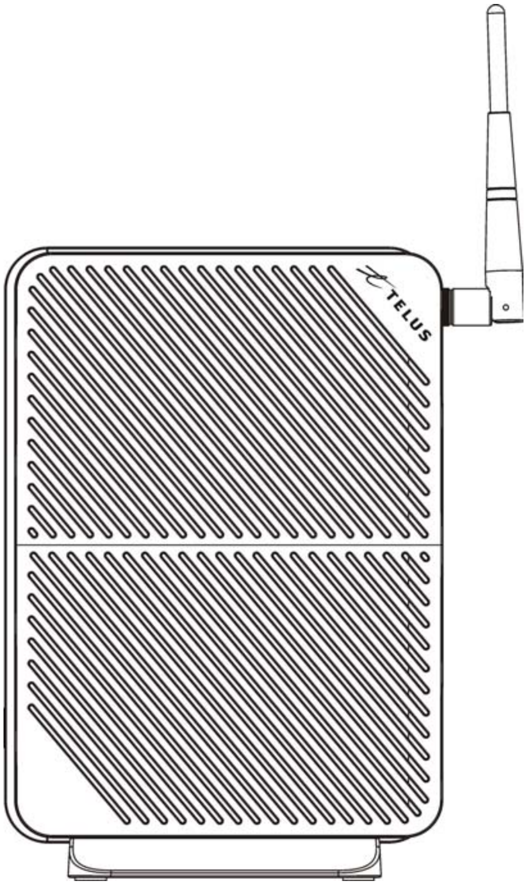
VSG1432

User Setup Guide

802.11n Wireless VDSL2 4-port Gateway



Default Login Details

IP Address	http://192.168.1.254
Username	admin
Password	telus

Firmware Version 1.10
Edition 1, 10/2011

ZyXEL

www.zyxel.com

Contents Overview

CHAPTER 1

Introducing the VSG1432

1.1 Overview

The VSG1432 is a VDSL2 router and Gigabit Ethernet gateway with a four-port built-in Ethernet switch and IEEE 802.11n wireless. The VSG1432 allows wired and wireless clients to safely access the Internet. The built-in firewall blocks unauthorized access to your network.

Only use firmware for your Device's specific model. Refer to the label on the bottom of your Device.

1.2 Managing the Device

Use the Web Configurator for management of the Device using a (supported) web browser. See Section 2.1.1 on page 13 for information on accessing the Web Configurator.

1.3 Good Habits for Managing the Device

Do the following things regularly to make the Device more secure and to manage the Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.

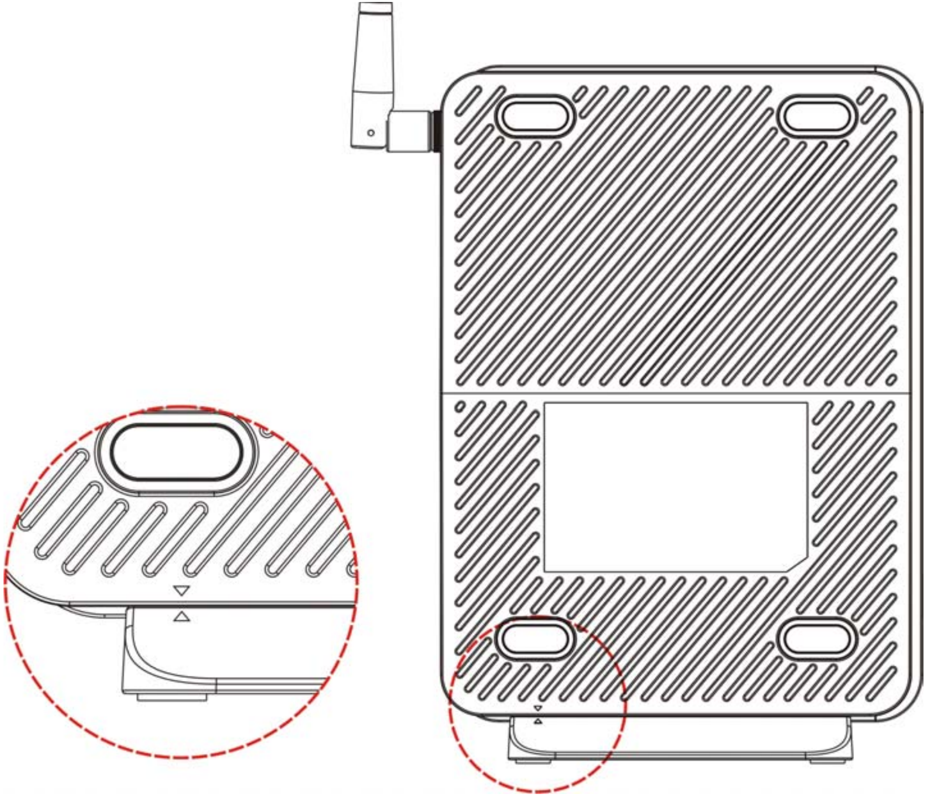
1.4 Hardware Setup

Place the Device flat on a desk or table or on the stand for a vertical installation.

Remove the Device's clear plastic covers before using it.

To connect the stand, line up the arrow on the stand with the arrow on the bottom of the device as shown.

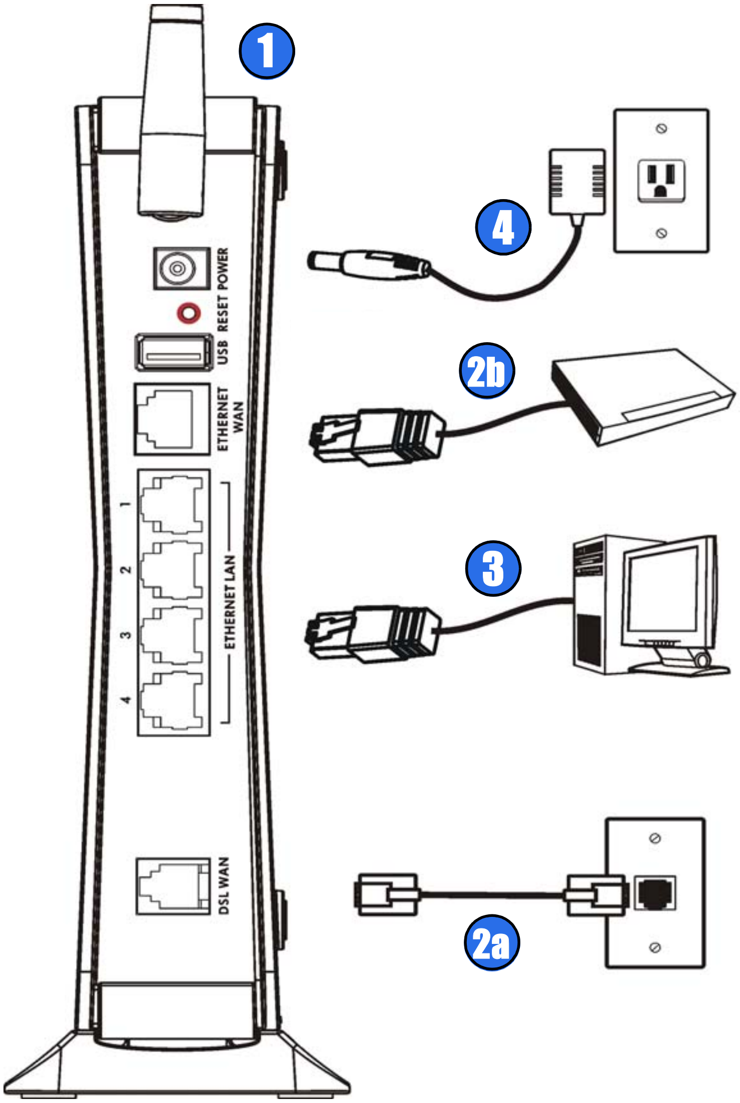
Figure 1 Connecting the Stand



1.5 Hardware Connections

To connect your Device:

Figure 2 Hardware Connections



1 Attach the antenna and point it up.

2 Do one of the following for your Internet connection:

2a **DSL WAN**: Use a telephone cable to connect your Device's **DSL WAN** port to a telephone jack (or the DSL or modem jack on a splitter if you have one).

2b **ETHERNET WAN**: If you already have a broadband router or modem, use an Ethernet cable to connect the **ETHERNET WAN** port to it for Internet access.

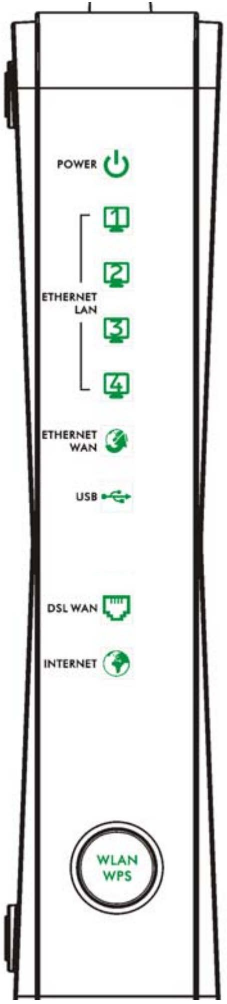
3 **ETHERNET LAN**: Use an Ethernet cable to connect a computer to an **ETHERNET LAN** port for initial configuration and/or Internet access.

4 **POWER**: Use the provided power adaptor to connect the **POWER** socket to an appropriate power source. Make sure the power at the outlet is on. After connecting the power adaptor, look at the lights on the front panel.

1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 3 LEDs on the Device



None of the LEDs are on if the Device is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Device is receiving power and ready for use.
		Blinking	The Device is self-testing.
	Red	On	The Device detected an error while self-testing, or there is a device malfunction.
		Off	The Device is not receiving power.
		Blinking	Firmware upgrade is in progress.
ETHERNET LAN 1-4	Green	On	The Device has a successful 100 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The Device is sending or receiving data to/from the LAN at 100 Mbps.
		Off	The Device does not have an Ethernet connection with the LAN.
ETHERNET WAN	Green	On	The Gigabit Ethernet connection is working.
		Blinking	The Device is sending or receiving data to/from the Gigabit Ethernet link.
		Off	There is no Gigabit Ethernet link.
USB	Green	On	The Device recognizes a USB connection.
		Blinking	The Device is sending/receiving data to /from the USB device connected to it.
		Off	The Device does not detect a USB connection.
DSL WAN	Green	On	The DSL line is up.
		Blinking	The Device is initializing the DSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The Device has an IP connection but no traffic. Your device has a WAN IP address and the DSL connection is up.
		Blinking	The Device is sending or receiving IP traffic.
		Off	There is no Internet connection or the gateway is in bridged mode.
WLAN/WPS	Green	On	The wireless network is activated.
		Blinking	The Device is communicating with other wireless clients.
	Green and Orange	Blinking	The Device is setting up a WPS connection.
		Off	The wireless network is not activated.

1.7 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to the default.

1 Make sure the **POWER** LED is on (not blinking and not red or flashing red).

2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

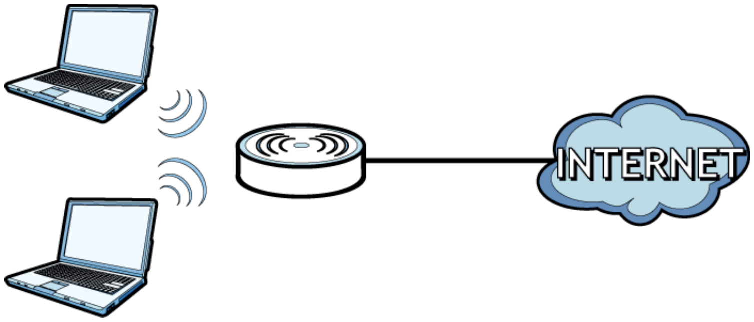
Note: The default username and password are on the label on the bottom of the Device.

1.8 Wireless Access

The Device is a wireless Access Point (AP) for wireless clients, such as notebook computers, smartphones or tablets. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables.

You can connect to your wireless network using the WPS button, without having to access the Web Configurator.

Figure 4 Wireless Access Example



1.8.1 Using the WLAN/WPS Button

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCMCIA card), which can be identified by the WPS logo: .

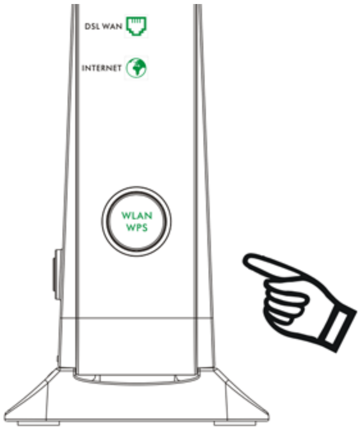
If the wireless network is turned off, enable wireless in the **Wireless** section of the Web Configurator. The **WLAN/WPS** LED will be green when wireless is enabled.

You can use the **WLAN/WPS** button to quickly set up a secure wireless connection between the Device and a WPS-compatible client device by adding one device at a time.

To activate WPS:

1 Make sure the **POWER** LED is green and not blinking.

2 Press the **WLAN/WPS** button for five seconds and release it.



3 Enable WPS on another WPS-enabled client device within range of the Device. If you do not know how to enable WPS on that client device, refer to its manual. The **WLAN/WPS** LED flashes green and orange while the Device sets up a WPS connection with the other WPS enabled client device.

4 Once the connection is successfully made, the **WLAN/WPS** LED shines green.

CHAPTER 2
User Setup Guide

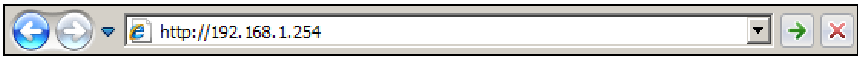
2.1 Overview

This guide shows you how to use the Device's various features.

- Setting Up a Secure Wireless Network, see page 14
- Setting Up Multiple Wireless Groups, see page 22
- Wireless MAC Authentication for Blocking a Computer's Access to the Wireless Network, see page 25
- Setting Up NAT Forwarding for a Game Server, see page 27
- Access Your Home Computer from the Internet Using DDNS, see page 30
- Firewall Setup, see page 32
- MAC Filter Setup for Blocking LAN Computers, see page 35
- Scheduler Rules and Parental Control, see page 37
- LAN DHCP for IP Addressing Assignment, see page 40
- Check the Firmware Version, see page 43
- Restore to Factory Default, see page 44

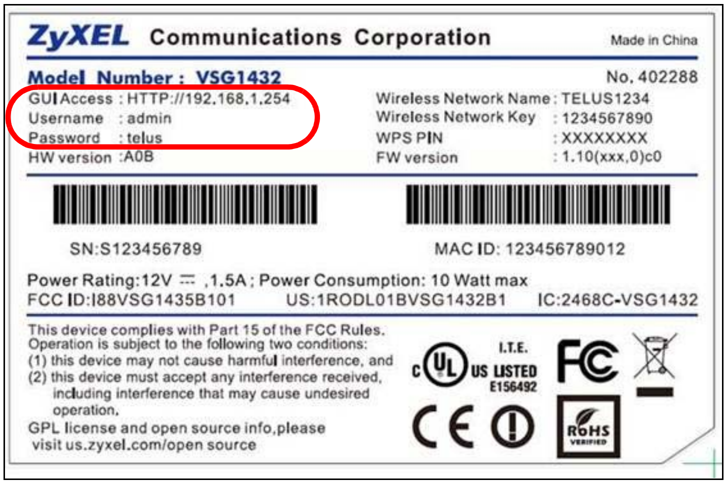
2.1.1 Access the Web Configurator for Setting Up the Device

You will need to log in to the Web Configurator to configure the Device. Enter the LAN IP address of the Device in your web browser. This is http://192.168.1.254 by default.



http://192.168.1.254

Note: The default LAN IP address, username and password are on the label on the bottom of the Device.



ZyXEL Communications Corporation Made in China

Model Number : VSG1432 No. 402288

GUI Access : HTTP://192.168.1.254
Username : admin
Password : telus
HW version :A0B

Wireless Network Name : TELUS1234
Wireless Network Key : 1234567890
WPS PIN : XXXXXXXX
FW version : 1.10(xxx,0)c0

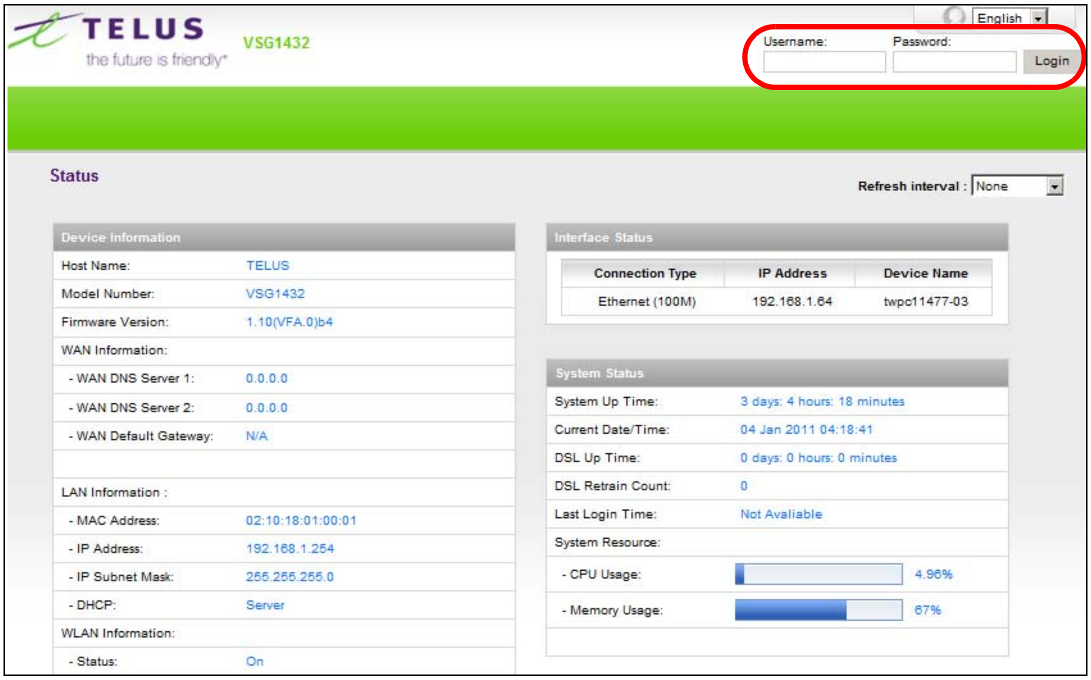
SN:S123456789 MAC ID: 123456789012

Power Rating:12V ⎓ ,1.5A ; Power Consumption: 10 Watt max
FCC ID:I88VSG1435B101 US:1RODL01BVSG1432B1 IC:2468C-VSG1432

This device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:
(1) this device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

GPL license and open source info,please visit us.zyxel.com/open source

Enter the **Username** and **Password** in the fields in the top right corner. The default **Username** is **admin** and the default **Password** is **telus**. Click **Login**.



Status

Refresh interval : None

Device Information	
Host Name:	TELUS
Model Number:	VSG1432
Firmware Version:	1.10(VFA.0)b4
WAN Information:	
- WAN DNS Server 1:	0.0.0.0
- WAN DNS Server 2:	0.0.0.0
- WAN Default Gateway:	N/A
LAN Information :	
- MAC Address:	02:10:18:01:00:01
- IP Address:	192.168.1.254
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- Status:	On

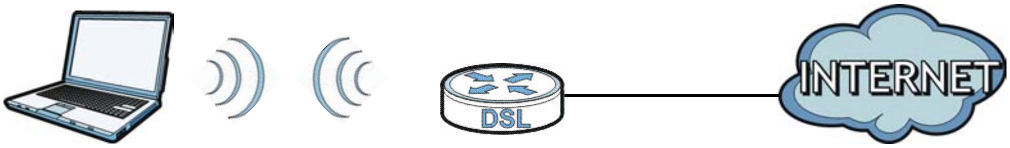
Interface Status

Connection Type	IP Address	Device Name
Ethernet (100M)	192.168.1.64	twpc11477-03

System Status	
System Up Time:	3 days: 4 hours: 18 minutes
Current Date/Time:	04 Jan 2011 04:18:41
DSL Up Time:	0 days: 0 hours: 0 minutes
DSL Retrain Count:	0
Last Login Time:	Not Avaliable
System Resource:	
- CPU Usage:	4.96%
- Memory Usage:	67%

2.2 Setting Up a Secure Wireless Network

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the Device serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.



