StarTech.com

Hard-to-find made easy®

300Mbps Wireless-N Guest WiFi Access Point / Account Generator - 2T2R 2.4GHz

R300WN22GAxx

*actual product may vary from photos

DE: Bedienungsanleitung - de.startech.com
FR: Guide de l'utilisateur - fr.startech.com
ES: Guía del usuario - es.startech.com
IT: Guida per l'uso - it.startech.com
NL: Gebruiksaanwijzing - nl.startech.com
PT: Guia do usuário - pt.startech.com

For the most up-to-date information, please visit: www.startech.com

Manual Revision: 09/08/2014

FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

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.

Changes or modifications not expressly approved by StarTech.com could void the user's authority to operate the equipment.

Industry Canada Statement

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

CAN ICES-3 (B)/NMB-3(B)

This device complies with Industry Canada licence-exempt RSS standard(s).
Operation is subject to the following two conditions:
(1) This device may not cause interference, and
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.
L'exploitation est autorisée aux deux conditions suivantes:
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

IC Radiation Exposure Statement

This equipment complies with IC RSS-102 radiation exposure limit set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 0.5cm between the radiator and your body.

Déclaration d'exposition à la radiation

Cet équipement respecte les limites d'exposition aux rayonnements IC définies pour un environnement non contrôlé. Cet équipement doit être installé et mis en marche à une distance minimale de 0.5 cm qui sépare l'élément rayonnant de votre corps.

L'émetteur ne doit ni être utilisé avec une autre antenne ou un autre émetteur ni se trouver à leur proximité.

FCC ID: TWS-GW-1

IC:11232A-R300WN22GA

The Country Code Selection feature is disabled for products marketed in the US/Canada

The device, for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Use of Trademarks, Registered Trademarks, and other Protected Names and Symbols

This manual may make reference to trademarks, registered trademarks, and other protected names and/or symbols of third-party companies not related in any way to StarTech.com. Where they occur these references are for illustrative purposes only and do not represent an endorsement of a product or service by StarTech.com, or an endorsement of the product(s) to which this manual applies by the third-party company in question. Regardless of any direct acknowledgement elsewhere in the body of this document, StarTech.com hereby acknowledges that all trademarks, registered trademarks, service marks, and other protected names and/or symbols contained in this manual and related documents are the property of their respective holders.

Table of Contents

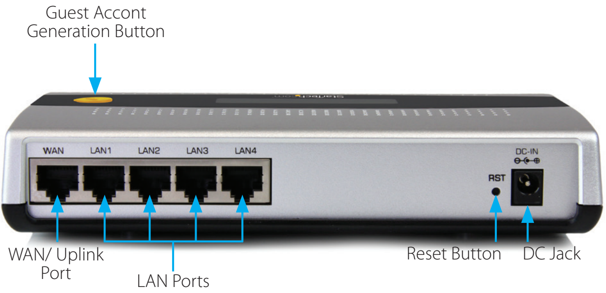
Introduction

Packaging Contents

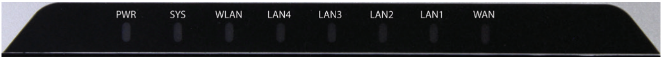
- 1 x Guest WiFi Access Point / Account Generator
- 1 x Ethernet Cable
- 2 x Screws for Wall Mounting
- 1 x Power Adapter
- 1 x Quick Start Guide
- 1 x Instruction Manual CD

Product Diagram

Product Overview



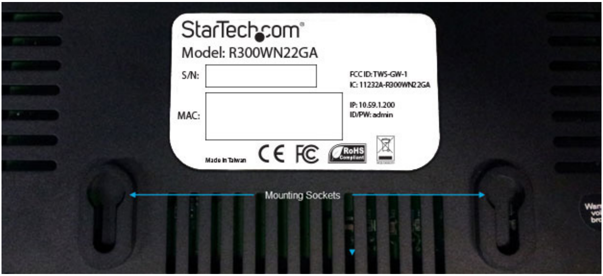
LED Indicators



LED	State	Description
PWR	Off	No power
	Green	Unit powered on
SYS	Off	Remains off while the unit is initializing
	Green	Initialization complete, system is ready to use
	Green (Blinking)	During firmware upgrades, this system LED will blink
WAN	Off	No network connection
	Green	10/100Mbps network connection established
	Green (Blinking)	Indicates WAN activity
LAN-1-4	Off	No network connection
	Green	10/100Mbps network connection established
	Green (Blinking)	Indicates LAN activity
WLAN	Off	The Wireless is not ready
	Green	Wireless connection established
	Green (Blinking)	Indicates Wireless activity

Installation

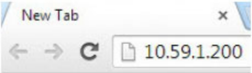
1. The Access Point is designed to sit on a flat surface (such as a desktop) or be securely mounted to a wall or similar surface. If you wish to mount the device, first prepare the surface by installing mounting screws (not included) otherwise skip to Step 5.



2. The distance between the two mounting sockets on the back of the Network Switch is approximately 106mm. Mark the distance on the wall, making sure your marks are straight and level.
3. Depending on the mounting surface, use the appropriate tools and hardware to install mounting screws into the surface. There should be a gap of approximately 2 mm between the head of the screw and the wall surface.
4. Place the Access Point so that the wide openings of the mounting sockets are over the screw heads. Slide the case downward so that the screw heads slide into the narrow slots.
5. Connect an Ethernet cable from the WAN port on the Access Point (AP) to your ISP modem (Cable, DSL, etc.).
6. Connect a second Ethernet cable from your computer to one of the LAN ports on the AP.
7. Connect the power adapter to the DC jack on the AP and wait approximately 30 second for the unit to initialize.

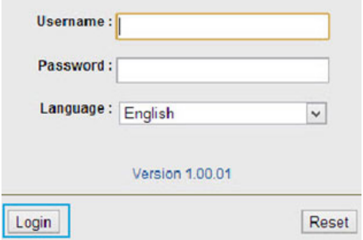
   Note: If the message Error: 0001 appears on the LCD screen, the AP did not detect a connection on the WAN port, please check your cabling.

8. Open your preferred web browser, enter the IP address of the Access Point (Default: **10.59.1.200**) into the address box and press Enter.



10.59.1.200

9. Login to the web GUI with your username / password (Default: **admin / admin**) and click Login.



Username :

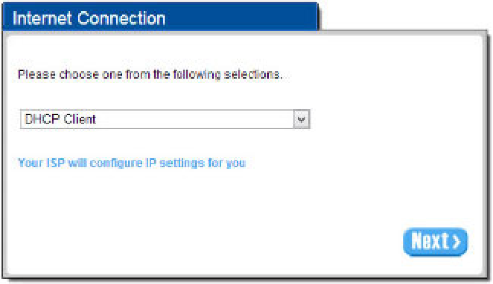
Password :

Language : English

Version 1.00.01

10. The Setup Wizard will bring you through the basic configuration requirements in 3 sections:

    Internet – Allows you to select the appropriate Internet connection type for your ISP



Internet Connection

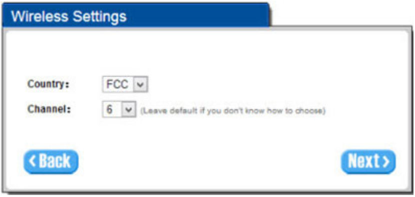
Please choose one from the following selections.

DHCP Client

Your ISP will configure IP settings for you

- DHCP Client – Allows the device to automatically obtain TCP/IP settings from your ISP Modem.
- Static IP – Manually enter your desired IP address settings.
- PPPoE (Point-to-Point Protocol over Ethernet) – Typically used for ADSL ISPs that require a username and password to connect
- PPTP Client (Point-to-Point Tunneling Protocol) – Typically used for European ADSL ISPs that require a username and password to connect.

Wireless – Allows you to specify basic wireless network settings



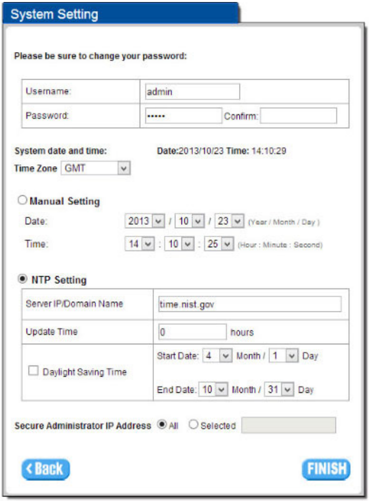
Wireless Settings

Country: FCC

Channel: 6 (Leave default if you don't know how to choose)

- Country – Choose between ETSI (European Telecommunications Standards Institute) or FCC (Federal Communications Commission – North America).
- Channel – Select the channel ID for wireless connection.

System – Allows you to specify basic system settings for the AP



System Setting

Please be sure to change your password:

Username:	admin
Password:	••••• Confirm:

System date and time: Date:2013/10/23 Time: 14:10:29

Time Zone GMT

○ Manual Setting

Date: 2013 / 10 / 23 (Year / Month / Day)

Time: 14 : 10 : 25 (Hour : Minute : Second)

● NTP Setting

Server IP/Domain Name	time.nist.gov
Update Time	0 hours
□ Daylight Saving Time	Start Date: 4 Month / 1 Day End Date: 10 Month / 31 Day

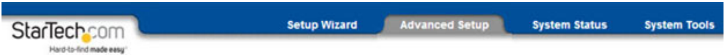
Secure Administrator IP Address ● All ○ Selected

- Username / Password – Change the default username and password.

  NOTE: It is strongly recommended to change the default security settings, to avoid unwanted access and/or configuration changes. Username and Password can consist of up to 20 alphanumeric characters and is case sensitive.

- System date and time – Specify the Time Zone and choose between manual date and time entry or NTP server settings.
- Secure Administrate IP Address – Administrator can specify 5 IP addresses or a range to allow remote control access from network.

11. Click **Finish** to complete the Setup Wizard.
12. Click the **Advanced Setup** tab on the top menu to further modify device settings.



Advanced Setup Menu

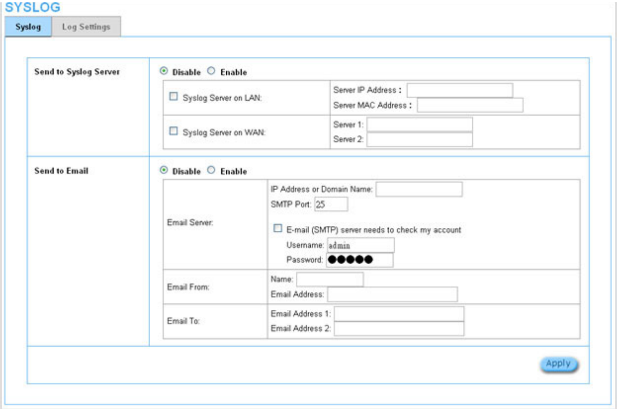
The Advanced Setup menu gives you access to all available device settings, so you can configure the device to suit your network requirements.

Click the **Apply** button in the bottom right corner of each section to save your changes (a restart of the device may be required for some changes).

