulunan ve Siemens AG veya SHC tarafından yapılan bildiriler Gigaset Communications GmbH tarafından yapılmış bildiriler olarak algılanmalıdır. Gigaset'ten memnun kalmanızı ümit ediyoruz.
RO	Stimate client, Gigaset Communications GmbH este succesorul legal al companiei Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), care, la rândul său, a continuat activitatea companiei Gigaset a Siemens AG. Orice afirmații efectuate de Siemens AG sau SHC și incluse în ghidurile de utilizare vor fi, prin urmare, considerate a aparține Gigaset Communications GmbH. Sperăm ca produsele Gigaset să fie la înălțimea dorințelor dvs.	RU	Уважаемые покупатель! Компания Gigaset Communications GmbH является правопреемником компании Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), которая, в свою очередь, приняла подразделение Gigaset в свое управление от компании Siemens AG. Поэтому любые заявления, сделанные от имени компании Siemens AG или SHC и встречающиеся в руководствах пользователя, должны восприниматься как заявления компании Gigaset Communications GmbH. Мы надеемся, что продукты Gigaset удовлетворяют вашим требованиям.
SR	Poštovani potrošaču, Gigaset Communications GmbH je pravni naslednik kompanije Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), kroz koju je nastavljeno poslovanje kompanije Gigaset kao dela Siemens AG. Stoga sve izjave od strane Siemens AG ili SHC koje se mogu naći u korisničkim uputstvima treba tumačiti kao izjave kompanije Gigaset Communications GmbH. Nadamo se da ćete uživati u korišćenju svog Gigaset uređaja.		
BG	Уважаеми потребители, Gigaset Communications GmbH е правопреемникът на Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), която на свой ред продължи бизнеса на подразделението Siemens AG. По тази причина всякакви изложения, направени от Siemens AG или SHC, които се намират в ръководствата за потребителя, следва да се разбират като изложения на Gigaset Communications GmbH. Надяваме се да ползвате с удоволствие вашия Gigaset.		
HU	Tisztelt Vásárló! A Siemens Home and Communication Devices GmbH & Co. KG (SHC) törvényes jogutódja a Gigaset Communications GmbH, amely a Siemens AG Gigaset üzletágának utódja. Ebből következően a Siemens AG vagy az SHC felhasználói kézikönyveiben található bármely kijelentést a Gigaset Communications GmbH kijelentésének kell tekinteni. Reméljük, megelégedéssel használja Gigaset készülékét.		

Gigaset
**SE565 Residential
Gateway
User's Guide**

SIEMENS

Part No. 007-6565-001

Software License and Limited Warranty

© Copyright 2006, Siemens Subscriber Networks, Inc.
All rights reserved. Printed in the U.S.A.

Siemens Subscriber Networks, Efficient Networks, the Efficient Networks logo, and Gigaset(tm) are trademarks of Siemens AG. All other names may be trademarks, service marks or registered trademarks held by their respective companies. This document is for information purposes only. Siemens Subscriber Networks is not responsible for errors or omissions herein. Siemens Subscriber Networks reserves the right to make changes to product specifications without notice.

Siemens Subscriber Networks, Inc. – End User Software License and Warranty

INSTALLATION OF THE HARDWARE AND SOFTWARE PROVIDED BY SIEMENS SUBSCRIBER NETWORKS, INC (SSN). CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS OF THE FOLLOWING SOFTWARE LICENSE AND LIMITED WARRANTY. IF YOU DO NOT ACCEPT THESE TERMS, PLEASE RETURN THE HARDWARE AND SOFTWARE AND SOFTWARE IN ITS ORIGINAL PACKAGING TO THE VENDOR FROM WHICH YOU PURCHASED IT FOR A FULL REFUND OF THE PURCHASE PRICE.

The following describes your license to use the software (the "Software") that has been provided with your Siemens customer premise equipment ("Hardware") and the limited warranty that Siemens Subscriber Networks provides on its Software and Hardware. Siemens Subscriber Networks reserves any right not expressly granted to the end user.

Software License

The Software is protected by copyright laws and international copyright treaties. The Software is licensed and not sold to you. The definition of Software includes, but not limited to, system and operating software marketed by Siemens Subscriber Networks, including firmware, embedded software, software provided on media, downloadable software, software for configuration or programmable logic elements, and all Siemens Subscriber Networks maintenance and diagnostic tools associated with the above mentioned software. Accordingly, while you own the media (such as CD ROM or floppy disk) on which the software is recorded, Siemens Subscriber Networks or its licensors retains ownership of the Software itself.

1. **Grant of License.** You may install and use one (and only one) copy of the Software in conjunction with the Siemens Subscriber Networks provided Hardware. You may make backup copies of the system configuration as required. If the Hardware is being installed on a network, you may install the Software on the network server or other server-side device on which the Hardware is being installed and onto the client-side devices.
2. **Restrictions.** The license granted is a limited license. You may NOT:
 - sublicense, assign, or distribute copies of the Software to others;
 - decompile, reverse engineer, disassemble or otherwise reduce the Software or any part thereof to a human perceivable form;
 - modify, adapt, translate or create derivative works based upon the Software or any part thereof; or
 - rent, lease, loan or otherwise operate for profit the Software.
2. **Transfer.** You may transfer the Software only where you are also transferring the Hardware. In such cases, you must remove all copies of the Software from any devices onto which you have installed it, and must ensure that the party to whom you transfer the Hardware receives this License Agreement and Limited Warranty.
3. **Upgrades Covered.** This License covers the Software originally provided to you with the Hardware, and any additional software that you may receive from Siemens Subscriber Networks, whether delivered via tangible media (CD ROM or floppy disk), down loaded from Siemens Subscriber Networks, or delivered through customer support. Any such additional software shall be considered "Software" for all purposes under this License.
4. **Export Law Assurances.** You acknowledge that the Software may be subject to export control laws and regulations of the U.S.A. You confirm that you will not export or re-export the Software to any countries that are subject to export restrictions.
5. **No Other Rights Granted.** Other than the limited license expressly granted herein, no license, whether express or implied, by estoppel or otherwise, is granted to any copyright, patent, trademark, trade secret, or other proprietary rights of Siemens Subscriber Networks or its licensors.
6. **Termination.** Without limiting Siemens Subscriber Networks's other rights, Siemens Subscriber Networks may terminate this license if you fail to comply with any of these provisions. Upon termination, you must return the Software and all copies thereof.

Limited Warranty

The following limited warranties provided by Siemens Subscriber Networks extend to the original end user of the Hardware/licensee of the Software and are not assignable or transferable to any subsequent purchaser/licensee.

1. **Hardware.** Siemens Subscriber Networks warrants that the Hardware will be free from defects in materials and workmanship and will perform substantially in compliance with the user documentation relating to the Hardware for a period of one year from the date the original end user received the Hardware.
2. **Software.** Siemens Subscriber Networks warrants that the Software will perform substantially in compliance with the end user documentation provided with the Hardware and Software for a period of ninety days from the date the original end user received the Hardware and Software. The end user is responsible for the selection of Hardware and Software used in the end user's network. Given the wide range of third-party hardware and applications, Siemens Subscriber Networks does not warrant the compatibility or uninterrupted or error free operation of our Software with the end user's systems or network.
3. **Exclusive Remedy.** Your exclusive remedy and Siemens Subscriber Networks's exclusive obligation for breach of this limited warranty is, in Siemens Subscriber Networks's sole option, either (a) a refund of the purchase price paid for the Hardware/Software or (b) repair or replacement of the Hardware/Software with new or remanufactured products. Any replacement Hardware or Software will be warranted for the remainder of the original warranty period or thirty days, whichever ever is longer.
4. **Warranty Procedures.** If a problem develops during the limited warranty period, the end user shall follow the procedure outlined below:
 - A. Prior to returning a product under this warranty, the end user must first call Siemens Subscriber Networks at (888) 286-9375, or send an email to Siemens Subscriber Networks at support@efficient.com to obtain a return materials authorization (RMA) number. RMAs are issued between 8:00 a.m. and 5:00 p.m. Central Time, excluding weekends and holidays. The end user must provide the serial number(s) of the products in order to obtain an RMA.
 - B. After receiving an RMA, the end user shall ship the product or defective component, including power supplies and cable, where applicable, freight or postage prepaid and insured, to Siemens Subscriber Networks at 4849 Alpha Road, Dallas Texas 75244, U.S.A. Within five (5) days notice from Siemens Subscriber Networks, the end user shall provide Siemens Subscriber Networks with any missing items or, at Siemens Subscriber Networks's sole option, Siemens Subscriber Networks will either (a) replace missing items and charge the end user or (b) return the product to the end user freight collect. The end user shall include a return address, daytime phone number and/or fax. The RMA number must be clearly marked on the outside of the package.
 - C. Returned Products will be tested upon receipt by Siemens Subscriber Networks. Products that pass all functional tests will be returned to the end user.
 - D. Siemens Subscriber Networks will return the repaired or replacement Product to the end user at the address provided by the end user at Siemens Subscriber Networks's expense. For Products shipped within the United States of America, Siemens Subscriber Networks will use reasonable efforts to ensure delivery within five (5) business days from the date received by Siemens Subscriber Networks. Expedited service is available at additional cost to the end user.
 - E. Upon request from Siemens Subscriber Networks, the end user must prove the date of the original purchase of the product by a dated bill of sale or dated itemized receipt.
5. **Limitations.**
 - The end user shall have no coverage or benefits under this limited warranty if the product has been subject to abnormal use, abnormal conditions, improper storage, exposure to moisture or dampness, unauthorized modifications, unauthorized repair, misuse, neglect, abuse, accident, alteration, improper installation, or other acts which are not the fault of Siemens Subscriber Networks, including acts of nature and damage caused by shipping.
 - Siemens Subscriber Networks will not honor, and will not consider the warranty voided, if: (1) the seal or serial number on the Product have been tampered with or (2) there has been any attempted or actual repair or modification of the Product by anyone other than an Siemens Subscriber Networks authorized service provider.
 - The limited warranty does not cover defects in appearance, cosmetic, decorative or structural items, including framing, and any non-operative parts.

- Siemens Subscriber Networks's limit of liability under the limited warranty shall be the actual cash value of the product at the time the end user returns the product for repair, determined by the price paid by the end user for the product less a reasonable amount for usage. Siemens Subscriber Networks shall not be liable for any other losses or damages.
- The end user will be billed for any parts or labor charges not covered by this limited warranty. The end user will be responsible for any expenses related to reinstallation of the product.
- THIS LIMITED WARRENTY IS THE ONLY WARRENTY SSN MAKES FOR THE PRODUCT AND SOFTWARE. TO THE EXTENT ALLOWED BY LAW, NO OTHER WARRENTY APPLIES, WETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY WARRENTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

6. **Out of Warranty Repair.** Out of warranty repair is available for a fixed fee. Please contact Siemens Subscriber Networks at the numbers provided above to determine out of warranty repair rate. End users seeking out of warranty repair should contact Siemens Subscriber Networks as described above to obtain an RMA and to arrange for payment of the repair charge. All shipping charges will be billed to the end-user.

General Provisions

The following general provisions apply to the foregoing Software License and Limited Warranty.

1. **No Modification.** The foregoing Limited Warranty is the end user's sole and exclusive remedy and is in lieu of all other warranties, express or implied. No oral or written information or advice given by Siemens Subscriber Networks or its dealers, distributors, employees or agents shall in any way extend, modify or add to the foregoing Software License and Limited Warranty. This Software License and Limited Warranty constitutes the entire agreement between Siemens Subscriber Networks and the end user, and supersedes all prior and contemporaneous representation, agreements or understandings, oral or written. This Software License and Limited Warranty may not be changed or amended except by a written instrument executed by a duly authorized officer of Siemens Subscriber Networks.

Siemens Subscriber Networks neither assumes nor authorizes any authorized service center or any other person or entity to assume for it any other obligation or liability beyond that which is expressly provided for in this Limited Warranty including the provider or seller of any extended warranty or service agreement.

The Limited Warranty period for Siemens Subscriber Networks supplied attachments and accessories is specifically defined within their own warranty cards and packaging.

2. **EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND OTHER DAMAGES.** TO THE FULL EXTENT PERMITTED BY LAW, IN NO EVENT SHALL SSN OR ITS LICENSORS BE LIABLE, WHETHER UNDER CONTRACT, WARRENTY, TORT OR ANY OTHER THEORY OF LAW FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, PERSONAL INJURY, LOSS OR IMPAIRMENT OF DATA OR BUSINESS INFORMATION, EVEN IF SSN HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES. SSN'S OR IT'S LICENSOR'S LIABILITY TO YOU (IF ANY) FOR ACTUAL DIRECT DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION, WILL BE LIMITED TO, AND SHALL NOT EXCEED, THE AMOUNT PAID FOR THE HARDWARE/ SOFTWARE.
3. **General.** This Software License and Limited Warranty will be covered by and construed in accordance with the laws of the State of Texas, United States (excluding conflicts of laws rules), and shall insure to the benefit of Siemens Subscriber Networks and its successor, assignees and legal representatives. If any provision of this Software License and Limited Warranty is held by a court of competent jurisdiction to be a invalid or unenforceable to any extent under applicable law, that provision will be enforced to the maximum extent permissible, and the remaining provisions of this Software License and Limited Warranty will remain in full force and effect. Any notices or other communications to be sent to Siemens Subscriber Networks must be mailed by certified mail to the following address:

Siemens Subscriber Networks, Inc.
4849 Alpha Road
Dallas, TX 75244
U.S.A.
Attn: Customer Service

Table of Contents

Chapter 1 Introduction

Features of the SE565 Gateway	1
Network (LAN) Features	1
Security Features	1
Configuration & Management	2
Advanced Gateway Functions	2
Minimum System Requirements.....	2
Package Contents	2
General Safety Guidelines.....	3
Physical Details	3
Front Panel LEDs.....	3
Rear Panel	4

Chapter 2 Installation

Installing Line Filters.....	5
Hardware Installation.....	6
PC Configuration	7
Checking TCP/IP Settings (pages 9x/ME)	8
Checking TCP/IP Settings (pages 2000)	9
Checking TCP/IP Settings (pages XP).....	10
Checking TCP/IP Settings (MAC OS 8.6 through 9.x).....	11
Checking TCP/IP Settings (MAC OSX).....	12
Configure Web Browser	13
For pages 9x/2000	13
For pages XP	13
Connecting to the Gateway	14
Using UPnP (pages XP and Me).....	14
Using your Web Browser	14
Gateway Setup Wizard.....	15
Home page	17
Menu Bar.....	17
Tool Bar	18

Chapter 3 Configuring Users and Devices

Configuring Users.....	19
Adding a User	20
Editing A User Profile	24
Deleting a User	25
Viewing User Logs	25
Configuring Devices	26

Chapter 4 Configuring Advanced Features

ISP Connection.....	28
ATM Virtual Circuits	29
Static Routes	30

Dynamic DNS.....	31
RIP (Routing Information Protocol)	32
Home Network.....	33
IP Network.....	34
Server Ports	35
LAN/WAN Port	36
UPnP (Universal Plug and Play)	37
 Chapter 5 Configuring Security Features	
Firewall Settings	41
Firewall Security: Level	42
Firewall Security: Attack Detection.....	43
Firewall Security: IP Filtering.....	45
Firewall: DMZ.....	51
Firewall: Snooze Control	52
Administrator Password.....	53
Address Translation.....	54
Address Translation With NAT	55
Address Translation With NAPT	56
 Chapter 6 Miscellaneous Configuration Options	
Customize.....	58
Color Palette	59
Time Zone	60
Reboot.....	61
 Chapter 7 Monitoring Gateway Health	
Statistics	63
Internet Stats.....	64
Home Networking Stats	65
Logging	66
Diagnostics	67

Congratulations on the purchase of your new Gigaset SE565 Residential Gateway. The SE565 Residential Gateway is a multi-function device providing the following services:

- Built-in DSL modem that provides shared Internet access for multiple users.
- Four-port 10/100 Ethernet Switch for 10Base-T or 100Base-T connections.
- Custom controls provided through SpeedStream software that allow you to configure the gateway to best meet your specific security and Internet-sharing needs.

Features of the SE565 Gateway

The SE565 Gateway incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Network (LAN) Features

- **Four-Port 10/100 Ethernet Switch**
The gateway incorporates a four-port 10/100 Ethernet switch, making it easy to create or extend your network. Optionally, you can configure the fourth port as a WAN port for connection to another broadband device.
- **DHCP Server Support**
Dynamic Host Configuration Protocol (DHCP) provides a dynamic, upon request, IP address to computers and other networked devices. Your gateway can act as a DHCP Server for devices on your local network.
- **Network Status and Statistics**
Using these diagnostic tools, you can easily monitor the status of each network connection and evaluate network performance.