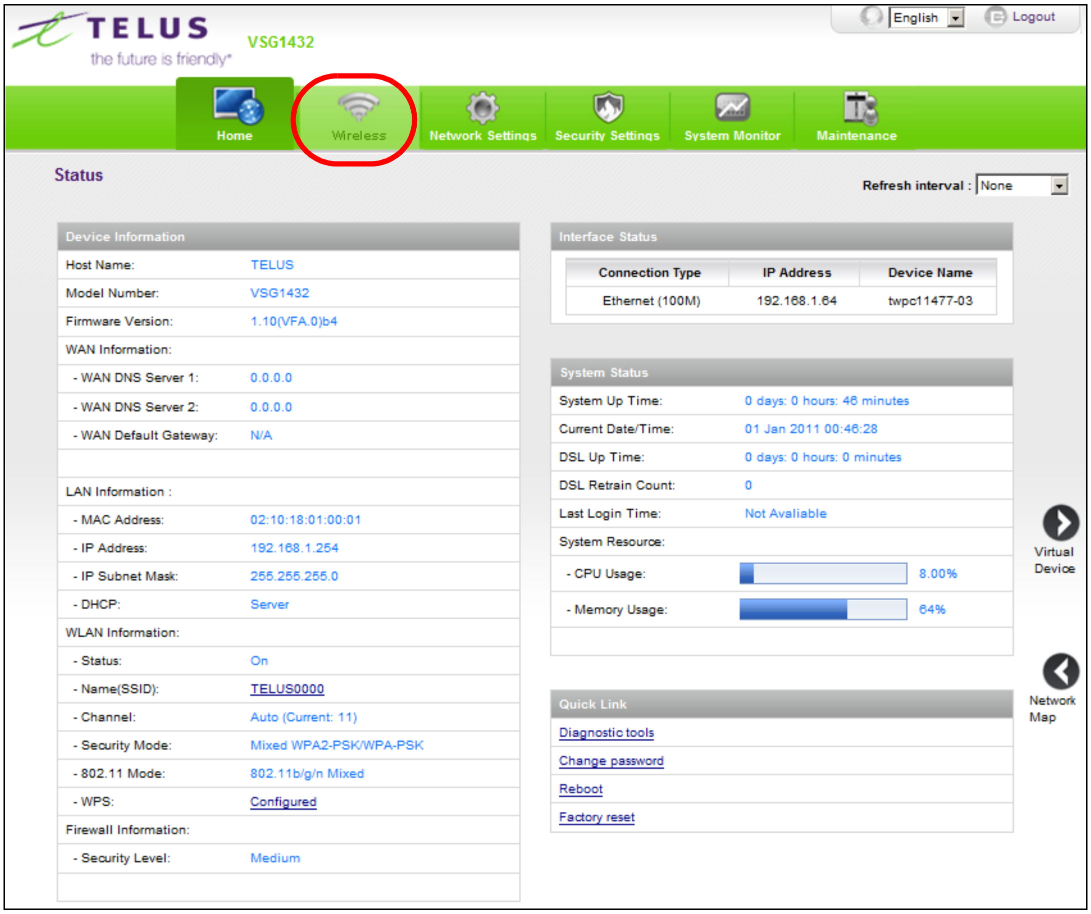
Thomas has to configure the wireless network settings on the Device. Then he can set up a wireless network using WPS (Section 2.2.2 on page 16) or manual configuration (Section 2.2.3 on page 20).

2.2.1 Configuring the Wireless Network Settings

This example uses the following parameters to set up a wireless network.

SSID	Example
Security Mode	Mixed WPA2-PSK/WPA-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b/g/n Mixed

1 Click **Wireless** to open the **Basic Wireless Setup** screen.



Status

Refresh interval : None

Device Information	
Host Name:	TELUS
Model Number:	VSG1432
Firmware Version:	1.10(VFA.0)b4
WAN Information:	
- WAN DNS Server 1:	0.0.0.0
- WAN DNS Server 2:	0.0.0.0
- WAN Default Gateway:	N/A
LAN Information :	
- MAC Address:	02:10:18:01:00:01
- IP Address:	192.168.1.254
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- Status:	On
- Name(SSID):	TELUS0000
- Channel:	Auto (Current: 11)
- Security Mode:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured
Firewall Information:	
- Security Level:	Medium

Interface Status

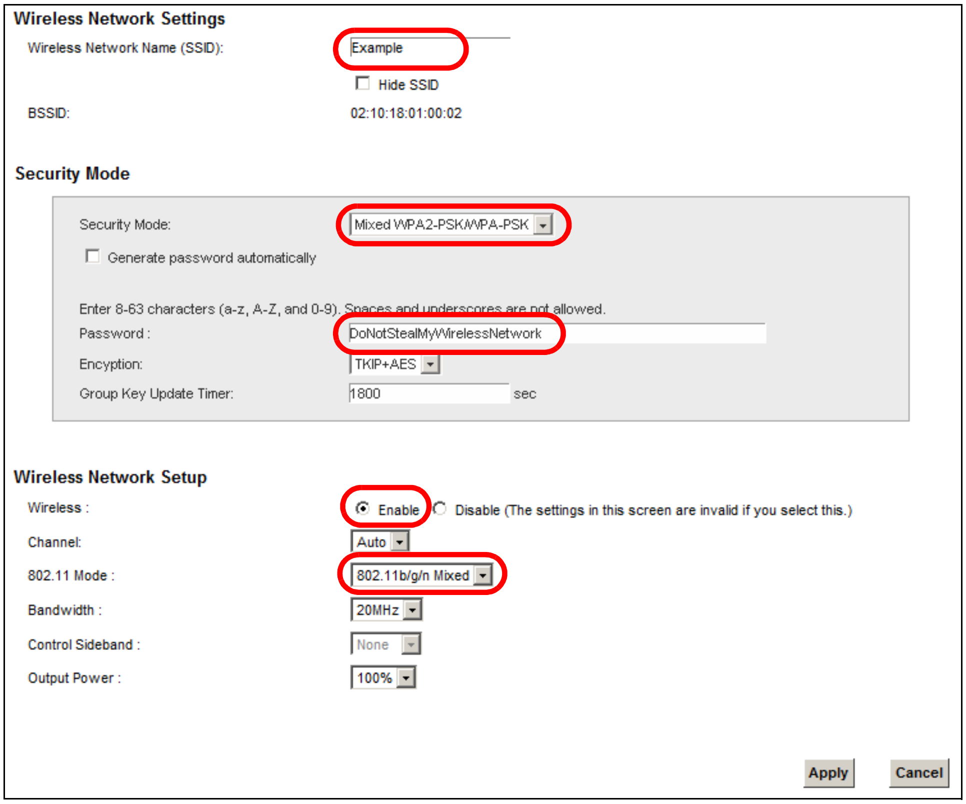
Connection Type	IP Address	Device Name
Ethernet (100M)	192.168.1.64	twpc11477-03

System Status	
System Up Time:	0 days: 0 hours: 46 minutes
Current Date/Time:	01 Jan 2011 00:46:28
DSL Up Time:	0 days: 0 hours: 0 minutes
DSL Retrain Count:	0
Last Login Time:	Not Avaliable
System Resource:	
- CPU Usage:	8.00%
- Memory Usage:	64%

Quick Link

- Diagnostic tools
- Change password
- Reboot
- Factory reset

1 Select **Mixed WPA2-PSK/WPA-PSK** as the security mode. Deselect **Generate password automatically** and enter the **Pre-Shared Key** in the **Password** field. Select **Enable** in the **Wireless** field. Select **802.11b/g/n Mixed** in the **802.11 Mode** field. Click **Apply**.



Wireless Network Settings

Wireless Network Name (SSID): Example

□ Hide SSID

BSSID: 02:10:18:01:00:02

Security Mode

Security Mode: Mixed WPA2-PSK/WPA-PSK

□ Generate password automatically

Enter 8-63 characters (a-z, A-Z, and 0-9). Spaces and underscores are not allowed.

Password : DoNotStealMyWirelessNetwork

Encyption: TKIP+AES

Group Key Update Timer: 1800 sec

Wireless Network Setup

Wireless : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Channel: Auto

802.11 Mode : 802.11b/g/n Mixed

Bandwidth : 20MHz

Control Sideband : None

Output Power : 100%

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the Device (see Section 2.2.2 on page 16). He can also use the notebook's wireless client to search for the Device (see Section 2.2.3 on page 20).

2.2.2 Using WPS

This section shows you how to set up a wireless network using WPS. It uses the Device as the AP and ZyXEL NWD210N as the wireless client which connects to the notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCMCIA card), which can be identified by the WPS logo: .

There are two WPS methods to set up the wireless client settings:

- **Push Button Configuration (PBC)** - simply press a button. This is the easier of the two methods.
- **PIN Configuration** - configure a Personal Identification Number (PIN) on the Device. A wireless client must also use the same PIN in order to download the wireless network settings from the Device.

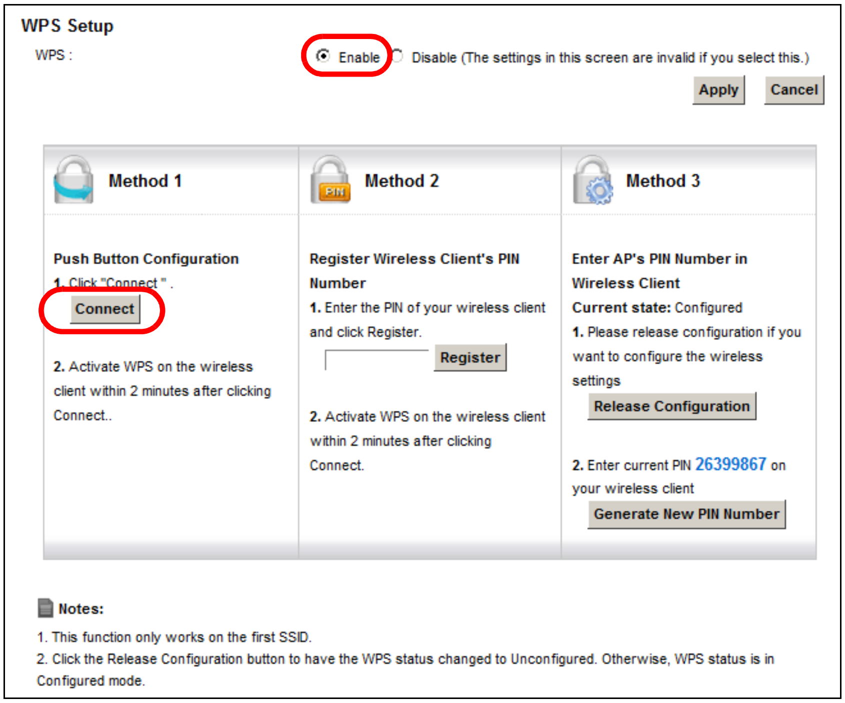
Push Button Configuration (PBC)

1 Make sure that your Device is turned on and your notebook is within the cover range of the wireless signal.

2 Make sure that you have installed the wireless client driver and utility in your notebook.

3 In the wireless client utility, go to the WPS setting page. Enable WPS and press the WPS button (**Start** or **WPS** button).

4 Push and hold the **WPS** button located on the Device’s front panel for more than 5 seconds. Alternatively, you may log into Device’s web configurator and go to the **Network Settings > Wireless > WPS** screen. Enable the WPS function and click **Apply**. Then click the **Connect** button.



WPS Setup

WPS : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Method 1

Push Button Configuration

1. Click "Connect" .

2. Activate WPS on the wireless client within 2 minutes after clicking Connect..

Method 2

Register Wireless Client's PIN Number

1. Enter the PIN of your wireless client and click Register.

2. Activate WPS on the wireless client within 2 minutes after clicking Connect.

Method 3

Enter AP's PIN Number in Wireless Client

Current state: Configured

1. Please release configuration if you want to configure the wireless settings

2. Enter current PIN 26399867 on your wireless client

Notes:

1. This function only works on the first SSID.

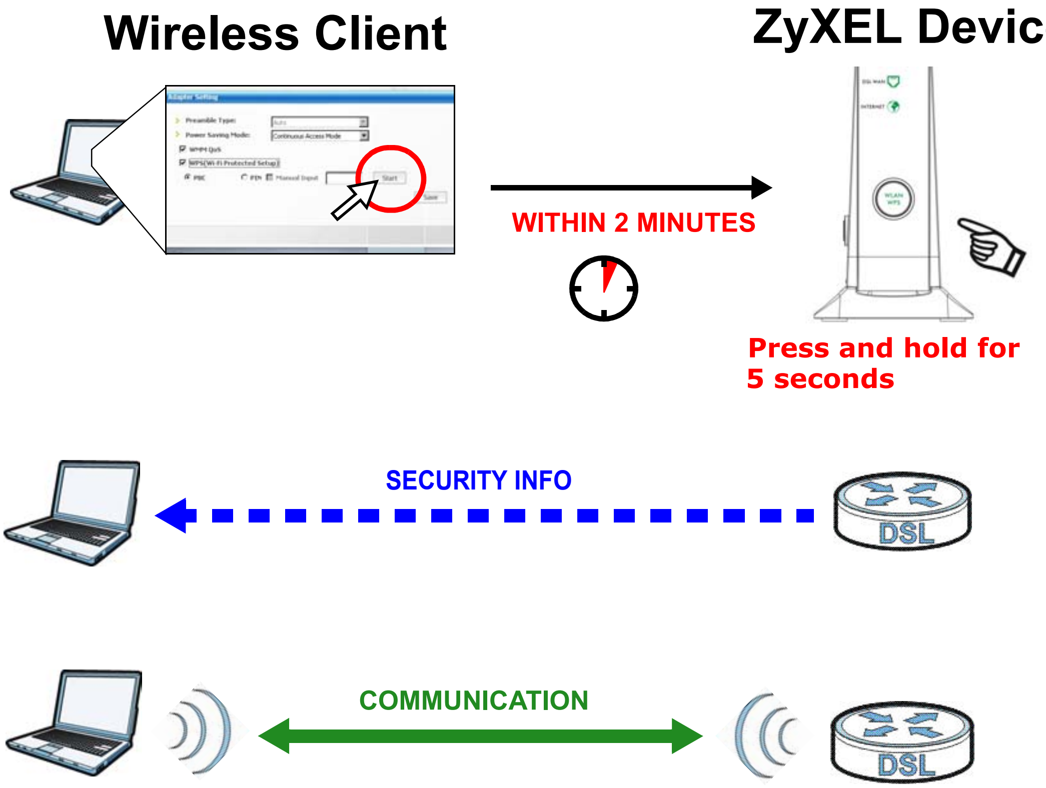
2. Click the Release Configuration button to have the WPS status changed to Unconfigured. Otherwise, WPS status is in Configured mode.

Note: Your Device has a WPS button located on its front panel as well as a WPS button in its configuration utility. Both buttons have exactly the same function: you can use one or the other.

Note: It doesn’t matter if the WPS button on the wireless client or AP is pressed first. You must press the button on the second device within two minutes of pressing the button on the first device.

The Device sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the Device securely.

The following figure shows you an example of how to set up a wireless network and its security by pressing a button on both Device and wireless client.

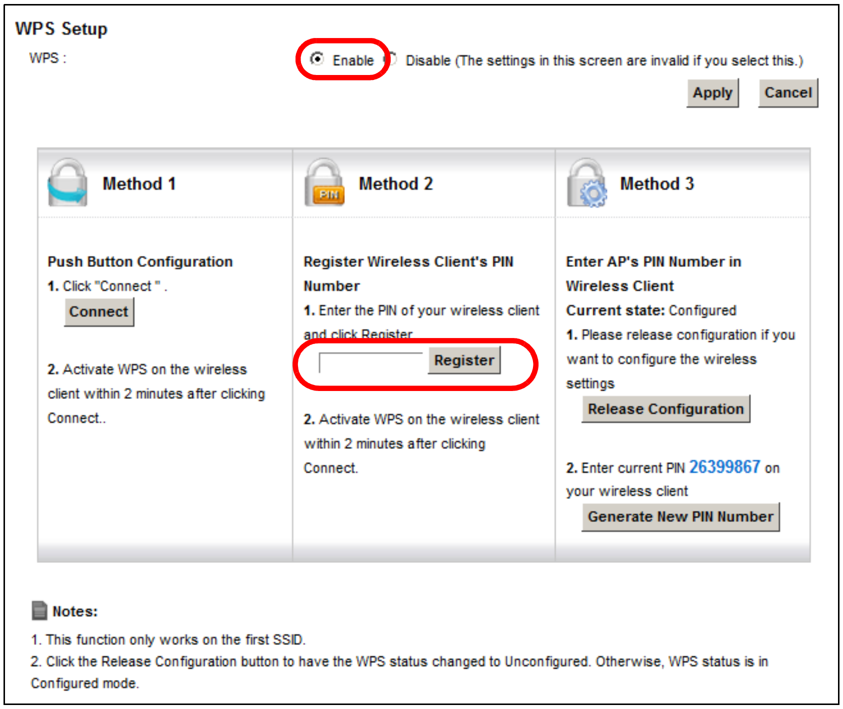


PIN Configuration

When you use the PIN configuration method, you need to use both the Device’s web configurator and the wireless client’s utility.

1 Launch your wireless client’s configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.

2 Log into Device’s web configurator and go to the **Wireless > WPS** screen. Enable the WPS function and click **Apply**.



WPS Setup

WPS : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Apply Cancel

Method 1

Push Button Configuration

1. Click "Connect " .

Connect

2. Activate WPS on the wireless client within 2 minutes after clicking Connect..

Method 2

Register Wireless Client's PIN Number

1. Enter the PIN of your wireless client and click Register

Register

2. Activate WPS on the wireless client within 2 minutes after clicking Connect.

Method 3

Enter AP's PIN Number in Wireless Client

Current state: Configured

1. Please release configuration if you want to configure the wireless settings

Release Configuration

2. Enter current PIN 26399867 on your wireless client

Generate New PIN Number

Notes:

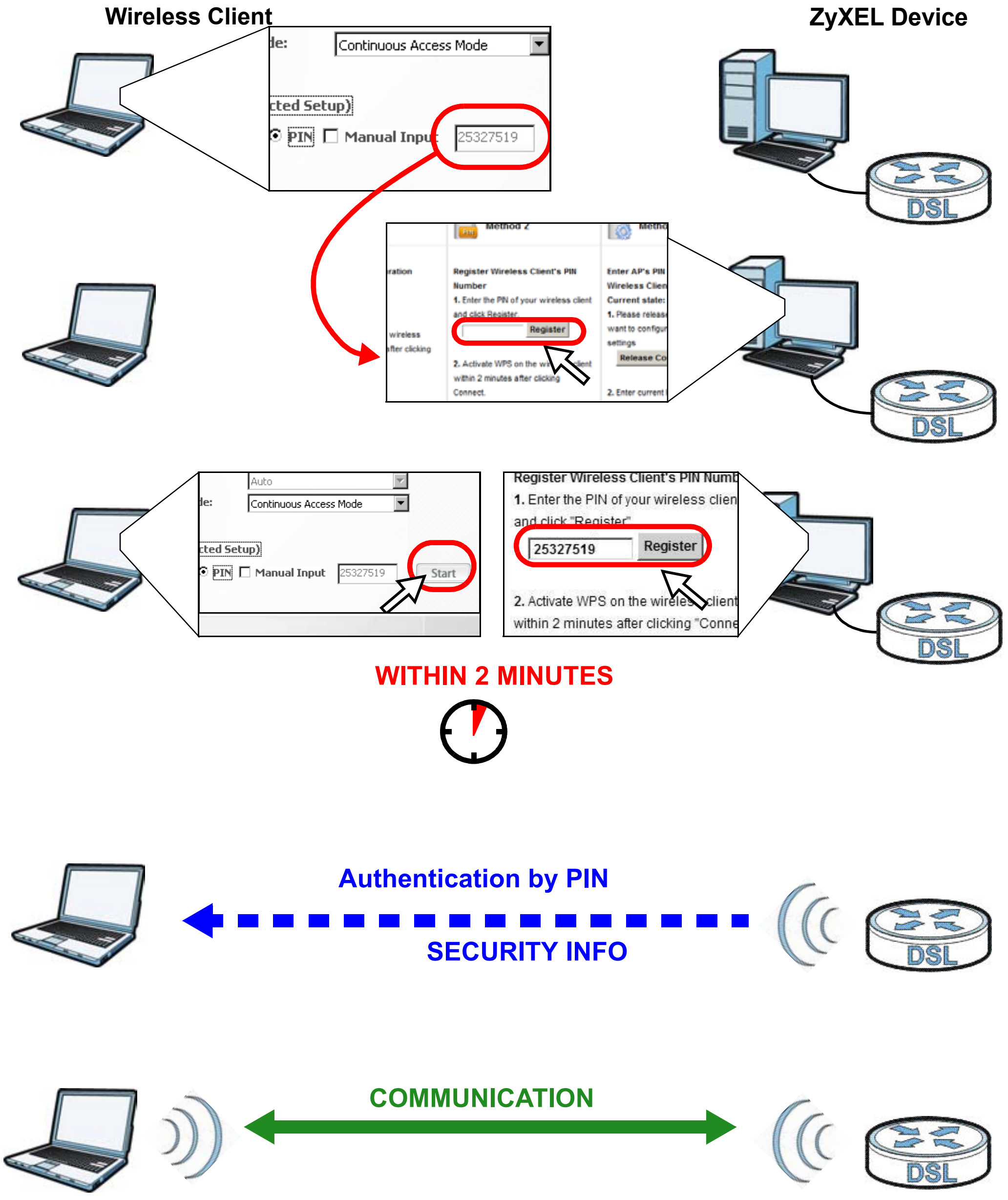
1. This function only works on the first SSID.

