Toolbar

The Gateway has three primary toolbar buttons: Users, Devices, and Gateway. The options for all the toolbar buttons differ depending on the user login. The administrator has the most authority with all options enabled, while the user has limited options based on the user profile for the login. Please see the table below for more information.

	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.
	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 Windows File Sharing.
	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.

Logging into the Gateway

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.

To log on to the Gateway:

1. Select a user from the **Log In** drop-down menu in the upper-left corner of the "Home" window.
2. Select a user from the **Username** drop-down menu.
3. Type the user password in **Password**.
4. Click **Go**. This displays the "Home" window.

Logging out of the Gateway

To log out of the Gateway:

1. Click **GO** next to **Log Out**. The system responds by displaying the "Home" window.

DRAFT

Chapter 5

Configuring Users and Devices

This chapter explains how to configure users and devices 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 toolbar: Users and Devices. Refer to Chapter 6, Configuring Gateway Options for details on configuring the features on the Gateway.

Configuring Users

Users are added and maintained from the “User Profiles” window accessed by clicking **Users** button on the toolbar. The “User Profiles” window provides details about all active user profiles if **Enable User Profiling** is selected.

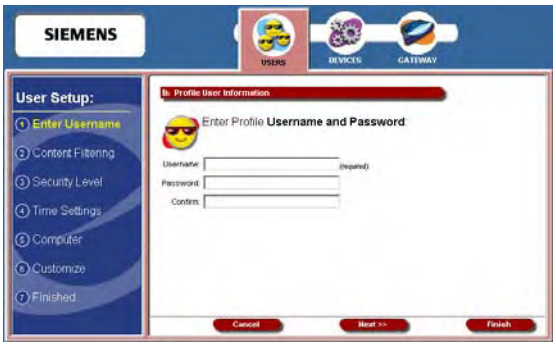
The **Enable User Profiling** option must be selected on the “User Profiles” window for the content filtering option to be operational.

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 “Users Profile” window, click the **Add New User** button in the left navigation pane. This displays the “Profile User Information” window.



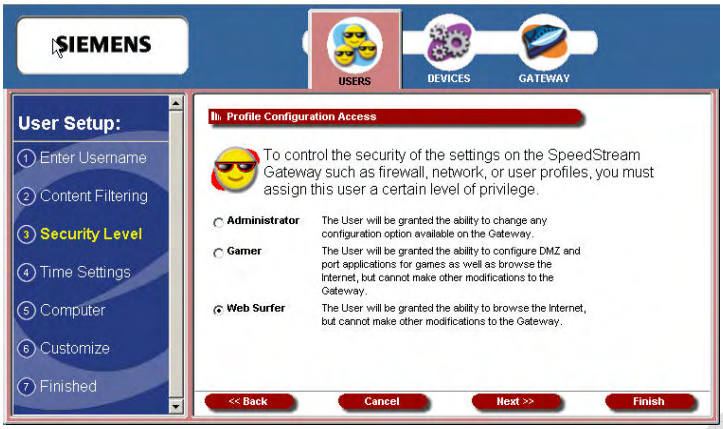
2. Type a user name in **Username**.
3. Type a password in **Password**.
4. Re-type the password in **Confirm**.
5. Click **Next**. This displays the "Profile Content Filtering" window. (At any time during user configuration, you can click **Finish** to complete the user profile and accept the defaults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

DRAFT

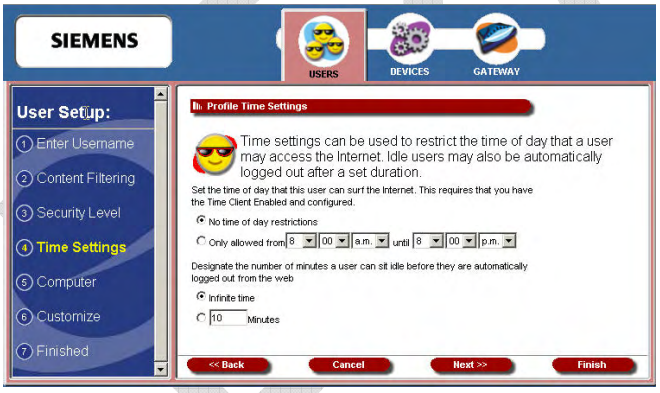


Profile configuration access defines the access permission for a user controlling what functions and features are available to that user.