Security Features

- **Password Protected Configuration**
Password protection is provided to prevent unauthorized users from modifying the gateway's configuration data and settings.
- **NAT Protection**
An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all your network users to share a single IP address, the location and even the existence of each computer is hidden. From the external viewpoint, there is no network, only a single device.
- **Stateful Inspection Firewall**
All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- **Attack Protection System**
Attacks can flood your Internet connection with invalid data packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The gateway incorporates protection against these types of attacks as well as other common hacker attacks.

Configuration & Management

- **Easy Setup**
Use your Web browser for quick and easy configuration.
- **UPnP Support**
Universal Plug and Play (UPnP) allows automatic discovery and configuration of the Gigaset Gateway. UPnP is supported by pages Me, XP, or later, operating systems.

Advanced Gateway Functions

- **DMZ**
One computer on your local network can be configured to allow unrestricted two-way communication with servers or individual users on the Internet. This provides the ability to run programs that are incompatible with firewalls.
- **Firewall Snooze**
Temporarily disable firewall protection to limit interference with games and other applications incompatible with firewalls.
- **Content Filter**
Use the Content Filter to block individual user access to undesirable Web sites. Content filtering can be defined differently for each user.
- **Time of Day Use Restrictions**
Limit the time of day during which individual users have access to the Internet. Time limitations can be defined differently for each user.

Minimum System Requirements

At a minimum, your computer must be equipped with the following to successfully install the gateway. Your Internet Service Provider may have additional requirements for use of their service.

- A network interface card (NIC) that supports 10/100 Ethernet.
- Operating system that supports TCP/IP.
- Microsoft Internet Explorer or Netscape Navigator versions 5.0 or later.

Package Contents

If any of the items are damaged or missing, please contact your Internet Service Provider for assistance.

- Model SE565 Gateway
- Power adapter
- CAT-5 Ethernet cable for LAN connections
- RJ11 cable for DSL connection
- Quick Start Guide
- CD-ROM containing user documentation

General Safety Guidelines

When using the Gigaset Gateway, observe the following safety guidelines:

- Never install telephone wiring during a storm.
- Avoid using a telephone during an electrical storm. Lightning increases the risk of electrical shock.
- Do not install telephone jacks in wet locations and never use the product near water.
- Do not exceed the maximum power load ratings for the product; otherwise, you risk dangerous overloading of the power circuit.

Physical Details

Familiarize yourself with the front panel and back panel of the gateway before installing components.

Front Panel LEDs



The front panel contains the following LEDs:

Power	Off	Power is off.
	Green	Power is on.
	Flashing	Flash write in progress.
	Red	The Power LED briefly shows red during power-up. This indicates that the SpeedStream is conducting the POST (Power-On Self Test) that is run each time the SpeedStream is powered on. Post error occurred if persistent.
xDSL Port	On	DSL connection is active.
	Off	No active DSL connection.
Link	Off	No data being transmitted or received.
	Flashing	Data is being transmitted or received.
LAN 1LAN 4	On	One or more Ethernet LAN ports are active.
	Off	No active Ethernet LAN port connection.

Rear Panel



The rear panel contains the following components.

xDSL Port (RJ11)	Connect the RJ11 DSL cable (looks like a telephone cord) here to use your DSL connection through an existing phone line.
Reset	Resets the gateway to default factory settings.
Four 10/100 Ethernet Ports	Connect the RJ45 Ethernet cable here to connect your computers, hubs, or switches to the router. You can configure port #4 as either a LAN or WAN port.
Power	Connect the supplied power adapter provided with the router here.
Power Button	Push this button to power the router on and off.

This chapter describes the steps you must take to install and configure the various components in your network to utilize the Siemens Residential Gateway. This includes [installing line filters](#), [setting up the hardware connections](#) to the Internet gateway, [configuring the PC](#) to use the Internet gateway for Internet access, [connecting to the gateway](#), and [setting up the gateway configuration](#).

Before you attempt the procedures in this chapter, ensure that you have the following minimum system requirements.

- DSL service and an Internet access account from an Internet Service Provider (ISP).
- Network cables for each device you intend to connect to the gateway.
- TCP/IP network protocol must be installed on all computers.

Note: Your configuration may vary slightly from the instructions and illustrations in this chapter. Refer to your service provider's documentation, or contact them with questions regarding your specific configuration.

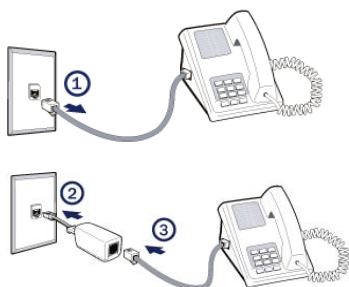
Installing Line Filters

Because DSL shares your telephone line, you may need to separate the two signals so they do not interfere with each other. A line filter (may be included with some models) prevents DSL traffic from disrupting the voice signal on the telephone line, and vice versa. Follow the procedures below to install line filters on any device (telephones, fax machines, caller ID boxes) that shares the same telephone line with your DSL. (Note, this section may not apply to you. Consult your provider if you are unsure.)

There are two types of filters to connect between the telephone and the wall plate:

- *In-line filter:* For use with standard desktop telephones.
- *Wall-mount filter:* For use with wall-mounted telephones.

DSL performance may be significantly degraded if the line filters are not installed in the correct direction, as illustrated below.



In-Line Filter

For each device sharing the same telephone line:

1. Unplug the device's cord from the telephone jack.
2. Plug the filter into the telephone jack.
3. Plug the telephone cord (or other device cord) into the filter.



Wall-Mount Filter

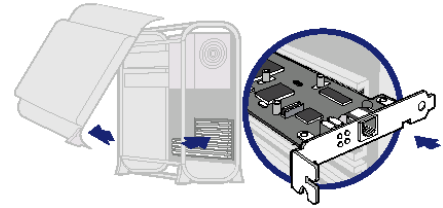
For a wall-mounted telephone, install a wall mount filter:

1. Remove the telephone.
2. Connect the wall mount filter to the wall plate.
3. Reconnect the telephone.

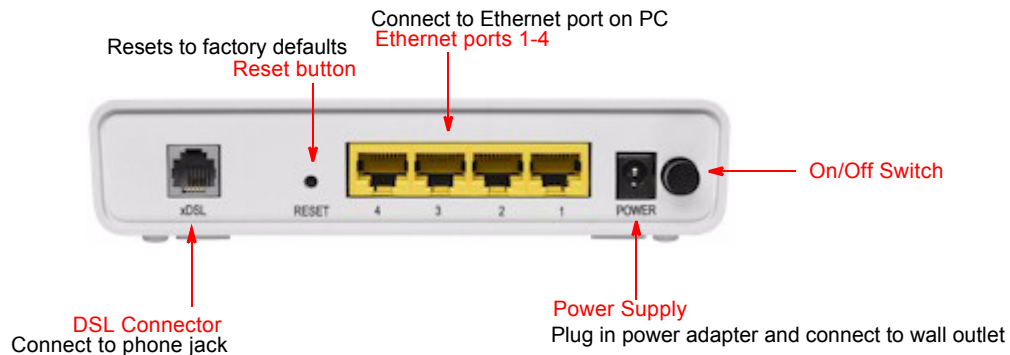
Hardware Installation

You may position the Gigaset Gateway at any convenient location in your office or home. No special wiring or cooling requirements are needed; however, you should comply with the safety guidelines specified in the [General Safety Guidelines](#) section.

You can connect the gateway to an existing Ethernet port on your computer. To connect the Gigaset device via the Ethernet interface, your computer must have an Ethernet adapter (also called a network interface card, or NIC) installed. If your computer does not have this adapter, install it before proceeding further. Refer to your Ethernet adapter documentation for complete installation instructions. Once you verify installation of an Ethernet adapter, perform the following procedure to connect the gateway to your computer.



The Gateway is connected to the PC and the Internet through cable connections on the back of the device.



1. With the PC powered off, connect one end of the RJ-45 cable to any of the Gigaset device's Ethernet ports on the back-panel and the other end of the Ethernet cable to the Ethernet port on the PC.
2. Connect the DSL cable (resembles a telephone cord) to the DSL port on the rear of the gateway. To reduce the risk of fire, use only 26 AWG gauge telecommunication cord to connect your DSL port on your gateway to a DSL telephone jack.
3. Connect the power adapter to the rear of the gateway and plug it into an electrical wall outlet.
4. Turn the modem on using the On/Off switch.
5. Power on all connected computers.

You can now configure the TCP/IP settings as detailed in the [PC Configuration](#) section.

PC Configuration

This section explains how to configure your personal computer to work with the gateway.

To access the Internet through the Gigaset Gateway, your PC must be configured to use the TCP/IP protocol suite over the Internet, and to accept Dynamic Host Configuration Protocol address assignments from the gateway.

The default network settings for the Gigaset Gateway are:

IP Address:192.168.254.254

Subnet Mask:255.255.255.0

By default, the gateway will act as a DHCP server, automatically providing a suitable IP address and related information to each computer when the computer boots up. For all non-server versions of pages, the TCP/IP setting defaults to act as a DHCP client. (If using the default gateway settings and the default pages TCP/IP settings, you do not need to make any changes.)

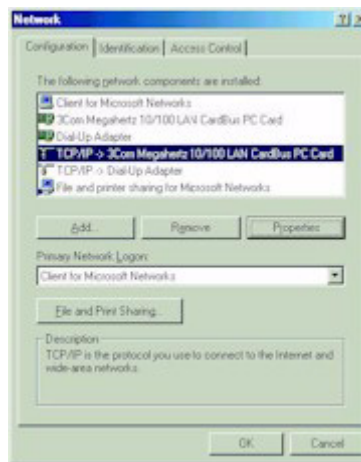
Although these are the default settings for the PC, it is a good idea to verify that they have not been changed. If TCP/IP is not already installed on your computer, refer to your system documentation or online help for instructions. Once installed, you should check the TCP/IP protocol settings to make sure they are correct for use with the gateway.

The instructions to check TCP/IP protocol settings differ between operating system. Check the settings using the instructions for your operating system:

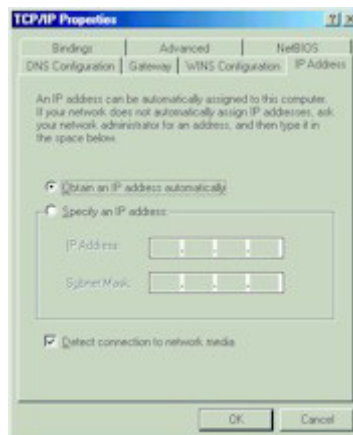
- [Checking TCP/IP Settings \(pages 9x/ME\)](#)
- [Checking TCP/IP Settings \(pages 2000\)](#)
- [Checking TCP/IP Settings \(pages XP\)](#)
- [Checking TCP/IP Settings \(MAC OS 8.6 through 9.x\)](#)
- [Checking TCP/IP Settings \(MAC OSX\)](#)

Checking TCP/IP Settings (pages 9x/ME)

1. Click **Start >Control Panel > Network**. This displays the Configuration tab on the Network page.



2. Select **TCP/IP** protocol for your network card.
3. Click **Properties**. This displays the TCP/IP Properties page. Click the **IP Address** tab.

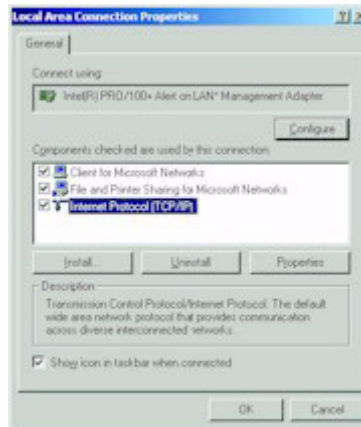


4. Ensure that the **Obtain an IP address automatically** option is selected. This is the default pages setting.
5. Click **OK** to close each dialog.
6. Restart the PC to ensure it obtains an IP address from the router.
7. Configure internet access using the procedure described in [Configure Web Browser](#).

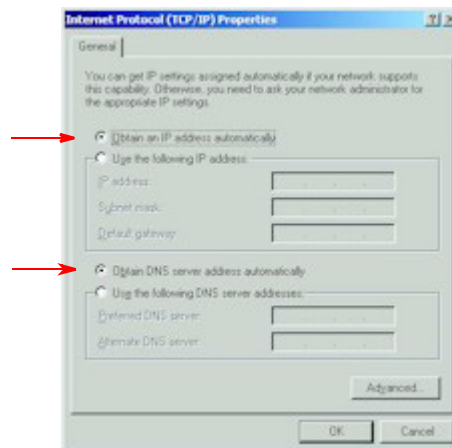
Checking TCP/IP Settings (pages 2000)

To configure pages 2000 to communicate through the Gigaset router:

1. Select **Start >Settings >Control Panel**. This displays the Control Panel page.
2. Double-click the **Network and Dial-up Connection** icon. This displays the Network and Dialup Connection page.
3. Right-click **Local Area Connections** and select **Properties**. This displays the Local Area Connections Properties page.



4. Select Internet Protocol (TCP/IP) from the list of components.
5. Click **Properties**. This displays the Internet Protocol (TCP/IP) Properties page.

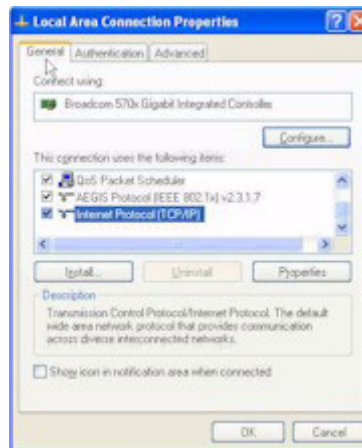


6. Ensure that the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options are selected.
7. Click **OK** to close each dialog.
8. Restart the PC to ensure it obtains an IP address from the router.
9. Configure internet access using the procedure described in [Configure Web Browser](#).

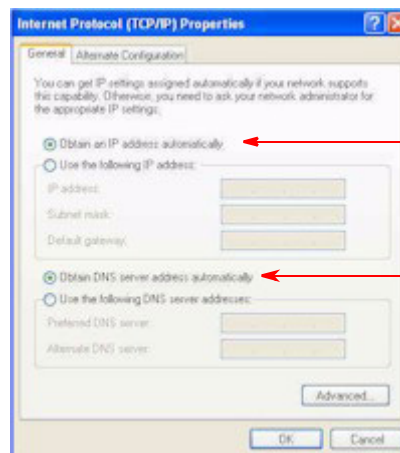
Checking TCP/IP Settings (pages XP)

To configure pages XP to communicate through the Gigaset router:

1. Click **Start >Settings>Network Connections** icon, then right-click **Local Area Connection** and select **Properties**. This displays the Local Area Connection Properties page.



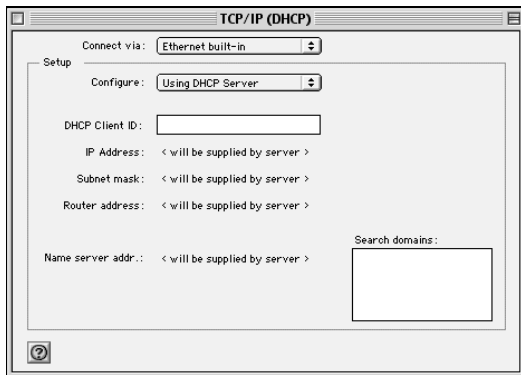
2. Select **Internet Protocol TCP/IP** (you may have to scroll down) and click **Properties**. This displays the Internet Protocol (TCP/IP) Properties page.



3. Ensure the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options are selected.
4. Restart the PC to ensure it obtains an IP address from the router.
5. Configure internet access using the procedure described in [Configure Web Browser](#).

Checking TCP/IP Settings (MAC OS 8.6 through 9.x)

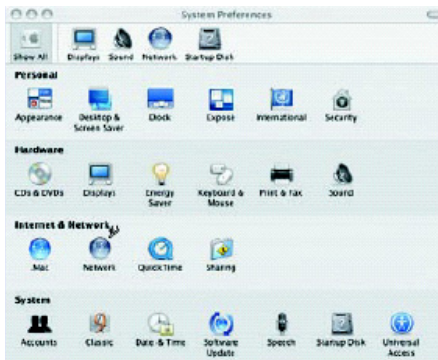
1. Select **Apple >Control Panel >TCP/IP**. This displays the TCP/IP page.