2. Click the Release Configuration button to have the WPS status changed to Unconfigured. Otherwise, WPS status is in Configured mode.

3 Enter the PIN number of the wireless client and click the **Register** button. Activate WPS function on the wireless client utility screen within two minutes.

The Device authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the Device securely.

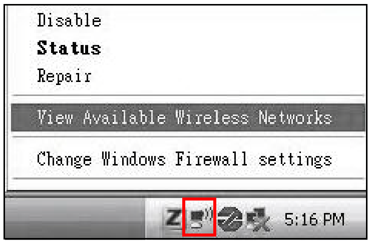
The following figure shows you how to set up a wireless network and its security on a Device and a wireless client by using PIN method.



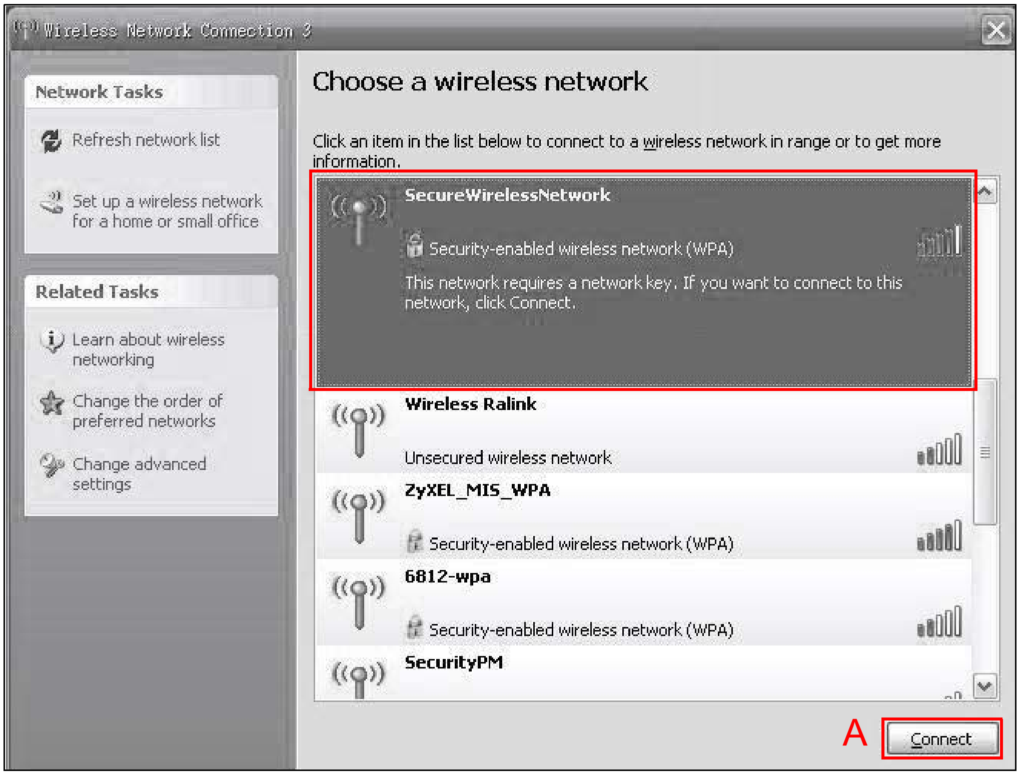
2.2.3 Without WPS

This section describes how to connect wirelessly to your Device. The connection procedure is shown here using Windows XP as an example.

1 Right-click the wireless adapter icon which appears in the bottom right of your computer monitor. Click **View Available Wireless Networks**.


Disable
Status
Repair
View Available Wireless Networks
Change Windows Firewall settings
5:16 PM

2 Select the Device’s **SSID** name and click **Connect** (A). The SSID “SecureWirelessNetwork” is given here as an example.


Wireless Network Connection 3
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

SecureWirelessNetwork
Security-enabled wireless network (WPA)
This network requires a network key. If you want to connect to this network, click Connect.

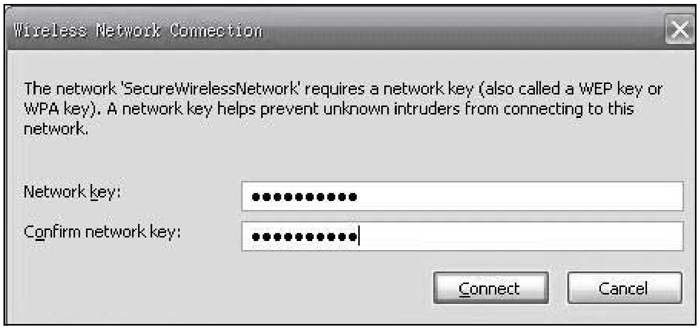
Wireless Ralink
Unsecured wireless network

ZyXEL_MIS_WPA
Security-enabled wireless network (WPA)

6812-wpa
Security-enabled wireless network (WPA)

SecurityPM

3 You are prompted to enter a password. Enter it and click **Connect**.



The network 'SecureWirelessNetwork' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Network key: ●●●●●●●●●●●

Confirm network key: ●●●●●●●●●●●

4 You may have to wait several minutes while your computer connects to the wireless network.

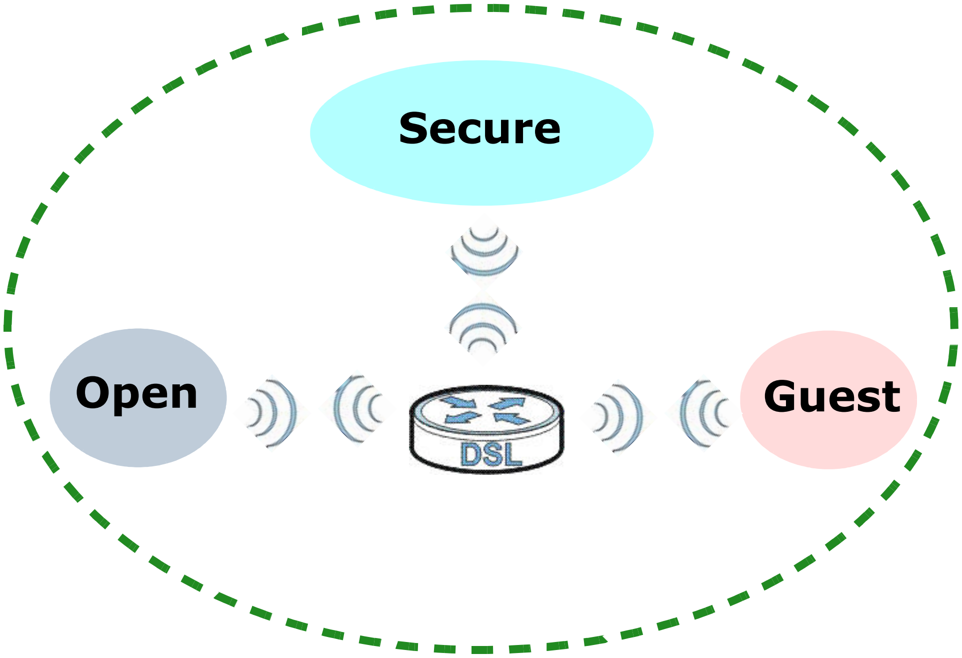
5 You should now be securely connected wirelessly to the Device.

Congratulations! Your computer is now ready to connect to the Internet wirelessly through your Device.

If you cannot connect wirelessly to the Device, check you have selected the correct SSID and entered the correct security key. If that does not work, ensure your wireless network adapter is enabled by clicking on the wireless adapter icon and clicking Enable.

2.3 Setting Up Multiple Wireless Groups

Thomas wants to create different wireless network groups for different types of users as shown in the following figure. Each group has its own SSID and security mode.

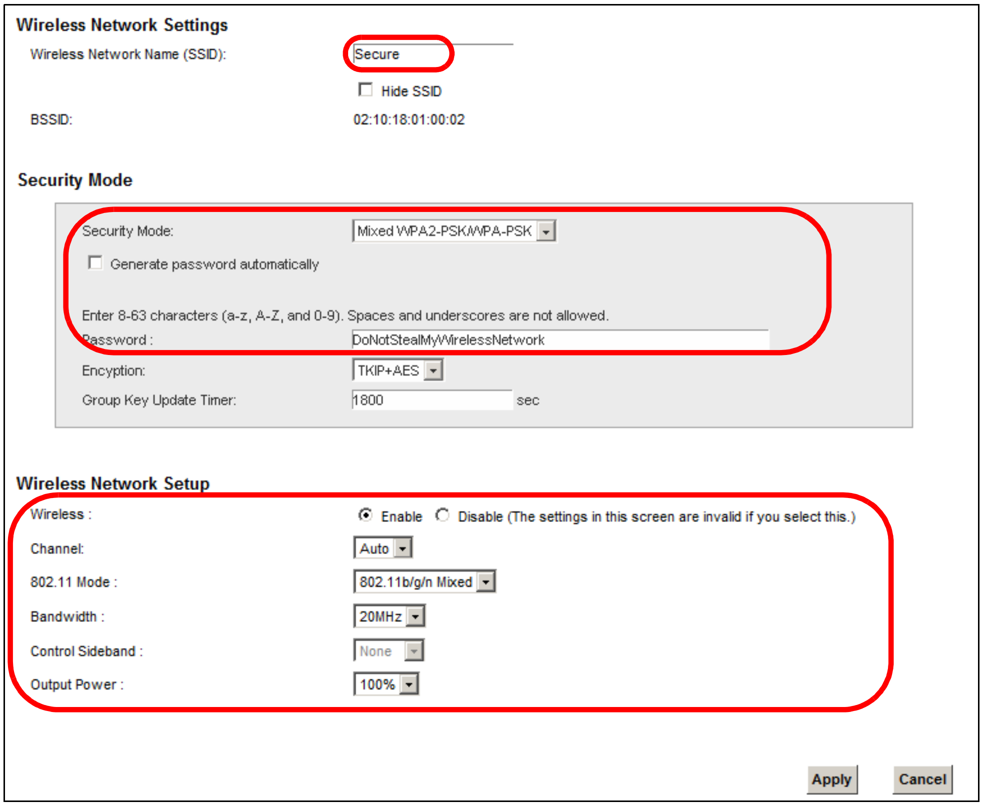


- Thomas will use the secured **Secure** wireless network group.
- Visitors will use the unsecured **Open** group.
- Guests will use the secured **Guest** group.

Company A will use the following parameters to set up the wireless network groups.

	SECURE	OPEN	GUEST
SSID	Secure	Open	Guest
Security Mode	Mixed WPA2-PSK/WPA-PSK	No Security	Mixed WPA2-PSK/WPA-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork		12345678

1 Click **Wireless** to open the **General** screen. Use this screen to set up a secure general wireless network group. Configure the screen using the provided parameters and click **Apply**.



Wireless Network Settings

Wireless Network Name (SSID): Secure

□ Hide SSID

BSSID: 02:10:18:01:00:02

Security Mode

Security Mode: Mixed WPA2-PSK/WPA-PSK

□ Generate password automatically

Enter 8-63 characters (a-z, A-Z, and 0-9). Spaces and underscores are not allowed.

Password : DoNotStealMyWirelessNetwork

Encyption: TKIP+AES

Group Key Update Timer: 1800 sec

Wireless Network Setup

Wireless : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Channel: Auto

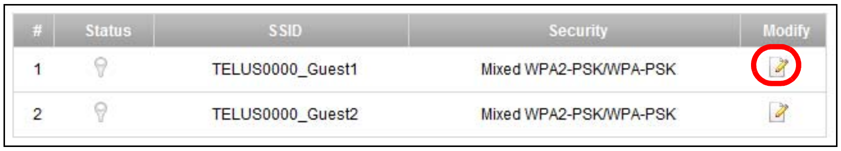
802.11 Mode : 802.11b/g/n Mixed

Bandwidth : 20MHz

Control Sideband : None

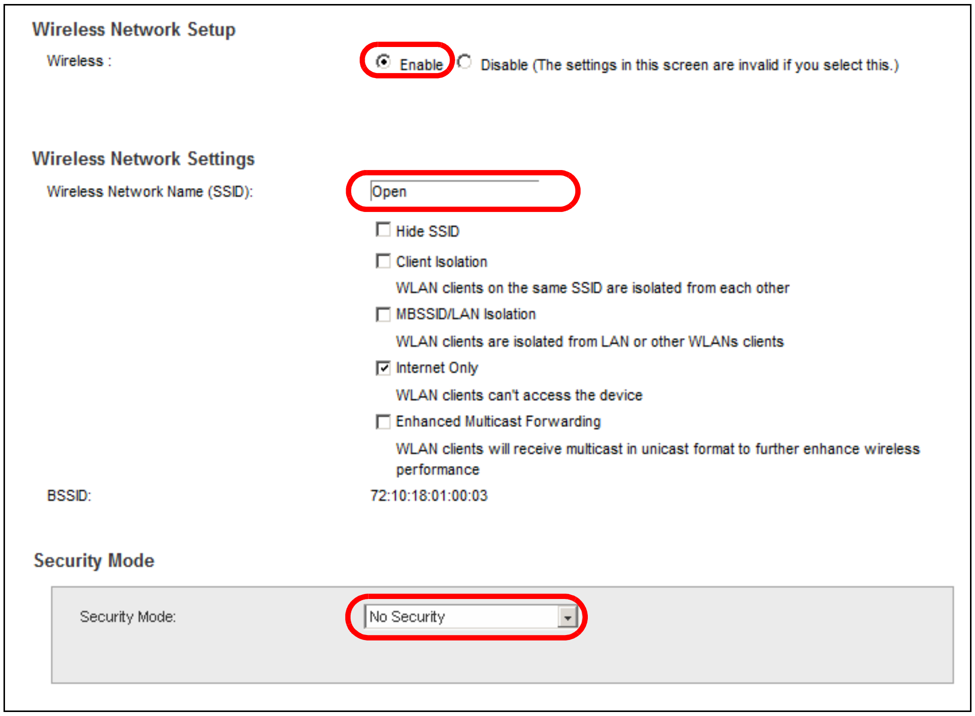
Output Power : 100%

2 Click **Wireless > Additional WLANs** to open the following screen. Click the **Edit** icon to configure the second wireless network group.



#	Status	SSID	Security	Modify
1		TELUS0000_Guest1	Mixed WPA2-PSK/WPA-PSK	✎
2		TELUS0000_Guest2	Mixed WPA2-PSK/WPA-PSK	✎

3 Configure the screen using the provided parameters and click **Apply**.



Wireless Network Setup

Wireless : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Wireless Network Settings

Wireless Network Name (SSID): Open

□ Hide SSID

□ Client Isolation

WLAN clients on the same SSID are isolated from each other

□ MBSSID/LAN Isolation

WLAN clients are isolated from LAN or other WLANs clients

☑ Internet Only

WLAN clients can't access the device

□ Enhanced Multicast Forwarding

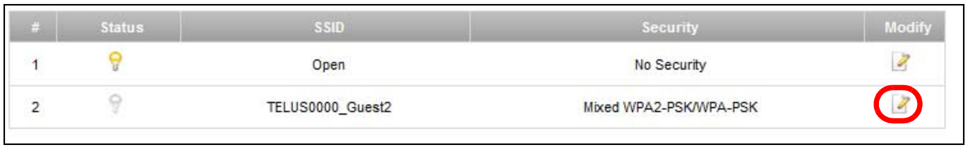
WLAN clients will receive multicast in unicast format to further enhance wireless performance

BSSID: 72:10:18:01:00:03

Security Mode

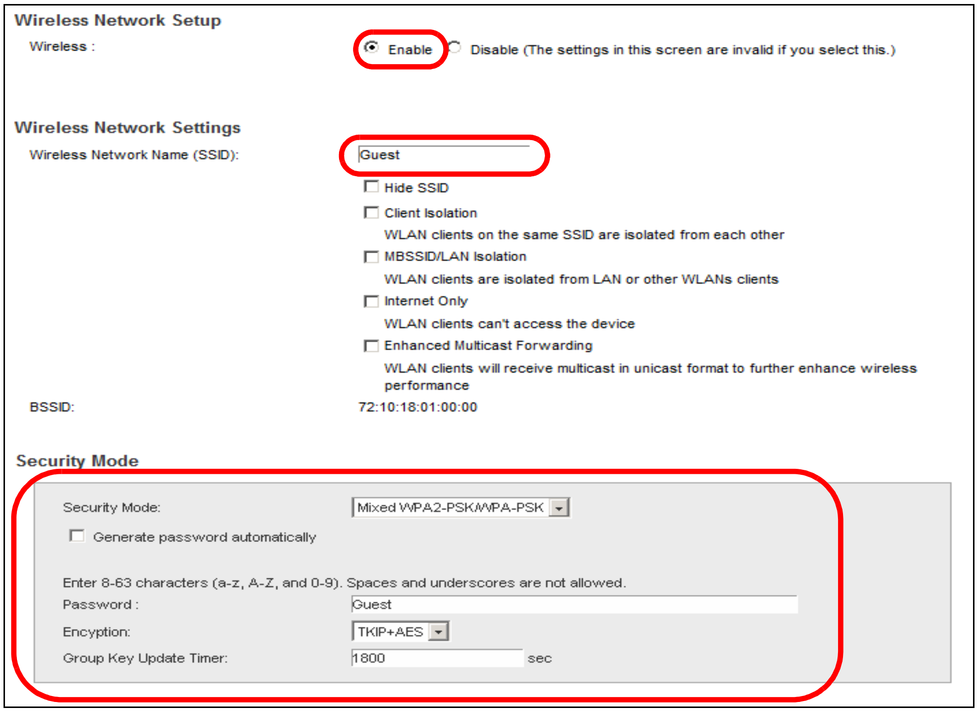
Security Mode: No Security

4 In the **Additional WLANs** screen, click the **Edit** icon to configure the third wireless network group.



#	Status	SSID	Security	Modify
1	●	Open	No Security	✎
2	○	TELUS0000_Guest2	Mixed WPA2-PSK/WPA-PSK	✎

5 Configure the screen using the provided parameters and click **Apply**.



Wireless Network Setup

Wireless : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Wireless Network Settings

Wireless Network Name (SSID): Guest

□ Hide SSID

□ Client Isolation

WLAN clients on the same SSID are isolated from each other

□ MBSSID/LAN Isolation

WLAN clients are isolated from LAN or other WLANs clients

□ Internet Only

WLAN clients can't access the device

□ Enhanced Multicast Forwarding

WLAN clients will receive multicast in unicast format to further enhance wireless performance

BSSID: 72:10:18:01:00:00

Security Mode

Security Mode: Mixed WPA2-PSK/WPA-PSK

□ Generate password automatically

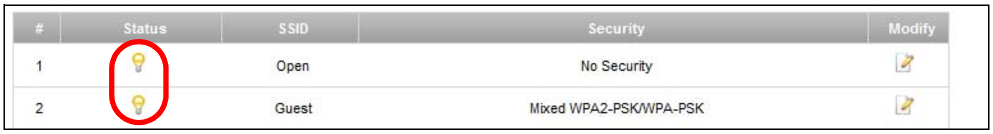
Enter 8-63 characters (a-z, A-Z, and 0-9). Spaces and underscores are not allowed.

Password : Guest

Encyption: TKIP+AES

Group Key Update Timer: 1800 sec

6 Check the status of **Open** and **Guest** in the **Additional WLANs** screen. The yellow bulbs signify that the SSIDs are active and ready for wireless access.