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**
     Use has access only to the Internet, not to the Gateway's configuration.

10. Click **Next**. This displays the "Profile Time Setting" window.



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 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.

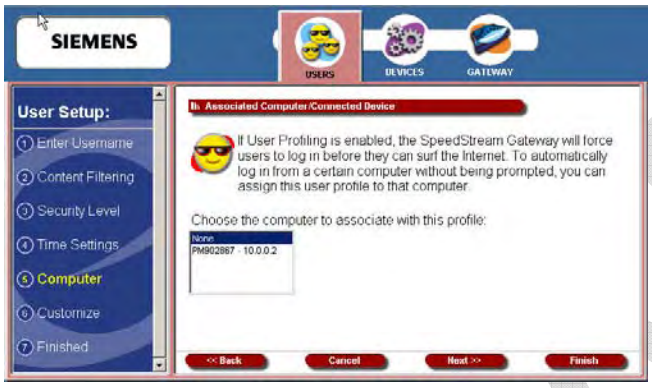
DRAFT

- **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" window.



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" window.

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

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

DRAFT

- 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" window. The icon of the user you just created is displayed in the left navigation pane.

DRAFT

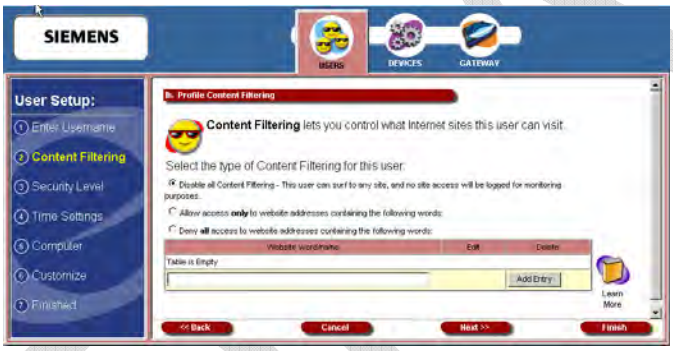
Editing A User Profile

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 "Users Profile" window, click the button in the left navigation pane corresponding to the user you want to edit. This displays the "Profile Monitor" window.

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



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

DRAFT

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 "Users Profile" window, click the button in the left navigation pane corresponding to the user you want to delete. This displays the "Profile Monitor" window.

2. Click **Delete User**.

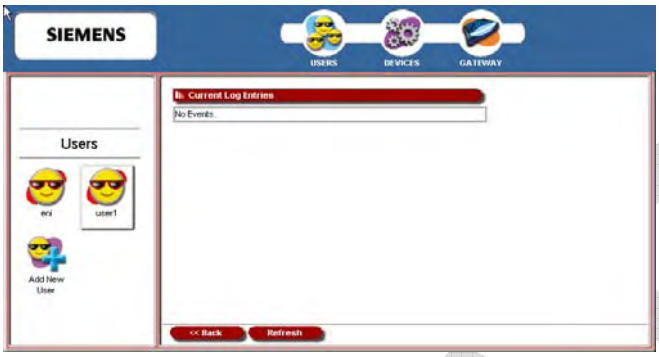
DRAFT

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 "Users Profile" window, click the button in the left navigation pane corresponding to the user you want to delete. This displays the "Profile Monitor" window.
2. Click **View User Log**. This displays the "Current Log Entries" window displaying all the log information about the user.