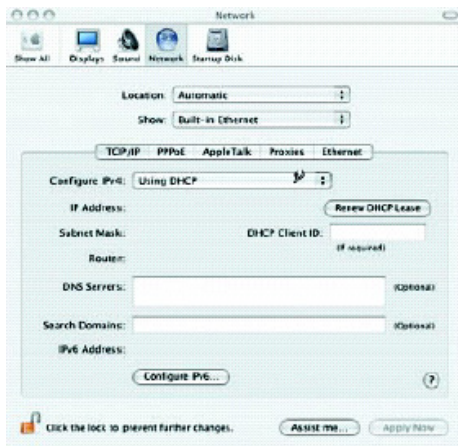
2. Select one of the following from the **Connect via** drop-down menu.
 - **Ethernet** or **Ethernet built-in** if connecting via Ethernet.
 - **Ethernet Adaptor [en0,en1,...]** if connecting via USB.
3. Select **Using DHCP Server** from the **Configure** drop-down menu.
4. Close the TCP/IP page and click **Save**.
5. Reboot when configuration is saved. Once rebooted, the computer will pull an IP address from the DHCP server on the gateway.
6. Configure the gateway using the procedure described in [Gateway Setup](#).

Checking TCP/IP Settings (MAC OSX)

1. Click **Apple -> System Preferences**. This displays the System Preferences page.



2. Double-click the **Network** icon under the **Internet & Network** section. This displays the Network page.



3. Select one of the following from the **Show** drop-down menu:
 - **Built-in Ethernet** if connecting via Ethernet.
 - **Ethernet Adaptor [en0,en1,...]** if connecting via USB.
4. Select **Using DHCP Server** from the **Configure IPv4** drop-down menu.
5. Click **Apply Now** and quit page.
6. Configure the gateway using the procedure described in [Gateway Setup](#).

Configure Web Browser

pages users must configure their Web browser to access the Internet via the Gateway rather than by a dial-up connection. Ensure that the gateway is installed correctly and the DSL line is functional. Then follow the appropriate procedure below for your operating system.

For pages 9x/2000

1. Select **Start>Settings>Control Panel** to display the Control Panel.
2. Double-click the **Internet Options** icon. This displays the Internet Properties page.
3. Click the **Connections** tab.
4. Click **Setup**.
5. Click **I want to set up my Internet connection manually**, or **I want to connect through a local area network (LAN)**, then click **Next**. This displays the Internet Connection Wizard page.
6. Click **I connect through a local area network (LAN)**, then click **Next**. This displays the Local Area Network Internet Configuration page.
7. Ensure all the boxes are deselected, then click **Next**. This displays the Set Up your Internet Mail Account page.
8. Click **No**, then click **Next**. This displays the Completing the Internet Connection Wizard page.
9. Click **Finish** to close the Internet Connection Wizard. Setup is now complete.
10. Configure the gateway using the procedure described in [Gateway Setup](#).

For pages XP

1. Select **Start>Settings>Control Panel**.
2. Double-click the **Internet Options** icon. This displays the Internet Options page.
3. Click the **Connections** tab.
4. Click **Setup**. This starts the **New Connection Wizard**.
5. Click **Next**.
6. Select **Connect to the Internet**, then click **Next**.
7. Select **Setup my connection manually**, then click **Next**.
8. Select **Connect using a broadband connection that is always on**, then click **Next**.
9. Click **Finish**.
10. Configure the gateway using the procedure described in [Gateway Setup](#).

Connecting to the Gateway

You can connect to the Gateway using [UPnP](#) (if it is enabled on your computer) or through the [Web browser](#).

Using UPnP (pages XP and Me)

If your pages operating system supports UPnP (Universal Plug and Play) and UPnP is enabled, an icon for the Gigaset Gateway appears in the system tray near the time display, notifying you that a new network device has been found and offering to create a new desktop shortcut to the newly discovered device.

Note: You must be logged in as administrator or be a user with administrative rights for pages 2000 and XP to be able to install the drivers for the gateway.

1. Unless you intend to change the IP address of the gateway, you can accept the desktop shortcut. Whether you accept the desktop shortcut or not, you can find UPnP devices in **My Network Places** (previously called Network Neighborhood).
2. Double-click the icon for the gateway (either on the desktop or in **My Network Places**) to access the gateway's configuration program.
3. Refer to the [Gateway Setup Wizard](#) section for details of the initial configuration process.

Using your Web Browser

The Gigaset Gateway contains an HTTP server that allows you to connect to the gateway and configure it from your Web browser (Microsoft Internet Explorer or Netscape Navigator, versions 5.0 or later).

To establish a connection from your computer to the gateway:

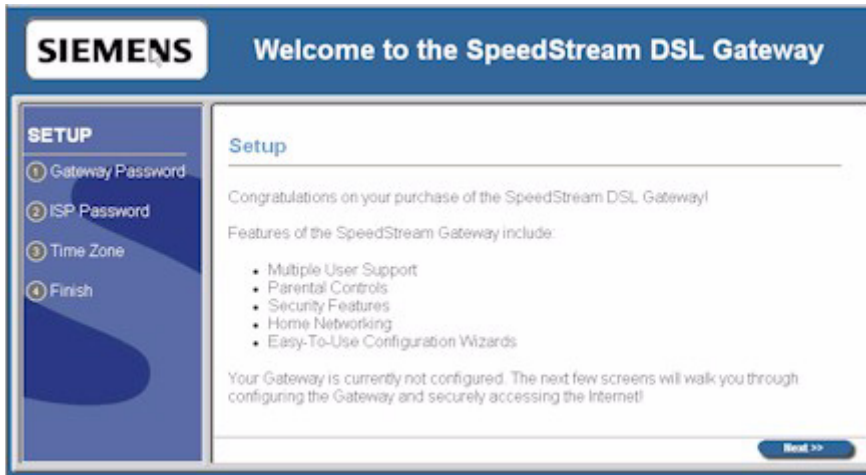
1. After installing the gateway, start your computer. If your computer is already running, reboot it.
2. Open your Internet Explorer or Netscape Navigator Web browser.
3. In the **Address** bar, type **192.168.254.254** and press the **Enter** key. This displays the Setup page.
4. Refer to the [Gateway Setup Wizard](#) section for details of the initial configuration process.

Gateway Setup Wizard

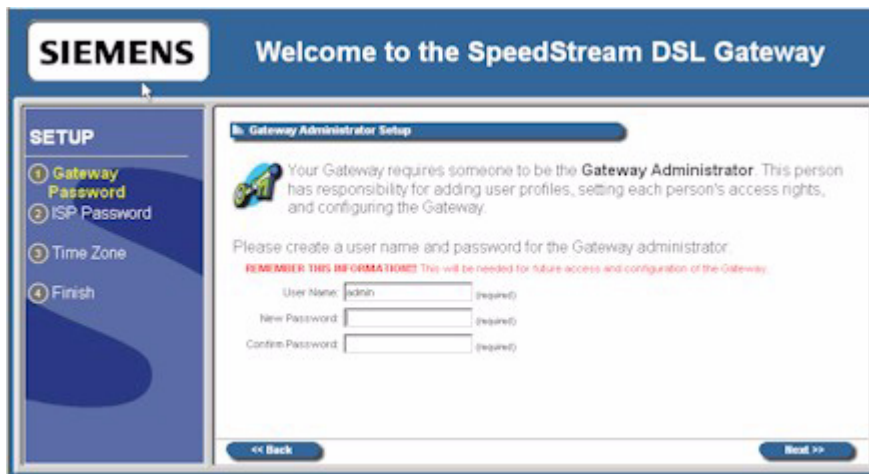
The first time you connect to the gateway, the Setup Wizard runs automatically. (The Setup Wizard also runs if the gateway's default settings are restored.) Proceed through the entire Setup Wizard to ensure accuracy of the installation.

Note: You will need to know the username and password for Internet service provided by your ISP. Check the information supplied by your ISP for details.

1. The first page of the Setup Wizard is the **Setup** page.



2. Click **Next** on the Setup page to begin setup. This displays the Gateway Administrator Setup page.



3. An administrator account has access rights to the gateway configuration pages. Optionally, change the admin user name to a different administrative name by typing the new administrative name in **User Name**. If you wish, simply leave the admin user name in **User Name**.
4. Type a password in **New Password** and re-type it in **Confirm Password**.

5. Click **Next**. This displays the ISP Password page.

6. Enter information as specified by your ISP.
7. Click **Next**. This displays the Configure Time Zone page.

Optionally set the time zone of the area of the world in which you live on the Configure Time Zone page. This option must be enabled to define time of day restrictions for users.

8. To set the time zone, select the **Yes** option for **Enable Time Client**.
9. Select your time zone from the **Select Time Zone** drop-down menu, then click **Next**. This displays the Finish page.
10. On the Finish page, click **Finish**. This displays the What do I do now? page. From this page you may click one of the following:
 - **Surf Now:** Your Web browser re-directs you to default home page of the Web browser you are using. You may return to the gateway's configuration interface at anytime should you choose to further configure the gateway.
 - **Continue:** Displays the [Home page](#) where you can create usage profiles/rules for different users, change the level or type of security used on the gateway, or define/configure your network to be managed by the gateway.

Home page

After finishing the Setup Wizard and clicking **Configure**, the Home page appears. This page also appears from now on when connecting to the gateway.



At the top of the Home page are two areas that provide access to the GUI: the [Menu Bar](#) and the [Tool Bar](#). Additionally, the Home page displays basic networking attributes of the modem including IP address and default gateway specifications.

Menu Bar

The Menu Bar contains two items: the Log In drop-down menu and the Help option.

Help

The **Help** option is used to display a help system for the gateway. Click the **Help** hyperlink to access help.

Log In Drop-down Menu

The **Log In** drop-down menu is used to log in or log out as a user or administrator. There are two types of primary users that log into the gateway: administrators and users. Administrators have rights to all of the configuration options available on the gateway. Users have limited access based on what is set by the administrator for each user. Pay special attention to **Login** in the top left-hand corner of the page to ensure that you are logged in to access all available features.



To log on to the gateway:




1. Select a user from the **Log In** drop-down menu.
2. Select a user from the **Username** drop-down menu.
3. Type the user password in **Password**.
4. Click **Go**. This displays the Home page.

To log out of the gateway, click **GO** next to **Log Out**. The system responds by displaying the Home page.



Tool Bar

Below the Menu Bar is a Tool Bar that contains a set of buttons to access various configuration and information pages on the Gateway: Users, Devices, Gateway.

	<p>Users Button: This button provides access to user profiles and the User Profile Wizard. This wizard guides you through the steps required to set up and configure individual user profiles. Once configured, you can use this option to view a user's profile.</p>
	<p>Devices Button: This button provides Access to network devices connected to the gateway. You can use this option to view shared files and resources on other computers if they are shared via pages File Sharing.</p>
	<p>Gateway Button: This button provides access to all gateway configuration options, security settings, gateway health monitoring, and Internet connection and network details. The settings available may differ depending upon your service provider.</p>

In the left navigation pane there is a set of configuration options for the selected Tool Bar button. These options differ depending on how a user is logged into the system. An administrator has full configuration rights (shown above), while a user has limited configuration rights.

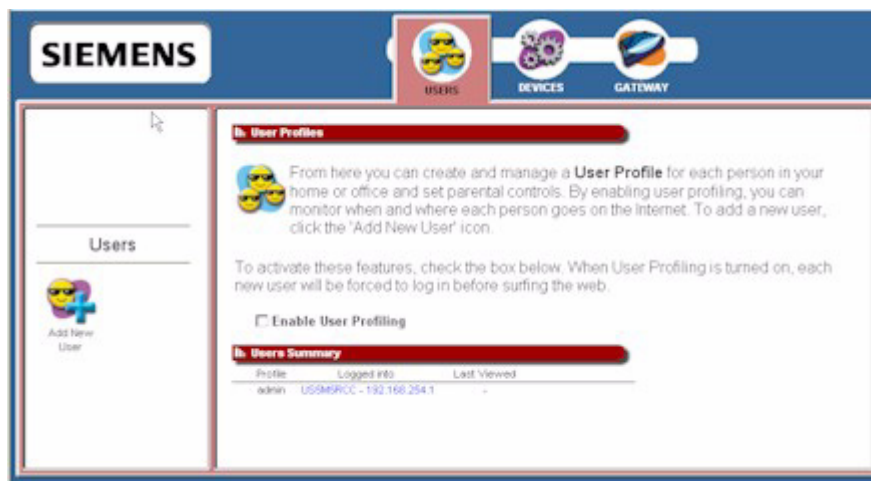
How to use the configuration screens provided with each button set is described in the following chapters:

- Refer to [Chapter 3, "Configuring Users and Devices"](#) for details on configuring users.
- Refer to [Chapter 3, "Configuring Users and Devices"](#) for details on configuring devices.
- Refer to [Chapter 4, "Configuring Advanced Features"](#) for details on configuring advanced features on the Gateway.

This chapter contains details for configuring users and devices on the gateway. This chapter is organized into two parts corresponding to the buttons in the tool bar: [Users](#) and [Devices](#).

Configuring Users

Users are added and maintained from the User Profiles page accessed by clicking the **Users** button on the tool bar. The User Profiles page provides details about all active user profiles, if **Enable User Profiling** is selected.



The **Enable User Profiling** option must be selected on the User Profiles page for the content filtering option to be operational.

Adding a User

This section describes how to add users to the gateway to restrict their access to gateway functions and to the Internet. You **MUST** be logged in as the administrator to add a user.

To add a user:

1. From the [User Profiles](#) page, click the **Add New User** button in the left navigation pane. This displays the Profile User Information page.

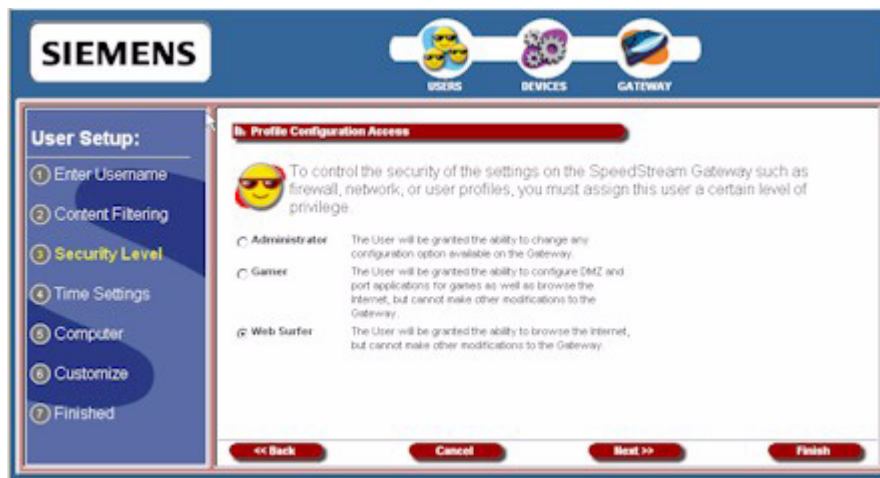
2. Type a user name in **Username**.
3. Type a password in **Password**.
4. Re-type the password in **Confirm**.
5. Click **Next**. This displays the Profile Content Filtering page. (At any time during user configuration, you can click **Finish** to complete the user profile and accept the defaults for this user.)

Content filtering restricts access to undesirable Web sites and Web content. The **Enable User Profiling** option must be selected on the [User Profiles](#) page for the content filtering option to be operational.

6. Select one of the following content filtering options:
 - **Disable all Content Filtering**
User has access to all Internet content without restrictions.
 - **Allow access only to website addresses containing the following words**
User has access only to the specified Web addresses or to addresses containing specified word entries defined in the Website word/name table.
 - **Deny all access to website addresses containing the following words**
User is denied access to all Web addresses specified as well as addresses that contain any words specified in the Website word/name table.
7. If the **Allow access only...** or **Deny all access...** option is selected, type a word or Web address in the box under the Website word/name table, then click **Add Entry**. The system responds by adding the word or Web address to the Website word/name table.

Note: The entries in the Website word/name table may be either modified or deleted at any time by clicking either **Edit** or **Delete** next to the corresponding word or Web address.

8. Click **Next**. This displays the Profile Configuration Access page. Profile configuration access defines the access permission for a user controlling what functions and features are available to that user.