Management

Syslog

The Syslog feature allows you to transmit event messages to your syslog server or email address for monitoring and troubleshooting



Send to Syslog Server: ● Disable ○ Enable

□ Syslog Server on LAN: Server IP Address : / Server MAC Address :

□ Syslog Server on WAN: Server 1: / Server 2:

Send to Email: ● Disable ○ Enable

Email Server: IP Address or Domain Name: / SMTP Port: 25

□ E-mail (SMTP) server needs to check my account

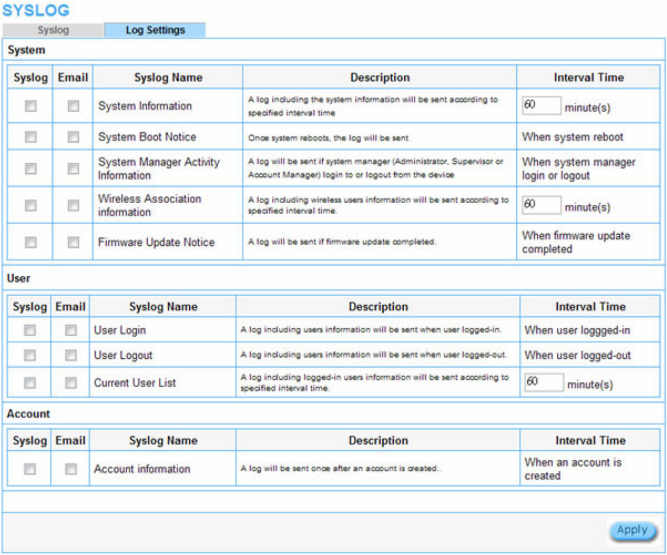
Username: admin

Password: ●●●●●

Email From: Name: / Email Address:

Email To: Email Address 1: / Email Address 2:

Item	Default	Description
Syslog	Disable	Enables or disables the syslog server function.
Syslog on LAN		
Server IP Address	Empty	Enter your syslog server LAN IP address.
Server MAC Address	Empty	Enter your syslog server MAC address.
Syslog on WAN		
Server 1 IP Address	Empty	Enter the WAN IP address of your first syslog server.
Server 2 IP Address	Empty	Enter the WAN IP address of your second syslog server.
Send to Email	Disable	Enables or disables the send to e-mail function.
E-mail Server		
IP Address or Domain Name	Empty	Enter your SMTP server IP address or domain name (max 50 characters).
SMTP Port	25	Acceptable SMTP port range is 25 or 2500 to 2599.
E-mail (SMTP) Server needs to check my account	Disable	If your SMTP server requires authentication before accepting e-mail, enable this option. These values (username and password) are supplied by your network administrator, SMTP server provider or ISP.
Username	Empty	Enter the username for your SMTP server (up to 64 characters).
Password	Empty	Enter the password for your SMTP server
Email From		
Name	Empty	Enter the name you would like to appear in the "Message From" field of your outgoing message (max 20 characters).
Email Address	Empty	Enter a From email address.
Email To		
Email Address 1	Empty	Enter an email address to receive the logs.
Email Address 2	Empty	Enter a secondary e-mail address to receive the logs.



SYSLOG

System

Syslog	Email	Syslog Name	Description	Interval Time
☐	☐	System Information	A log including the system information will be sent according to specified interval time	60 minute(s)
☐	☐	System Boot Notice	Once system reboots, the log will be sent	When system reboot
☐	☐	System Manager Activity Information	A log will be sent if system manager (Administrator, Supervisor or Account Manager) login to or logout from the device	When system manager login or logout
☐	☐	Wireless Association information	A log including wireless users information will be sent according to specified interval time.	60 minute(s)
☐	☐	Firmware Update Notice	A log will be sent if firmware update completed.	When firmware update completed

User

Syslog	Email	Syslog Name	Description	Interval Time
☐	☐	User Login	A log including users information will be sent when user logged-in.	When user loggged-in
☐	☐	User Logout	A log including users information will be sent when user logged-out.	When user logged-out
☐	☐	Current User List	A log including logged-in users information will be sent according to specified interval time.	60 minute(s)

Account

Syslog	Email	Syslog Name	Description	Interval Time
☐	☐	Account information	A log will be sent once after an account is created..	When an account is created

Item	Interval Time	Description
System		

System Information	5~60 minutes	System information would be sent according to specified interval time.
		Format:
		PRODUCT=GW-1;VER=2.00.00;LOGNAME=DVI; DATE=07Mar26;TIME=11:30:00;
		WANMAC=09-00-0e-00-00-01;LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03; IP_ADDRESS=210.66.37.21; SYS_UP_TIME=14D23H34M21S;WANTXOK=99999;
		WANRXOK=99999;WANTXERROR=99999;WANRXERROR=99999; LANTXOK=99999;LANRXOK=99999;LANTXERROR=99999; LANRXERROR=99999;WIRELESSTXOK=99999;WIRELESSRXOK=99999; WIRELESSTXERROR=99999;WIRELESSRXERROR=99999;

System Boot Notice	When system rebooted	If device have been rebooted or restarted, the log would be sent.
		Format:
		PRODUCT=GW-1;VER=2.00.00;LOGNAME=SUN; DATE=07Mar26;TIME=15:23:32;
		WANMAC=09-00-0e-00-00-01;LANMAC=09-00-0e-00-00-02;WLANMAC=09-00-0e-00-00-03; IP_ADDRESS=210.66.37.21; SYS_NAME=Cafehotspot;LOCATION=East;CITY=Taipei;
		COUNTRY=Taiwan; FIRMWARE=v1.01.02;MESSAGE=System_Up;
		Message = System_Reboot

System Manager Activity Information	When system manager login or logout	A log will be sent if system manager (Administrator) login to or logout from the device. **Format:** PRODUCT=GW-1;VER=2.00.00;LOGNAME=SUN; DATE=07Mar26;TIME=15:23:32; WANMAC=09-00-0e-00-00-01;LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03; IP_ADDRESS=210.66.37.21; SYS_NAME=Cafehotspot;LOCATION=East;CITY= Taipei; COUNTRY=Taiwan; FIRMWARE=v1.01.02; MESSAGE=System_Up; **Account Name** = Admin **Status** = Login | Logout | Idle_Time_Out

Wireless Association Information	5~60 minutes.	A log including wireless users information will be sent according to specified interval time.
		Format:
		PRODUCT=GW-1;VER=2.00.00;LOGNAME=WAI; DATE=07Mar26;TIME=15:23:32;
		WANMAC=09-00-0e-00-00-01;LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03; IP_ADDRESS=210.66.37.21;
		USER_NUM=15;SEQ=1-5;USER_MAC=02-34-3e-01-00;

Firmware Update Notice	When firmware update completed	A log will be sent if firmware update completed **Format:** PRODUCT=GW-1;VER=2.00.00;LOGNAME=FUN; DATE=07Mar26;TIME=15:23:32; WANMAC=09-00-0e-00-00-01;LANMAC=09-00-0e-00-00-02; LANMAC=09-00-0e-00-00-03; IP_ADDRESS=210.66.37.21; MESSAGE=Success;OLD_FRIMWARE=v1.00.01; NEW_FIRMWARE=v1.00.02 **Message** = Success | Fail

User		

User Login	When a user logs in	A log including users information will be sent when a user logs in
		Format:
		PRODUCT=GW-1;VER=2.00.00;LOGNAME=ULI;DATE=07Mar26; TIME=15:23:32;WANMAC=09-00-0e-00-00-01;
		LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03;
		IP_ADDRESS=210.66.37.21;USER_NAME=asdfg12;USER_IP=10.59.1.1; USER_MAC=02-34-3e-01-00;INTERFACE=Ethernet;
		USER_TYPE=Dynamic;
		User Type = Guest/ Employee

User Logout	When user logged-out	A log including users information will be sent when user logged –out
		Format:
		PRODUCT=GW-1;VER=2.00.00;LOGNAME=ULO;DATE=07Mar26; TIME=15:23:32;WANMAC=09-00-0e-00-00-01;
		LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03;
		IP_ADDRESS=210.66.37.21;USER_NAME=asdfg12;USER_IP=10.59.1.1; USER_MAC=02-34-3e-01-00;INTERFACE=Ethernet; USER_TYPE=Dynamic;RXDATA=1234; TXDATA=1234; USED_TIME=24:00:00;LOGOUT_TYPE=Time_Up;TIME_LEFT=24:00:00
		User Type = Guest/ Employee

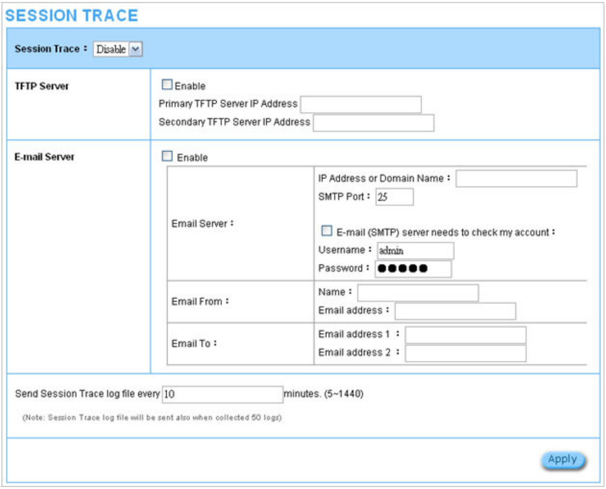
Current User List	.5~60 minutes.	A log including logged-in users information will be sent according to specified interval time
		Format:
		PRODUCT=GW-1;VER=2.00.00;LOGNAME=CUL;DATE=07Mar26; TIME=15:23:32;WANMAC=09-00-0e-00-00-01;
		LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03;
		IP_ADDRESS=210.66.37.21;USER_NUM=0;SEQ=1-5; USER_NAME=asdfg12,USER_IP=10.59.1.2,USER_MAC=02-34-3e-01-00, INTERFACE=Ethernet,USER_TYPE=Dynamic,RXDATA=1234,
		TXDATA=1234,USED_TIME=24:00:00,SESSION=100,WLAN_SIG=N/A;

Account		

Account Information	When an account is created	A log will be sent when an account is created
		Format:
		PRODUCT=GW-1;VER=2.00.00;LOGNAME=ACI;DATE=07Mar26; TIME=15:23:32;WANMAC=09-00-0e-00-00-01;
		LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03; IP_ADDRESS=210.66.37.21;USER_NAME=asdfg12; ACCOUNT_TYPE=TimetoFinish; ACCOUNT_SERIAL=000002;
		ACCOUNT_PRICE= USD20.00; ACCOUNT_USAGE_TIME=10:59:59;

Session Trace

Session Trace is an intelligent function to help you trace user behavior. When Session Trace is enabled, the system will collect information such as destination IP, destination port, source IP, source MAC, source port from every user and send the collected information in text file format to a specified TFTP server or Email Server.