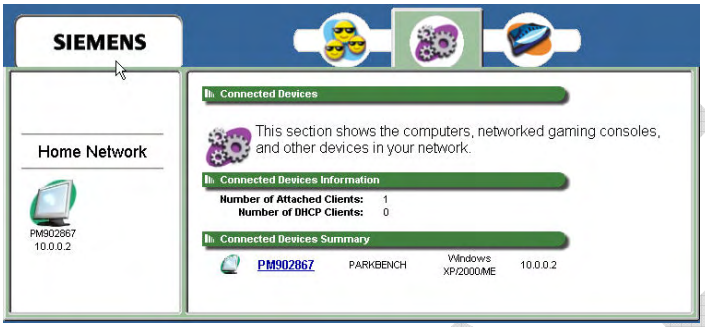
DRAFT

Configuring Devices

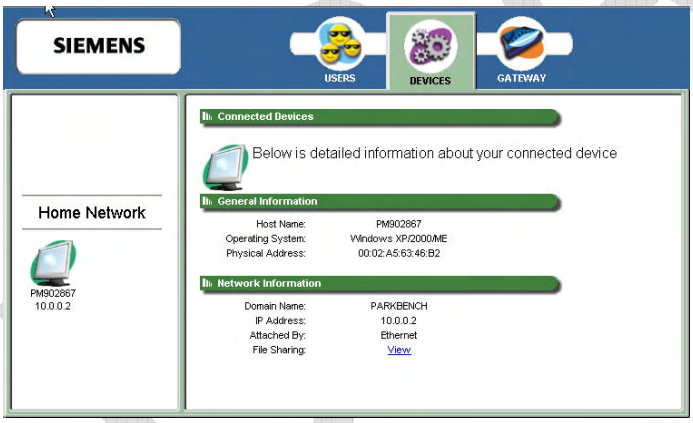
The Devices option allows you to view devices connected to your Gateway. If you are logged in as the administrator, you can view all the connected devices to the Gateway. If you are logged in as a specific user, you can only view devices associated with that user logon.

To use the Devices option:

1. Click **Devices** in the toolbar. This displays the "Connected Devices" window 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" window, which displays both general and network information about the selected device.



DRAFT

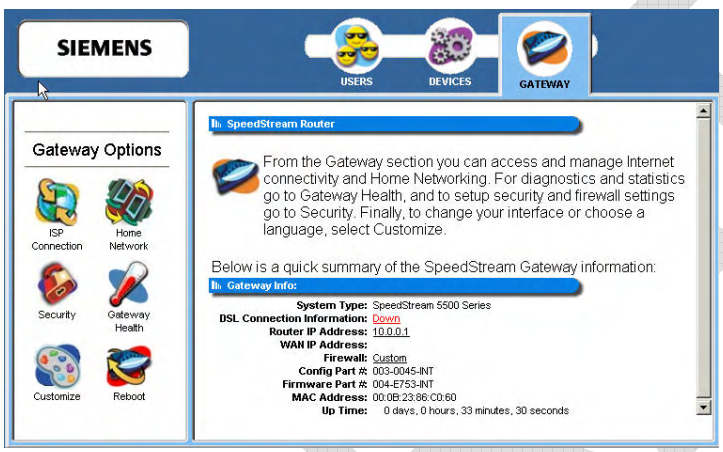
Chapter 6

Configuring Advanced Features

This chapter explains how to configure advanced features on the Gateway.

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 toolbar on the "Main" window. 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.



Gateway Options discussed in this chapter

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

Get information about ISP connections. You can also use this option to set ISP configuration parameters. This should only be done when instructed by your ISP.

View network-related information

Configure security for the Gateway.

Reboot the Gateway.