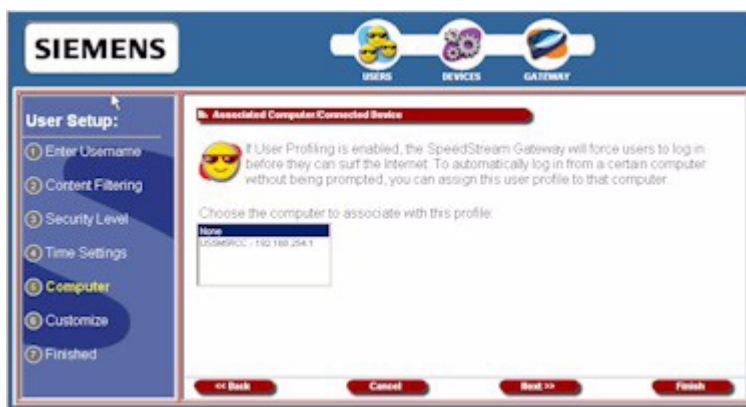
9. Select one of the following profiles and click.
 - **Administrator**
User has access to the Internet and all of the configuration tools on the gateway.
 - **Gamer**
User has access to the Internet as well as the gateway's commonly used tools for gamers, including Port Configuration and DMZ.
 - **Web Surfer**
User has access only to the Internet, not to the gateway's configuration.

10. Click **Next**. This displays the Profile Time Setting page.



Profile time settings are used to limit a user's ability to use the Internet during certain times of the day or night. You can also define the amount of time a user stays logged on to the Internet without Web surfing activity (Idle Time). To use the time of day restrictions, you must have the Time Client enabled. Please see the [Gateway Setup Wizard](#) section for more information.

11. Select one of the following time of day options to control the time of day a user can access the internet:
- **No time of day restrictions**
The user can access the Internet at any time.
 - **Only allowed from**
The user can only access the Internet at the time range set in the time drop-down menus. Be sure to specify the **from** and **until** times the user can access the Internet.
12. Select one of the following options to designate the number of minutes a user can sit idle before they are automatically logged out from the web:
- **Infinite Time**
The user is never automatically logged out of the Internet.
 - **Minutes**
Type a time interval in minutes in **Minutes**. This time represents how long a user may be idle before automatically being logged out of the Internet.
13. Click **Next**. This displays the Associated Computer/Connected Device page.

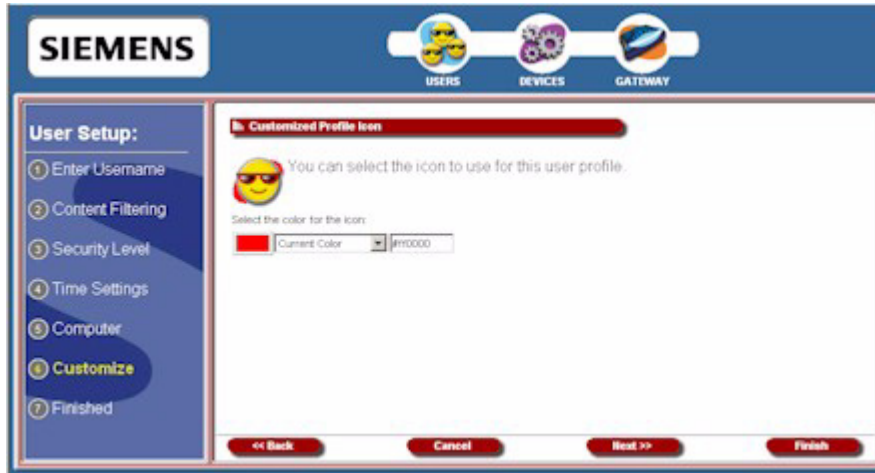


Some users consistently use a particular computer to surf the Internet. To simplify logging in for these users, you can use the Associated Computer option to automatically log a particular user into the gateway with their username and password when they access the Internet from the specified computer.

14. Select one of the following:

- A specific device to associate with the profile. All computers and devices currently on the network, powered on, and detected by the gateway are displayed in the computer list.
- **None.** The user can log in from any device.

15. Click **Next**. This displays the Customized Profile Icon page.



All user profiles have an icon that displays in the left navigation pane of the User Profiles page. You may customize the color of this icon using the Customized Profile Icon page.

16. To select a color, do one of the following:

- Select a color from the drop-down menu.
- Type a numeric color value in the box next to the color drop-down menu. The number is based on RGB (Red Green Blue) values. For example, the color red is represented by a value of ff0000, green is represented by a value of 00ff00, and blue is represented by a value of 0000ff. **Note:** If you are entering a numeric value for the color, ensure that the # is in front of your numeric value.

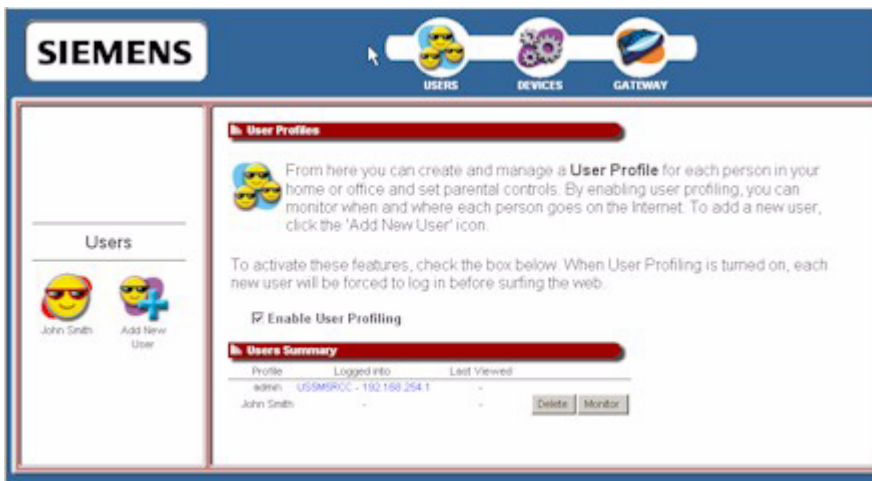
17. Click **Finish**. This displays the User Profile page. The icon of the user you just created is displayed in the left navigation pane.

Editing A User Profile

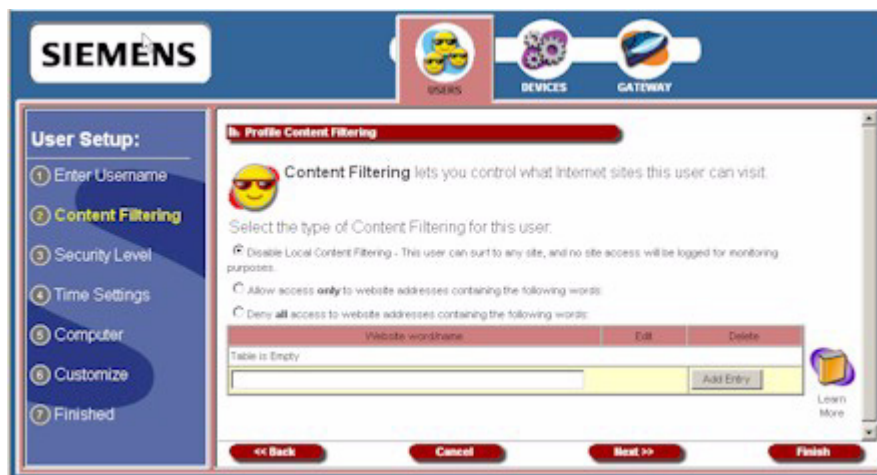
This section describes how to edit a user profile. You must be logged in as the administrator to edit a user profile.

To edit a user profile:

1. From the [User Profiles](#) page, click the button in the left navigation pane corresponding to the user you want to edit. This displays the Profile Monitor page.



2. Click **Edit Profile**. This displays the Profile Content Filtering page with the **User Setup** pane in the left navigation pane.



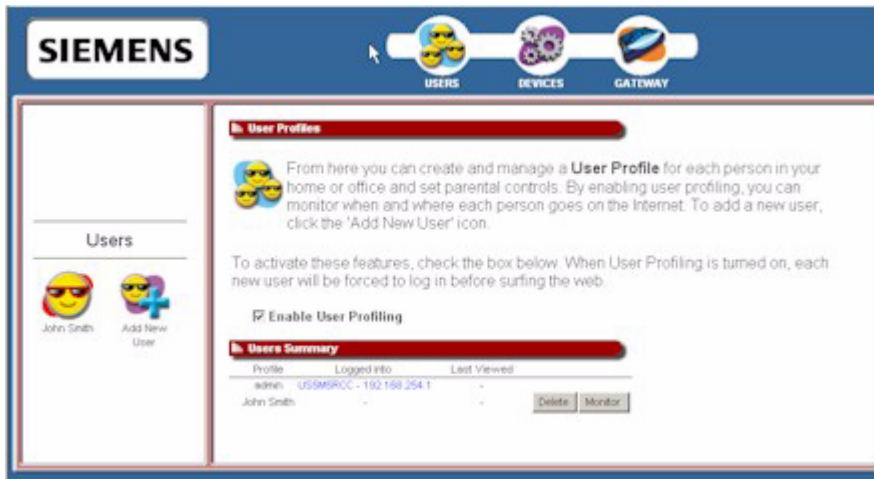
3. Click on any item in the **User Setup** list to display the appropriate page.
4. Make any changes.
5. Once you have made all the changes you want, click **Finish**.

Deleting a User

This section describes how to delete a user. You must be logged in as the administrator to delete a user.

To delete a user:

1. From the [User Profiles](#) page, click the button in the left navigation pane corresponding to the user you want to delete. This displays the Profile Monitor page.



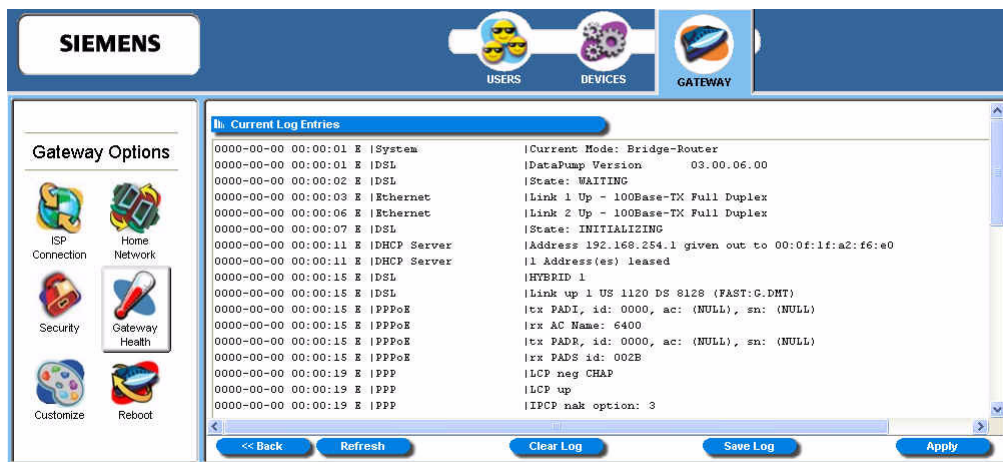
2. Click **Delete User**.

Viewing User Logs

User logs provide time stamped information about the activity of the user over the network.

To view user logs:

1. From the [User Profiles](#) page, click the button in the left navigation pane corresponding to the user you want to delete. This displays the Profile Monitor page.
2. Click **View User Log**. This displays the Current Log Entries page displaying all the log information about the user.

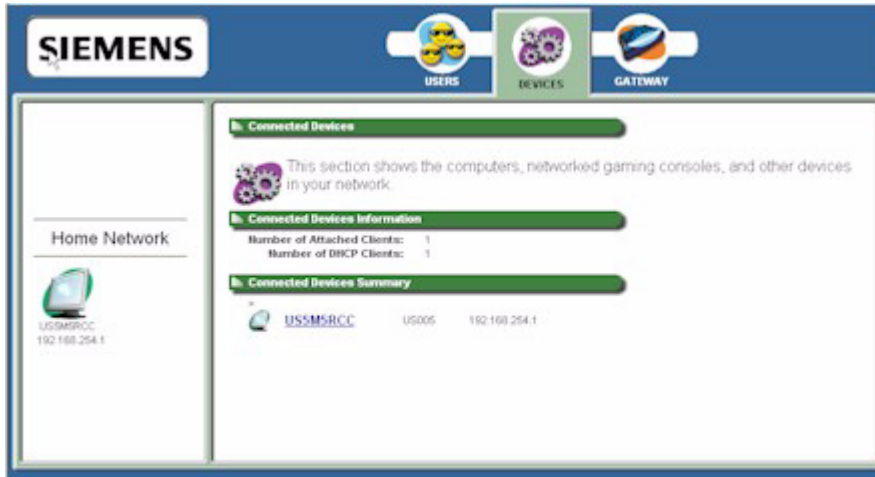


Configuring Devices

The Devices option allows you to view devices connected to your gateway. If you are logged in as the administrator, you can view all the connected devices to the gateway. If you are logged in as a specific user, you can only view devices associated with that user login.

To use the Devices option:

1. Click **Devices** in the tool bar. This displays the Connected Devices page displaying general information about devices on your network.

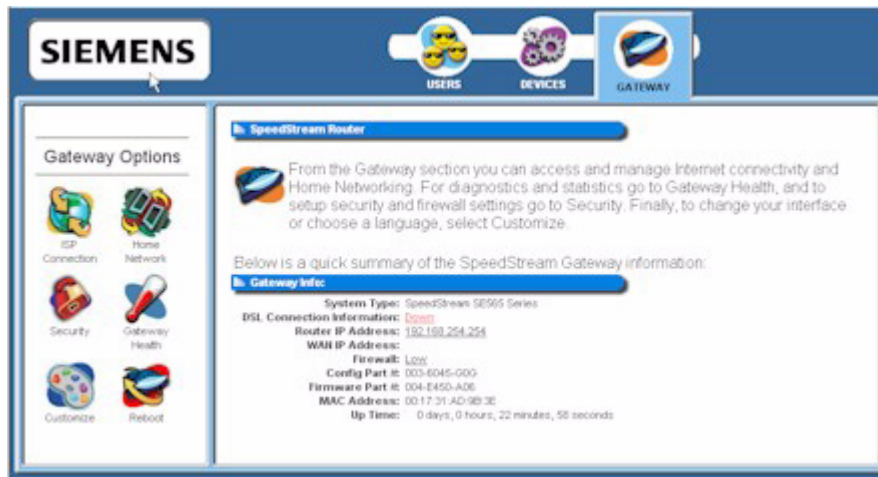


2. Click the icon of a connected device in the left navigation pane, or click the device hyperlink under **Connected Devices Summary**. This displays the Connected Devices page, which displays both general and network information about the selected device.

Configuring Advanced Features

This chapter contains details for configuring the many advanced features available with your gateway. Some of the features described below require at least a mid-level understanding of networking principles. These features are provided to allow configuration flexibility for advanced users.

These advanced features are accessed through the **Gateway** button available on the tool bar on the Main page. The options that display under the **Gateway Options** pane in the left navigation pane are based on how you logged into the system. If you logged in as the administrator, all options are turned on and enabled. If you logged in as a user, only the Gateway Health, Customize, and Reboot options are enabled.



This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Options** panel.



Get information about your [ISP connection](#). You can also use this option to set ISP configuration parameters. This should only be done when instructed by your ISP.

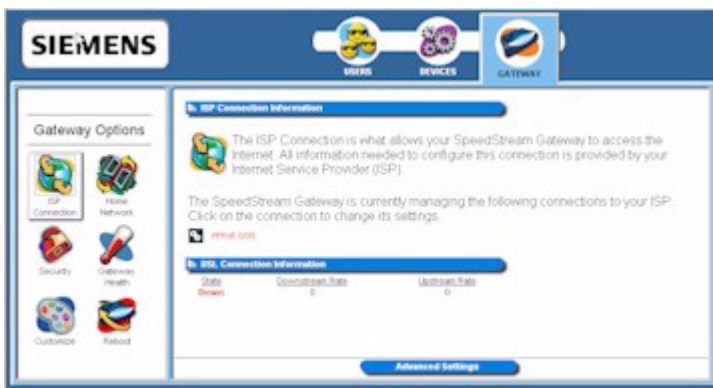


View and configure [network-related](#) information.