SESSION TRACE

Session Trace : Disable

TFTP Server

□ Enable

Primary TFTP Server IP Address

Secondary TFTP Server IP Address

E-mail Server

□ Enable

Email Server :

IP Address or Domain Name :

SMTP Port : 25

□ E-mail (SMTP) server needs to check my account :

Username : admin

Password : ●●●●●

Email From :

Name :

Email address :

Email To :

Email address 1 :

Email address 2 :

Send Session Trace log file every 10 minutes. (5~1440)

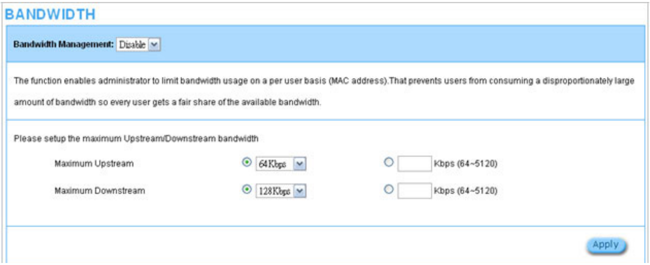
(Note: Session Trace log file will be sent also when collected 50 logs)

Item	Default	Description
Session Trace	Disable	Disables or enables session trace function.
Primary TFTP Server IP Address	Empty	Enter the IP address of the primary TFTP server.
Secondary TFTP Server IP Address	Empty	Enter the IP address of the secondary TFTP server.
Send Session Trace log file every	10 minutes	Send the session trace log file at the specified interval. Acceptable range is from 5 to 1440 minutes
Send to Email	Disable	Enables or disables the send to e-mail function.
E-mail Server		
IP Address or Domain Name	Empty	Enter the SMTP server IP address or domain name (max 50 characters).
SMTP Port	Empty	Acceptable SMTP port range is 25, or from 2500 to 2599.

E-mail (SMTP) Server needs to check my account	Disable	If your SMTP server requires authentication before accepting e-mail, enable this option. These values (username and password) are supplied by your network administrator, SMTP server provider or ISP.
Username	Empty	Enter the username for the SMTP server (max 64 characters).
Password	Empty	Enter the password for the SMTP server.
Email From		
Name	Empty	Enter the name you would like to appear in the “message from” field of your outgoing message (max 20 characters).
Email Address	Empty	Enter a From email address.
Email To		
Email Address 1	Empty	Enter an email address to receive the logs.
Email Address 2	Empty	Enter a secondary email address to receive the logs.

Bandwidth Management

The Bandwidth Management function enables you to limit bandwidth usage on a per user basis (by MAC address), preventing users from consuming a disproportionately large amount of bandwidth.



BANDWIDTH

Bandwidth Management: Disable

The function enables administrator to limit bandwidth usage on a per user basis (MAC address).That prevents users from consuming a disproportionately large amount of bandwidth so every user gets a fair share of the available bandwidth.

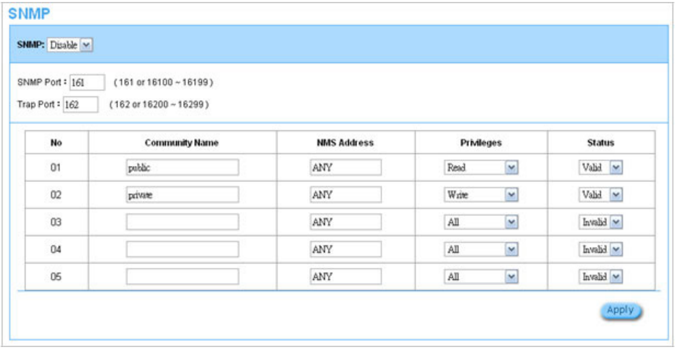
Please setup the maximum Upstream/Downstream bandwidth

Maximum Upstream	● 64Kbps	○ Kbps (64~5120)
Maximum Downstream	● 128Kbps	○ Kbps (64~5120)

Item	Default	Description
Bandwidth	Disable	Enables or disables Bandwidth Management.
Maximum Upstream	64Kbps	Specify the max upstream bandwidth (64 – 5120 Kbps).
Maximum Downstream	128Kbps	Specify the max downstream bandwidth (64 – 5120 Kbps).

SNMP

The SNMP configuration menu allows you to access to your device via Simple Network Management Protocol.



SNMP

SNMP: Disable

SNMP Port : 161 (161 or 16100 ~ 16199)

Trap Port : 162 (162 or 16200 ~ 16299)

No	Community Name	NMS Address	Privileges	Status
01	public	ANY	Read	Valid
02	private	ANY	Write	Valid
03		ANY	All	Invalid
04		ANY	All	Invalid
05		ANY	All	Invalid

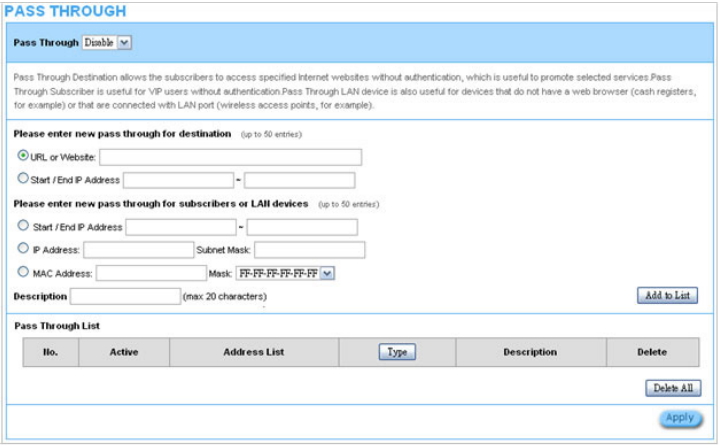
Item	Default	Description
SNMP	Disable	Disables or enables SNMP management.
SNMP Port	161	If SNMP is enabled, you can specify the SNMP port number. The allowed SNMP port numbers are 161 (default), or from 16100-16199 and Trap port numbers are 162 (default), or from 16200-16299. This Port setting is useful for remote control via NAT.
Trap Port	162	
Configuration		
Community Name	Public/Private	Every unit with SNMP enabled must be configured to recognize one or more community names (up to 20 characters). The default setting for the community of entry 1 is "public" and for the entry 2 is "private" and others are empty.
NMS Address	ANY	The address of the Network Management Station.
Privileges	Read/Write	Choose "Read", "Write", "Trap Recipients" or "All" for different privileges.
Status	Valid/Invalid	Choose "Valid" or "Invalid" to enable / disable the community entry. The default setting of entry 1, 2 are valid and others are invalid.

Security

Pass Through

The Pass Through function allows you to specify devices that can pass through the AP, without being checked and authorized.

Click the **Add to List** button once you've created a new entry.



PASS THROUGH

Pass Through: Disable

Pass Through Destination allows the subscribers to access specified Internet websites without authentication, which is useful to promote selected services.Pass Through Subscriber is useful for VIP users without authentication.Pass Through LAN device is also useful for devices that do not have a web browser (cash registers, for example) or that are connected with LAN port (wireless access points, for example).

Please enter new pass through for destination (up to 50 entries)

● URL or Website:

○ Start / End IP Address: -

Please enter new pass through for subscribers or LAN devices (up to 50 entries)

○ Start / End IP Address: -

○ IP Address: Subnet Mask:

○ MAC Address: Mask: FF-FF-FF-FF-FF-FF

Description (max 20 characters)

Pass Through List

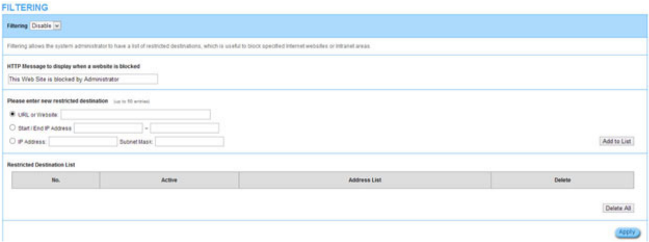
No.	Active	Address List	Type	Description	Delete

Item	Default	Description
Pass Through	Disable	Enables or disables the pass through function.
Destination URL/IP Address Pass Through		
URL or Website	Empty	Enter the URL Page (e.g. http://www.yahoo.com – Max 50 characters).
Start / End IP Address	Empty	Enter the range of IP address you want to allow.
Subscriber IP/MAC Address or LAN Device Pass Through		
Start / End IP Address	Empty	Enter the range of IP address you want to allow.
IP Address (single)	Empty	Enter the IP address you want to allow.
Subnet Mask	Empty	Enter the subnet mask.
MAC Address	Empty	Enter the MAC address you want to allow.
Mask	Empty	Enter the subnet mask.
Pass Through List		
No.	-	The index number of pass through address.
Active	Disable	Click the check box to activate or deactivate the pass through address.
Address List	-	Displays the pass through address(s).
Type	-	Displays the type of pass through address.
Delete	-	Select the check boxes and click 'Delete' to delete the pass through address(s).

Click the **Delete All** button to clear the list of all entries.

Filtering

The Filtering function allows you to maintain a list of restricted destinations, which can be used to block access to specified Internet sites or intranet areas globally (applies to Guest and Employee networks).



FILTERING

Filtering: Disable

Filtering allows the system administrator to have a list of restricted destinations, which is useful to block specified Internet websites or intranet areas.

HTTP Message to display when a website is blocked: This Web Site is blocked by Administrator

Please enter new restricted destination (up to 10 entries)

● URL or Website:

○ Start / End IP Address: -

○ IP Address: Subnet Mask:

Restricted Destination List

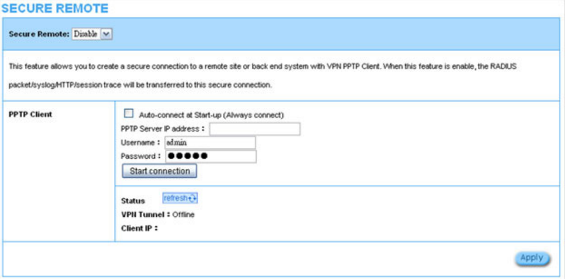
No.	Active	Address List	Delete

Item	Default	Description
Filtering	Disable	Enables or disables the pass through function.
HTTP Message to display when a website is blocked	This Web Site is blocked by Administrator	Enter the message you would like to display to the user when they attempt to access a restricted area.
Start / End IP Address	Empty	Enter the range of IP addresses you want to allow.
Please enter new restricted destination		
URL or Website	Empty	Enter the URL you would like to restrict.
Start / End IP Address	Empty	Enter a range of IP addresses you want to restrict.
IP Address (single)	Empty	Enter the IP address you want to restrict.
Subnet Mask	Empty	Enter the subnet mask.
Restricted Destination List		
No.	-	The index number of filtered destinations.
Active	Disable	Click the check box to activate or deactivate the filtered address.
Address List	-	Displays the filtered address(es).
Delete	-	Select the check boxes and click 'Delete' to delete the pass through address(es).

Click the **Delete All** button to clear the list of all entries.

Secure Remote

The Secure Remote feature allows you to create a secure connection to a remote site or back-end system through a VPN PPTP Client. If "Secure Remote" is enabled, the RADIUS packet / syslog will be transferred to this secure connection.