DRAFT

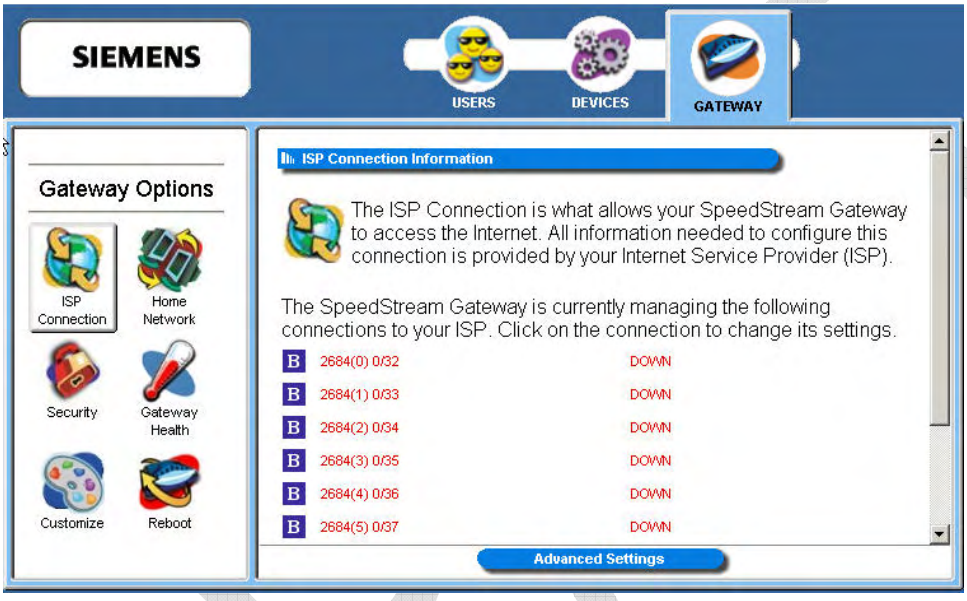
ISP Connection

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.

WARNING: If this feature is not properly configured your Internet connection may terminate.

To use the ISP connection function:

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

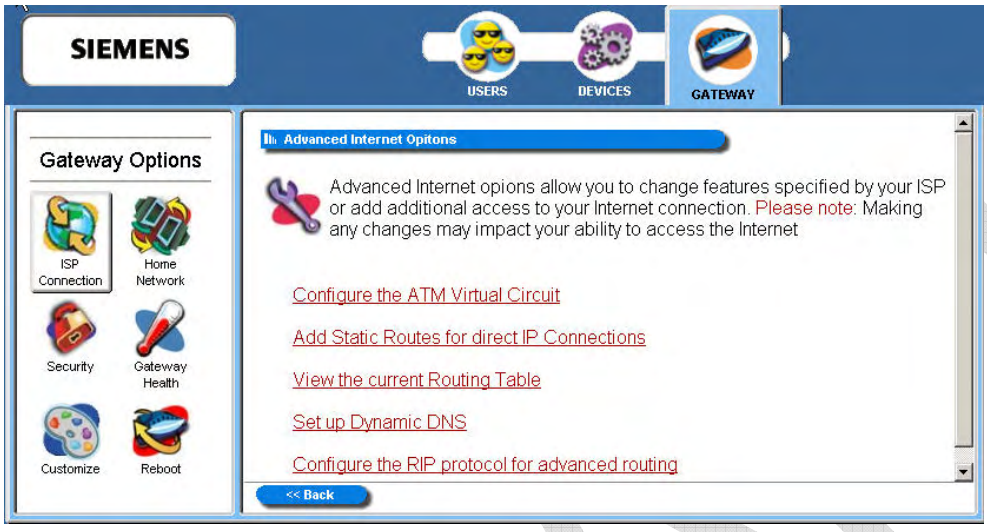


2. Click one of the ISP connections (in red) to reconfigure that connection. Please check with your ISP for the information required to reconfigure a connection.
3. Optionally refer to the section titled Advanced Settings for details on configuring advanced ISP connection settings.

Advanced ISP Settings

The Gateway provides access to additional, advanced ISP configuration settings. All the 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 the advanced settings, click **Advanced Settings** from the "ISP Connection Information" window. This displays the "Advanced Internet Options" window.