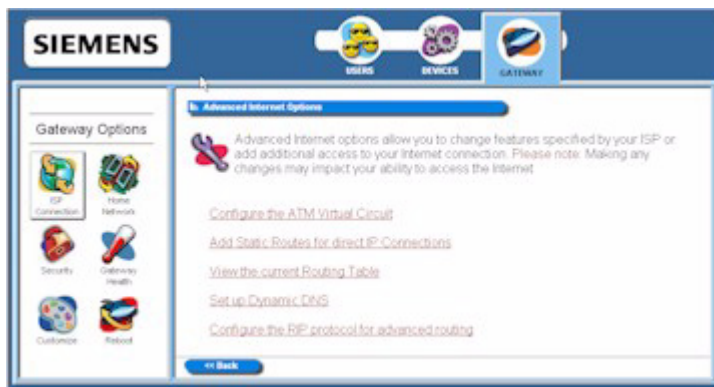
ISP Connection

The **ISP Connection** option displays all active and available Internet connections. Many of the settings for this option are intended for use only by advanced users. This option may not be available depending on your ISP. You must be logged in as an administrator to use this option. To use the ISP connection function:

1. Click the **ISP Connection** button in the left navigation pane. This displays the ISP Connection Information page listing all the ISP connections being managed by the gateway.



2. Click one of the ISP connections (in red) to reconfigure that connection. This displays the Advanced Internet Options page.



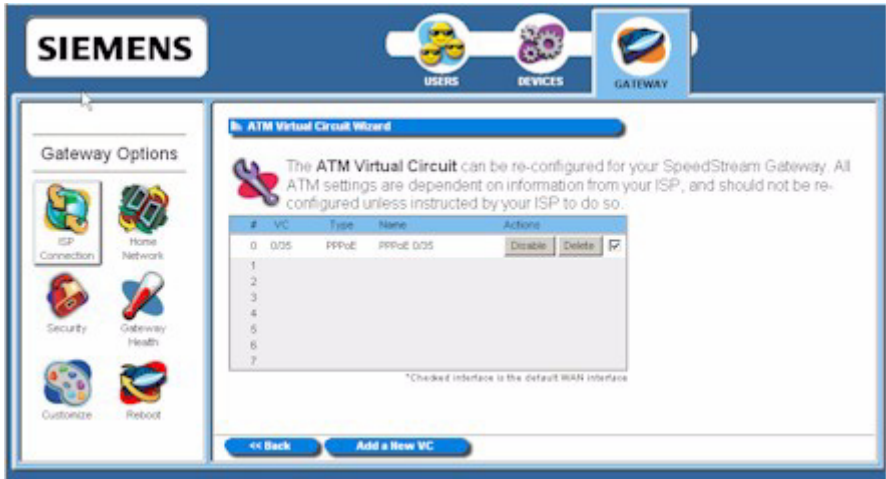
All the advanced options in this section should only be configured with the help and guidance of your ISP. Incorrect changes to any of these options could result in the failure of your Internet connection. To access one of these options, click its link on the Advanced Internet Options page.

Configure the ATM Virtual Circuits	Create/configure a PVC (Permanent Virtual Circuit) across a network. A PVC is used to maintain a permanent connection between two points on a network.
Add Static Routes for direct ISP Connections	Configure static routes to remote equipment. Static routing allows a pre-defined route to be set for the transmission of data.
Set up Dynamic DNS	Set up dynamic DNS. Dynamic DNS translates IP addresses into alphanumeric names.
Configure the RIP protocol for advanced routing	Configure the protocol that allows the gateway to determine the shortest path between two points on the network.

ATM Virtual Circuits

Use the ATM virtual circuit advanced option to create and configure a Permanent Virtual Circuit (PVC). A PVC is used to maintain a permanent connection between two points on a network. Changes to ATM settings should not be made unless you are advised to do so by your Internet Service Provider.

To access the ATM virtual circuit option, click the **Configure ATM Virtual Circuit** hyperlink on the [Advanced Internet Options](#) page. This displays the ATM Virtual Circuit Wizard page.



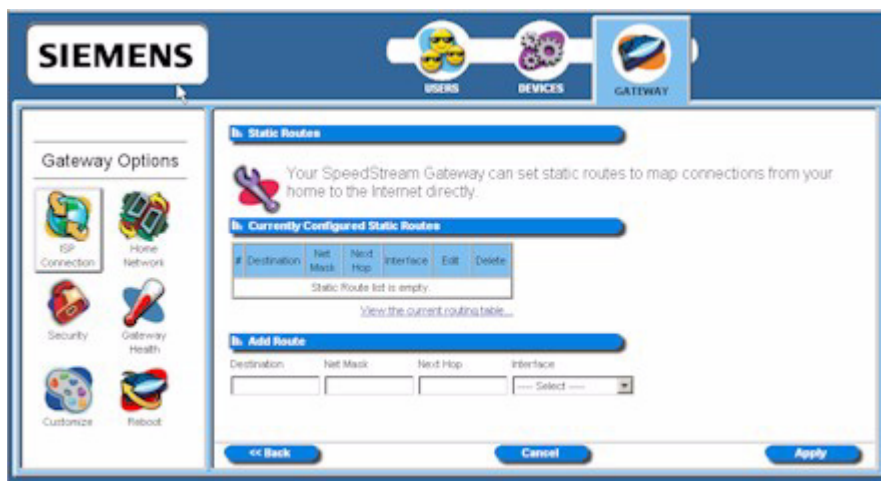
Make any modifications advised by your ISP.

Static Routes

Use the static routes advanced option to configure static routes to remote equipment. Static routing allows a pre-defined route to be set for the transmission of data. Static routes take precedence over all dynamic routing options and also provide enhanced security over dynamic routing.

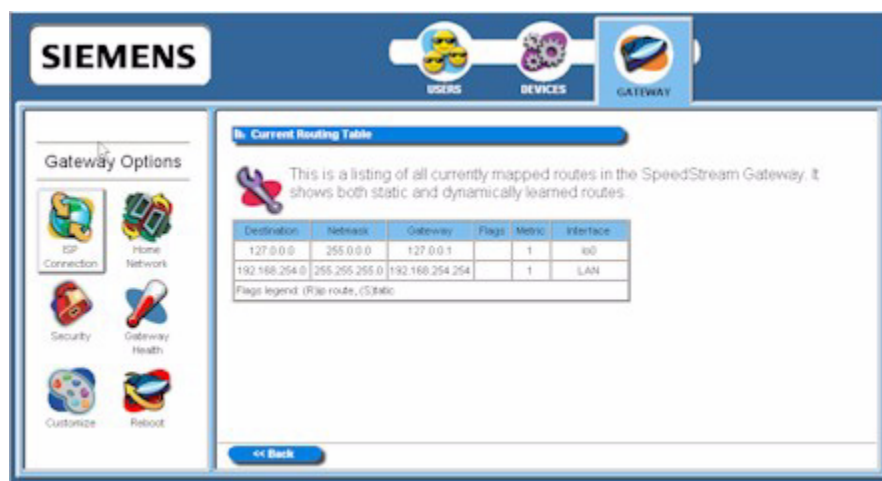
To configure the static routes:

1. Click the **Add Static Routes for Direct IP Connections** hyperlink from the [Advanced Internet Options](#) page. This displays the Static Routes page.



2. Type the IP address of the destination device in **Destination**.
3. Type the net mask of the destination device in **Net Mask**.
4. Optionally, type the IP address of a destination gateway in **Next Hop**.
5. Select a connection type from the **Interface** drop-down menu.
6. Click **Apply**. The system responds by adding your new route to the routing table.

To view the current routing table, click the **View the current routing table** hyperlink. This displays a table of routing information including destination IP address, subnet mask, flags, Gateway, metric and interface of all static and dynamic routes for network devices.



Dynamic DNS

Use the dynamic DNS advanced option to set up dynamic DNS. Dynamic DNS translates IP addresses into alphanumeric names. For example, an IP address of 333.136.249.80 could be translated into siemens.com. To use the DDNS service, you must register for the service. You can register from the following web page: www.dydns.org/services/dydns.

Once registered, you must set up your DNS data on the gateway. Once this is done users can connect to your servers (or DMZ computer) from the Internet using your Domain name. Refer to the section in this document titled [Firewall: DMZ](#) for more information on DMZs.

To set up Dynamic DNS on the gateway:

1. Click the **Set up Dynamic DNS** hyperlink from the [Advanced Internet Options](#) page. This displays the Set Up Dynamic DNS page.

2. Select the **Enable** option.
3. Type the name provided to you by www.dydns.org in **Service Username**.
4. Type your www.dydns.org password in **Password**.
5. Type the domain or host name provided by www.dydns.org in **Host Name 1**.
6. Optionally, if you have more than one domain or host name, type it in **Host Name 2**.
7. Click **Apply**. The system responds by registering your domain or host name to www.dydns.org.

RIP (Routing Information Protocol)

Using RIP, the gateway is able to determine the shortest distance between two points on the network based on the addresses of the originating devices. RIP (Routing Information Protocol) is based on distance algorithms to calculate the shortest path. The shortest path is based on the number of hops between two points.

To use the RIP option:

1. Click the **Configure the RIP protocol for advanced routing** hyperlink from the [Advanced Internet Options](#) page. This displays the RIP Configuration page.

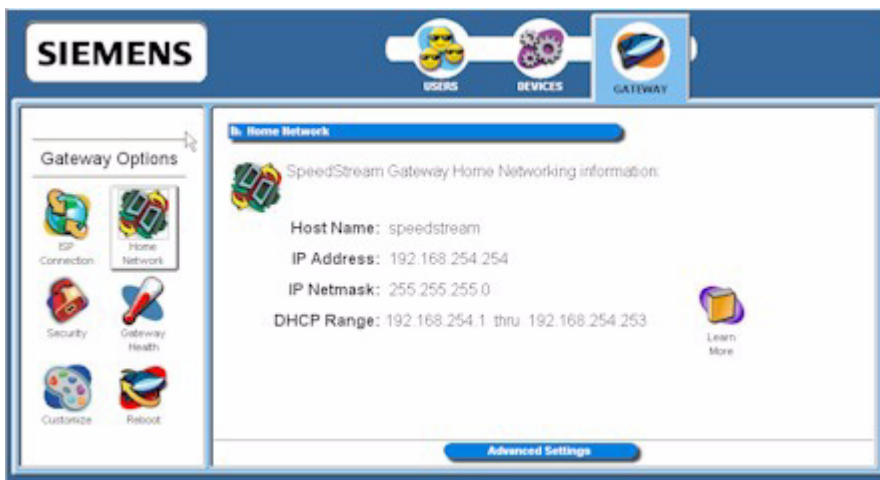


2. Select one of the following options from under the **RIP Version** heading next to the connection of your choice:
 - **1:** Provides essential RIP packet formatting for routing information packets.
 - **2:** Provides enhanced packet formatting for routing information packets by providing the following: IP address, subnet mask, next hop, and metric (shows how many gateways the routing packet crossed to its destination).
 - **1&2:** A combination of both types of RIP packets.
3. Select an **Active Mode** checkbox next to a corresponding connection to enable it.
4. Click **Apply**. This displays the Your Settings Have Been Saved page.
5. Optionally, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your gateway.

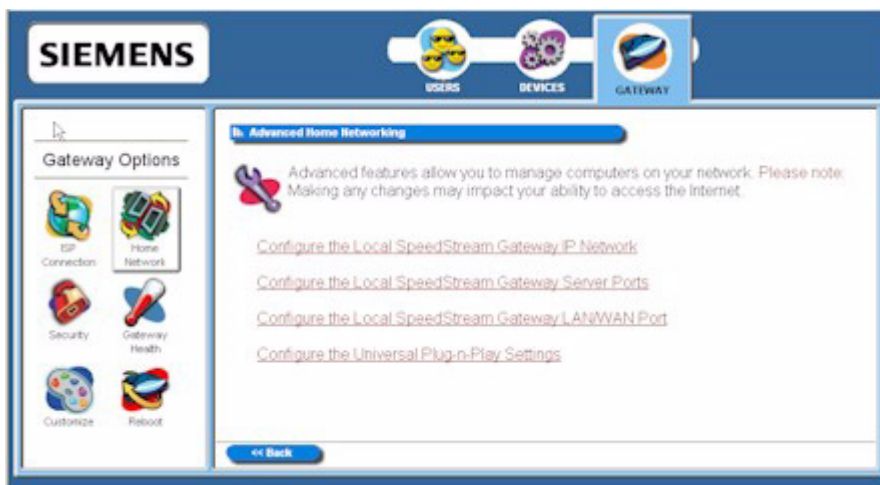
Home Network

The Home Network option displays all network-related information. You must be logged in as the administrator to access this option. To use the Home Network option:

1. Click the **Home Network** button on the **Gateway Options** pane. This displays the Home Network page containing information about the home network.



2. Optionally, click **Advanced Settings** to display a list of advanced features that allow you to manage the computers on your network. This displays the Advanced Home Networking page.



The advanced options are listed below. To access one of these options, click its link on the Advanced Home Networking page.

[IP Network](#)

Define the range for assigning IP addresses.

[Server Ports](#)

Specify the ports used by common applications such as HTTP, FTP, and Telnet.

[LAN/WAN Port](#)

Configure Ethernet port #4 as either a LAN (network) port or as a WAN (Internet connection) port.

[UPnP \(Universal Plug and Play\)](#)

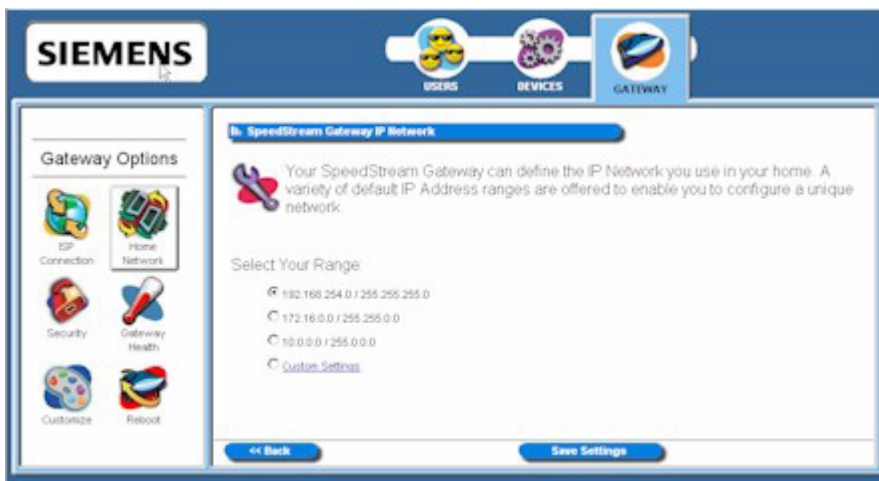
Configure UPnP. UPnP allows the Gateway to communicate directly with certain pages operating systems.

IP Network

The gateway provides the flexibility to use different ranges of IP addresses to be assigned by the DHCP Server housed in the gateway. DHCP (Dynamic Host Configuration Protocol) allows computers to obtain either permanent or temporary IP addresses from a central server.

To configure the IP network option:

1. Click the **Configure the local SpeedStream Gateway IP Network** hyperlink. This displays the SpeedStream Gateway IP Network page.



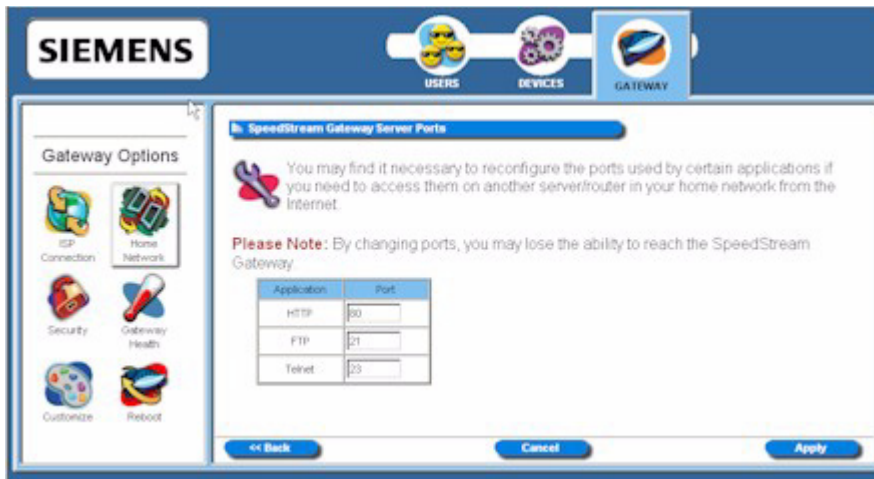
2. Select a range from the displayed options and click **Save Settings**. Be sure to select an IP address range that is not in conflict with any existing devices.
3. Optionally, click the **Custom Settings** hyperlink for advanced configuration. Please contact your ISP for more information on configuring the options for custom settings.