SECURE REMOTE

Secure Remote: Disable

This feature allows you to create a secure connection to a remote site or back end system with VPN PPTP Client. When this feature is enable, the RADIUS packet/syslog/HTTP/session trace will be transferred to this secure connection.

PPTP Client

□ Auto-connect at Start-up (Always connect)

PPTP Server IP address :

Username : admin

Password : ●●●●●

Start connection

Status refresh

VPN Tunnel : Offline

Client IP :

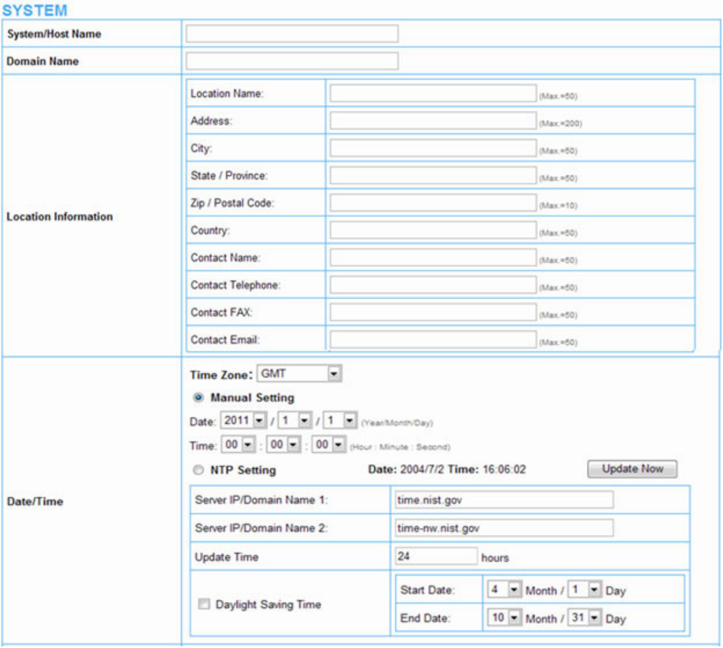
Apply

Item	Default	Description
Auto-connect at Start-up (Always connect)	Disable	Click the check box to automatically establish the PPTP connection.
PPTP Server IP address	Empty	Enter the PPTP server IP address provided by your ISP.
Username	Empty	Enter the username provided by your ISP. The user name can consist of up to 80 alphanumeric characters and is case-sensitive.
Password	Empty	Enter the user password provided by your ISP (Max 80 case-sensitive alphanumeric characters).
Start connection		Click the button to Start / Stop the PPTP connection.
refresh		Click the Refresh button to update the connection status.
VPN Tunnel		Displays the status.
Client IP		Displays the IP address.

System

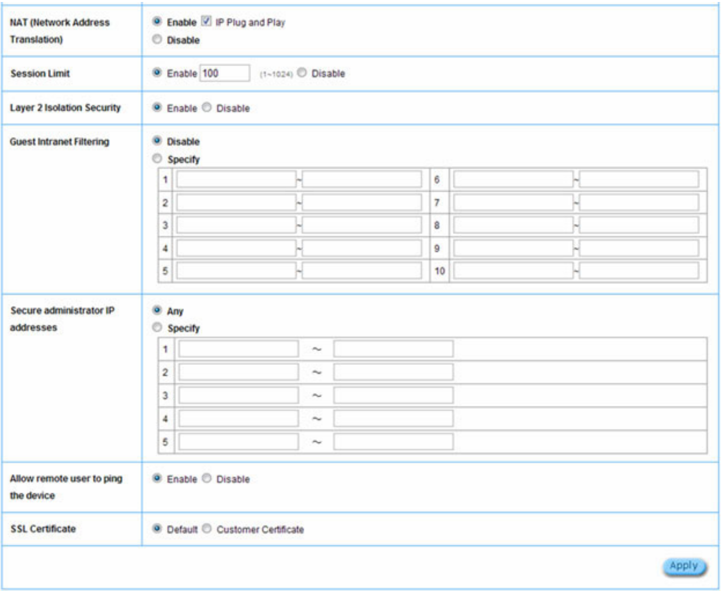
System

The System menu defines basic system settings.



SYSTEM

System/Host Name	
Domain Name	
Location Information	Location Name: (Max.=50) Address: (Max.=200) City: (Max.=50) State / Province: (Max.=50) Zip / Postal Code: (Max.=10) Country: (Max.=50) Contact Name: (Max.=50) Contact Telephone: (Max.=50) Contact FAX: (Max.=50) Contact Email: (Max.=50)
Date/Time	Time Zone: GMT ● Manual Setting Date: 2011 / 1 / 1 (Year/Month/Day) Time: 00 : 00 : 00 (Hour : Minute : Second) ○ NTP Setting Date: 2004/7/2 Time: 16:06:02 Update Now Server IP/Domain Name 1: time.nist.gov Server IP/Domain Name 2: time-nw.nist.gov Update Time 24 hours ☐ Daylight Saving Time Start Date: 4 Month / 1 Day End Date: 10 Month / 31 Day



NAT (Network Address Translation)	● Enable ☑ IP Plug and Play ○ Disable
Session Limit	● Enable 100 (1~1024) ○ Disable
Layer 2 Isolation Security	● Enable ○ Disable
Guest Intranet Filtering	● Disable ○ Specify 1 ~ 6 ~ 2 ~ 7 ~ 3 ~ 8 ~ 4 ~ 9 ~ 5 ~ 10 ~
Secure administrator IP addresses	● Any ○ Specify 1 ~ 2 ~ 3 ~ 4 ~ 5 ~
Allow remote user to ping the device	● Enable ○ Disable
SSL Certificate	● Default ○ Customer Certificate

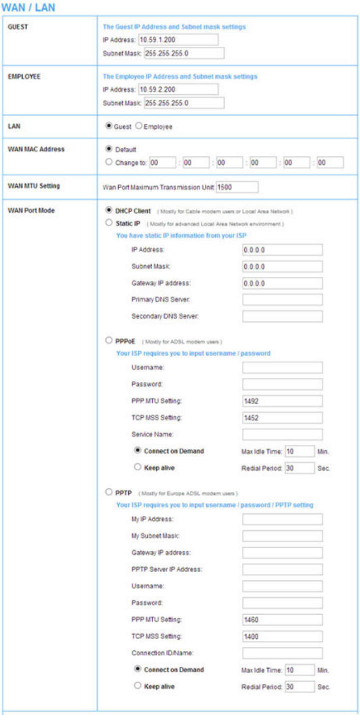
Item	Default	Description
System/Host Name	Empty	Enter a system name (Max 40 alphanumeric characters).
Domain Name	Empty	Enter a domain name (Max 80 1 characters).
Location Information	Empty	Enter your location and contact information if desired.
Date/Time		
Time Zone	GMT	Select the appropriate time zone for your location.

Manual Setting		
Date (Year/Month/Day)	-	Manually set the date for the system (Ranges from 2011 to 2035).
Time (Hour:Minute:Second)	-	Set the system time.
NTP Setting		
Server IP / Domain Name 1	Empty	Enter the primary IP address or domain name of NTP server (Max100 characters).
Server IP / Domain Name 2	Empty	Enter the secondary IP address or domain name of NTP server (Max100 characters).
Update Time	24 Hours	Enter the frequency (hours) in which to update the time.
Daylight Saving Time	Disable	Enables or disables Daylight Saving Time (DST).
	Month/ Day	Set the Daylight Saving Time (DST) start and end times.
NAT (Network Address Translation)	Enable	Enables or disables the Network Address Translation function
IP Plug and Play (iPnP Technology)	Enable	Enables or disables plug & play function. When enabled, the user needn't change their network configuration to access the Internet.
Session Limit	Enable, 100	Limits the number of sessions allowed per user at one time, when enabled.
Layer 2 Isolation Security	Enable	If IP Plug and Play is enabled, you can enable the Layer 2 Isolation Security function. When Layer 2 Isolation Security is enabled, users connected to the AP cannot communicate with each other.
Guest Intranet Filtering	Disable	When enabled, you can specify up to 10 IP addresses or ranges that Guest users cannot visit.
Secure administrator IP Addresses	Any	Specify up to 5 IP addresses or ranges to allow remote administrative access from only those specified

Allow remote user to ping the device	Enable	This function allows remote users to ping the AP. Ping is normally used to test the physical connection between two devices, to ensure that everything is working correctly.
SSL Certificate	Default	Options: Default or Customer Certificate

WAN/LAN

The WAN / LAN menu allows you to configure IP addressing and WAN connection settings.



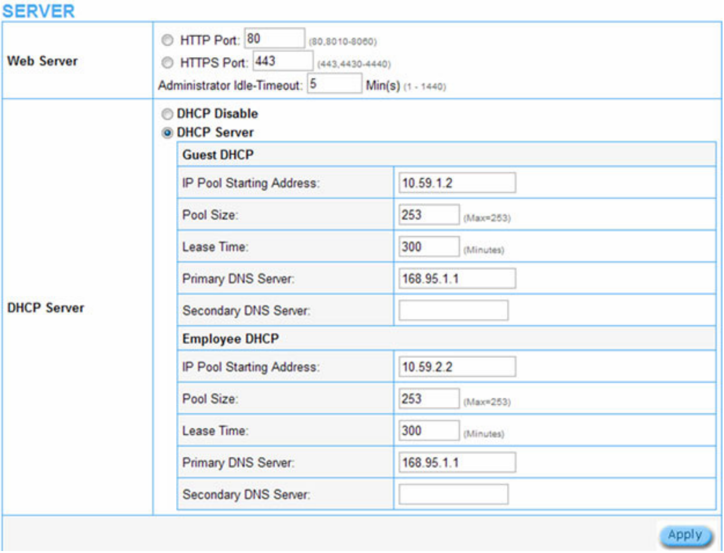
WAN / LAN

GUEST	The Guest IP Address and Subnet mask settings IP Address: 10.59.1.200 Subnet Mask: 255.255.255.0
EMPLOYEE	The Employee IP Address and Subnet mask settings IP Address: 10.59.2.200 Subnet Mask: 255.255.255.0
LAN	● Guest ○ Employee
WAN MAC Address	● Default ○ Change to: 00 : 00 : 00 : 00 : 00 : 00
WAN MTU Setting	Wan Port Maximum Transmission Unit 1500
WAN Port Mode	● DHCP Client (Mostly for Cable modem users or Local Area Network) ○ Static IP (Mostly for advanced Local Area Network environment) You have static IP information from your ISP IP Address: 0.0.0.0 Subnet Mask: 0.0.0.0 Gateway IP address: 0.0.0.0 Primary DNS Server: Secondary DNS Server: ○ PPPoE (Mostly for ADSL modem users) Your ISP requires you to input username / password Username: Password: PPP MTU Setting: 1492 TCP MSS Setting: 1452 Service Name: ● Connect on Demand Max Idle Time: 10 Min. ○ Keep alive Redial Period: 30 Sec. ○ PPTP (Mostly for Europe ADSL modem users) Your ISP requires you to input username / password / PPTP setting My IP Address: My Subnet Mask: Gateway IP address: PPTP Server IP Address: Username: Password: PPP MTU Setting: 1460 TCP MSS Setting: 1400 Connection ID/Name: ● Connect on Demand Max Idle Time: 10 Min. ○ Keep alive Redial Period: 30 Sec.