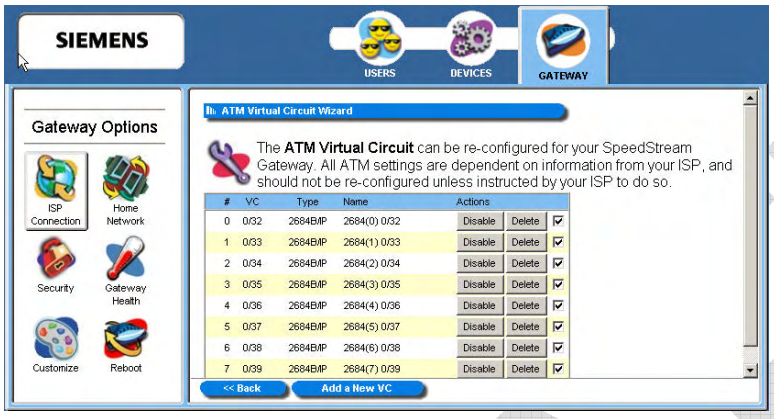
The advanced options are listed below. To access one of these options, click its link on the "Advanced Internet Options" window.

Configure the ATM Virtual Circuit	Create and 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.
View the Current Routing Table	View a table of routing information of all static and dynamic routes for network devices.
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" window. This displays the "ATM Virtual Circuit Wizard" window.



Make any modifications advised by your ISP.

DRAFT

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" window. This displays the "Static Routes" window.

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.

DRAFT

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 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" window. This displays the "Set Up Dynamic DNS" window.

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.

DRAFT

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" window. This displays the "RIP Configuration" window.

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 routers 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" window.
5. Optionally, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your Gateway.

DRAFT

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" window 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" window.

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

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.
Wireless Network	Configure the wireless equipment in your Gateway.
UPnP	Configure UPnP. UPnP allows the Gateway to communicate directly with certain Windows operating systems.

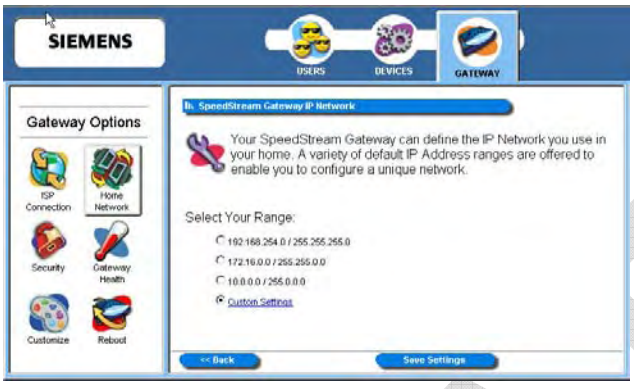
DRAFT

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 Gigaset Gateway IP Network** hyperlink. This displays the "Gigaset Gateway IP Network" window.



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 Gigaset Gateway Server Ports** hyperlink. This displays the "Gigaset Gateway Server Ports" window.

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" window.
6. Optionally, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your Gateway.

DRAFT

LAN/WAN Port

If 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 Gigaset Gateway LAN/WAN Port** hyperlink. This displays the "Gigaset Gateway LAN/WAN Port" window.

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**.

DRAFT

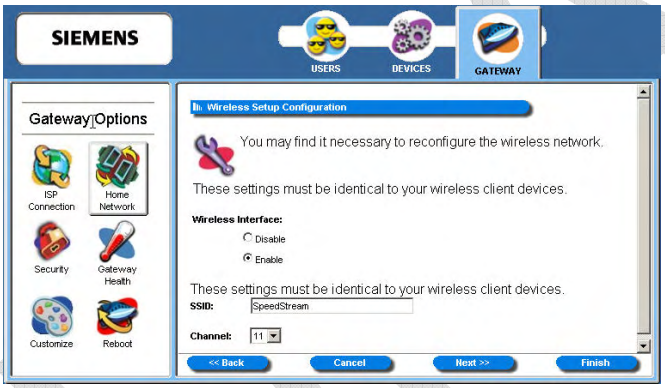
Wireless Network

Configure the wireless network using this option. The wireless settings on the Gateway must match those of any wireless clients on your network.