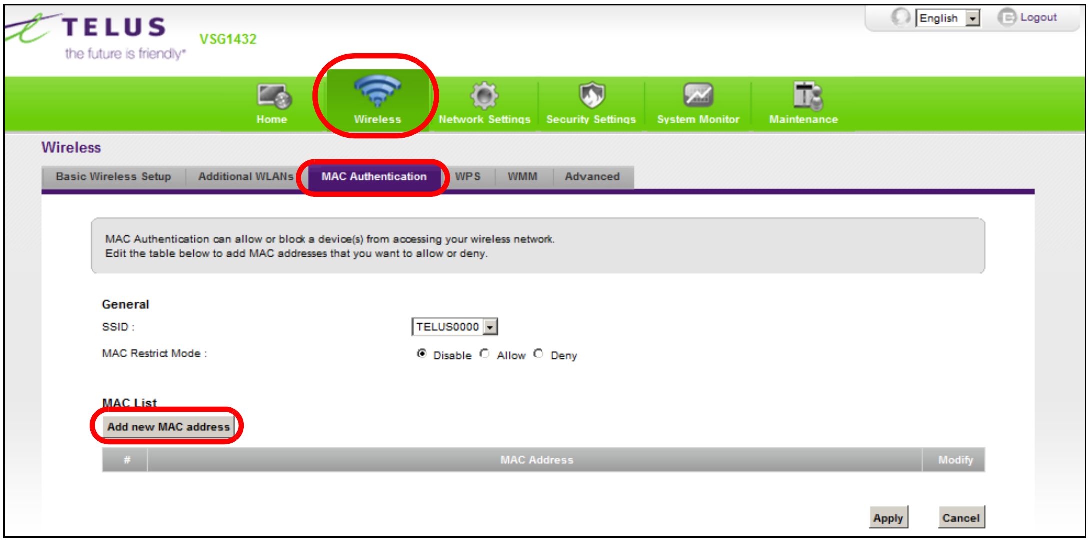
#	Status	SSID	Security	Modify
1	💡	Open	No Security	✎
2	💡	Guest	Mixed WPA2-PSK/WPA-PSK	✎

2.4 Wireless MAC Authentication for Blocking a Computer’s Access to the Wireless Network

This example shows how to configure **MAC Authentication** to use a computer’s MAC address to block it from accessing the wireless network.

Note: MAC Authentication is not a highly secure method of security.

1 Click the **Wireless** icon and click the **MAC Authentication** tab. In the **MAC Authentication** screen, click the **Add new MAC address** button.



MAC Authentication can allow or block a device(s) from accessing your wireless network.
Edit the table below to add MAC addresses that you want to allow or deny.

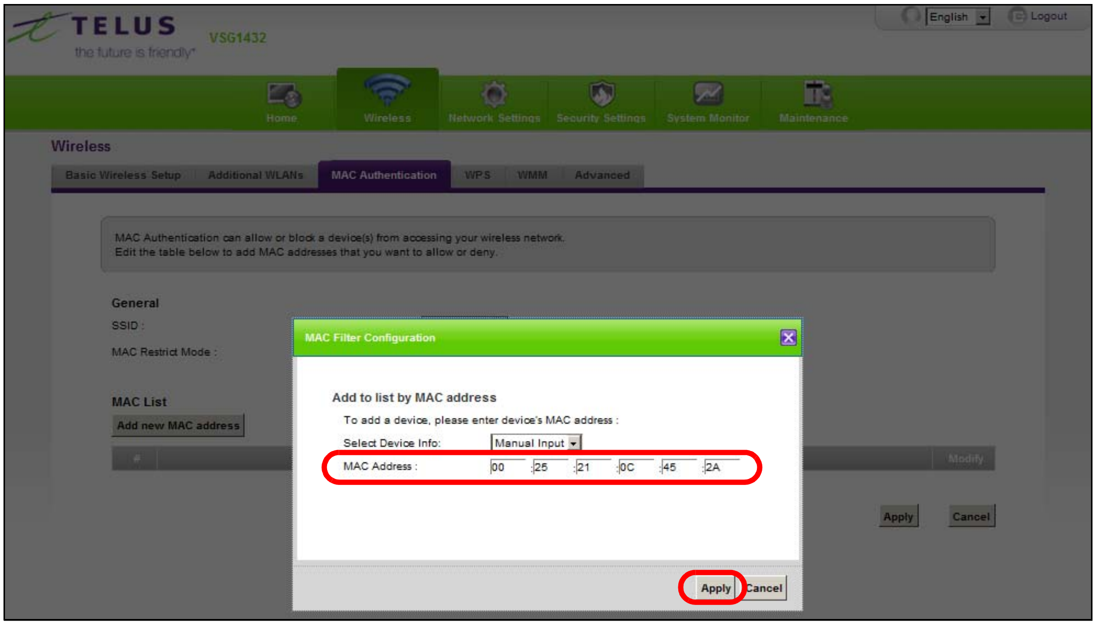
General

SSID : TELUS0000

MAC Restrict Mode : ● Disable ○ Allow ○ Deny

MAC List

2 In the **MAC Address** field, enter the MAC Address of the computer to block and click **Apply**.



MAC Authentication can allow or block a device(s) from accessing your wireless network.
Edit the table below to add MAC addresses that you want to allow or deny.

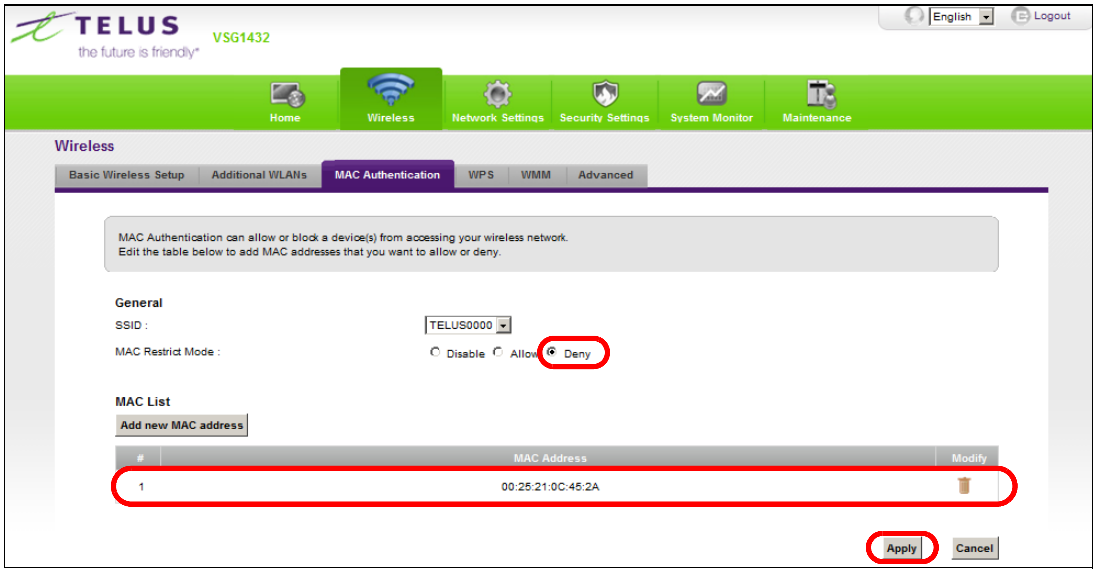
Add to list by MAC address

To add a device, please enter device's MAC address :

Select Device Info: Manual Input

MAC Address : 00 : 25 : 21 : 0C : 45 : 2A

3 The MAC Address will appear in the **MAC List**. In the **MAC Restrict Mode** field select **Deny**. Then, click **Apply**.



MAC Authentication can allow or block a device(s) from accessing your wireless network.
Edit the table below to add MAC addresses that you want to allow or deny.

General

SSID : TELUS0000

MAC Restrict Mode : ○ Disable ○ Allow ● Deny

MAC List

Add new MAC address

#	MAC Address	Modify
1	00:25:21:0C:45:2A	

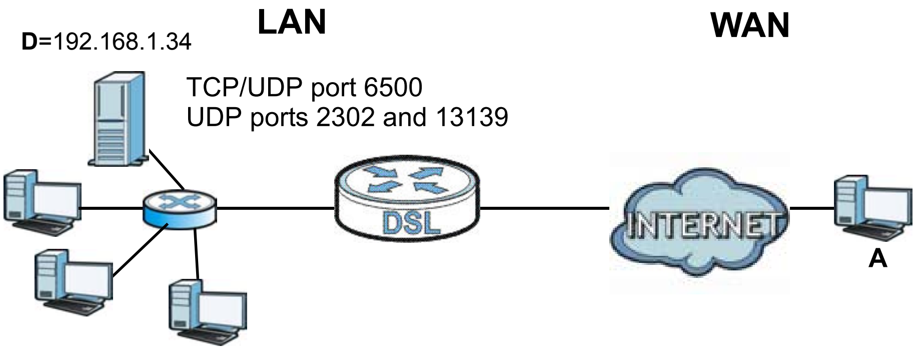
Apply Cancel

2.5 Setting Up NAT Forwarding for a Game Server

Thomas manages a Civilization IV server on a computer behind the Device. In order for players on the Internet (like **A** in the figure below) to communicate with the server, Thomas can use port forwarding or application forwarding. Application forwarding can be easier to set up since you do not need to specify port numbers manually.

Note: You cannot configure an application forwarding rule that uses the same ports as a configured port forwarding rule.

Note: If firewall is enabled, you may also need to configure an Access Control List rule for the relevant ports. See Access Control List.



2.5.1 Port Forwarding

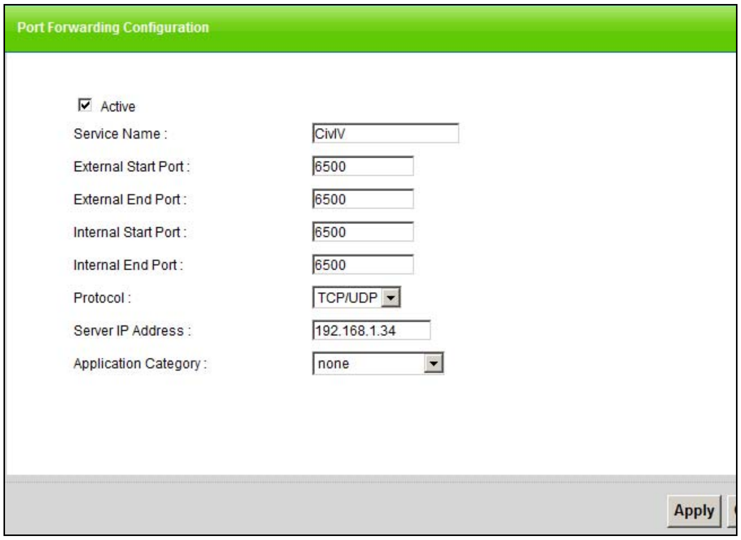
Thomas needs to configure the port settings and IP address on the Device. Traffic should be forwarded to TCP/UDP port 6500, and UDP ports 2302 and 13139 of the server computer which has an IP address of 192.168.1.34.

Thomas may set up the port settings by configuring the port settings for the server computer.

1 Click **Network Settings > NAT > Add new rule** and configure the screen with the following values:

Service Name	**CivIV**
External Port/s	Enter **6500** as the **Start** and **End** port.
Server IP Address	Enter the IP address of the server. This is **192.168.1.34** for this example.
Protocol	Select **TCP/UDP**. This should be the protocol supported by the server.

2 The screen should look as follows. Click **Apply**.

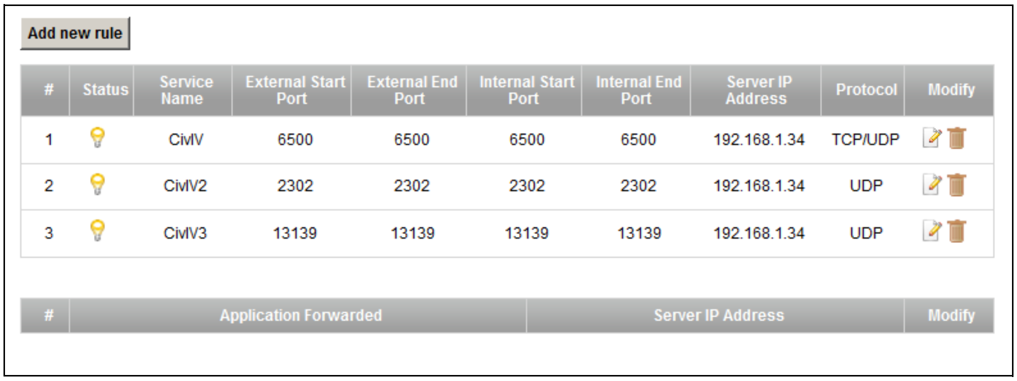


Port Forwarding Configuration

☑ Active

Service Name :	CivIV
External Start Port :	6500
External End Port :	6500
Internal Start Port :	6500
Internal End Port :	6500
Protocol :	TCP/UDP
Server IP Address :	192.168.1.34
Application Category :	none

3 Repeat steps 1 and 2 for UDP ports 2302 and 13139. The port forwarding settings you configured appear in the table.



#	Status	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Protocol	Modify
1	💡	CivIV	6500	6500	6500	6500	192.168.1.34	TCP/UDP	✎ 🗑
2	💡	CivIV2	2302	2302	2302	2302	192.168.1.34	UDP	✎ 🗑
3	💡	CivIV3	13139	13139	13139	13139	192.168.1.34	UDP	✎ 🗑

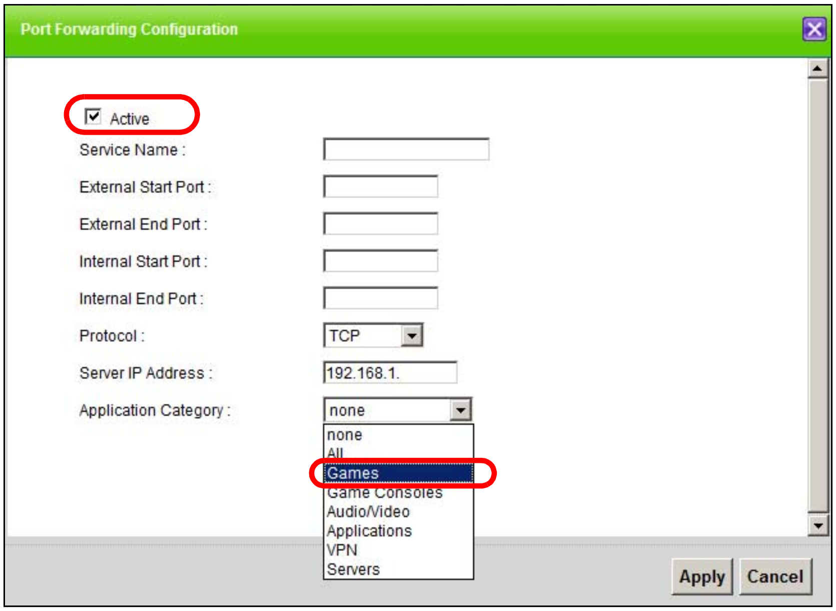
#	Application Forwarded	Server IP Address	Modify

Players on the Internet then can have access to Thomas' server.

2.5.2 Application Forwarding

Application forwarding can be used instead of port forwarding for forwarding traffic to the server.

1 Click **Network Settings > NAT > Add new rule**. Select **Active** and in the **Application Category** dropdown menu, select **Games**.



Port Forwarding Configuration

☑ Active

Service Name :

External Start Port :

External End Port :

Internal Start Port :

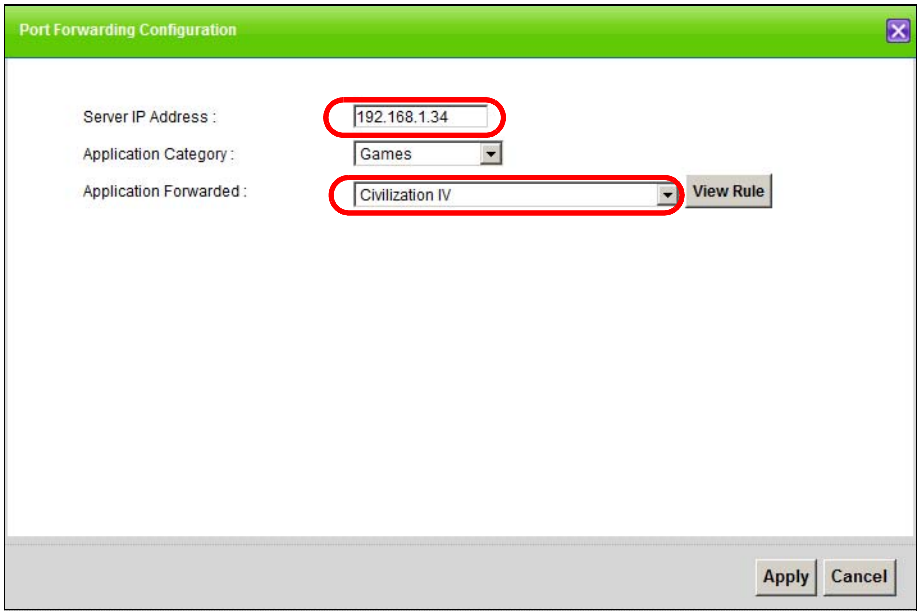
Internal End Port :

Protocol : TCP

Server IP Address : 192.168.1.

Application Category : none

1 The following screen appears. Enter the **Server IP Address** as **192.168.1.34** and in the **Application Forwarded** dropdown menu, select **Civilization IV**. Click **Apply**.



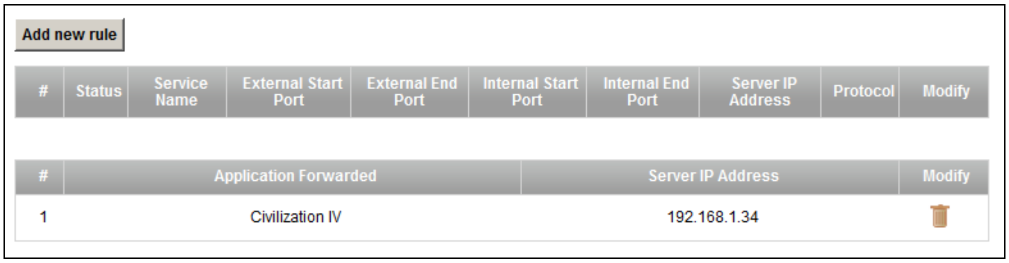
Port Forwarding Configuration

Server IP Address : 192.168.1.34

Application Category : Games

Application Forwarded : Civilization IV

2 The application forwarding settings you configured appear in the table.



#	Status	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Protocol	Modify

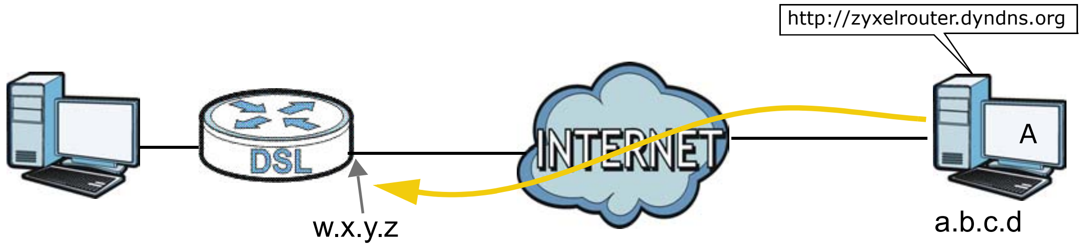
#	Application Forwarded	Server IP Address	Modify
1	Civilization IV	192.168.1.34	🗑

2.6 Access Your Home Computer from the Internet Using DDNS

If you connect your Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to access your home computer from the Internet. The Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access your home computer using a domain name.

Note: You will need to enable remote desktop server service on your home computer. The remote desktop server feature is only included in Windows Professional, Business and Ultimate versions.

Note: If firewall is enabled, you may also need to configure an Access Control List rule for the relevant ports. See Access Control List.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial covers:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your Device
- Configuring Port Forwarding on your Device
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

2.6.1 Registering a DDNS Account on www.dyndns.org

1 Open a browser and type **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4 Add a new DDNS host name. This tutorial uses the following settings as an example.