Item	Default	Description
Guest WLAN IP Address Setting		
IP Address	10.59.1.200	Enter the internal LAN IP address for the device.
Subnet Mask	255.255.255.0	Enter the subnet mask for the IP address entered above.
Employee WLAN IP Address Setting		
IP Address	10.59.2.200	The internal LAN IP address of your Wireless Subscriber Server Gateway.
Subnet Mask	255.255.255.0	Enter the subnet mask for the IP address.
LAN	Guest	Guest LAN: Configures the LAN ports to allow access to the Internet with authentication required (Guest ID / Key). Employee LAN: Configures the LAN ports to allow access to the Internet without authentication.
WAN MAC Address	Default	The default MAC address is set to the WAN physical interface on the device.
WAN Port Mode	DHCP Client	DHCP Client: Allows the device to obtain the IP address and other TCP/IP settings from your ISP. Static IP: Allows you to specify the IP address information for the WAN port. PPPoE: Allows you to enter a username / password and connection information for your WAN connection (typically for North American ADSL connections). PPTP: Allows you to enter a username / password and connection information for your WAN connection (typically for European ADSL connections).

Server

The Server menu allows you to configure Web and DHCP server settings.



SERVER

Web Server	○ HTTP Port: 80 (80,8010-8060) ○ HTTPS Port: 443 (443,4430-4440) Administrator Idle-Timeout: 5 Min(s) (1 - 1440)
DHCP Server	○ DHCP Disable ● DHCP Server

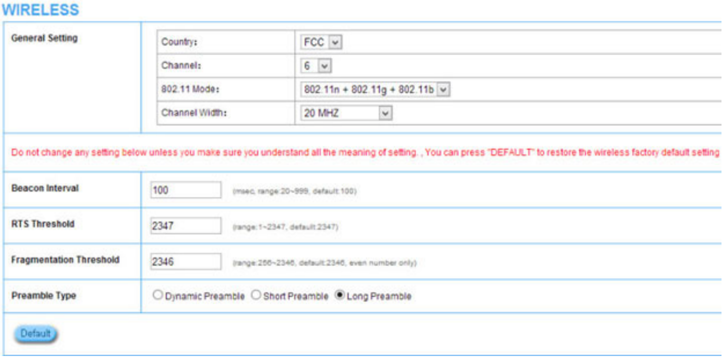
Guest DHCP	
IP Pool Starting Address:	10.59.1.2
Pool Size:	253 (Max=253)
Lease Time:	300 (Minutes)
Primary DNS Server:	168.95.1.1
Secondary DNS Server:	
Employee DHCP	
IP Pool Starting Address:	10.59.2.2
Pool Size:	253 (Max=253)
Lease Time:	300 (Minutes)
Primary DNS Server:	168.95.1.1
Secondary DNS Server:	

Item	Default	Description
Web Server		
HTTP Port	80	Enter the HTTP port number (80 or from 8010 to 8060). For access to the AP under NAT, enter using the format: "http://[IP Address]:[Port Number]"
HTTPS Port	443	Enter the HTTPS port number (443 or from 4430 to 4440). For access to the AP under NAT, enter using the format: "http://[IP Address]:[Port Number]"

Administrator Idle-Timeout	5 Minutes	Enter an idle timeout duration in minutes (From 1-1440). If the idle time out is set as 5 minutes, it means that if the administrator doesn't send packet in 5 minutes, the administrator will be logged out.
DHCP Server		
DHCP Server	DHCP Server	DHCP Disable: Disable the DHCP server function. DHCP Server: Enable DHCP server function.
Guest DHCP		
DHCP Pool Starting Address	10.59.1.2	Enter the Starting IP address for the Guest address pool.
Pool Size	253	Enter a DHCP pool size range (From 1 to 253).
Lease Time	300 Minutes	Enter a lease time value in minutes (From 1 to 71582788).
Primary DNS Server	168.95.1.1	Enter the IP address of the primary DNS server.
Secondary DNS Server	Empty	Enter the IP address of the secondary DNS server.
Employee DHCP		
DHCP Pool Starting Address	10.59.2.2	Enter the Starting IP address for the Employee address pool.
Pool Size	253	Enter a DHCP pool size range (From 1 to 253).
Lease Time	300 Minutes	Enter a lease time value in minutes (From 1 to 71582788).
Primary DNS Server	168.95.1.1	Enter the IP address of the primary DNS server.
Secondary DNS Server	Empty	Enter the IP address of the secondary DNS server.

Wireless

The Wireless menu allows you to configure your desired wireless mode and applicable settings.



WIRELESS

General Setting

Country: FCC

Channel: 6

802.11 Mode: 802.11n + 802.11g + 802.11b

Channel Width: 20 MHZ

Do not change any setting below unless you make sure you understand all the meaning of setting. , You can press "DEFAULT" to restore the wireless factory default setting

Beacon Interval: 100 (msec, range:20~999, default:100)

RTS Threshold: 2347 (range:1~2347, default:2347)

Fragmentation Threshold: 2346 (range:256~2346, default:2346, even number only)

Preamble Type: ○ Dynamic Preamble ○ Short Preamble ● Long Preamble

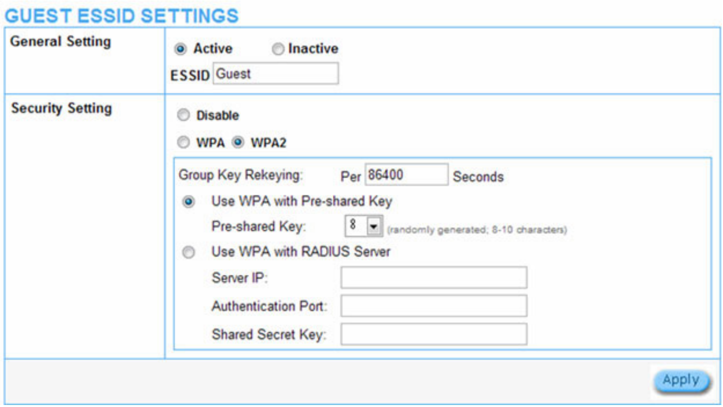
Item	Default	Description
General Settings		
Country	FCC	Select the Country code: -ESTI (Europe; Channel 1~13) -FCC (North America; Channel 1~11)
Channel	6	Select the channel ID for wireless connection.
802.11 mode		Select one of the following modes: -802.11n+802.11g+802.11b -802.11n+802.11g -802.11g+802.11n -802.11n only -802.11g only -802.11b only

Channel Width	Auto 20/40MHz	
Beacon Interval	200	Indicates the frequency interval of the beacon (From 1 to 1000).
RTS Threshold	2347	This valid range is from 256-2342. This setting determines the packet size at which the AP issues a Request To Send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the AP, or in areas where clients are far apart and can detect only the AP (not each other).
Fragmentation Threshold	2432	This setting determines the size at which packets are fragmented. Enter a setting ranging from 256 to 2432 bytes. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
Preamble Type	Long Preamble	The preamble type is a section of data at the head of a packet that contains information the AP and client devices need when sending and receiving packets. Select from Long, Short or Dynamic preamble types.

Guest Setting

Guest ESSID Settings

The Guest ESSID Settings menu allows you to configure your guest wireless settings and security.



GUEST ESSID SETTINGS

General Setting

● Active ○ Inactive

ESSID: Guest

Security Setting

○ Disable

○ WPA ● WPA2

Group Key Rekeying: Per 86400 Seconds

● Use WPA with Pre-shared Key

Pre-shared Key: 8 (randomly generated; 8-10 characters)

○ Use WPA with RADIUS Server

Server IP:

Authentication Port:

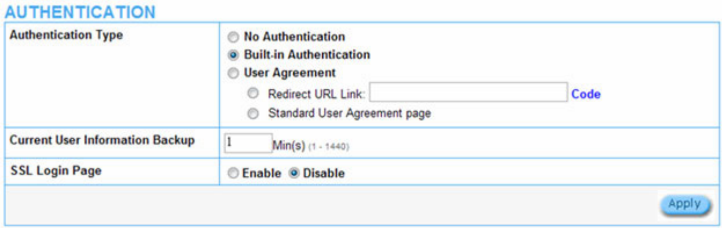
Shared Secret Key:

Item	Default	Description
General Settings	Active	Activate or de-activate the Guest wireless connection interface.
ESSID	Guest	The ESSID is the unique name that is shared among all points in a wireless network. It is case sensitive and must not exceed 32 characters.
Security	Enable	Disable to allow users to communicate with the device without any data encryption. Enable to use WPA or WPA2 data encryption.
Group Key Re-Keying	86400 Seconds	Enter a number in seconds to set the force re-keying interval.

Pre-shared Key	Empty	The AP will randomly generate keys at the length specified here. (8-10 characters)
Use WPA with RADIUS	Disable	
Server IP	Empty	Enter the RADIUS server IP address or domain name (Max 15 characters).
Authentication Port	1812	Enter the authentication port number (From 0 to 65535).
Shared Secret Key	Empty	Enter the RADIUS key

Authentication

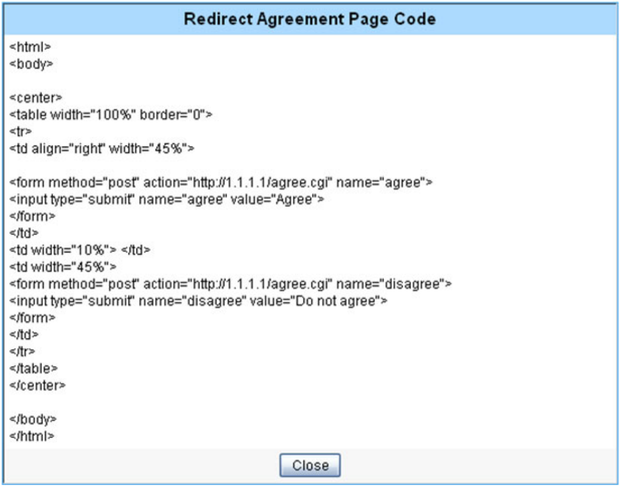
The Authentication menu allows you to configure the type of guest user authentication required.