To configure the wireless network:

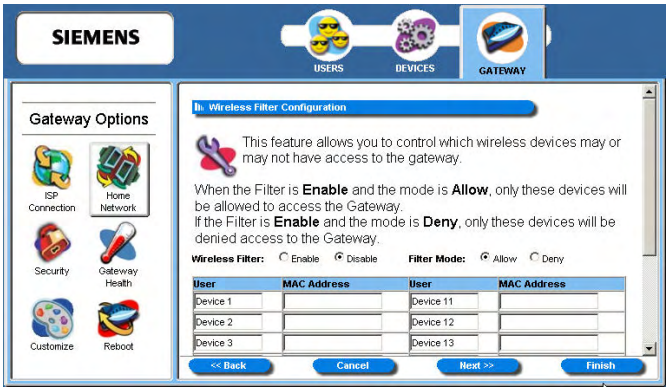
1. Click the **Configure the Local Gigaset Gateway Wireless Network** hyperlink. This displays the "Wireless Summary" window.

2. Click **Begin Wireless Wizard**. This displays the "Wireless Setup Configuration" window.



3. Select **Enable** to enable the **Wireless Interface**.
4. Type your wireless network ID in **SSID** (Service Set Identifier).
5. Optionally, select a channel ID from the **Channel** drop-down menu. This is typically done if you experience any interference with your wireless Gateway.
6. Click **Next**. This displays the "Wireless Security Configuration" window.

DRAFT



Set the wireless security level from the "Wireless Security Configuration" window. All wireless devices attached to the Gateway **MUST** have the same wireless security settings for your network to have proper communications and security.

7. From the **Security Mode** drop-down menu, select one of the following options:

   - **WEP 64-bits**
     Wireless Equivalency Privacy. WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 64-bit encryption, which is the least secure WEP option. Please see the section in this document titled Wireless Setup WEP 64-Bit Option (Advanced Home Networking) for more information.

   - **WEP 128-bits**
     Wireless Equivalency Privacy. WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is a most secure WEP option. Please see the section in this document titled Wireless Setup WEP 128-Bit Option (Advanced Home Networking) for more information.

   - **WPA PSK**
     Wi-Fi Protected Access. WPA security changes encryption keys after a specified amount of time. This is the most secure option for wireless networks. Please see the section in this document titled Wireless Setup WPA PSK Option (Advanced Home Networking) for more information.

8. Optionally, select the **Enable SSID Broadcast** option so wireless users can see the existence of the wireless Gateway with the associated SSID.

DRAFT

Wireless Setup WEP 64-Bit Option (Advanced Home Network)

WEP security offers the same security offered by a wired LAN with encrypted packets. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer.

To use the WEP 64-bit option:

1. From the "Wireless Security Configuration" window, select **WEP 64-bits** from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless 64-bit WEP Configuration" window.

3. Select one of the following **Authentication** options:
   - **Open System**
     Open system keys are always authenticated at the device level. After authentication, data is encrypted between the Gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
   - **Shared Key**
     Shared keys accept a string of unencrypted data from a device. The Gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
4. Type a phrase in **Passphrase**. The passphrase is used to generate the 64-bit keys. The passphrase can be between 1 and 32 characters.
5. Click **Generate Keys**. The system responds by generating keys that display in the boxes under **Passphrase**. Four different keys are generated.
6. Select one of the four keys to use for encryption.
7. Click **Next**. This displays the "Wireless Filter Configuration" window.

DRAFT

Wireless Setup WEP 128-Bit Option (Advanced Home Network)

WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is the most secure WEP option. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer.

To use the WEP 128-bit option:

1. From the "Wireless Security Configuration" window, select **WEP 128-bits** from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless 128-bit WEP Configuration" window.