Server Ports

Common applications such as HTTP (Web site traffic), FTP, and Telnet use pre-defined incoming port numbers for compatibility with other services. If you wish to change the ports used by these applications you may do so using this option. This feature is recommended for use by advanced users only.

To configure the server port option:

1. Click the **Configure the Local SpeedStream Gateway Server Ports** hyperlink. This displays the SpeedStream Gateway Server Ports page.



2. Optionally, type a port number in **HTTP**. The default port for this field is 80.
3. Optionally, type a port number in **FTP**. The default port for this field is 21.
4. Optionally, type a port number in **Telnet**. The default port for this field is 23.
5. Click **Apply**. This displays the Your settings have been saved page.
6. Optionally, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your gateway.

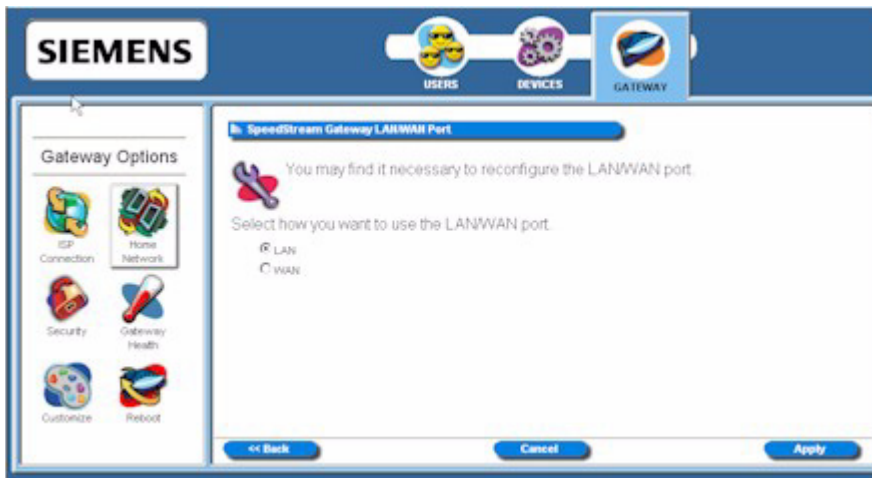
LAN/WAN Port

Your gateway contains four Ethernet ports, Ethernet port #4 can be used as either a LAN (network) port or as a WAN (Internet connection) port. Select the appropriate option to define whether the port is used as a fourth local network port or as a connection for another broadband device.

Note: For configuration of the port as a WAN port, you may be required to consult your Internet Service Provider for the appropriate settings.

To configure the LAN/WAN port:

1. Click the **Configure the Local SpeedStream Gateway LAN/WAN Port** hyperlink. This displays the SpeedStream Gateway LAN/WAN Port page.



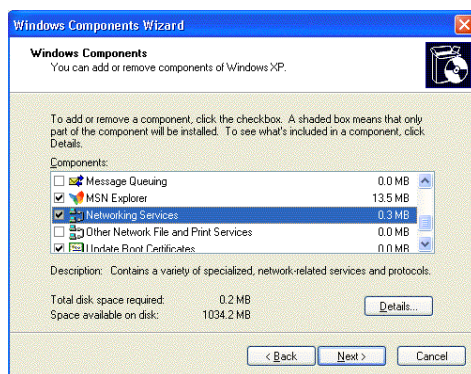
2. Select one of the following options:
 - **LAN** (Local Area Network)
Use the port as a connection to the network located in your home or premises.
 - **WAN** (Wide Area Network)
Use the port as a connection to a large connected network such as the Internet that is spread over a large geographic area. If you select the WAN option, please contact your ISP for instructions on how to configure this option.
3. Click **Apply**.

UPnP (Universal Plug and Play)

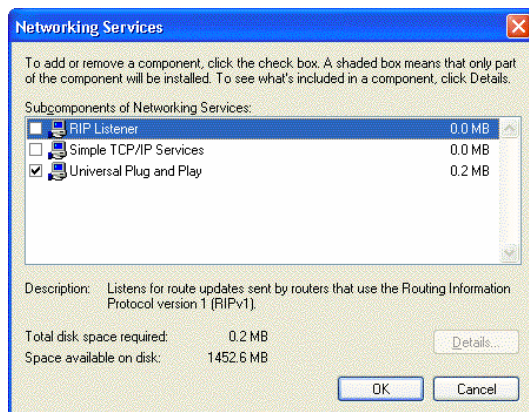
Microsoft UPnP allows the Gateway to communicate directly with certain pages operating systems to trade information about the special needs of certain applications (such as messaging programs and interactive games) as well as provide information about other devices on the network. This communication between the operating system and Gateway greatly reduces the amount of manual configuration required to use new applications and devices.

Only certain versions of pages XP and computer support the UPnP (Universal Plug and Play) function. Before configuring this option, make sure that UPnP is installed on your computer and enabled. Follow the steps below for installing UPnP components.

1. Select **Start>Control Panel**.
2. Select **Add or Remove Programs>Add/Remove pages Components** to open the pages Components Wizard page.

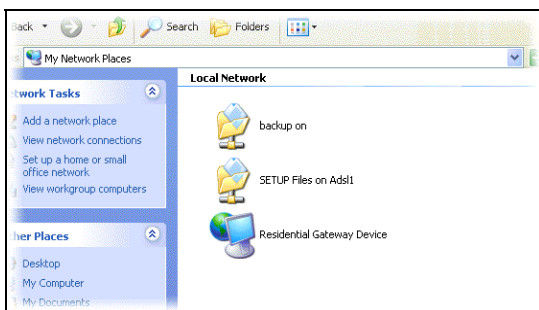


3. Select **Network Services** and click **Details**. This displays the Networking Services page.



4. Select **Universal Plug and Play**.
5. Click **OK**. The system installs the UPnP components automatically.

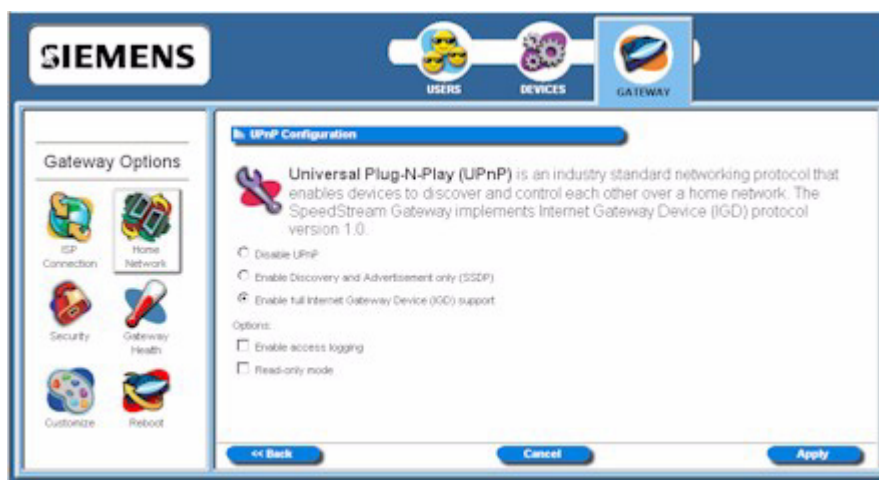
6. After finishing the installation, go to **My Network Places**. You will find an icon for the UPnP function called Residential Gateway Device.



7. Double-click the icon. The Gateway will open another Web page for UPnP functions. Now, NAT functionality is available. The Gateway will create virtual servers automatically when it detects the computer running Internet applications that require this configuration.

Now you can configure the Gateway for UPnP. To configure UPnP on the Gateway:

8. Click **Configure the Universal Plug and Play Settings** link to display the UPnP Configuration page:



9. Select one of the following operating modes to enable or disable UPnP.
 - **Disable UPnP**
Prevents the Gateway from using the UPnP feature to communicate with other devices or your operating system. Also may be disabled if your operating system does not support UPnP.
 - **Enable Discovery and Advertisement only (SSDP)**
Sends information about new devices (hardware) detected only. No information concerning software applications or services is transmitted.
 - **Enable full Internet Gateway Device (IGD) support**
Allows the Gateway to communicate freely with computers on the network about new devices, software applications, and services as needed to ensure they are working with minimal manual configuration required.

10. Select one of the following control options.
 - **Enable Access Logging**
Logs UPnP transactions to the system log.
 - **Read Only Mode**
Can read configuration information from a device; cannot modify the device configuration.
11. Click **Apply** to accept the settings. This displays the UPnP finish page.
12. Click **Reboot**.

Configuring Security Features

This chapter contains details for configuring the security features available with your gateway. Some of the features described below require at least a mid-level understanding of networking principles. These features are provided to allow configuration flexibility for advanced users.

Your gateway provides broad security measures against unwanted users. Security also allows for the configuration of the gateway firewall, administrator password, (NAT) Network Address Translation, and DMZ (Demilitarized Zone) configuration.



These security features are accessed through the **Gateway** button available on the tool bar on the Main page. Click the **Security** button to configure security for the gateway. (This button is displayed only if you logged in as the administrator.)

Clicking the Security button displays the Security Options page containing icons to access the security features.



This section is organized into parts that correspond to the following buttons shown on the Security Options page.



Configure the [network firewall](#). A firewall is a system designed to prevent unauthorized access to or from a private network.



Configure [address translation](#). Address translation hides individual users/computers behind a single outward-facing address. Hiding internal addresses allows greater security for your network.



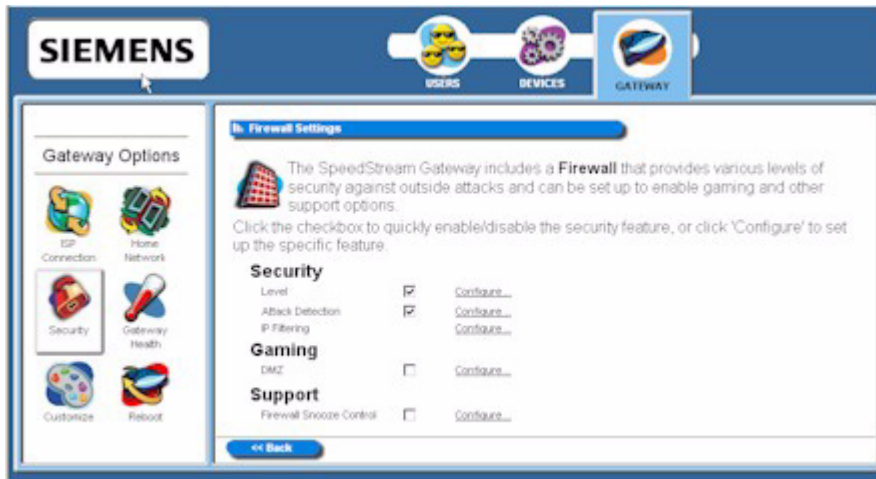
Change [administrative password](#).

Firewall Settings

A firewall is a system designed to prevent unauthorized access to or from a private network. The firewall page provides a listing of options to be enabled or disabled as well as links to configure the more complex details of each feature.

To configure the firewall:

1. From the [Security Options](#) page, click **Firewall Settings**. This displays the Firewall Settings page.



2. Select the checkboxes for all **Security** options you wish to enable. This can be any of the following:
 - **Level**
Enable security level access is from the gateway to the Internet or other networks. Click **Configure** to configure Security Level feature. This displays the [Firewall Level Configuration](#) page.
 - **Attack Detection**
Enable protection from common hacker attacks to your computer/network from the Internet. Click **Configure** to configure the Attack Detection feature. This displays the [Attack Detection Configuration](#) page.
 - **IP Filtering**
Configure inbound and outbound filter rules if your firewall Level setting is Custom. Click **Configure** to configure IP filter rules. This displays the [Firewall IP Filter Configuration Wizard](#) page.
3. Select **DMZ** for the **Gaming** option if you want to enable DMZ. Click **Configure** to configure firewall DMZ option. This displays the [Firewall DMZ Configuration](#) page.
4. Select the checkboxes for all **Support** options you wish to enable. This can be any of the following:
 - **Firewall Snooze Control**
Bypass the firewall for a set amount of time so outside support personnel can access your gateway or network or so you can run an application that conflicts with the firewall. Click **Configure** to configure the snooze control. This displays the [Firewall Snooze Control](#) page.

Firewall Security: Level

Security level refers to how much access is permitted from your gateway to the Internet or other networks.

To enable and configure the security level feature:

1. Select **Level** from the [Firewall Settings](#) page.
2. Click the **Configure** hyperlink next to **Level**. This displays the Firewall Level Configuration page.



3. Select the firewall security level from the **Select Firewall Level** drop-down menu. This can be one of the following:
 - **Off**
No firewall protection. Data can move freely both in and out of the gateway.
 - **Low**
Provides basic firewall protection. Attack detection is enabled and only ports well known to the gateway can allow the flow of data.
 - **High**
Provides maximum firewall protection. Only certain applications are allowed through the firewall or traffic that is already "in conversation" with an application from the host PC and host application. (ICSA 3.0a Compliant.)
 - **Custom**
Set your own rules for firewall protection. This option should be used by advanced users only. If you select this option, you must set customized rules for both inbound and outbound traffic using the [IP Filtering](#) option.
4. Click **Apply**.

Firewall Security: Attack Detection

If the Attack Detection System is enabled, the gateway provides protection against the most common hacker attacks that attempt to access your computer/network from the Internet. Intrusion attempts can also be logged to provide a record of attempts and their source (when available).

To enable and configure the attack detection feature:

1. Select **Attack Detection** from the [Firewall Settings](#) page.
2. Click the **Configure** hyperlink next to **Attack Detection** option. This displays the Firewall Attack Detection System Configuration page.



3. Select **Enable Attack Detection**.
4. Select **Filter** for each event in the list you want to filter or, if you want to filter all events, select **Filter All**. This provides maximum protection against malicious intrusion from outside your network.
5. Select **Log** for each event in the list you want to log or, if you want to log all events, select **Log All**.
6. Click **Apply**.

Below is a description of each event that can be monitored.

- **Same Source and Destination Address**

An outside device can send a SYN (synchronize) packet to a host with the same source and destination address (including port) causing the system to hang. When the receiving host tries to respond to the source address in the packet, it ends up just sending it back to itself. This packet could ping-pong back and forth over 200 times (consuming CPU resources) before being discarded.

- **Broadcast Source Address**

An outside device can send a ping to your gateway broadcast address using a forged source address. When your system responds to these pings, it is brought down by echo replies.

- **LAN Source Address on LAN**

An outside device can send a forged source address in an incoming IP packet to block trace back.

- **Invalid IP Packet Fragment**

An outside device can send fragmented data packets that can bring down your system. IP packets can be fairly large in size. If a link between two hosts transporting a packet can only handle smaller packets, the large packet may be split (or fragmented) into smaller ones. When the packet fragments get to the destination host, they must be reassembled into the original large packet like pieces of a puzzle. A specially crafted invalid fragment can cause the host to crash.

- **TCP NULL**

An outside device can send an IP packet with the protocol field set to TCP but with an all null TCP header and data section. If your gateway responds to this attack, it will bring down your system.

- **TCP FIN**

An outside device can send an attack using TCP FIN. This attack never allows a data packet to finish transmitting and brings down your system.

- **TCP XMAS**

An outside device can send an attack using TCP packets with all the flags set. This causes your system to slow to a halt.

- **Fragmented TCP Packet**

An outside device can send an attack using fragmented packets to allow an outside user Telnet access to a device on your network.

- **Fragmented TCP Header**

An outside device can send an attack using TCP packets with only a header and no payload. When numerous packets are sent through the gateway in this manner, your system slows and halts.

- **Fragmented UDP Header**

An outside device can send an attack using fragmented UDP headers to bring down a device on your network.

- **Fragmented ICMP Header**

An outside device can send an attack using fragmented ICMP headers to bring down a device on your network.

- **Inconsistent UDP/IP header lengths**

An outside device can send an attack using inconsistent UDP/IP headers to bring down a device on your network.

- **Inconsistent IP header lengths**

An outside device can send an attack using changes in the IP header to zero the fragment offset field. This will be treated as a complete packet when received and cause your system to halt.

Firewall Security: IP Filtering

Define inbound and outbound IP filter rules using this procedure. IP filtering rules can only be defined if the **Firewall Level** setting is **Custom**. This method of firewall protection is recommended for advanced users only.