AUTHENTICATION

Authentication Type	○ No Authentication ● Built-in Authentication ○ User Agreement ○ Redirect URL Link: Code ○ Standard User Agreement page
Current User Information Backup	1 Min(s) (1 - 1440)
SSL Login Page	○ Enable ● Disable

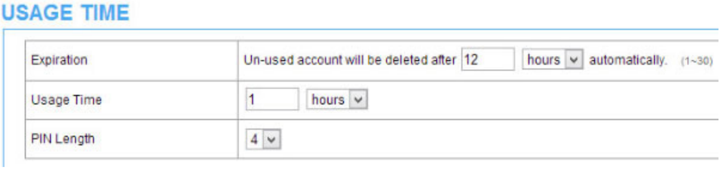
Item	Default	Description
Authentication Type	Built-in Authentication	**No Authentication:** Subscriber can direct access the Internet without enter username and password. **Built-in Authentication:** The AP provides "Built-in Authentication" that allows you to build up an Internet service without extra authentication software. When selected, you can generate the subscriber account inside the AP, and the system will authenticate the subscriber login according to the generated account. **User Agreement:** Subscriber must accept the service usage agreement before they can access the Internet. The Standard User Agreement page can be configured in the Guest Settings > Customization section
Redirect URL Link	Empty	Enter the URL where your agreement page is located or click the button to create your own (sample code below). The maximum character length of the URL Link is 200.
Current User Information Backup	1 Min(s)	The system automatically backs up account information and unused account to flash ROM. This function allow administrator to adjust the backup interval in minutes (From 1 to 1440).
SSL Login Page	Disable	Enables or disables SSL security of login page.



```
<html>
<body>

<center>
<table width="100%" border="0">
<tr>
<td align="right" width="45%">

<form method="post" action="http://1.1.1.1/agree.cgi" name="agree">
<input type="submit" name="agree" value="Agree">
</form>
</td>
<td width="10%"> </td>
<td width="45%">
<form method="post" action="http://1.1.1.1/agree.cgi" name="disagree">
<input type="submit" name="disagree" value="Do not agree">
</form>
</td>
</tr>
</table>
</center>

</body>
</html>
```

Usage Time

The Usage Time menu allows you to manage account expiration and usage duration settings.



Expiration	Un-used account will be deleted after 12 hours automatically. (1~30)
Usage Time	1 hours
PIN Length	4

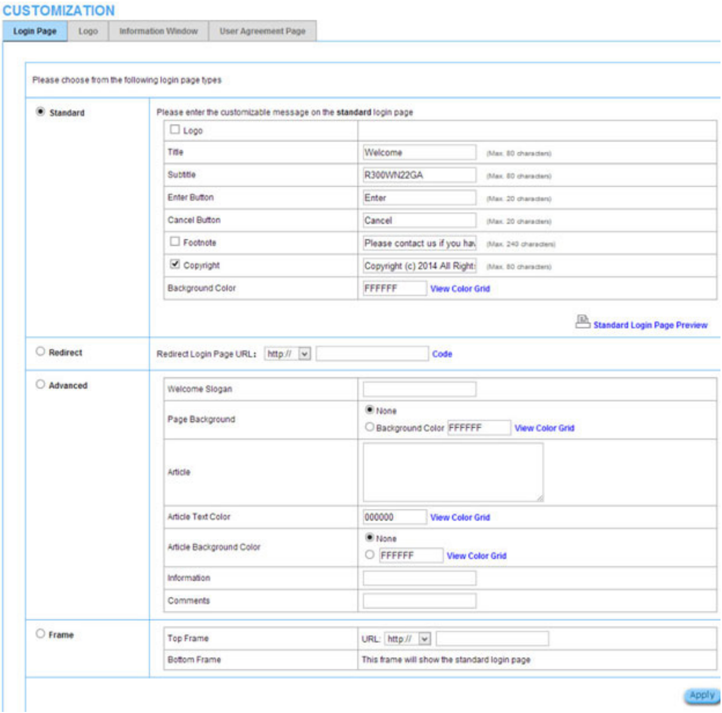
Item	Default	Description
Expiration	12 hours	Enter the number of hours/days that unused accounts should be deleted after (Max 30 Hours / Days).
Usage Time	3 hours	Enter the number of hours/days the guest account should remain valid for (Max 30 Hours / Days).
PIN Length	4	The field range is 4-6 characters.

Customization

The Customization menu allows you to create a custom login page, add a logo, create an information pop-up window and user agreement as needed.

Login Page Tab

Provides several different options for you to create or redirect guest users to your login page.



Please choose from the following login page types

● Standard

Please enter the customizable message on the **standard** login page

□ Logo	
Title	Welcome (Max. 80 characters)
Subtitle	R300WN22GA (Max. 80 characters)
Enter Button	Enter (Max. 20 characters)
Cancel Button	Cancel (Max. 20 characters)
□ Footnote	Please contact us if you hav (Max. 240 characters)
☑ Copyright	Copyright (c) 2014 All Right: (Max. 80 characters)
Background Color	FFFFFF View Color Grid

○ Redirect

Redirect Login Page URL: http:// Code

○ Advanced

Welcome Slogan	
Page Background	● None ○ Background Color FFFFFF View Color Grid
Article	
Article Text Color	000000 View Color Grid
Article Background Color	● None ○ FFFFFF View Color Grid
Information	
Comments	

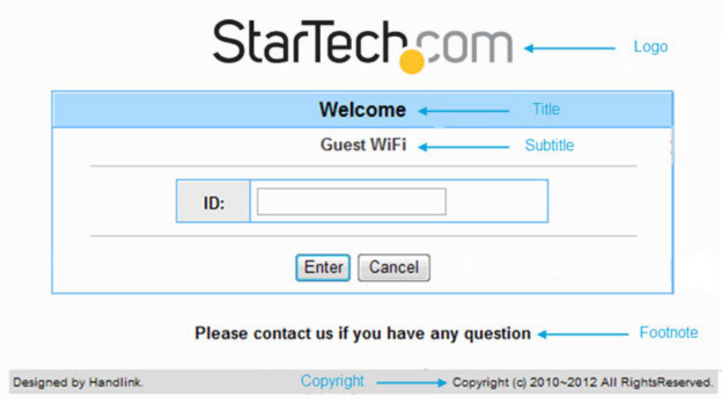
○ Frame

Top Frame	URL: http://
Bottom Frame	This frame will show the standard login page

Standard

Item	Default	Description
Logo	Disable	Select the check box to display the logo file specified on the **Logo** tab. **Note:** You will receive an error message if no logo has been specified.
Title	Welcome	Enter a page title for the top of the login box (Max 80 characters).
Subtitle	Guest Wifi	Enter the subtitle name of subscriber login page (Max 80 characters).
Footnote	Diable	Enter a footnote if desired e.g. "Please contact Customer Service, EXT 1000 for assistance" (Max 240 characters).
Copywrite	Enable	Enter a copyright note for the bottom of the login page (Max 80 characters).
Background Colour	FFFFFF	Enter your desired background color in Hexadecimal.

- *Sample Standard Page*


Welcome

Guest WiFi

ID:

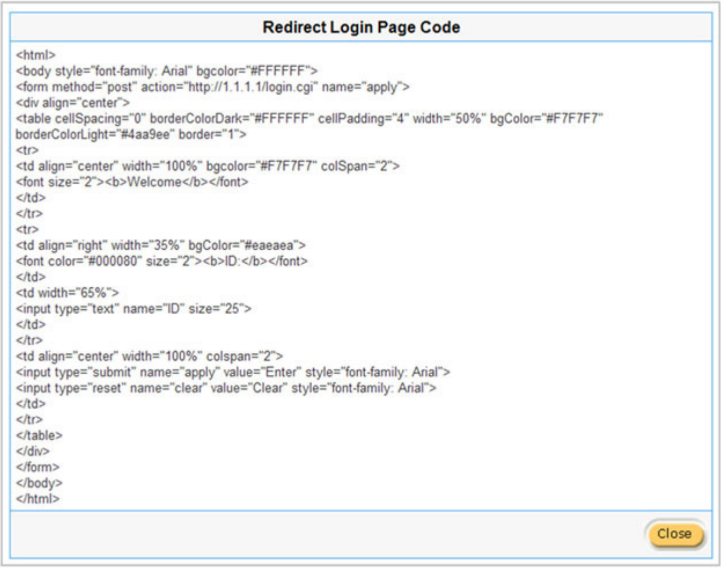
Please contact us if you have any question

Designed by Handlink.

Copyright (c) 2010~2012 All RightsReserved.

Redirect

Item	Default	Description
Redirect	Disable	Enter the URL where your login page is located (Max 200 characters), or click the button to create your own (sample code below).



Redirect Login Page Code

```
<html>
<body style="font-family: Arial" bgcolor="#FFFFFF">
<form method="post" action="http://1.1.1.1/login.cgi" name="apply">
<div align="center">
<table cellSpacing="0" borderColorDark="#FFFFFF" cellPadding="4" width="50%" bgColor="#F7F7F7"
borderColorLight="#4aa9ee" border="1">
<tr>
<td align="center" width="100%" bgcolor="#F7F7F7" colSpan="2">
<font size="2"><b>Welcome</b></font>
</td>
</tr>
<tr>
<td align="right" width="35%" bgColor="#eaeaea">
<font color="#000080" size="2"><b>ID:</b></font>
</td>
<td width="65%">
<input type="text" name="ID" size="25">
</td>
</tr>
<td align="center" width="100%" colspan="2">
<input type="submit" name="apply" value="Enter" style="font-family: Arial">
<input type="reset" name="clear" value="Clear" style="font-family: Arial">
</td>
</tr>
</table>
</div>
</form>
</body>
</html>
```

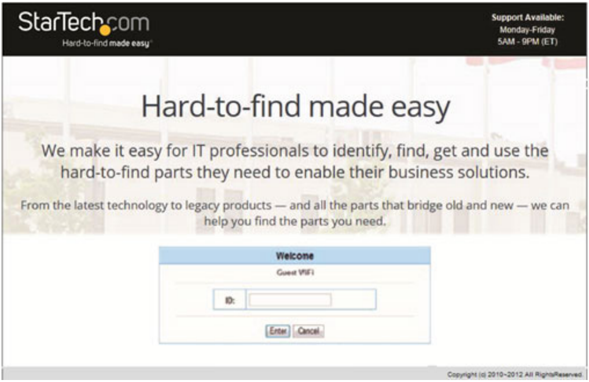
Advanced

Item	Default	Description
Welcome Slogan	Welcome	Enter a Welcome slogan (Max 80 characters).
Page Background	None	Enter your desired page background color in Hexadecimal.
Article	Empty	Enter a paragraph for advisement or announcements (Max 1024 characters).
Article Text Colour	000000	Enter your desired text color in Hexadecimal.
Article Background Color	None	Enter your desired article background color in Hexadecimal.
Information	Empty	Enter desired information such as address, telephone number and fax (Max 80 characters).
Coments	Empty	Enter a footnote comment if desired e.g. "Please contact Customer Service, EXT 1000 for assistance" (Max 240 characters).

Frame

Item	Default	Description
Top Frame URL Link	Empty	Enter the URL where your top frame content is located (Max 200 characters).
Bottom Frame	–	This frame will show the standard login page.

- *Sample Framed Page*



StarTech.com
Hard-to-find made easy

Support Available:
Monday-Friday
5AM - 9PM (ET)

Hard-to-find made easy

We make it easy for IT professionals to identify, find, get and use the hard-to-find parts they need to enable their business solutions.

From the latest technology to legacy products — and all the parts that bridge old and new — we can help you find the parts you need.