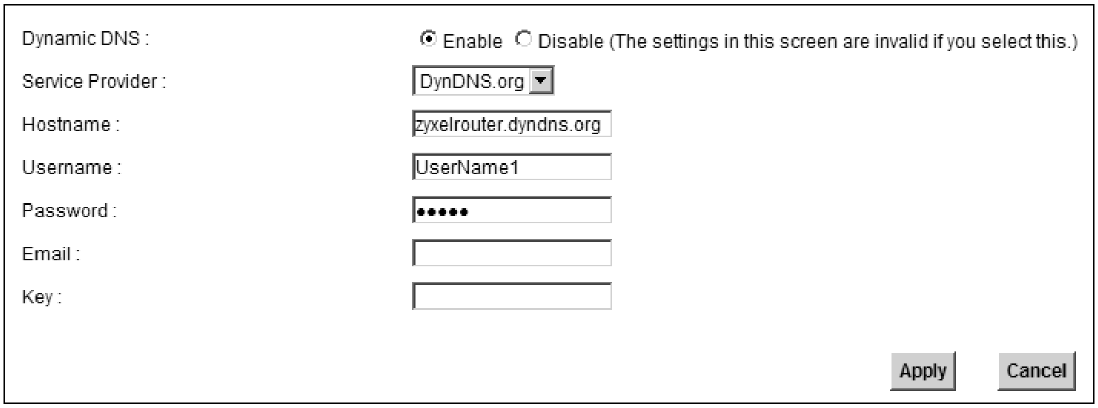
- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your Device is currently using. You can find the IP address on the Device's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the Device later.

2.6.2 Configuring DDNS on Your Device

Configure the following settings in the **Network Setting > DNS Setting > Dynamic DNS** screen.

- Select **Enable Dynamic DNS**.
- Select **DynDNS.org** as the service provider.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**).



Dynamic DNS :	● Enable ○ Disable (The settings in this screen are invalid if you select this.)
Service Provider :	DynDNS.org
Hostname :	zyxelrouter.dyndns.org
Username :	UserName1
Password :	●●●●●
Email :	
Key :	

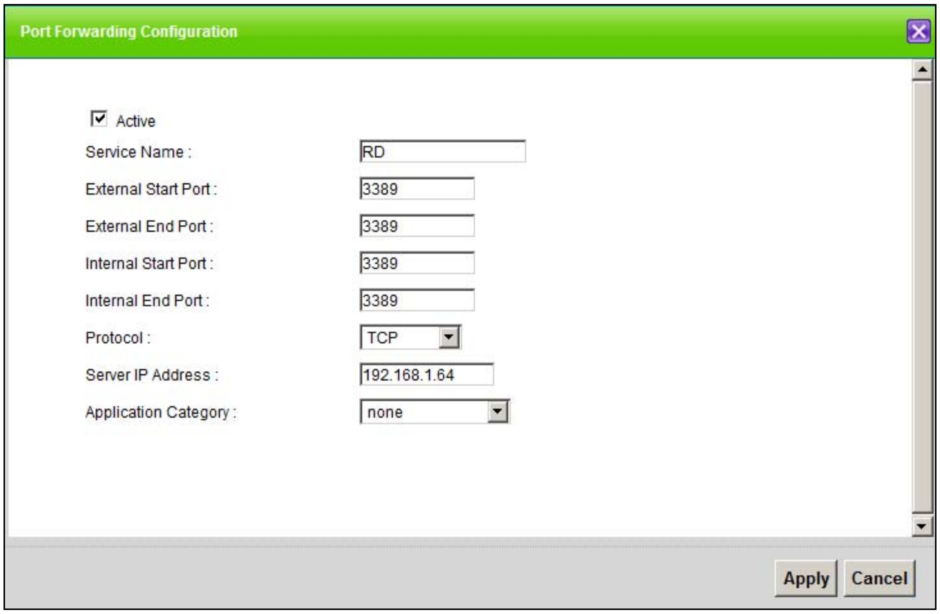
Click **Apply**.

2.6.3 Configuring Port Forwarding on your Device

Configure the following settings in the **Network Setting > NAT > Port Forwarding > Add new rule** screen.

- Select **Active**.
- Type **RD** in the **Service Name**.
- Type **3389** in the **External/Internal Start/End Port** fields. This is the listening port for Windows remote desktop.

- Select the **TCP** in the **Protocol** field.
- Type the LAN IP address of your computer in the **Server IP Address** field. To check this on your home computer, click **Start**, **All Programs**, **Accessories** and then **Command Prompt**. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. This example uses **192.168.1.64**. You will also need to configure a Static DHCP rule for this IP address. See Configuring Static DHCP.



☑ Active

Service Name :	RD
External Start Port :	3389
External End Port :	3389
Internal Start Port :	3389
Internal End Port :	3389
Protocol :	TCP
Server IP Address :	192.168.1.64
Application Category :	none

Click **Apply**.

2.6.4 Testing the DDNS Setting

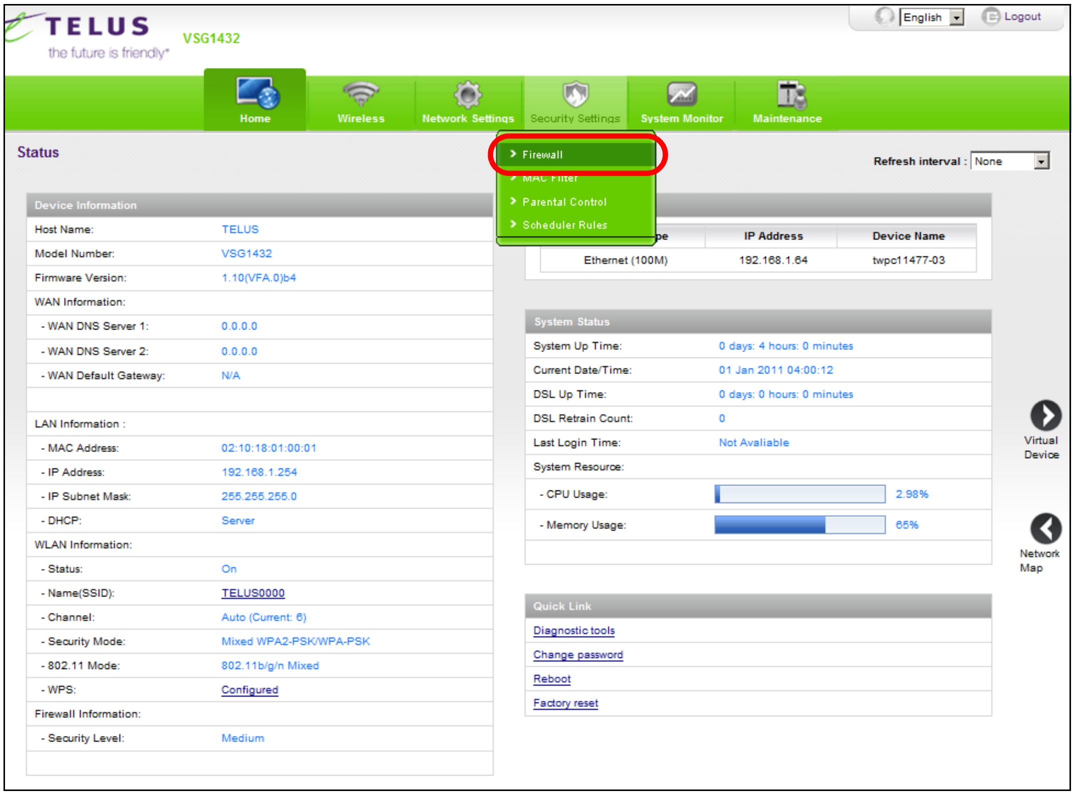
Now you should be able to access the Device from the Internet. To test this:

1. Open the remote desktop client application on the remote computer (using the IP address **a.b.c.d**) that is connected to the Internet.
2. Type **http://zyxelrouter.dyndns.org** and press [Enter].
3. Your computer’s remote desktop login page should appear.

2.7 Firewall Setup

The following example shows how to change firewall security level settings.

1 Place your mouse over the **Security Settings** icon, and click **Firewall** in the drop down.



Status

Device Information	
Host Name:	TELUS
Model Number:	VSG1432
Firmware Version:	1.10(VFA.0)b4
WAN Information:	
- WAN DNS Server 1:	0.0.0.0
- WAN DNS Server 2:	0.0.0.0
- WAN Default Gateway:	N/A
LAN Information :	
- MAC Address:	02:10:18:01:00:01
- IP Address:	192.168.1.254
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- Status:	On
- Name(SSID):	TELUS0000
- Channel:	Auto (Current: 6)
- Security Mode:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured
Firewall Information:	
- Security Level:	Medium

...pe	IP Address	Device Name
Ethernet (100M)	192.168.1.64	twpc11477-03

System Status	
System Up Time:	0 days: 4 hours: 0 minutes
Current Date/Time:	01 Jan 2011 04:00:12
DSL Up Time:	0 days: 0 hours: 0 minutes
DSL Retrain Count:	0
Last Login Time:	Not Avaliable
System Resource:	
- CPU Usage:	2.98%
- Memory Usage:	65%

Quick Link

Diagnostic tools

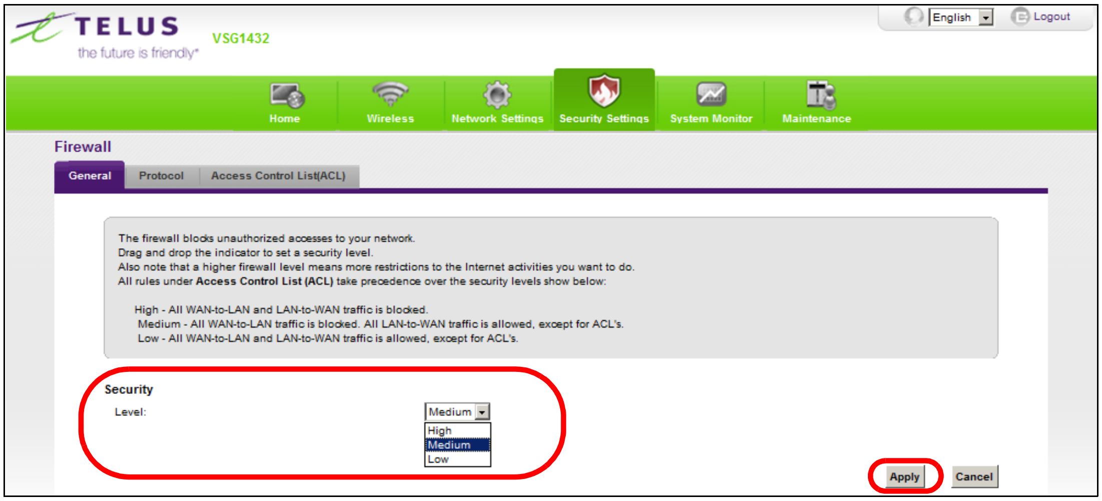
Change password

Reboot

Factory reset

2 In the security **Level** dropdown, you can select **High**, **Medium** or **Low**:

- High - All WAN-to-LAN and LAN-to-WAN traffic is blocked.
- Medium - All WAN-to-LAN traffic is blocked. All LAN-to-WAN traffic is allowed, except for Access Control Lists (ACL's).
- Low - All WAN-to-LAN and LAN-to-WAN traffic is allowed, except for ACL's.



Firewall

The firewall blocks unauthorized accesses to your network.
Drag and drop the indicator to set a security level.
Also note that a higher firewall level means more restrictions to the Internet activities you want to do.
All rules under **Access Control List (ACL)** take precedence over the security levels show below:

High - All WAN-to-LAN and LAN-to-WAN traffic is blocked.
Medium - All WAN-to-LAN traffic is blocked. All LAN-to-WAN traffic is allowed, except for ACL's.
Low - All WAN-to-LAN and LAN-to-WAN traffic is allowed, except for ACL's.

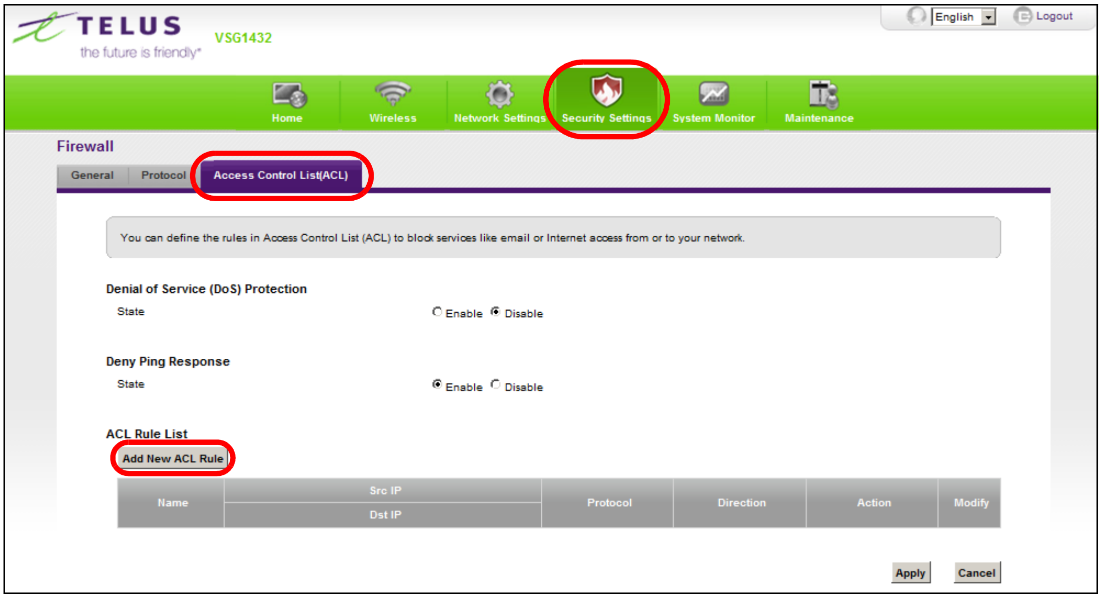
Security

Level: Medium

2.7.1 Access Control List

The following access control list example shows how to allow a hypothetical connection to/from the Internet.

1 Click the **Access Control List (ACL)** tab. Finally, click the **Add New ACL Rule** button.



You can define the rules in Access Control List (ACL) to block services like email or Internet access from or to your network.

Denial of Service (DoS) Protection

State ○ Enable ● Disable

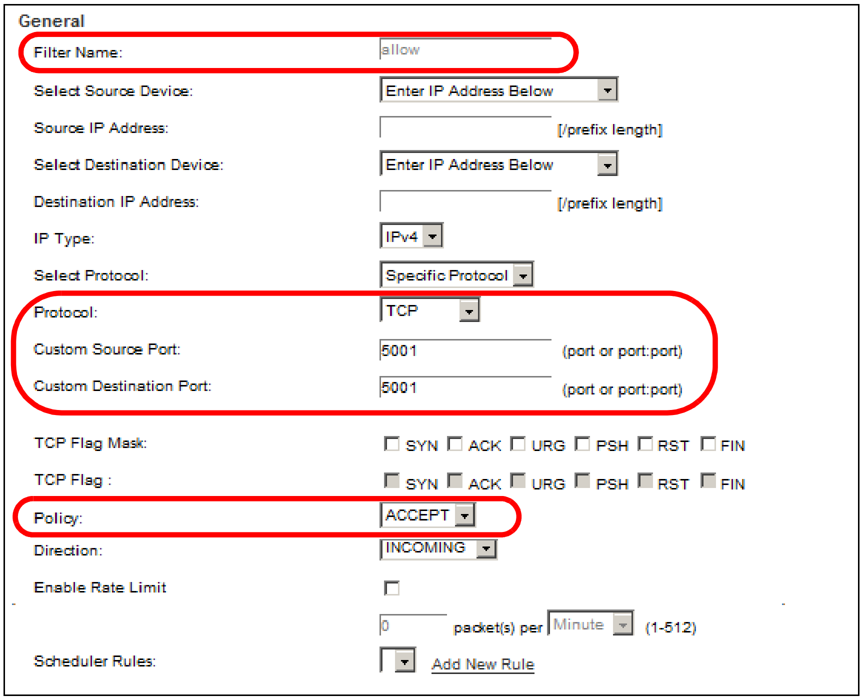
Deny Ping Response

State ● Enable ○ Disable

ACL Rule List

Name	Src IP Dst IP	Protocol	Direction	Action	Modify

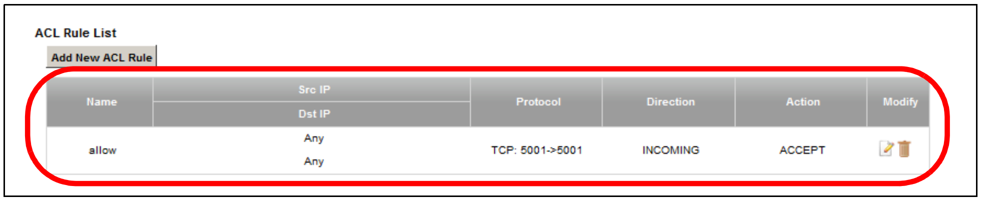
2 In the **Access Control List (ACL)** screen, configure the screen as follows and click **Apply**.



General

Filter Name:	allow
Select Source Device:	Enter IP Address Below
Source IP Address:	[/prefix length]
Select Destination Device:	Enter IP Address Below
Destination IP Address:	[/prefix length]
IP Type:	IPv4
Select Protocol:	Specific Protocol
Protocol:	TCP
Custom Source Port:	5001 (port or port:port)
Custom Destination Port:	5001 (port or port:port)
TCP Flag Mask:	□ SYN □ ACK □ URG □ PSH □ RST □ FIN
TCP Flag :	□ SYN □ ACK □ URG □ PSH □ RST □ FIN
Policy:	ACCEPT
Direction:	INCOMING
Enable Rate Limit	□
	0 packet(s) per Minute (1-512)
Scheduler Rules:	Add New Rule

3 On completing the configuration procedure for this Internet firewall rule, the **Rules** screen should look like the following.



ACL Rule List

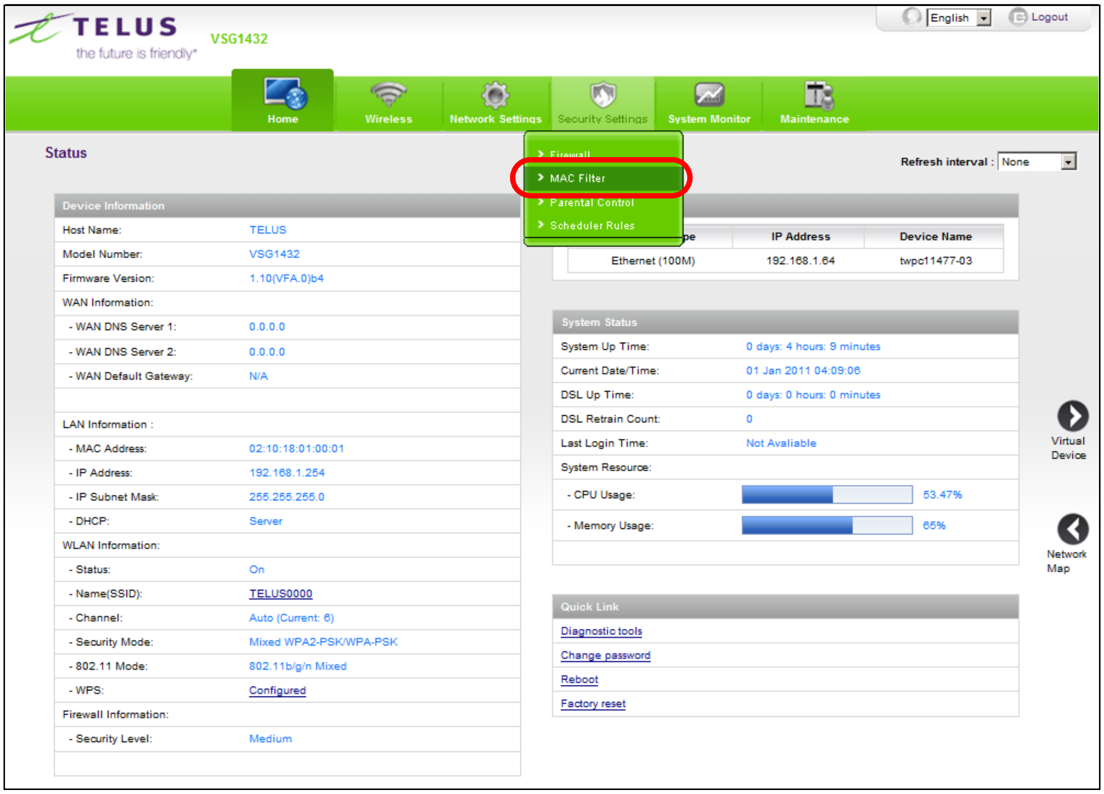
Add New ACL Rule

Name	Src IP Dst IP	Protocol	Direction	Action	Modify
allow	Any Any	TCP: 5001->5001	INCOMING	ACCEPT	📝🗑

2.8 MAC Filter Setup for Blocking LAN Computers

The following example shows how to create a MAC filter rule to block a computer from accessing the Device.