3. Select one of the following **Authentication** options:
   - **Open System**
     Open system keys are always authenticated at the device level. After authentication, data is encrypted between the Gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
   - **Shared Key**
     Shared keys accept a string of unencrypted data from a device. The Gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
4. Type a phrase in **Passphrase**. The passphrase is used to generate the 128-bit key. The passphrase can be between 1 and 32 characters.
5. Click **Generate Keys**. The system responds by generating keys that display in the boxes under **Passphrase**.
6. Select one of the keys to use for encryption.
7. Click **Next**. This displays the "Wireless Filter Configuration" window.

DRAFT

Wireless Setup WPA PSK Option (Advanced Home Network)

WPA security changes encryption keys after a specified amount of time. This is the most secure option for wireless networks. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer.

To use the WPA option:

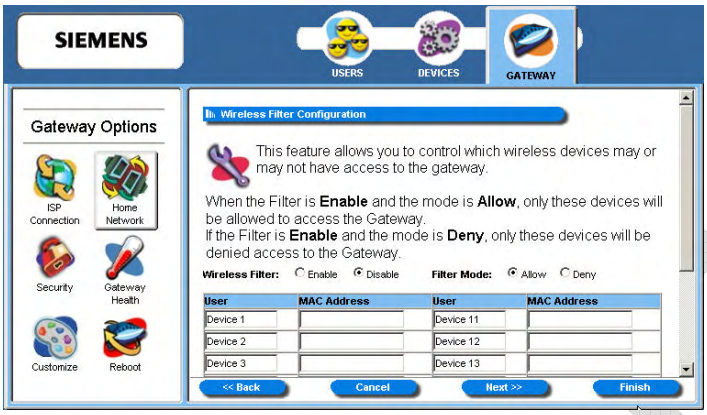
1. From the "Wireless Security Configuration" window, select **WPA PSK** from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless WPA Configuration" window.

3. Select one of the following from the **Algorithms** drop-down menu:
   - **TKIP**
     Temporal Key Integrity Protocol is a more powerful security protocol than WEP. This option verifies the security configuration after encryption keys are determined, synchronizes changing of the unicast encryption key for each frame, and determines a unique starting unicast encryption key for each pre-shared key authentication.
   - **AES**
     Advanced Encryption Standard) supports a private key algorithm that ranges from 128 to 256 bits.
4. Type a key in **Shared Key**. The shared key is used to generate a dynamic encryption key for Gateway security.
5. Type a numeric value (in seconds) in **Group Key Renewal** to specify time to lapse between changing the key. The minimum time value is 30.
6. Click **Next**. This displays the "Wireless Filter Configuration" window.

DRAFT

Wireless Filter and Options Configuration

Control access to the Gateway of wireless devices based on the MAC address of the device using the "Wireless Filter Configuration" window. A MAC (Media Access Control) address refers to a hardware address that uniquely identifies each device of a network. Refer to the user documentation for each device you wish to deny or allow access for a particular MAC address.



To configure the wireless filter:

1. Select one of the following **Wireless Filter** options:
   - **Enable**
     Enable wireless filtering.
   - **Disable**
     Disable wireless filtering. If wireless filtering is disabled, all devices have access to the Gateway.
2. If wireless filtering is enabled, select one of the following **Filter Mode** options:
   - **Allow**
     Permits access to all the MAC addresses entered in the table.
   - **Deny**
     Restricts Gateway access to all the MAC addresses entered in the table.
3. Type the MAC address in the **MAC Address** column next to each device you either want to permit or restrict access.
4. Click **Next**. This displays the "Wireless Options Configuration" window.

DRAFT

5. Optionally, configure the following items:

   - **Data Transfer Rate**
     If a particular wireless client is unable to auto-negotiate a connection to the Gateway, the data transfer rate may be set to a specific data rate such as 11 Mbps for 802.11b wireless clients.
   - **RTS/CTS Threshold**
     A group of wireless clients may experience difficulty communicating with the Gateway without interrupting each other's communications. If this occurs, the RTS/CTS threshold may be set to a higher number to allow them each a longer period in which to communicate with the Gateway before the priority is switched to another wireless client wishing to transmit data.
   - **Fragmentation Threshold**
     The fragmentation threshold may be lowered to improve reliability in an excessively "noisy" wireless environment if changing channels does not provide significant enough improvement.