Welcome

Guest WiFi

ID:

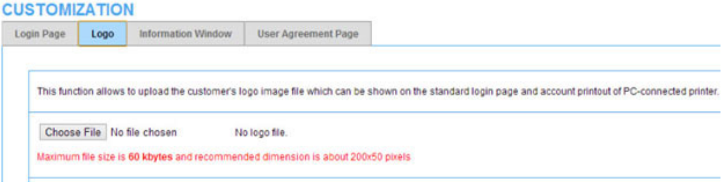
Copyright (c) 2010-2012 All RightsReserved.

Top Frame

Bottom Frame

Logo Tab

The Logo tab allows you to upload your company logo for use on the login page.



CUSTOMIZATION

This function allows to upload the customer's logo image file which can be shown on the standard login page and account printout of PC-connected printer.

No file chosen

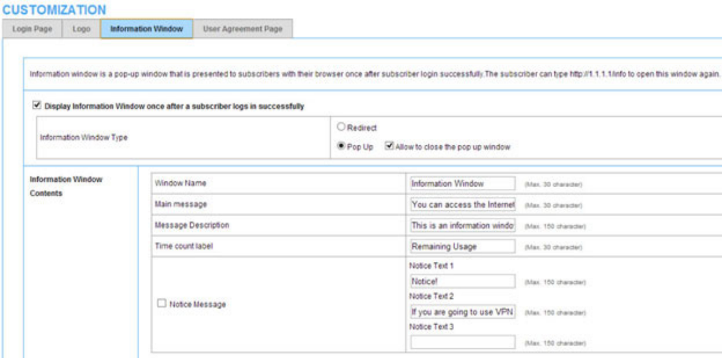
No logo file.

Maximum file size is **60 kbytes** and recommended dimension is about 200x50 pixels

Item	Default	Description
File Path	Empty	Click Choose File to select a file from your local PC

Information Window Tab

The Information Window tab allows you to create a customized message to new guests after they log in.



CUSTOMIZATION

Information window is a pop-up window that is presented to subscribers with their browser once after subscriber login successfully.The subscriber can type http://1.1.1.1/info to open this window again.

☑ Display Information Window once after a subscriber logs in successfully

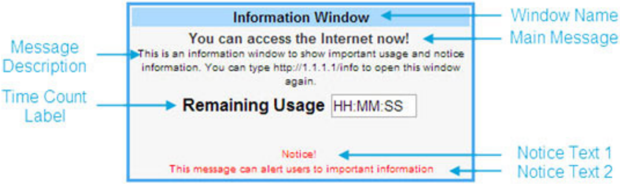
Information Window Type: ○ Redirect ● Pop Up ☑ Allow to close the pop up window

Information Window Contents

Window Name	Information Window	(Max. 30 character)
Main message	You can access the Internet	(Max. 30 character)
Message Description	This is an information windo	(Max. 150 character)
Time count label	Remaining Usage	(Max. 30 character)
□ Notice Message	Notice Text 1 Notice!	(Max. 150 character)
	Notice Text 2 If you are going to use VPN	(Max. 150 character)
	Notice Text 3	(Max. 150 character)

Item	Default	Description
Display Information Window after a subscriber logs in successfully	Enabled – Pop Up	**Redirect:** Displays the Information Window in the same tab that the user logs in from. **Pop Up:** Shows a pop up message when the user logs in.
Window Name	Information Window	Enter the window name to be shown in the title bar (Max 30 characters).
Main Message	You can access the Internet now!	Enter your main message / heading (Max 30 characters).
Message Description	This is an information...	Enter your desired message text to display (Max 150 characters).
Time Count Label	Remaining Usage	Enter your desired label for the usage counter (Max 30 characters).
Notice Message	Disabled	Enter notice text as desired, which will appear at the bottom of the Information Window in red (Max 150 characters per level 1-3).

- *Sample Information Window*



Information Window

You can access the Internet now!

This is an information window to show important usage and notice information. You can type http://1.1.1.1/info to open this window again.

Remaining Usage HH:MM:SS

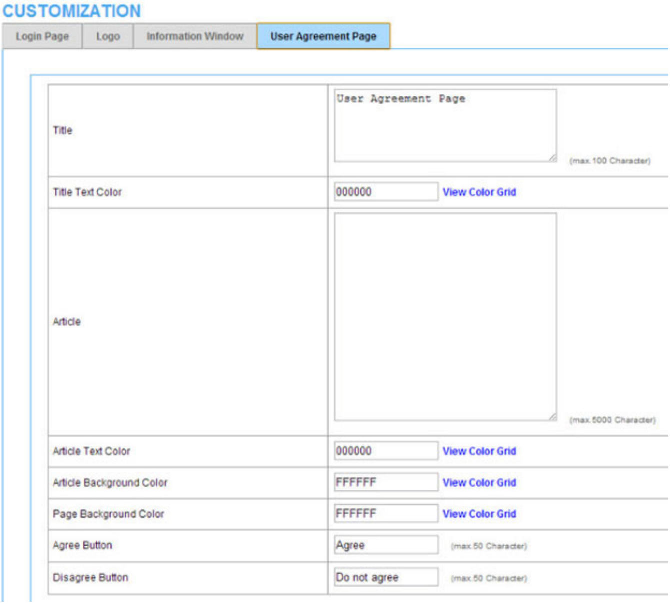
Notice!

This message can alert users to important information

User Agreement Tab

The User Agreement tab allows you to create a customized user agreement page for guest users.

Note: The User Agreement screen can be enabled under **Guest Settings** > **Authentication**



CUSTOMIZATION

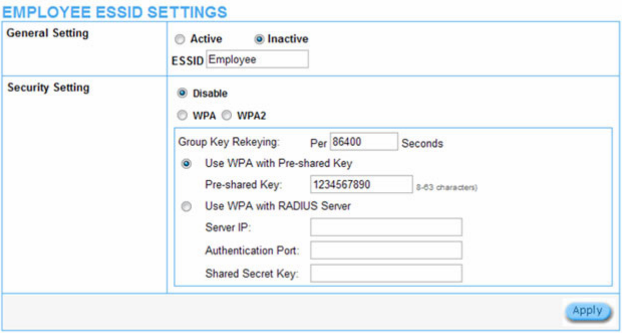
Title	User Agreement Page (max 100 Character)
Title Text Color	000000 View Color Grid
Article	(max 5000 Character)
Article Text Color	000000 View Color Grid
Article Background Color	FFFFFF View Color Grid
Page Background Color	FFFFFF View Color Grid
Agree Button	Agree (max 50 Character)
Disagree Button	Do not agree (max 50 Character)

Item	Default	Description
Title	User Agreement Page	Enter the window name to be shown in the title bar (Max 100 characters).
Title Text Colour	000000	Enter your desired title text color in Hexadecimal.
Article	Empty	The article is allowed the administrator to input a paragraph in the subscriber login page for advisement or announcement (Max 1024 characters).
Article Text Colour	000000	Enter your desired text color in Hexadecimal.
Article Background Color	FFFFFF	Enter your desired article background color in Hexadecimal.
Page Background Color	FFFFFF	Enter your desired page background color in Hexadecimal.
Agree Button	Agree	Enter the button text for the agree button (Max 50 characters).
Disagree Button	Disagree	Enter the button text for the disagree button (Max 50 characters).

Employee Setting

Employee ESSID Settings

The Employee ESSID Settings menu allows you to configure your employee wireless settings and security.



EMPLOYEE ESSID SETTINGS

General Setting: ○ Active ● Inactive

ESSID: Employee

Security Setting: ● Disable ○ WPA ○ WPA2

Group Key Rekeying: Per 86400 Seconds

● Use WPA with Pre-shared Key

Pre-shared Key: 1234567890 8-63 characters)

○ Use WPA with RADIUS Server

Server IP:

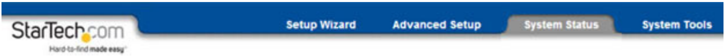
Authentication Port:

Shared Secret Key:

Item	Default	Description
General Settings	Active	Activate or de-activate the wireless connection interface.
ESSID	Employee	The ESSID is the unique name that is shared among all points in a wireless network. It is case sensitive and must not exceed 32 characters.
Security	Enable	Select disable to allow users to communicate with the device without any data encryption. Select enable to use WPA or WPA2 data encryption.
Group Key Re-Keying	86400 Seconds	Enter a number in seconds to set the force re-keying interval.
Pre-shared Key	Empty	The AP will randomly generate keys at the length specified here. (8-10 characters)
Use WPA with RADIUS	Disable	
Server IP	Empty	Enter the RADIUS server IP address or domain name (Max 15 characters).

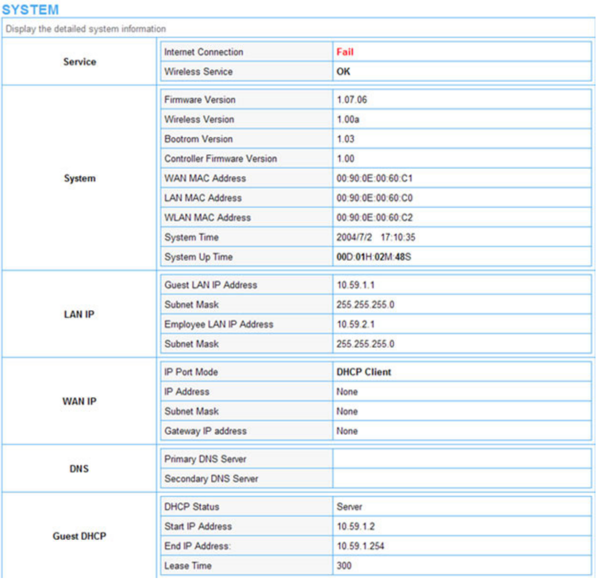
Authentication Port	1812	Enter the authentication port number from 0 to 65535.
Shared Secret Key	Empty	Enter the RADIUS key

System Status Menu



System Report

The System report displays current basic system information, including: service connection status, host name, LAN, WAN, DHCP Configuration, DNS, SSL Certificate, network traffic Information and the system firmware version number.



SYSTEM

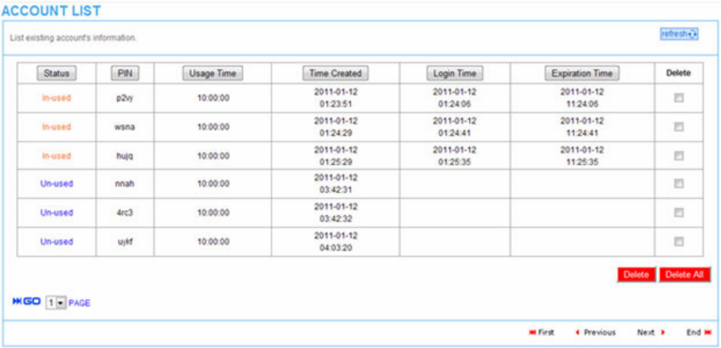
Display the detailed system information

Service	Internet Connection	Fail
	Wireless Service	OK
System	Firmware Version	1.07.06
	Wireless Version	1.00a
	Bootrom Version	1.03
	Controller Firmware Version	1.00
	WAN MAC Address	00:90:0E:00:60:C1
	LAN MAC Address	00:90:0E:00:60:C0
	WLAN MAC Address	00:90:0E:00:60:C2
	System Time	2004/7/2 17:10:35
	System Up Time	00D:01H:02M:48S
LAN IP	Guest LAN IP Address	10.59.1.1
	Subnet Mask	255.255.255.0
	Employee LAN IP Address	10.59.2.1
	Subnet Mask	255.255.255.0
WAN IP	IP Port Mode	DHCP Client
	IP Address	None
	Subnet Mask	None
	Gateway IP address	None
DNS	Primary DNS Server	
	Secondary DNS Server	
Guest DHCP	DHCP Status	Server
	Start IP Address	10.59.1.2
	End IP Address:	10.59.1.254
	Lease Time	300

Account List

The Account List displays all account information on this device, including: the status, PIN, usage time, time created, login time, expiration time and status.