1 Place your mouse over the **Security Settings** icon, and click **MAC Filter** in the drop down.



Status

Refresh interval : None

Device Information	
Host Name:	TELUS
Model Number:	VSG1432
Firmware Version:	1.10(VFA.0)b4
WAN Information:	
- WAN DNS Server 1:	0.0.0.0
- WAN DNS Server 2:	0.0.0.0
- WAN Default Gateway:	N/A
LAN Information :	
- MAC Address:	02:10:18:01:00:01
- IP Address:	192.168.1.254
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- Status:	On
- Name(SSID):	TELUS0000
- Channel:	Auto (Current: 6)
- Security Mode:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured
Firewall Information:	
- Security Level:	Medium

pe	IP Address	Device Name
Ethernet (100M)	192.168.1.64	twpc11477-03

System Status	
System Up Time:	0 days: 4 hours: 9 minutes
Current Date/Time:	01 Jan 2011 04:09:06
DSL Up Time:	0 days: 0 hours: 0 minutes
DSL Retrain Count:	0
Last Login Time:	Not Avaliable
System Resource:	
- CPU Usage:	53.47%
- Memory Usage:	65%

Quick Link

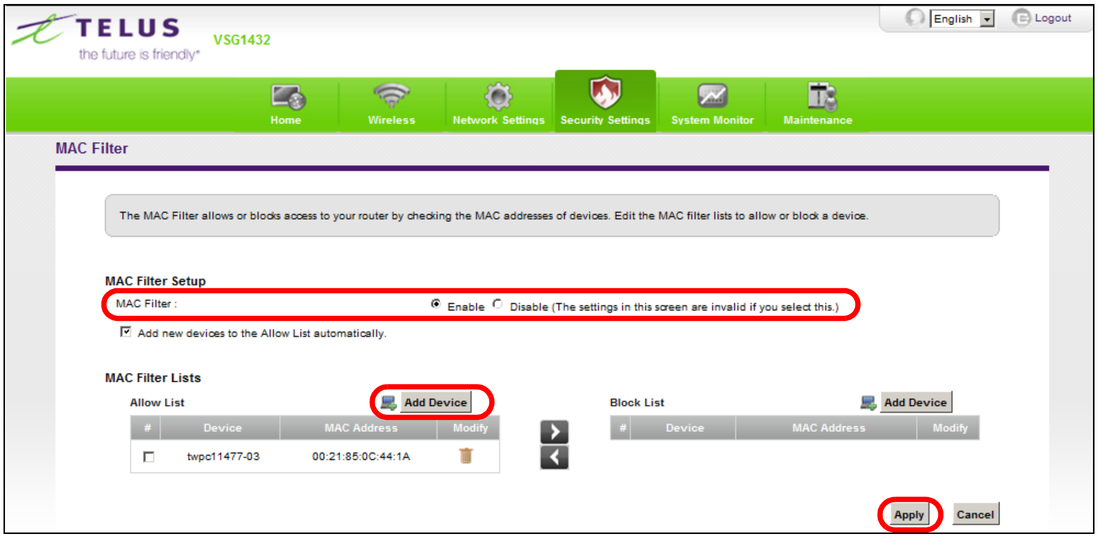
Diagnostic tools

Change password

Reboot

Factory reset

2 In the **MAC Filter** screen, select **Enable** as follows and click **Apply**. To add a device to the **MAC Filter Lists**, click the **Add Device** button.



MAC Filter

The MAC Filter allows or blocks access to your router by checking the MAC addresses of devices. Edit the MAC filter lists to allow or block a device.

MAC Filter Setup

MAC Filter : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

☑ Add new devices to the Allow List automatically.

MAC Filter Lists

Allow List — Add Device

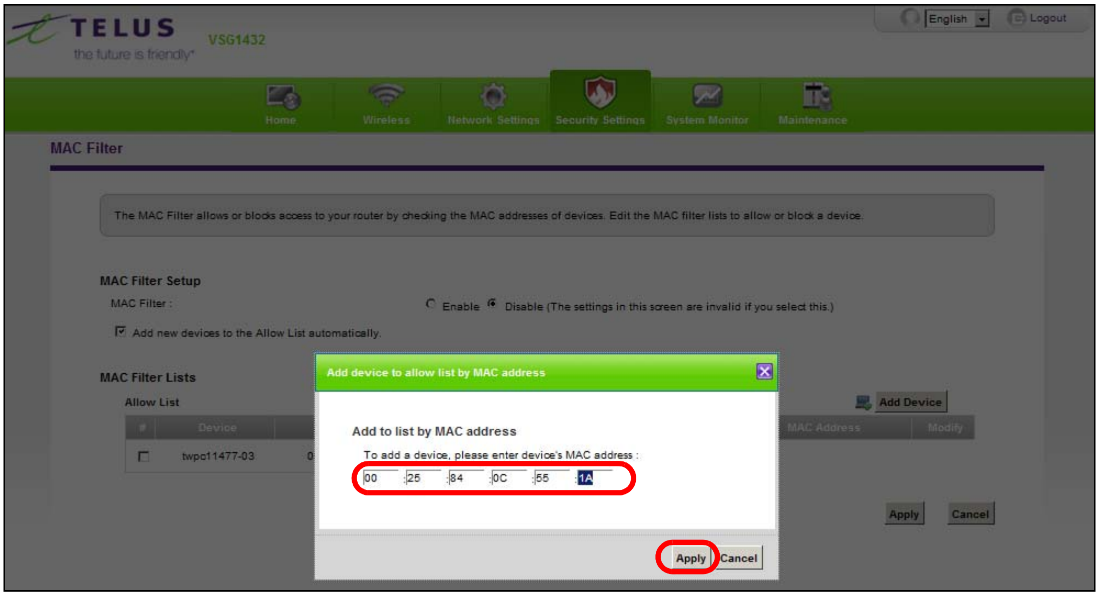
#	Device	MAC Address	Modify
□	twpc11477-03	00:21:85:0C:44:1A	

Block List — Add Device

#	Device	MAC Address	Modify

Apply Cancel

3 Enter the MAC address of the computer you want to block and cilck **Apply**.


TELUS
the future is friendly
VSG1432
English
Logout
Home
Wireless
Network Settings
Security Settings
System Monitor
Maintenance
MAC Filter
The MAC Filter allows or blocks access to your router by checking the MAC addresses of devices. Edit the MAC filter lists to allow or block a device.
MAC Filter Setup
MAC Filter :
Enable
Disable (The settings in this screen are invalid if you select this.)
Add new devices to the Allow List automatically.
MAC Filter Lists
Allow List
Add Device
Device
MAC Address
Modify
twpc11477-03
Apply
Cancel

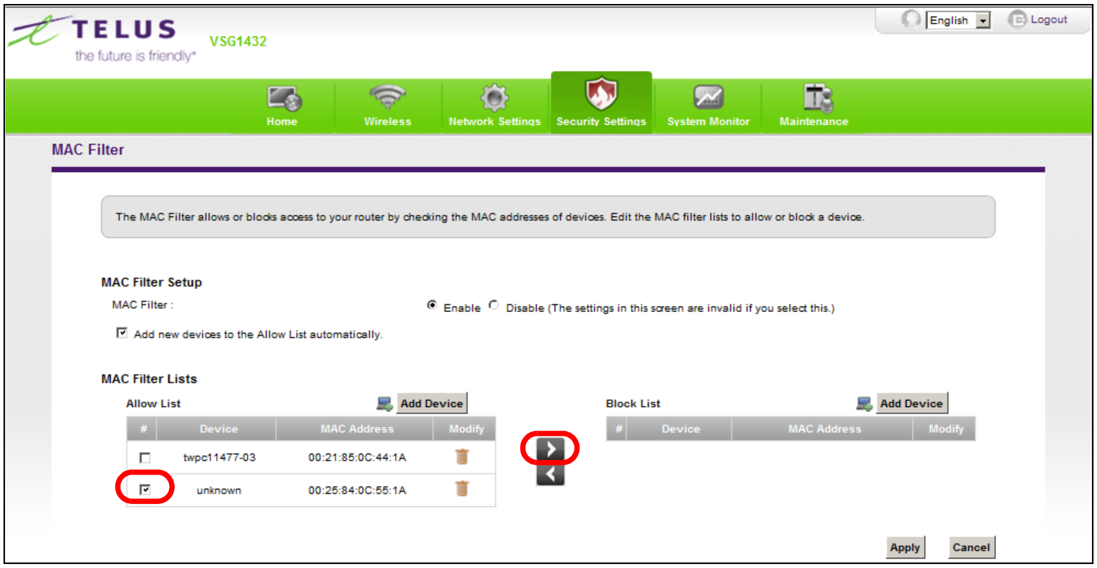
Add device to allow list by MAC address

Add to list by MAC address

To add a device, please enter device's MAC address : 00 : 25 : 84 : 0C : 55 : 1A

Apply Cancel

4 The new entry will appear in the **Allow List**. Select the check box next to the entry and click the right hand arrow to move it to the **Block List**.



MAC Filter

The MAC Filter allows or blocks access to your router by checking the MAC addresses of devices. Edit the MAC filter lists to allow or block a device.

MAC Filter Setup

MAC Filter : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

☑ Add new devices to the Allow List automatically.

MAC Filter Lists

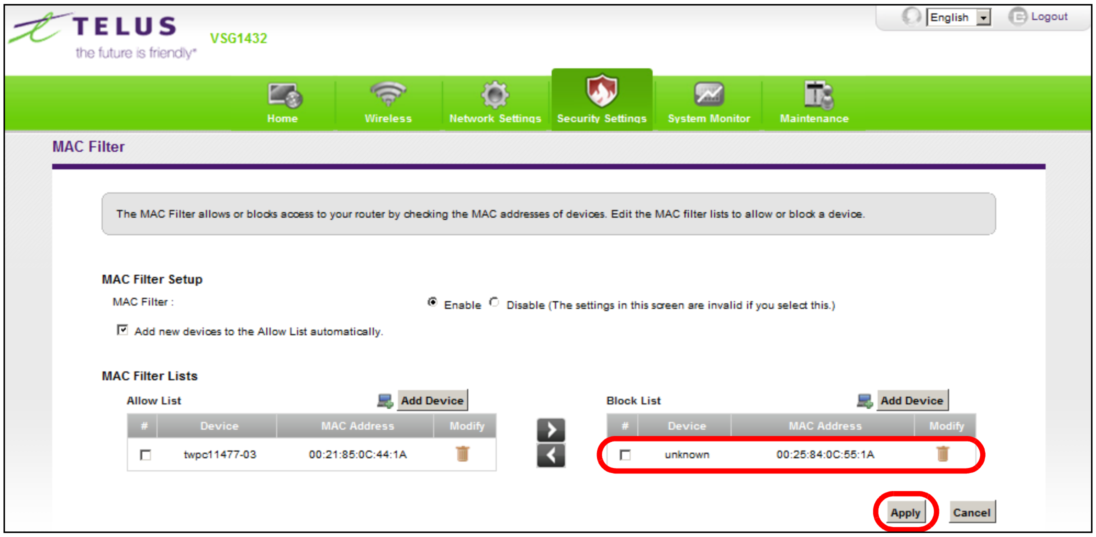
Allow List — Add Device

#	Device	MAC Address	Modify
□	twpc11477-03	00:21:85:0C:44:1A	
☑	unknown	00:25:84:0C:55:1A	

Block List — Add Device

#	Device	MAC Address	Modify

5 The entry will now appear in the **Block List**. Click **Apply**.



MAC Filter

The MAC Filter allows or blocks access to your router by checking the MAC addresses of devices. Edit the MAC filter lists to allow or block a device.

MAC Filter Setup

MAC Filter : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

☑ Add new devices to the Allow List automatically.

MAC Filter Lists

Allow List — Add Device

#	Device	MAC Address	Modify
□	twpc11477-03	00:21:85:0C:44:1A	

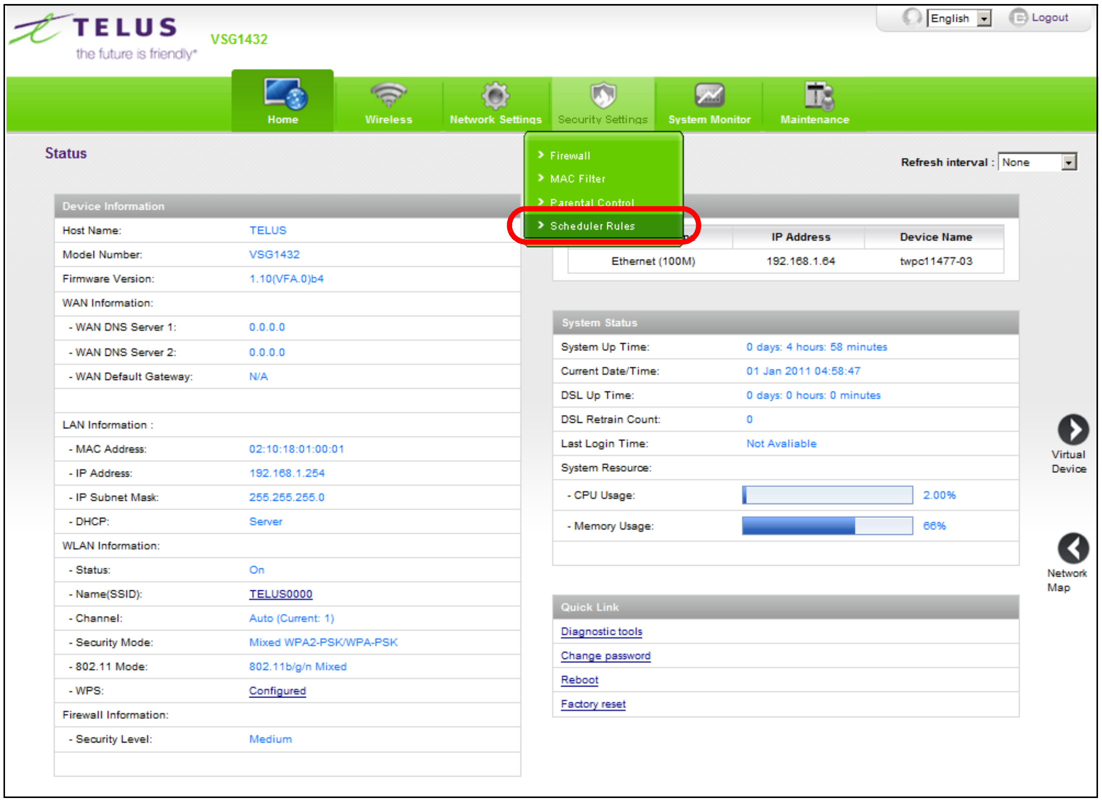
Block List — Add Device

#	Device	MAC Address	Modify
□	unknown	00:25:84:0C:55:1A	

2.9 Scheduler Rules and Parental Control

The following example creates a Parental Control to block web access from a selected computer during a specified time period. You will first configure a Scheduler Rule.

1 Place your mouse over the **Security Settings** icon, and click **Scheduler Rules** in the drop down.



Status

Refresh interval : None

Device Information	
Host Name:	TELUS
Model Number:	VSG1432
Firmware Version:	1.10(VFA.0)b4
WAN Information:	
- WAN DNS Server 1:	0.0.0.0
- WAN DNS Server 2:	0.0.0.0
- WAN Default Gateway:	N/A
LAN Information :	
- MAC Address:	02:10:18:01:00:01
- IP Address:	192.168.1.254
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- Status:	On
- Name(SSID):	TELUS0000
- Channel:	Auto (Current: 1)
- Security Mode:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured
Firewall Information:	
- Security Level:	Medium

	IP Address	Device Name
Ethernet (100M)	192.168.1.64	twpc11477-03

System Status	
System Up Time:	0 days: 4 hours: 58 minutes
Current Date/Time:	01 Jan 2011 04:58:47
DSL Up Time:	0 days: 0 hours: 0 minutes
DSL Retrain Count:	0
Last Login Time:	Not Avaliable
System Resource:	
- CPU Usage:	2.00%
- Memory Usage:	66%

Quick Link

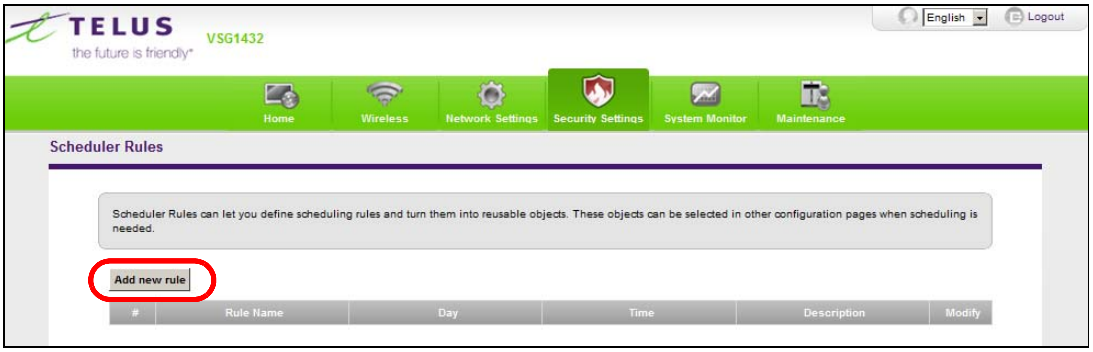
Diagnostic tools

Change password

Reboot

Factory reset

2 In the **Scheduler Rules** screen, click the **Add new rule** button.

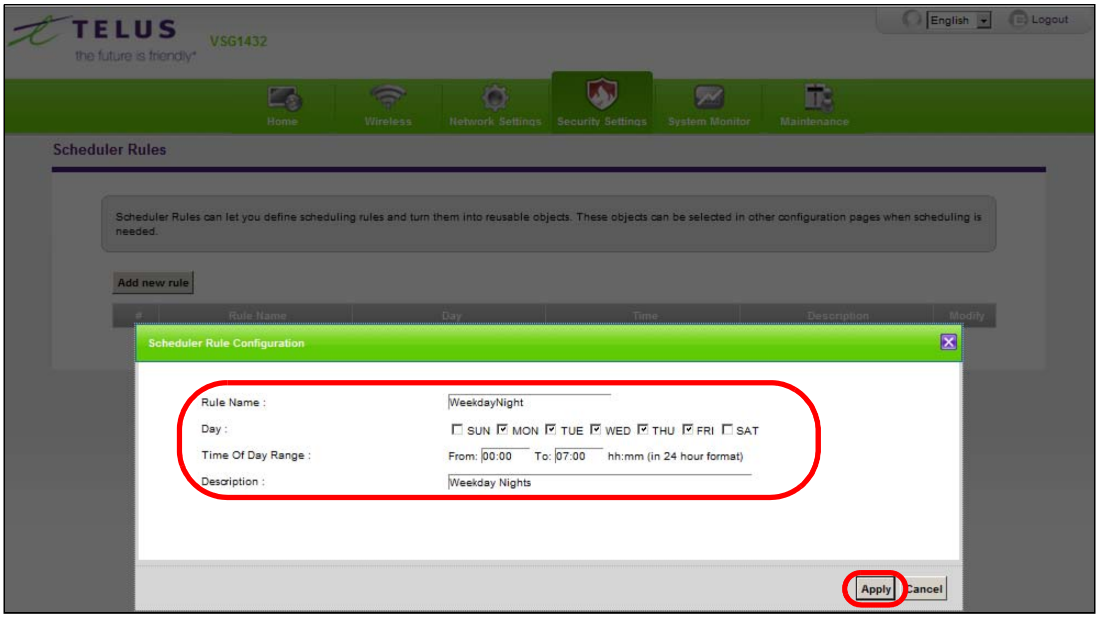


Scheduler Rules

Scheduler Rules can let you define scheduling rules and turn them into reusable objects. These objects can be selected in other configuration pages when scheduling is needed.

#	Rule Name	Day	Time	Description	Modify

3 Enter the configuration information as below and click **Apply**.



Scheduler Rules

Scheduler Rules can let you define scheduling rules and turn them into reusable objects. These objects can be selected in other configuration pages when scheduling is needed.