If you wish to reset the options in the "Wireless Options Configuration" window, click **Restore Default Values**. The system responds by restoring all the advanced features on this page.

6. Click **Next**. This displays the "Wireless Wizard" finish window.
7. Click **Finish** to save the settings.
8. Click **Reboot** for your wireless configuration to take effect.

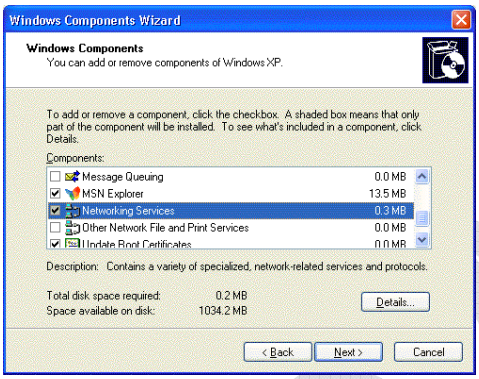
DRAFT

UPnP (Universal Plug and Play)

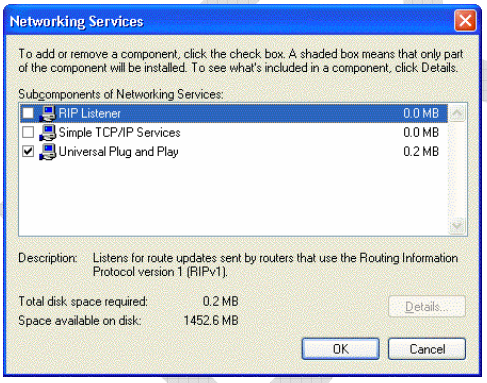
Microsoft UPnP allows the Gateway to communicate directly with certain Windows operating systems to trade information about the special needs of certain applications (such as messaging programs and interactive games) as well as provide information about other devices on the network. This communication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

Only certain versions of Windows 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 Windows Components** to open the "Windows Components Wizard" window**.**

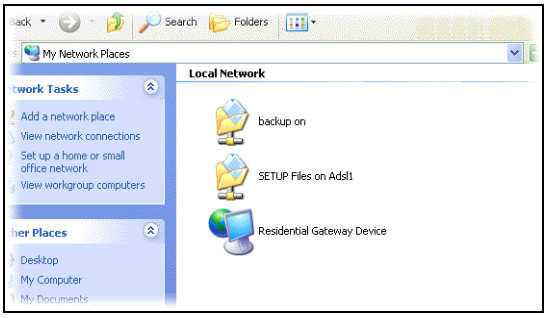


3. Select **Network Services** and click **Details**. This displays the "Networking Services" window.



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.

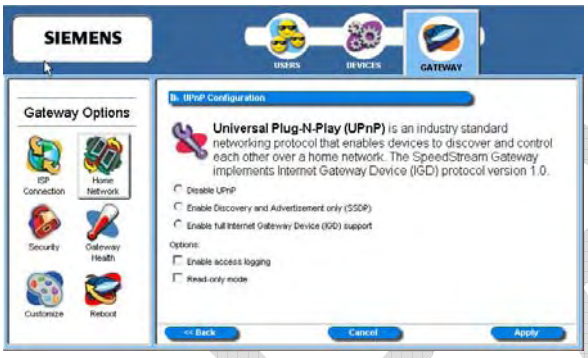
DRAFT



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:

1. Click **Configure the Universal Plug and Play Settings** link to display the "UPnP Configuration" window:



2. 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.

3. 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.

4. Click **Apply** to accept the settings. This displays the UPnP finish window.
5. Click **Reboot**.

DRAFT