To define IP filtering rules:

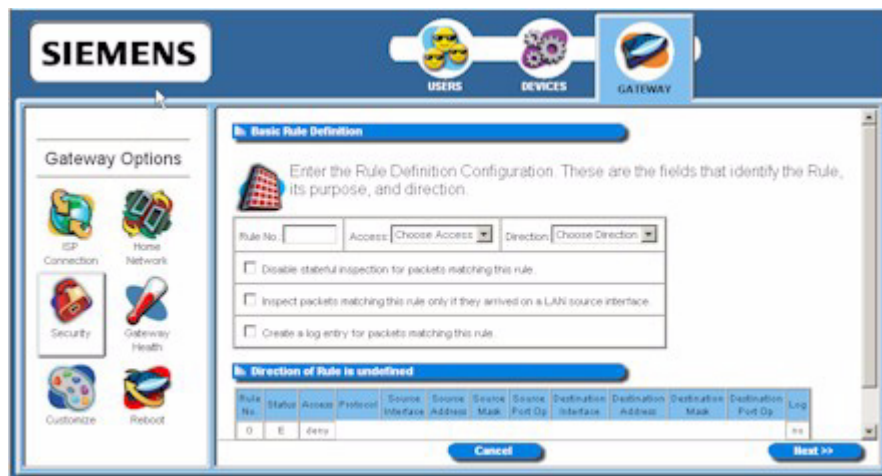
1. Click the Configuration hyperlink next to the IP Filter option on the [Firewall Settings](#) page. This displays the Firewall IP Filter Configuration Wizard page.



2. Do one of the following:
 - Click **Add New IP Filter Rule** to add new IP filter rules. This displays the Basic Rule Definition page.
 - Click **Clone IP Filter Level** to clone IP filter rules already defined. This displays the Clone Rule Definition page. Once cloned, you can modify the existing rules.

Add New IP Filter Rules

The Basic Rule Definition page is displayed when you select **Add New IP Filter Rule** from the [Firewall IP Configuration Wizard](#) page. Using this option, you can define both inbound and outbound rules. Each rule defined is added to the Rule Definition table.



To add a new rule:

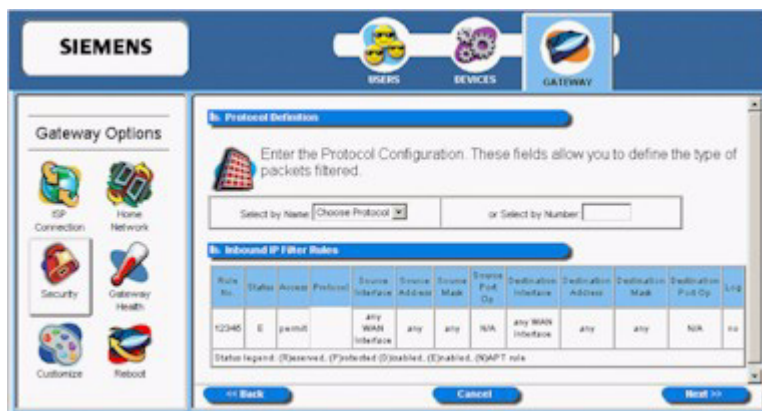
1. Type up to a five digit numeric value in **Rule No** to uniquely identify the rule.

2. Select either **Permit** or **Deny** from the **Access** drop-down menu. Select **Permit** to allow the rule and **Deny** to prohibit the rule.
3. Select either **Inbound** or **Outbound** from the **Direction** drop-down menu. **Inbound** refers to data coming into the gateway, while **Outbound** refers to data transmitted from the gateway.
4. Optionally, select **Disable stateful inspection for packets matching this rule**.
5. Optionally, select **Create a log entry for packets matching this rule**. When selected, an entry is placed in the log file when packets match this rule.
6. Click **Next**. This displays the Source and Destination Definition page.



7. Under the **Source** heading, select a network connection from the **Network Interface** drop-down menu.
8. Select one of the following options:
 - **Any IP Address**
Select this option if this rule applies to any IP address from the source.
 - **This IP Address**
Select this option if a rule applies to a specific IP address from the source.
9. If you selected **This IP Address**, enter an IP address in the **IP Address** field and do one of the following:
 - Enter a netmask in the **Netmask** field.
 - Select **or Host** to use your gateway netmask as the source netmask.
10. Under the **Destination** heading, select a network connection from the **Network Interface** drop-down menu.
11. Select one of the following options:
 - **Any IP Address**
Select this option if this rule applies to any IP address of the destination.
 - **This IP Address**
Select this option if a rule applies to a specific IP address of the destination.
12. If you selected **This IP Address**, enter an IP address in the **IP Address** field and do one of the following:
 - Enter a netmask in the **Netmask** field.
 - Select **or Host** to use your gateway netmask as the destination netmask.

13. Click **Next**. This displays the Protocol Definition page.



14. Do one of the following:

- Select one of the following protocol options from the **Select by Name** drop-down menu. This defines the types of packets filtered.
 - **Any Protocol**
 - **TCP** (Transmission Control Protocol):
Provides reliable, sequenced, and unduplicated delivery of bytes to remote or local users. Click **Next** to display the [TCP/UDP Options page](#).
 - **UDP** (User Datagram Protocol):
Provides for the exchange of datagrams without acknowledgement or guaranteed delivery. Click **Next** to display the [TCP/UDP Options page](#).
 - **ICMP** (Internet Control Message Protocol):
A mechanism that provides for peer communication. The most commonly used application for this protocol is the PING command. Click **Next** to display the [ICMP Options page](#).
 - **GRE** (Generic Routing Encapsulation):
A tunneling protocol that is used primarily for VPN (Virtual Private Networks).
- Type a protocol number in the **Select by Number** field.

15. Click **Finish**.

TCP/UDP Options page

The TCP/UDP Options page is displayed if you select TCP or UDP protocol from the [Protocol Definition](#) page. If you selected either of these protocol types, you must identify the source and destination ports.

1. Select one of the following options from the **Source Port Operator** drop-down menu and the **Destination Port Operator** drop-down menu:
 - **any**
Any port is acceptable as the source/destination port.
 - **less than or equal to**
A port less than or equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
 - **equal to**
A port equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
 - **greater than or equal to**
a port greater than or equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
 - **range**
Any port between the value of the entry in the **Port 1** field and the value in the **Port 2** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** and **Port 2** fields.
2. Optionally, select **Check TCP syn packets** if you wish this rule to prevent the blocking of synchronization packets for pre-existing sessions.
3. Click **Next**.
4. Click **Finish**.

ICMP Options page

The ICMP Options page is displayed if you select **ICMP protocol** from the [Protocol Definition](#) page.



1. Do one of the following:
 - Select any of the ICMP options you wish to filter.
 - Select **All Types** to filter all options.
2. Click **Next**.
3. Click **Finish**.

Clone IP Filter Rules

The Clone Rule Definitions page is displayed when you select **Clone IP Filter Level** from the [Firewall IP Filter Configuration Wizard](#) page. Using this option, you can clone either high or low level rules and modify them according to your needs. If you choose to clone IP filter rules, the rules already defined in the Rule Definition table are discarded.



To clone IP filter rules:

1. Select one of the following from the **Select preconfigured firewall level for cloning** drop-down menu.
 - **Low**
Clones low-level IP filter rules.
 - **High**
Clones high-level IP filter rules.
2. Click **Apply**. This displays the Firewall IP Filter Configuration Wizard page with the selected rule set showing in the Rule Definition table.
3. Disable or delete any rule as desired.

Firewall: DMZ

The DMZ feature allows a computer on your home network to circumvent the firewall and have direct access to the internet. This feature is primarily used for gaming. The gateway allows you to configure a temporary or permanent DMZ (Demilitarized Zone) to bypass the firewall for network or Internet gaming. If the DMZ feature is enabled, you must select the computer to be used as the DMZ computer/host. This function is recommended for use only when you require this special level of unrestricted access as it leaves your gateway and network exposed to the Internet with no firewall protection.

To enable and configure the DMZ:

1. Select **DMZ** from the [Firewall Settings](#) page.
2. Click the **Configure** hyperlink next to **DMZ**. This displays the Firewall DMZ Configuration page.



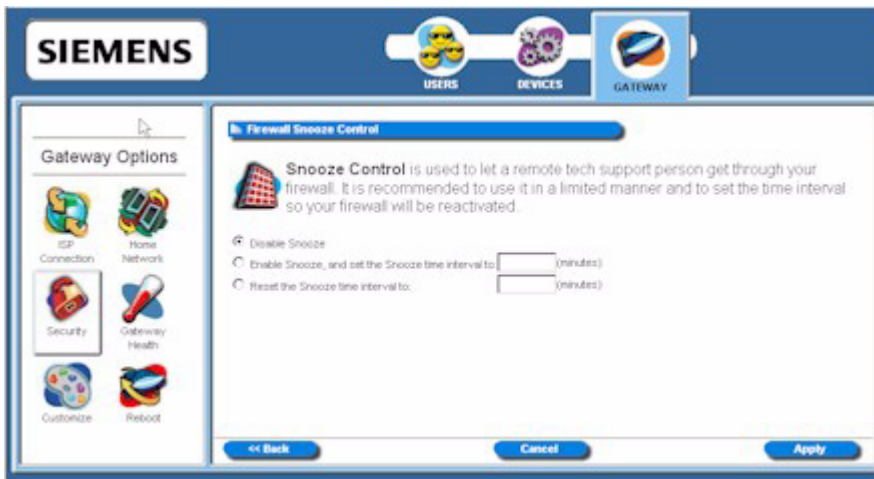
3. Select one of the following DMZ enable options:
 - **Disable DMZ**
The firewall is not bypassed.
 - **Enable DMZ with this Host IP address**
The firewall is bypassed through an IP address typed in the box next to this field.
 - **Enable DMZ with this Host IP address**
The firewall is bypassed through an IP address that is selected from the **Select Host** drop-down menu next to this field. Select the desired host from the drop down.
4. Select one of the following time element options:
 - **Make Settings Permanent**
DMZ settings are permanent unless changed by the administrator.
 - **Make Settings Last for**
DMZ settings last for only the time (in minutes) entered in the box next to this option.
5. Click **Apply**.

Firewall: Snooze Control

The snooze feature allows you to bypass the firewall for a set amount of time so outside support personnel can access your gateway or network, or so you can run an application that conflicts with the firewall. This function is recommended for use only when you require this special level of unrestricted access as it leaves your gateway and network exposed to the Internet with no firewall protection.

To enable and configure snooze control:

1. Select **Firewall Snooze Control** from the [Firewall Settings](#) page.
2. Click the **Configure** hyperlink next to **Firewall Snooze Control**. This displays the Firewall Snooze Control page.



3. Select one of the following options:
 - **Disable Snooze**
Disables all snooze control. In this mode, the firewall is not bypassed.
 - **Enable Snooze, and set the Snooze time interval to**
Enables snooze for a specified time period. Be sure to enter the number of minutes to define how long the firewall should be disabled.
 - **Reset the Snooze time interval to**
Reset the snooze control time period. Use this option if you need a time extension for an open snooze session. Be sure to specify the additional amount of time (minutes) the firewall should be disabled.
4. Click **Apply**.

Administrator Password

You may change the gateway's administrator password at any time if you have administrative rights to the gateway. To change the administrator password:

1. From the Security Options page, click the **Admin Password** button. This displays the Enter Network Password page.
2. Provide the administrator log on ID and password, then click **OK**. This displays the gateway Administrator Setup page.

The screenshot shows the 'Gateway Administrator Setup' page. At the top, there is a blue header with the 'SIEMENS' logo and three navigation icons: 'USERS', 'DEVICES', and 'GATEWAY'. Below the header, on the left, is a 'Gateway Options' sidebar with icons for 'ISP Connection', 'Home Network', 'Security', 'Gateway Health', 'Customize', and 'Reboot'. The main content area is titled 'b. Gateway Administrator Setup' and contains the following text: 'Your Gateway requires someone to be the **Gateway Administrator**. This person has responsibility for adding user profiles, setting each person's access rights, and configuring the Gateway.' Below this, it says 'Please create a user name and password for the Gateway administrator. Please enter unique information to configure the SpeedStream DSL Gateway.' There are three input fields: 'User Name' (with 'admin' entered), 'New Password' (with '*****' entered), and 'Confirm Password' (with '*****' entered). Each field has a '(required)' label. At the bottom of the form are two buttons: '<< Back' and 'Save Settings'.

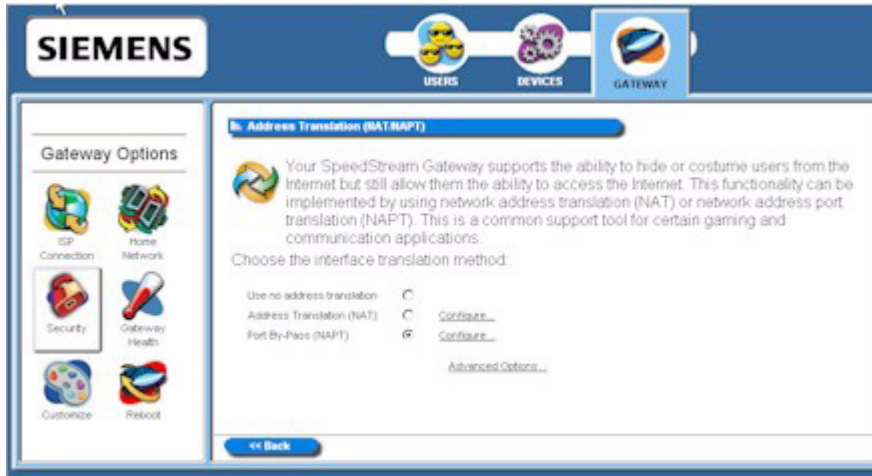
3. Make any desired changes to the **User Name**, **New Password**, and **Confirm Password**.
4. Click **Save Settings**.

Address Translation

The Address Translation feature provides different methods of keeping individual users/computers hidden behind a single outward-facing address, while still allowing them to access the Internet and related applications. If you have more than one available Internet connection interface, they will all be displayed in the drop-down menu for ease of selection.

To enable and configure the address translation feature:

1. From the [Security Options](#) page, select the **Address Translation** button. This displays the Address Translation (NAT/NAPT) page.



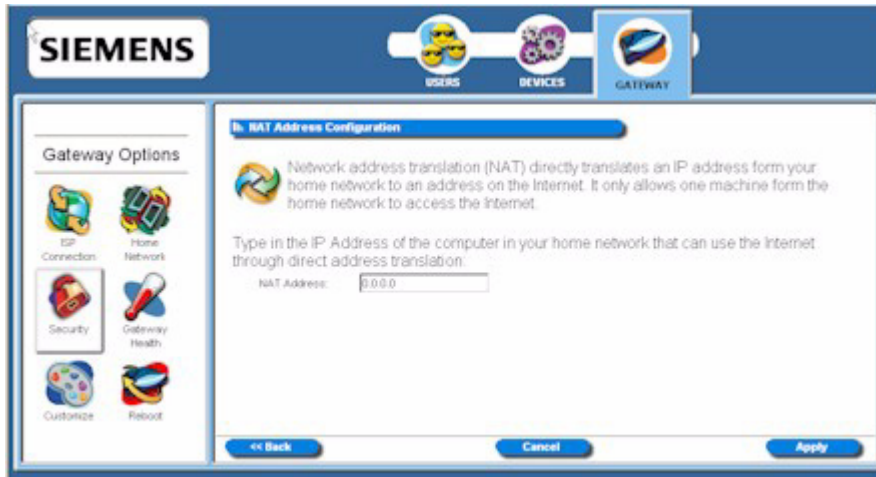
2. Select an interface from the **Select Interface** drop-down menu.
3. Select one of the following options:
 - **Use no address translation**
Disables address translation.
 - **Address Translation (NAT)**
Uses NAT for address translation. NAT is an Internet standard that allows a LAN to use one set of IP addresses for internal traffic and a second set for external traffic. This displays the [NAT Address Configuration](#) page.
 - **Port By-Pass (NAPT)**
Uses NAPT for address translation. Only TCP, UDP, and ICMP protocols support NAPT. NAPT allows many devices connected to the gateway access to the Internet while masking the identification of the internal IP addresses. This displays the [Port By-Bass Configuration](#) page.

Address Translation With NAT

Network Address Translation (NAT) translates an IP address from your home network to an address on the Internet. It allows only one machine to access the Internet.