Scheduler Rule Configuration

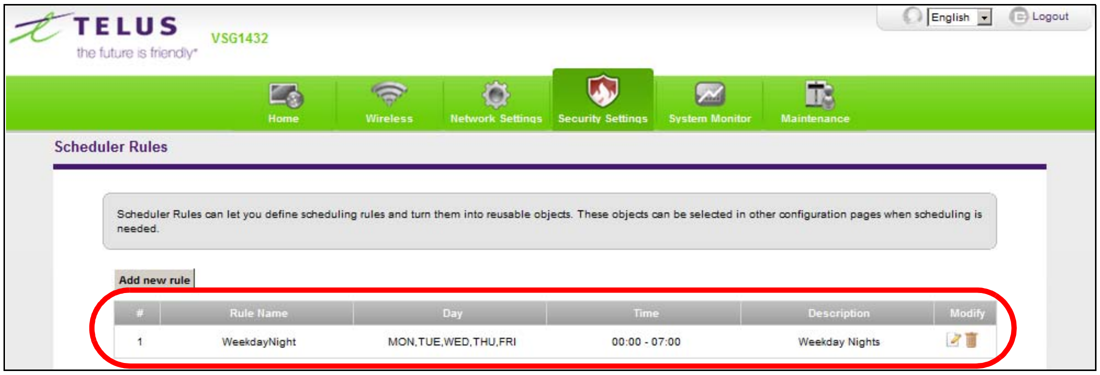
Rule Name : WeekdayNight

Day : □ SUN ☑ MON ☑ TUE ☑ WED ☑ THU ☑ FRI □ SAT

Time Of Day Range : From: 00:00 To: 07:00 hh:mm (in 24 hour format)

Description : Weekday Nights

4 On completing the configuration procedure for this schedule rule, the rule should appear in the rule list as below.

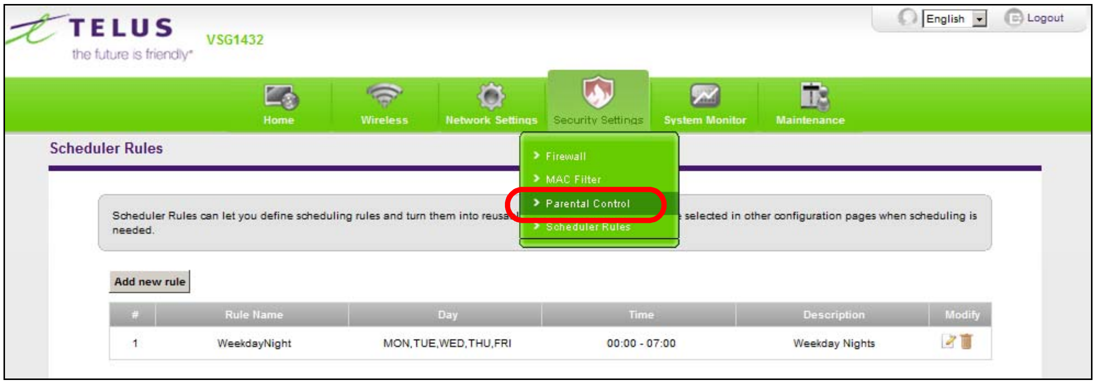


Scheduler Rules

Scheduler Rules can let you define scheduling rules and turn them into reusable objects. These objects can be selected in other configuration pages when scheduling is needed.

#	Rule Name	Day	Time	Description	Modify
1	WeekdayNight	MON,TUE,WED,THU,FRI	00:00 - 07:00	Weekday Nights	

5 Now, configure the **Parental Control** rule. Place your mouse over the **Security Settings** icon, and click **Parental Control** in the drop down.

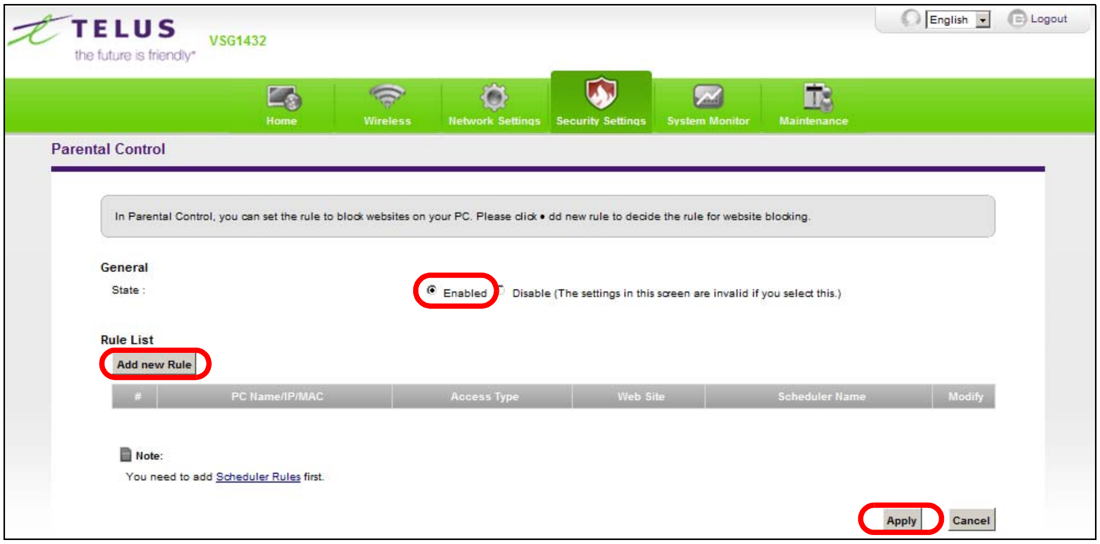


Scheduler Rules

Scheduler Rules can let you define scheduling rules and turn them into reusa selected in other configuration pages when scheduling is needed.

#	Rule Name	Day	Time	Description	Modify
1	WeekdayNight	MON,TUE,WED,THU,FRI	00:00 - 07:00	Weekday Nights	

6 Select **Enabled** then click **Apply**. Then click **Add new Rule**.



Parental Control

In Parental Control, you can set the rule to block websites on your PC. Please click • dd new rule to decide the rule for website blocking.

General

State : ● Enabled ○ Disable (The settings in this screen are invalid if you select this.)

Rule List

Add new Rule

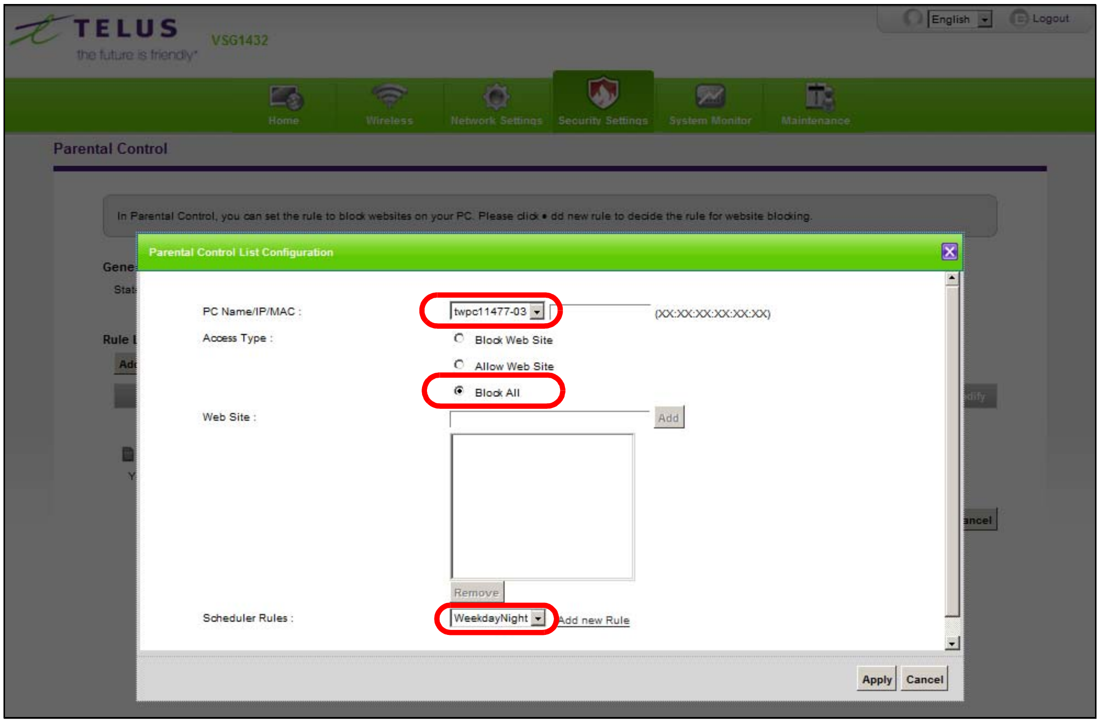
#	PC Name/IP/MAC	Access Type	Web Site	Scheduler Name	Modify

Note:

You need to add Scheduler Rules first.

Apply Cancel

7 Select the desired computer in the **PC Name/IP/MAC** field and select **Block All**. In the **Scheduler Rules** menu, select **WeekdayNight**. Click **Apply**.



Parental Control List Configuration

PC Name/IP/MAC : twpc11477-03 (XX:XX:XX:XX:XX:XX)

Access Type : ○ Block Web Site ○ Allow Web Site ● Block All

Web Site : Add

Remove

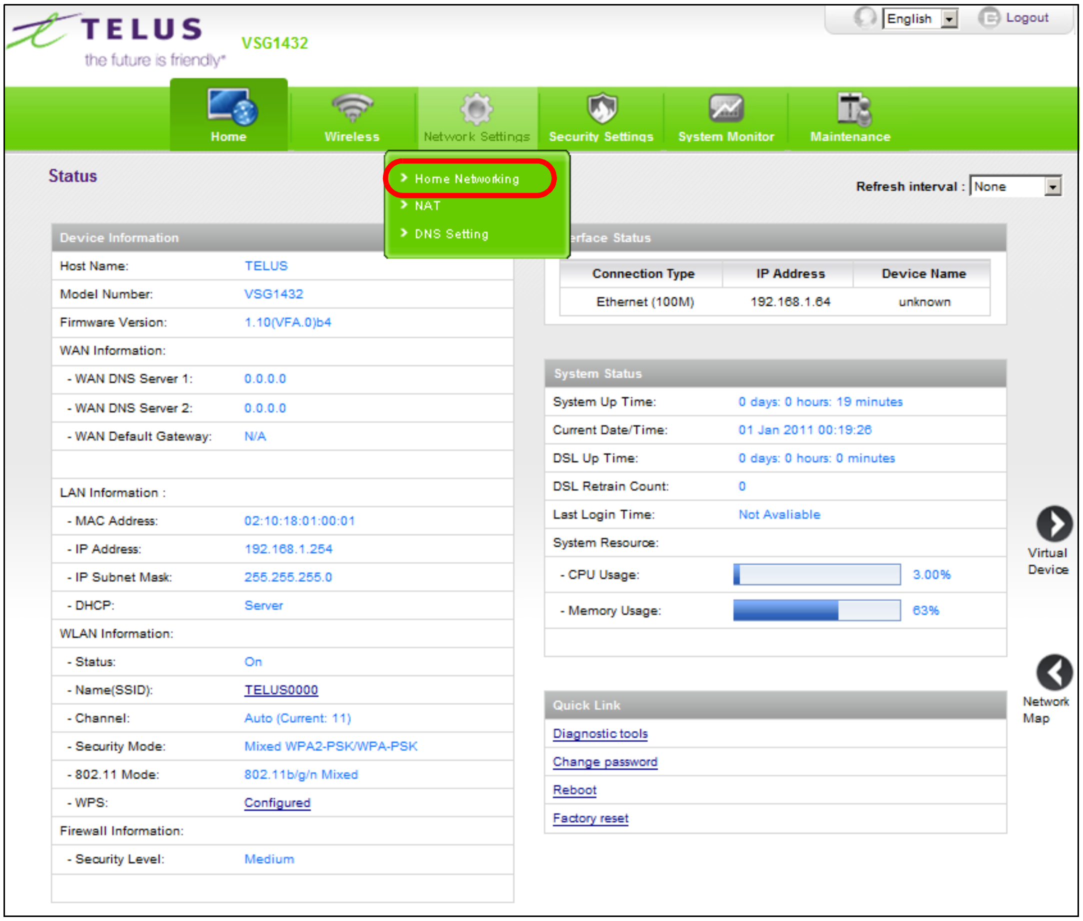
Scheduler Rules : WeekdayNight Add new Rule

Apply Cancel

2.10 LAN DHCP for IP Addressing Assignment

The following example shows how to configure LAN DHCP settings.

1 Place your mouse over the **Networking Settings** icon, and click **Home Networking** in the drop down.



Status

Refresh interval : None

Device Information	
Host Name:	TELUS
Model Number:	VSG1432
Firmware Version:	1.10(VFA.0)b4
WAN Information:	
- WAN DNS Server 1:	0.0.0.0
- WAN DNS Server 2:	0.0.0.0
- WAN Default Gateway:	N/A
LAN Information :	
- MAC Address:	02:10:18:01:00:01
- IP Address:	192.168.1.254
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- Status:	On
- Name(SSID):	TELUS0000
- Channel:	Auto (Current: 11)
- Security Mode:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured
Firewall Information:	
- Security Level:	Medium

erface Status

Connection Type	IP Address	Device Name
Ethernet (100M)	192.168.1.64	unknown

System Status	
System Up Time:	0 days: 0 hours: 19 minutes
Current Date/Time:	01 Jan 2011 00:19:26
DSL Up Time:	0 days: 0 hours: 0 minutes
DSL Retrain Count:	0
Last Login Time:	Not Avaliable
System Resource:	
- CPU Usage:	3.00%
- Memory Usage:	63%

Quick Link

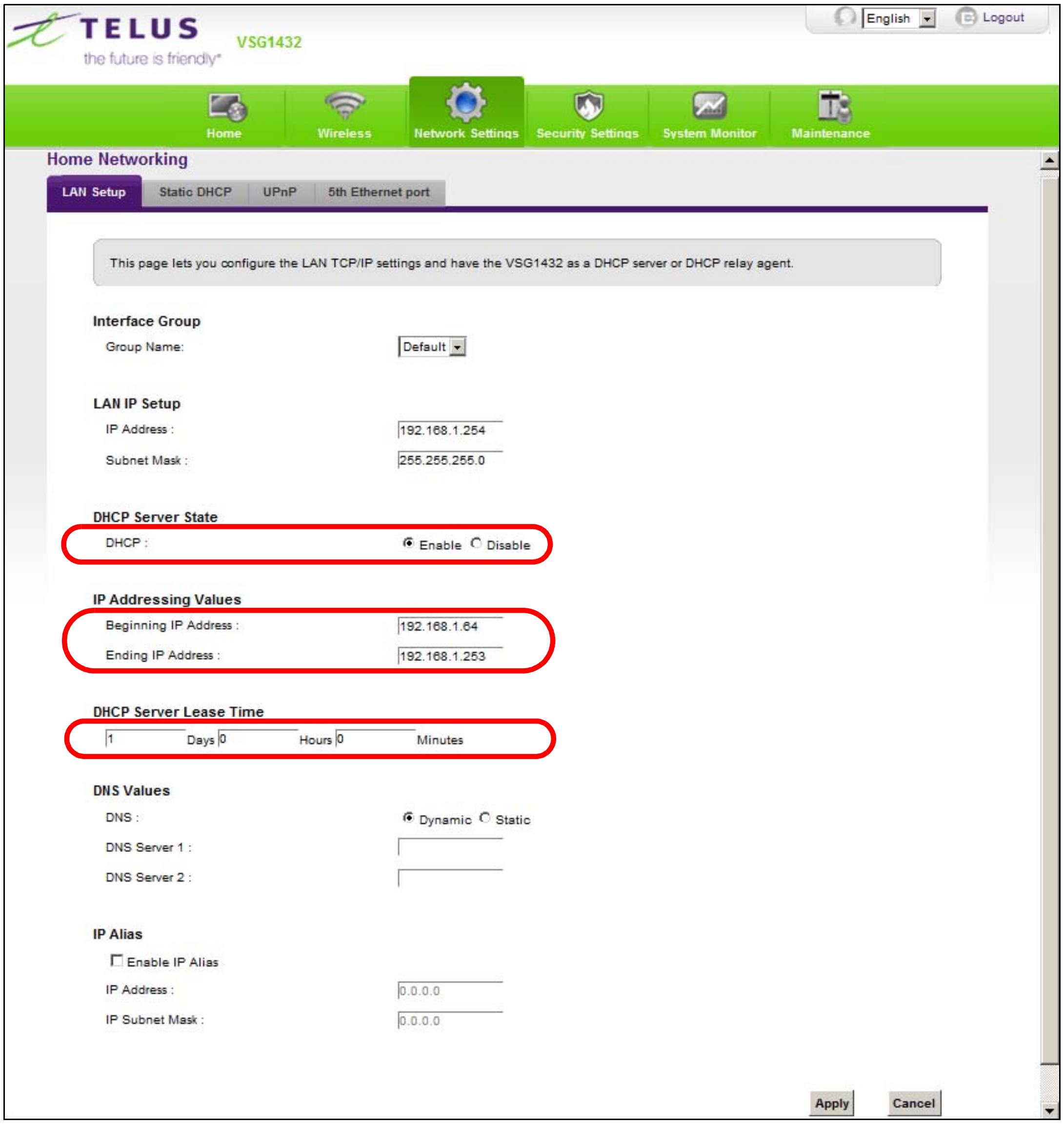
Diagnostic tools

Change password

Reboot

Factory reset

2 In the **IP Addressing Values** section, you can change the DHCP server IP address range. In the **DHCP Server Lease Time** section you can specify how long an IP address is leased to a LAN computer. Click **Apply**.



Home Networking

This page lets you configure the LAN TCP/IP settings and have the VSG1432 as a DHCP server or DHCP relay agent.

Interface Group

Group Name: Default

LAN IP Setup

IP Address : 192.168.1.254

Subnet Mask : 255.255.255.0

DHCP Server State

DHCP : ● Enable ○ Disable

IP Addressing Values

Beginning IP Address : 192.168.1.64

Ending IP Address : 192.168.1.253

DHCP Server Lease Time

1 Days 0 Hours 0 Minutes

DNS Values

DNS : ● Dynamic ○ Static

DNS Server 1 :

DNS Server 2 :

IP Alias

□ Enable IP Alias

IP Address : 0.0.0.0

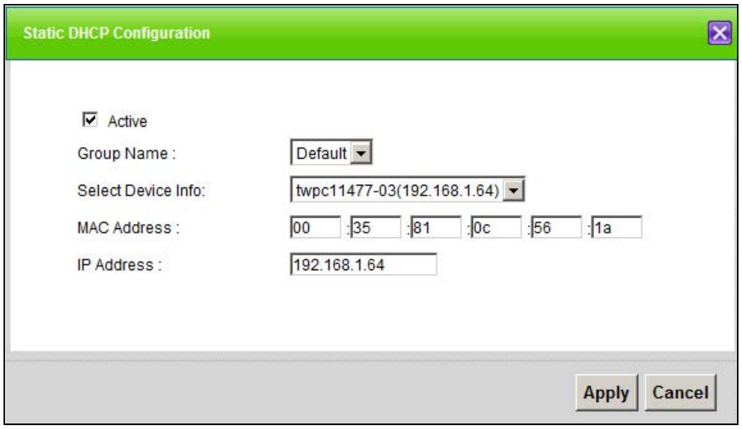
IP Subnet Mask : 0.0.0.0

2.10.1 Configuring Static DHCP

Configure the following settings in the **Network Setting > Home Networking > Static DHCP > Add** screen.

- Select **Active**.

- Select your computer in the **Select Device Info** field. The computer's MAC Address will be displayed in the **MAC Address** field. The computer's current LAN IP Address will be displayed in the **IP Address** field.



Static DHCP Configuration

☑ Active

Group Name : Default

Select Device Info: twpc11477-03(192.168.1.64)

MAC Address : 00 : 35 : 81 : 0c : 56 : 1a

IP Address : 192.168.1.64

- Click **Apply**.