To enable and configure NAT address translation:

1. Select **Address Translation (NAT)** from the [Address Translation \(NAT/NAPT\)](#) page.
2. Click the **Configure** hyperlink next to **Address Translation (NAT)**. This displays the NAT Address Configuration page.



3. Type the IP address of the one computer in your network that you wish to have access to the Internet.
4. Click **Apply**.

Address Translation With NAPT

Many applications require special port access to the Internet in order to function. By enabling Network Address Port Translation (NAPT), multiple computers in your home network have access to the Internet by translating port addresses to an Internet IP address while masking their IP addresses from outside users. Only TCP, UDP, and ICMP protocols support NAPT.

To enable and configure NAPT address translation:

1. Select **Port By-Pass (NAPT)** from the [Address Translation \(NAT/NAPT\)](#) page.
2. Click the **Configure** hyperlink next to **Port By-Pass (NAPT)**. This displays the Port-By-Pass Configuration page.



3. To enable an application for NAPT, click the desired application from the **Available Applications** list. The application is moved to the **Enabled Applications** list.
4. Optionally, click the **Add a custom bypass entry** hyperlink. This displays the advanced features on the Port By-Pass Configuration page. The advanced option allows you to configure special port access to the Internet.



5. Do one of the following:
 - Select one of the following services from the **Select service by name** drop-down menu.
 - **Telnet**
Telnet is a program that allows you to connect to other computers over the Internet. This options uses port 23.
 - **HTTP** (Hyper Text Transfer Protocol)
HTTP is the standard method of transferring all types of information over the Internet. This option uses port 80.
 - **FTP** (File Transfer Protocol)
FTP is used to transfer files in both ASCII and Binary format between local and remote devices. This option uses port 21.
 - **SNMP** (Signaling Network Management Protocol)
SNMP is a protocol used by network management applications to help manage a network. This option uses port 161.
 - **SMTP** (Simple Mail Transfer Protocol)
SMTP is used for sending email between servers. This port uses port 25.
 - **PPTP** (Point-to-Point Tunneling Protocol)
PPTP is a protocol that allows VPN (Virtual Private Network) applications. This option uses port 1723.
 - **Domain**
Domain is used for DNS options. This option uses port 53.
 - Select a protocol from the **Select Protocol** drop-down menu. This can be one of the following:
 - **TCP** (Transmission Control Protocol)
Provides reliable, sequenced, and unduplicated delivery of bytes to a remote or local user.
 - **UDP** (User Datagram Protocol)
A connectionless mode protocol that provides the delivery of packets to a remote or local user.
 - **ICMP** (Internet Control Message Protocol)
A method by which IP software on a host or router can communicate to pass information to other machines.
 - **GRE** (Generic Routing Encapsulation)
This protocol is used to provide tunneling for a VPN connection.
6. If you selected a protocol, type the range of UDP or TCP ports in the appropriate boxes
7. Select one of the following options:
 - **Redirect selected protocol/service to this router**
The protocol or service that you select is directed to your router.
 - **Redirect selected protocol/service to IP Address**
The protocol or service that you select is directed to an IP address on your LAN that you type in the box next to this field.
8. Click **Apply**.

Miscellaneous Configuration Options

This chapter explains how to customize the appearance of the configuration program and to reboot the router. This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Options** pane.



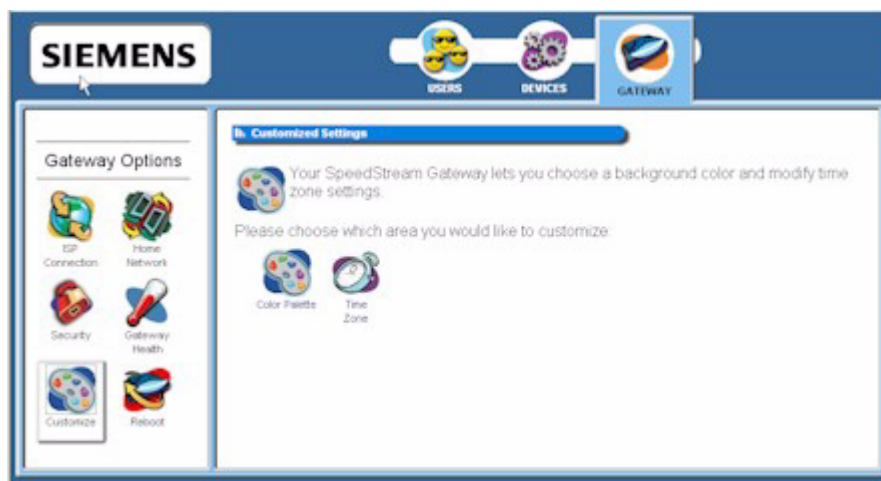
[Customize](#) the router's display.



[Reboot](#) the router.

Customize

You are able to control the background color, language, and time zone settings of your router using customization options. To access the customization options, click the **Customization** button from the **Gateway Options** pane. This displays the Customized Settings page.



Customization options discussed in this chapter:

[Customize](#) the appearance of the configuration interface/program.



Color Palette



Time Zone

Configure [time parameters](#) to automatically synchronize the router's internal date and time settings with those of your selected time zone.

Color Palette

Multiple color selections are available to customize the appearance of the configuration interface/program.

To configure the color palette:

1. From the Customized Settings page, click the **Color Palette** button. This displays the Customized Colors page.



2. Using the color drop-down menus from the different display options, select the colors you wish to use in the system.
3. Optionally, type a numeric color value in the box next to the particular color drop-down menu. The number is based on RGB (Red Green Blue) values. For example, the color red is represented by a value of ff0000, green is represented by a value of 00ff00, and blue is represented by a value of 0000ff. If you are entering a numeric value for the color, ensure that the # is in front of your numeric value.

Click **Reset System Default Colors** if you want to reset all system color schemes to the factory settings.

4. Click **Apply**.

Time Zone

Using this option, you can configure the time parameters to automatically synchronize the router's internal date and time settings with those of your selected time zone. This time will be used to control time restrictions you may set for users as well as in entries in the system log.

To enable and configure the time zone feature:

1. From the Customized Settings page, click the **Time Zone** button. This displays the Configure Time Zone page.



2. Select **Yes** for **Enable Time Client**.
3. Select a time zone from the **Select Time Zone** drop-down menu.

Note: The router's time server is unable to determine whether your time zone is currently observing daylight savings time. If you are currently observing daylight savings time, select an alternate time zone that matches your time settings during daylight savings time observation periods.

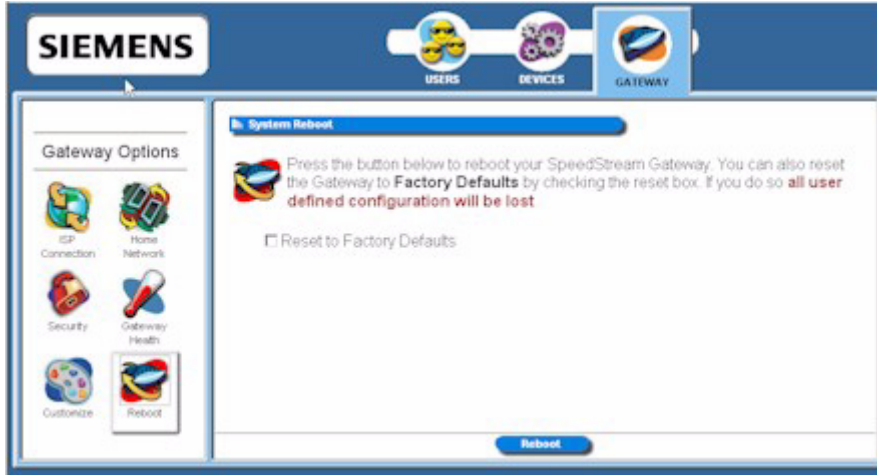
4. Click **Apply**.

Reboot

You can reboot the router using the Reboot option, or you can reset the router to factory defaults using the reset option. Reboot should be used when the router needs to be restarted. The router can also be rebooted using the power switch on the rear panel of the router. This option can be used at either the user or administrator level.

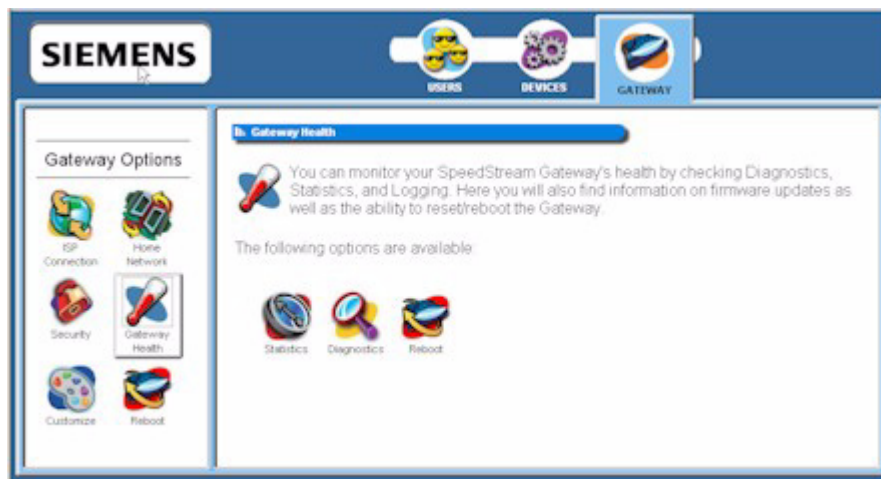
To reboot or reset factory defaults on the router:

1. Click the **Reboot** button from the **Gateway Options** pane. This displays the System Reboot page.



2. If you want the factory default settings to be reset, click **Reset to Factory Defaults**. Reset should be used when you find it necessary to recover the factory default settings. This may be necessary when a custom configuration did not go as planned, when a new configuration is desired, or when the router does not appear to be working properly. This option resets all custom settings, users, and passwords on your router. You must be logged on as the administrator to use this option.
3. Click **Reboot**.

This chapter describes how to monitor the health of the gateway. The gateway health options are used to gauge the various measures of gateway's health. To use the gateway health options, click the **Gateway Health** button from the **Gateway Options** pane. This displays the Gateway Health page.



This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Health** pane.



Statistics

Used to measure the Internet [statistics](#), home networking statistics, security statistics, and the different gateway log files.



Reboot

[Reboot](#) the system or resets all settings to gateway factory defaults.

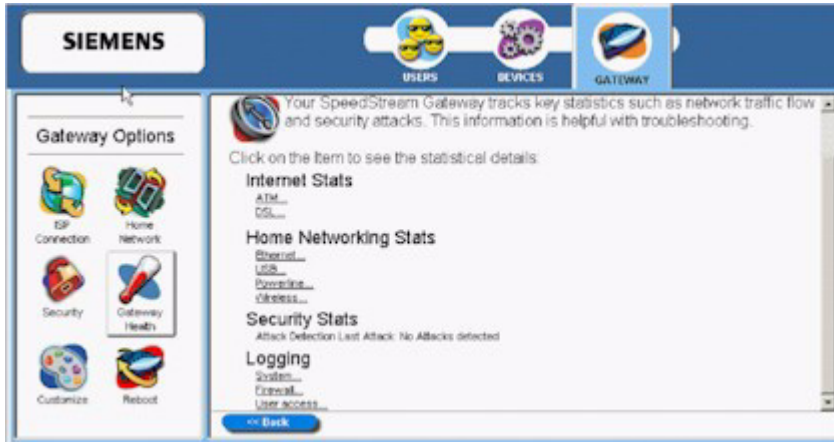


Diagnostics

Runs a [diagnostic](#) program against a selected connection on your gateway.

Statistics

You can display statistics for the Internet, Home Networking, Security, and Logging. To display any of these statistics, click the **Statistics** button from the [Gateway Health](#) page. This displays the SpeedStream Gateway Statistics page.



Click the hyperlink for the type of statistics you wish to view. These fall into four categories:

- **Internet Stats**
[Internet statistics](#) are commonly used by your Internet Service provider to diagnose service-related issues. Internet statistics include either [ATM](#) or [DSL](#) statistics.
- **Home Networking Stats**
[Home Networking statistics](#) are helpful for troubleshooting issues on your home network. These statistics are displayed for each physical interface connected to the gateway. (USB connection is not available on this model.)
- **Security Stats**
Security breach attempts are shown for any firewall rules or attack detection services you have defined on the Firewall customization page.
- **Logging**
Extensive activity logs are provided for advanced troubleshooting and administrative use. The following types of logs are available: [System](#), [Firewall](#), and [User Access](#).

Internet Stats

Internet statistics are commonly used by your Internet Service provider to diagnose service-related issues. Internet statistics include either [ATM](#) or [DSL](#) statistics.

ATM Statistics

View status and statistical information for the WAN-side Asynchronous Transfer Mode (ATM) network connection. WAN-side connection to the service provider is based on an Asynchronous Transfer Mode (ATM) network connection. In addition, statistical information is provided for each Virtual Circuit (VC) configured under the ATM Adaptation Layer (AAL).

To view ATM statistics, click the **ATM** hyperlink under **Internet Stats**.



DSL Statistics

View status and statistical information for the Digital Subscriber Line (DSL) when the physical WAN-side connection to the service provider is achieved through a DSL line. Statistical information is accumulated over periodic intervals and may be displayed for up to a 24 hour period.

To view DSL statistics, click the **DSL** hyperlink under **Internet Stats**.



Home Networking Stats

Home Networking statistics are helpful for troubleshooting issues on your home network. These statistics are displayed for each physical interface connected to the gateway.

View status and statistical information for LAN-side Ethernet connectivity.

Pay special attention to the status (up or down) reported for each Ethernet port to verify that each cable is connected properly and detected by the gateway.

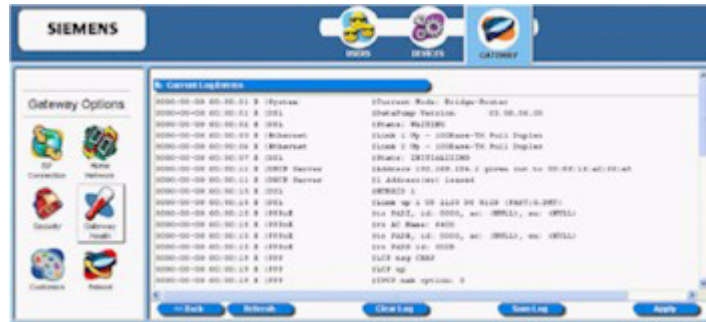


Logging

Extensive activity logs are provided for advanced troubleshooting and administrative use. The following types of logs are available: [System](#), [Firewall](#), and [User Access](#).

System Logging

System logging displays gateway status, user login, interfaces accessed, etc. Activity displayed in the system log is defined using the checkboxes provided at the bottom of the page. Click **Apply** after making any changes. The system log can be cleared or saved to a text file using the appropriate buttons, Clear Log or Save Log.



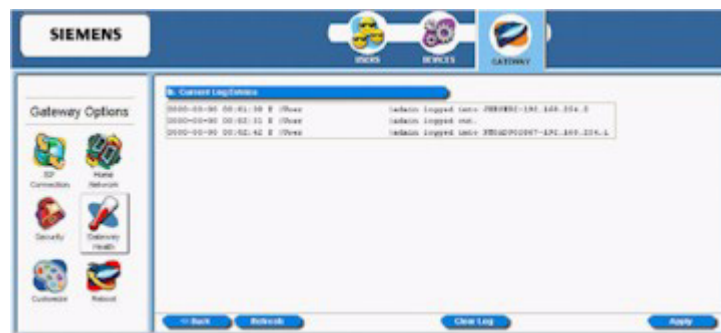
Firewall Logging

Firewall Logging displays attempts (both failures and successes) to access data through the firewall. Firewall log entries are defined on the **Firewall Settings Configuration** page found under the **Security** menu.



User Access

User Access logging displays activity related to users logging in or out of the gateway. Both successful and unsuccessful attempts by username are recorded.



Diagnostics

The gateway provides diagnostic tests and data for each interface. This data is commonly requested by technical support to assist in troubleshooting. To access this feature, click the **Diagnostics** button from your [Gateway Health](#) page. This displays the Diagnostics page.



To use the diagnostic option:

1. Select a connection to test from the **Connection to Test** drop-down menu. You must move all the way to the bottom of this page to display this drop-down menu.
2. Click **Run Diagnostics**. The system responds by displaying the results in the different tables. Pay special attention to any tests that report a failing condition and check the connections for these interfaces before running the diagnostics again.
3. Click **Apply**.