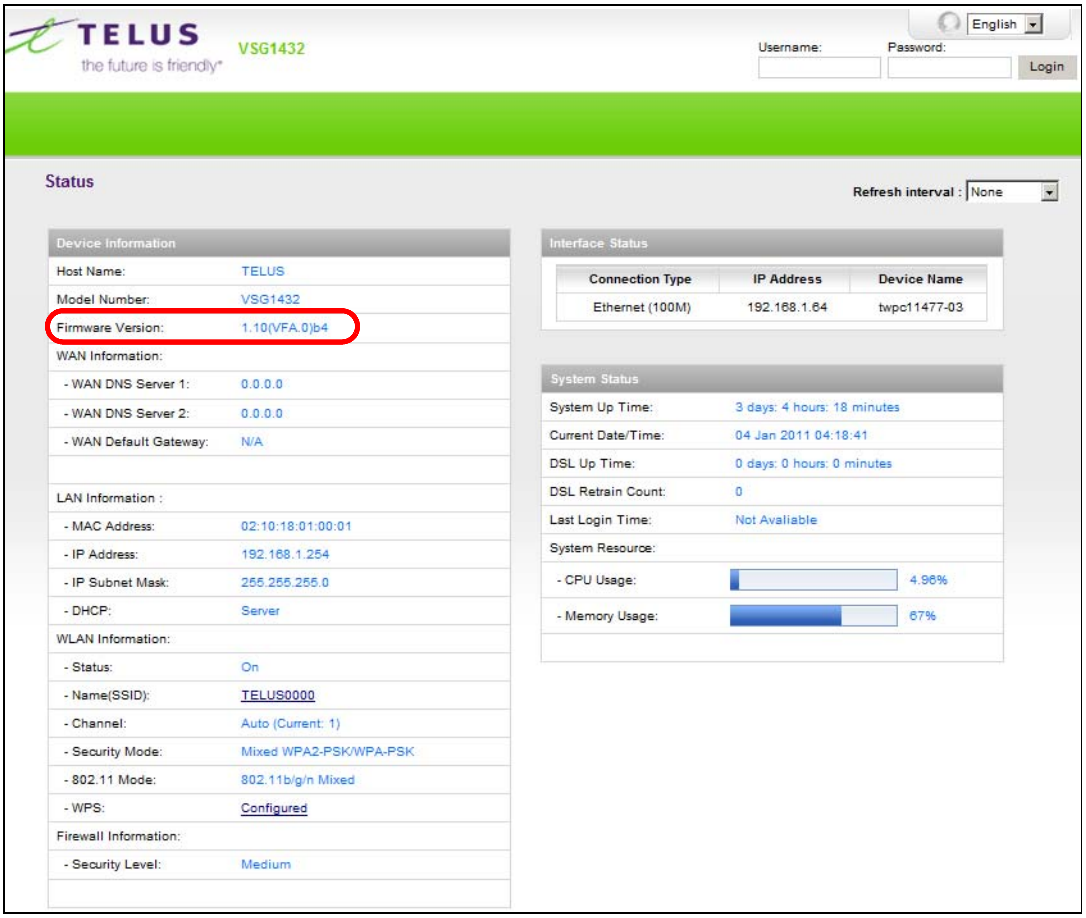
2.11 Check the Firmware Version

The following procedure shows how to check the firmware version that is installed on the Device.

1 In your web browser, enter the LAN IP address of the Device. The default is http://192.168.1.254.

http://192.168.1.254

2 The **Status** screen will display. The **Firmware Version** field displays the current firmware version.



Status

Refresh interval : None

Device Information

Host Name:	TELUS
Model Number:	VSG1432
Firmware Version:	1.10(VFA.0)b4
WAN Information:	
- WAN DNS Server 1:	0.0.0.0
- WAN DNS Server 2:	0.0.0.0
- WAN Default Gateway:	N/A
LAN Information :	
- MAC Address:	02:10:18:01:00:01
- IP Address:	192.168.1.254
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- Status:	On
- Name(SSID):	TELUS0000
- Channel:	Auto (Current: 1)
- Security Mode:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured
Firewall Information:	
- Security Level:	Medium

Interface Status

Connection Type	IP Address	Device Name
Ethernet (100M)	192.168.1.64	twpc11477-03

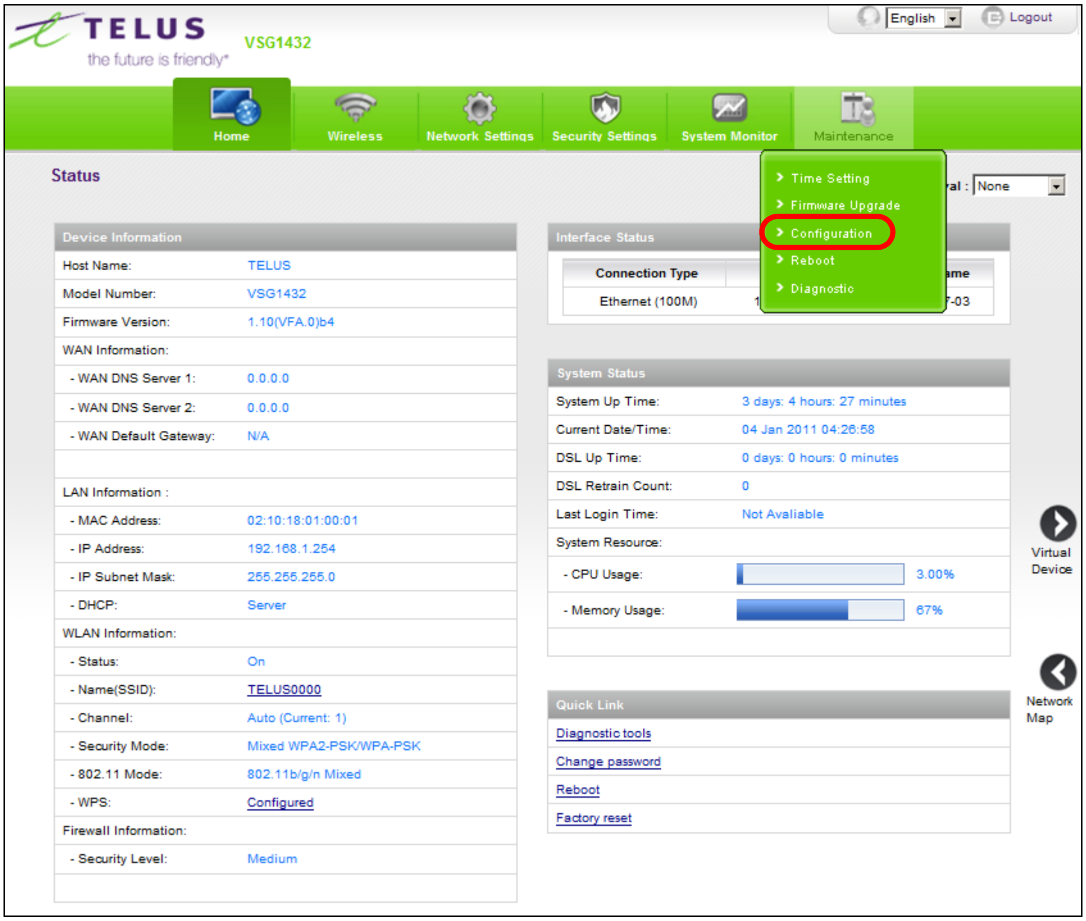
System Status

System Up Time:	3 days: 4 hours: 18 minutes
Current Date/Time:	04 Jan 2011 04:18:41
DSL Up Time:	0 days: 0 hours: 0 minutes
DSL Retrain Count:	0
Last Login Time:	Not Avaliable
System Resource:	
- CPU Usage:	4.96%
- Memory Usage:	67%

2.12 Restore to Factory Default

The following procedure shows how to restore the factory default settings to the Device.

1 Place your mouse over the **Maintenance** icon, and click **Configuration** in the drop down.



Status

Device Information	
Host Name:	TELUS
Model Number:	VSG1432
Firmware Version:	1.10(VFA.0)b4
WAN Information:	
- WAN DNS Server 1:	0.0.0.0
- WAN DNS Server 2:	0.0.0.0
- WAN Default Gateway:	N/A
LAN Information :	
- MAC Address:	02:10:18:01:00:01
- IP Address:	192.168.1.254
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- Status:	On
- Name(SSID):	TELUS0000
- Channel:	Auto (Current: 1)
- Security Mode:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured
Firewall Information:	
- Security Level:	Medium

Interface Status

Connection Type	1	ame
Ethernet (100M)	1	7-03

System Status	
System Up Time:	3 days: 4 hours: 27 minutes
Current Date/Time:	04 Jan 2011 04:26:58
DSL Up Time:	0 days: 0 hours: 0 minutes
DSL Retrain Count:	0
Last Login Time:	Not Avaliable
System Resource:	
- CPU Usage:	3.00%
- Memory Usage:	67%

Quick Link

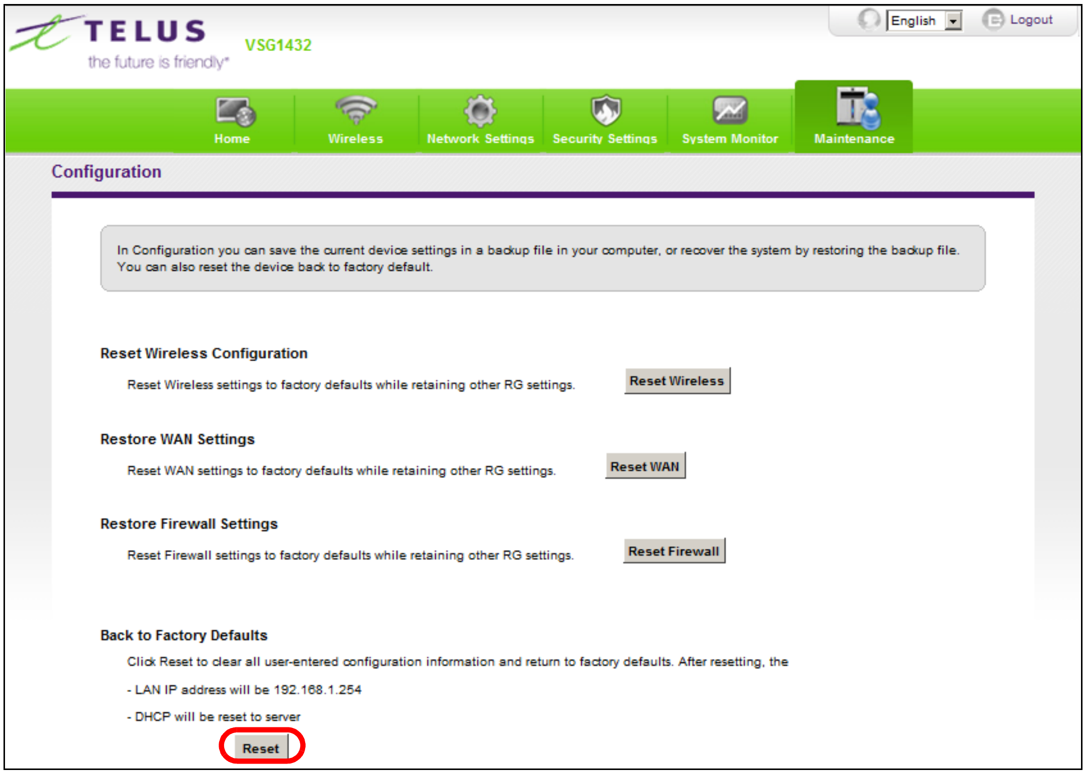
Diagnostic tools

Change password

Reboot

Factory reset

2 In the **Back to Factory Defaults** section, click the **Reset** button.



Configuration

In Configuration you can save the current device settings in a backup file in your computer, or recover the system by restoring the backup file. You can also reset the device back to factory default.

Reset Wireless Configuration

Reset Wireless settings to factory defaults while retaining other RG settings.

Restore WAN Settings

Reset WAN settings to factory defaults while retaining other RG settings.

Restore Firewall Settings

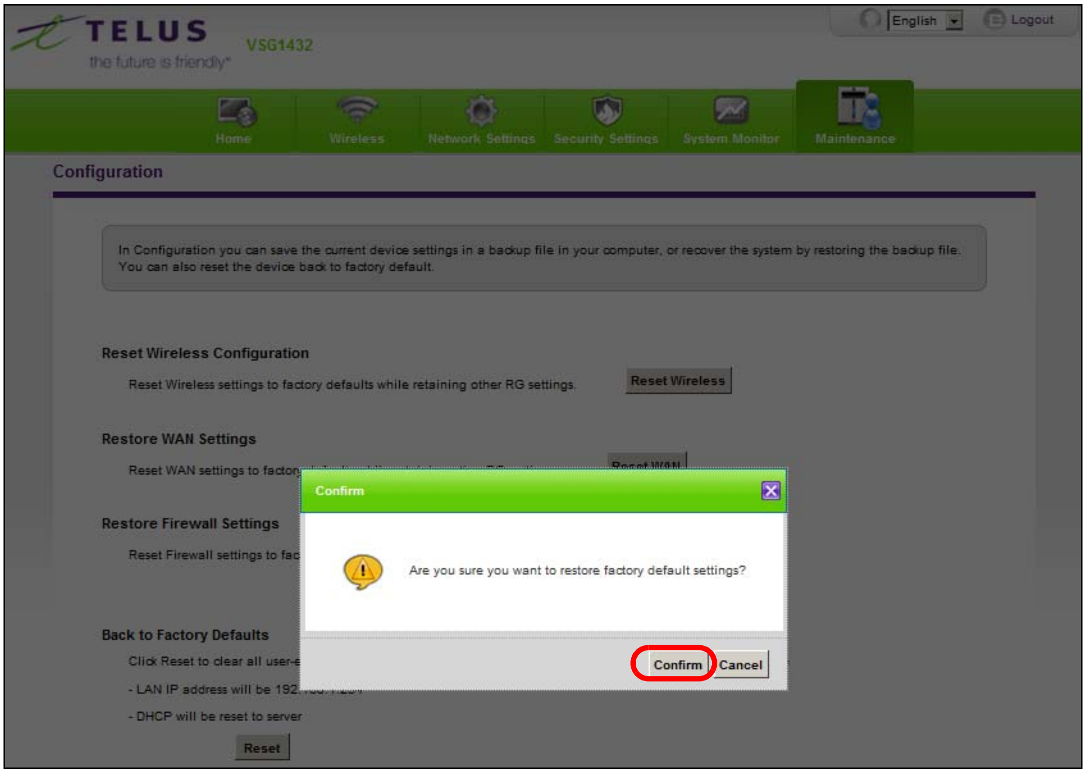
Reset Firewall settings to factory defaults while retaining other RG settings.

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- LAN IP address will be 192.168.1.254
- DHCP will be reset to server

3 Click **Confirm**.

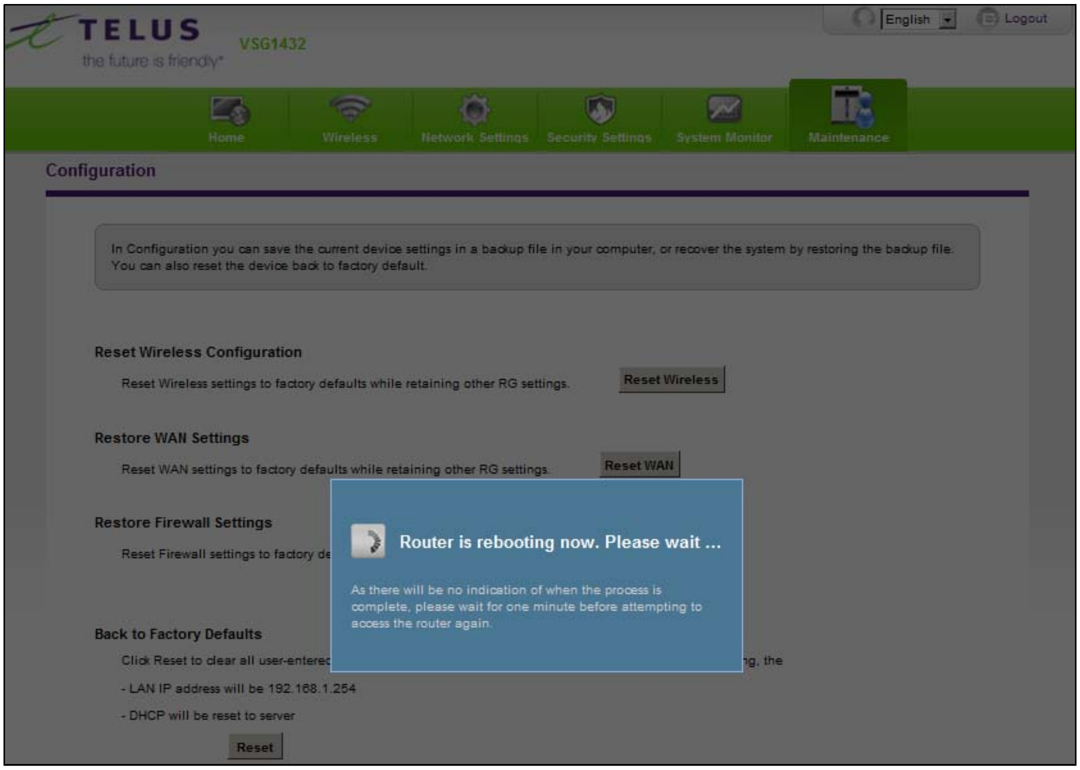


Are you sure you want to restore factory default settings?

4 The Reboot screen will display.

Note: The Power LED will start flashing. When it once again becomes solid green, the modem will be configured to its default settings and will be ready to be reconfigured. To reprogram your modem, follow the instructions provided by your ISP.

Note: The default username and password are on the label on the bottom of the Device.



Configuration

In Configuration you can save the current device settings in a backup file in your computer, or recover the system by restoring the backup file. You can also reset the device back to factory default.

Reset Wireless Configuration

Reset Wireless settings to factory defaults while retaining other RG settings. Reset Wireless

Restore WAN Settings

Reset WAN settings to factory defaults while retaining other RG settings. Reset WAN

Restore Firewall Settings

Reset Firewall settings to factory de

Router is rebooting now. Please wait ...

As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

Back to Factory Defaults

Click Reset to clear all user-enterec ng, the

- LAN IP address will be 192.168.1.254

- DHCP will be reset to server

Reset

CHAPTER 3

Troubleshooting

3.1 Overview

This section offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Device Access and Login
- Internet Access

3.2 Power, Hardware Connections, and LEDs

None of the LEDs turn on.

1 Make sure the Device is plugged in.

2 Make sure you are using the power adaptor or cord included with the Device.

3 Make sure the power adaptor or cord is connected to the Device and plugged in to an appropriate power source. Make sure the power source is turned on.

4 Unplug the the Device's power adapter, and plug it back in.

5 Try plugging the power adaptor into a different power outlet.

6 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 1.6 on page 8.

2 Check the hardware connections.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Unplug the the Device's power adapter, and plug it back in.

5 If the problem continues, contact the vendor.

3.3 Device Access and Login

I forgot the IP address for the Device.

1. The default LAN IP address is 192.168.1.254.
2. If you changed the IP address and have forgotten it, you might get the IP address of the Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Device (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 2.12 on page 44.

I forgot the password.

1. The default username and password is on the cover of this guide and on the label on the bottom of the Device.
2. If this does not work, you have to reset the device to its factory defaults. See Section 2.12 on page 44.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.254.
   - If you changed the IP address, use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Device.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.6 on page 8.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
4. Reset the device to its factory defaults, and try to access the Device with the default IP address. See Section 2.12 on page 44.
5. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to an **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the Device.

1 Make sure you have entered the password correctly. The default username and password is on the cover of this User's Guide. The field is case-sensitive, so make sure [Caps Lock] is not on.

2 Unplug the the Device's power adapter, and plug it back in.

3 If this does not work, you have to reset the device to its factory defaults. See Section 2.12 on page 44.

3.4 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.6 on page 8.

2 If you are trying to access the Internet wirelessly, make sure that you enabled the wireless LAN in the Device and your wireless client and that the wireless settings in the wireless client are the same as the settings in the Device.

3 Disconnect all the cables from your device, and follow the directions in Section 1.5 on page 7 again.

4 If you are connecting through a DSL conection, make sure you have the **DSL WAN** port connected to a telephone jack (or the DSL or modem jack on a splitter if you have one).

5 If you are connecting through an Ethernet WAN connection, make sure you have the **ETHERNET WAN** port connected to a broadband modem or router in your network.

6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the Device), but my Internet connection is not available anymore.

1 Your session with the Device may have expired. Try logging into the Device again.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.6 on page 8.

3 Unplug the the Device’s power adapter, and plug it back in.

4 If the problem continues, contact your ISP.

3.5 Wireless Internet Access

What factors may cause intermittent or unstable wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What is a Server Set ID (SSID)?

An SSID is a name that uniquely identifies a wireless network. The AP and all the clients within a wireless network must use the same SSID.

What wireless security modes does my Device support?

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your ZyXEL device are as follows:

- **WPA2-PSK:** (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WEP:** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

Technical Specifications

The following table summarize the Device’s hardware and firmware features.

Hardware Specifications

Gigabit Ethernet WAN Port	One RJ-45 connector for GBE WAN
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
Wireless Functionality	Allow the IEEE 802.11b, IEEE 802.11g and/or IEEE 802.11n wireless clients to connect to the Device wirelessly. Enable wireless security (WEP, WPA-PSK, WPA2-PSK, Mixed WPA2-PSK/WPA-PSK) and/or MAC filtering to protect your wireless network.
DSL Port	One RJ-11 connector for DSL over POTS
Power Adaptor Output	12 V 1.5 A
Power Adaptor Input	100 ~ 240 VAC 50~60HZ