This page will refresh automatically every 5 minutes, or you can click the **Refresh** button in the top right corner to update manually.



ACCOUNT LIST

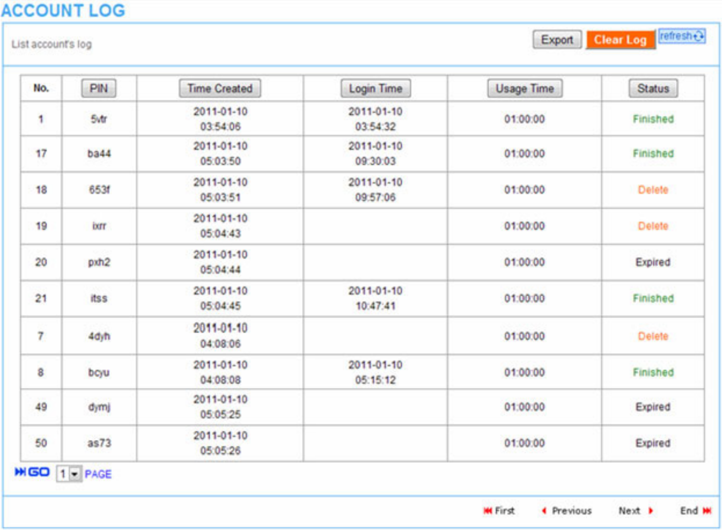
List existing account's information.

Status	PIN	Usage Time	Time Created	Login Time	Expiration Time	Delete
In-used	p2vy	10:00:00	2011-01-12 01:23:51	2011-01-12 01:24:06	2011-01-12 11:24:06	☐
In-used	wsna	10:00:00	2011-01-12 01:24:29	2011-01-12 01:24:41	2011-01-12 11:24:41	☐
In-used	hujq	10:00:00	2011-01-12 01:25:29	2011-01-12 01:25:35	2011-01-12 11:25:35	☐
Un-used	nnah	10:00:00	2011-01-12 03:42:31			☐
Un-used	4rc3	10:00:00	2011-01-12 03:42:32			☐
Un-used	uykf	10:00:00	2011-01-12 04:03:20			☐

- Click the **Delete** button to delete checked accounts
- Click **Delete All** to clear the list
- Click the column headings to change the sorting

Account Log

The Account Log displays account activity information.



ACCOUNT LOG

List account's log

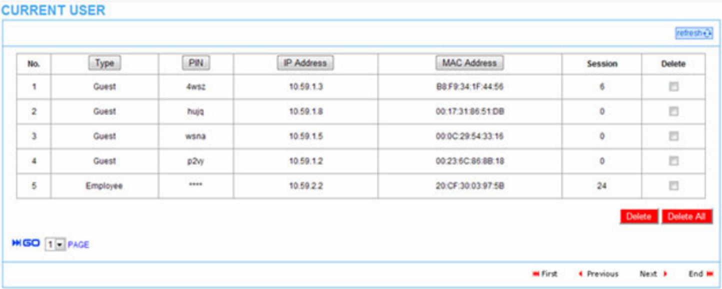
No.	PIN	Time Created	Login Time	Usage Time	Status
1	5vtr	2011-01-10 03:54:06	2011-01-10 03:54:32	01:00:00	Finished
17	ba44	2011-01-10 05:03:50	2011-01-10 09:30:03	01:00:00	Finished
18	653f	2011-01-10 05:03:51	2011-01-10 09:57:06	01:00:00	Delete
19	ixrr	2011-01-10 05:04:43		01:00:00	Delete
20	pxh2	2011-01-10 05:04:44		01:00:00	Expired
21	itss	2011-01-10 05:04:45	2011-01-10 10:47:41	01:00:00	Finished
7	4dyh	2011-01-10 04:08:06		01:00:00	Delete
8	bcyu	2011-01-10 04:08:08	2011-01-10 05:15:12	01:00:00	Finished
49	dymj	2011-01-10 05:05:25		01:00:00	Expired
50	as73	2011-01-10 05:05:26		01:00:00	Expired

- Click the **Export** button to export the contents of the log to a text file (filename: export.log)
- Click **Clear Log** to empty the log contents
- Click the column headings to change the sorting

Current User Report

The Current User report displays currently logged-in user status and allows the administrator to disconnect users if needed.

This page will refresh automatically every 5 minutes, or you can click the Refresh button in the top right corner to update manually.



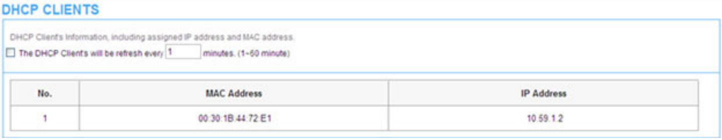
CURRENT USER

No.	Type	PIN	IP Address	MAC Address	Session	Delete
1	Guest	4wsz	10.59.1.3	B8:F9:34:1F:44:56	6	□
2	Guest	hujq	10.59.1.8	00:17:31:86:51:DB	0	□
3	Guest	wsna	10.59.1.5	00:0C:29:54:33:16	0	□
4	Guest	p2vy	10.59.1.2	00:23:6C:86:8B:18	0	□
5	Employee	****	10.59.2.2	20:CF:30:03:97:5B	24	□

- Click **Delete** to disconnect the checked users
- Click **Delete All** to disconnect all current users
- Click the column headings to change the sorting

DHCP Clients Report

The DHCP Clients report displays the current DHCP addressing table.



DHCP CLIENTS

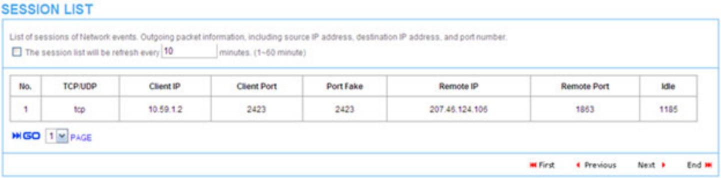
DHCP Client's Information, including assigned IP address and MAC address.

□ The DHCP Client's will be refresh every 1 minutes. (1~60 minute)

No.	MAC Address	IP Address
1	00:30:1B:44:72:E1	10.59.1.2

Session List

The Session List displays the real-time session usage information for the AP.



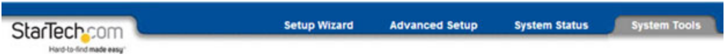
SESSION LIST

List of sessions of Network events. Outgoing packet information, including source IP address, destination IP address, and port number.

□ The session list will be refresh every 10 minutes. (1~60 minute)

No.	TCP/UDP	Client IP	Client Port	Port Fake	Remote IP	Remote Port	Idle
1	tcp	10.59.1.2	2423	2423	207.46.124.106	1863	1185

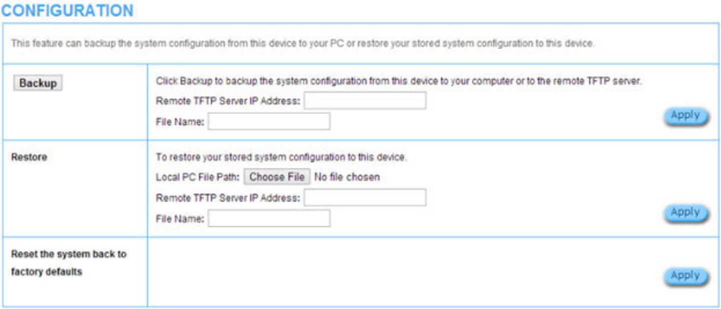
System Tools Menu



The System Tools Menu allows you to upgrade Firmware, change passwords and backup or restore configuration files.

Configuration

The Configuration menu allows you to backup or restore the configuration settings for the device.



CONFIGURATION

This feature can backup the system configuration from this device to your PC or restore your stored system configuration to this device.

Backup	Click Backup to backup the system configuration from this device to your computer or to the remote TFTP server. Remote TFTP Server IP Address: File Name: Apply
Restore	To restore your stored system configuration to this device. Local PC File Path: Choose File No file chosen Remote TFTP Server IP Address: File Name: Apply
Reset the system back to factory defaults	Apply

Item	Default	Description
Backup	-	Click the button to save the system configuration to a file computer. (export.cfg)
Remote TFTP Server IP Address	Empty	Enter the IP address of the TFTP Server.
File Name	Empty	Enter your desired file name.
Restore		
Local PC File Path	Empty	Click Choose File to select a file from your local PC
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.
Reset the system back to factory defaults	-	Click Apply and confirm to erase all configuration settings and revert back to factory default.

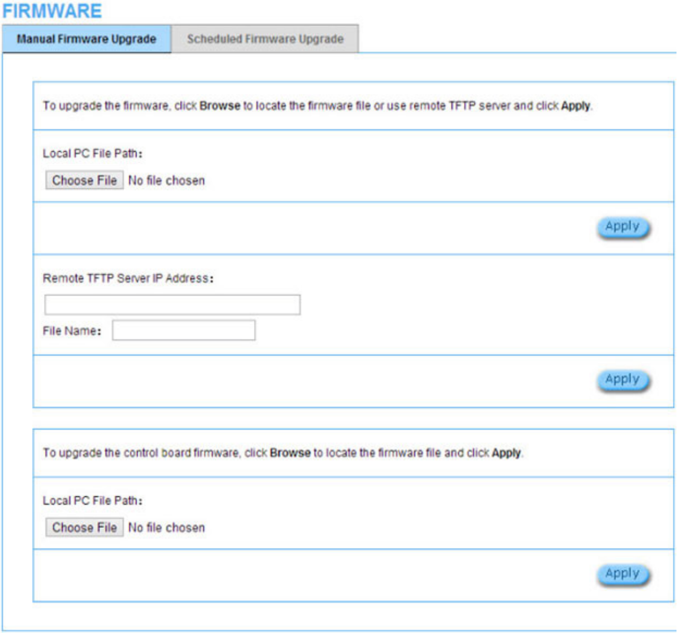
Firmware Upgrade

The Firmware Upgrade menu lets you upload a new firmware file manually or as a scheduled task.

Note: Do not power off the device during the firmware upgrade process to avoid damage to the unit.

Manual Firmware Upgrade Tab

The Manual Firmware Upgrade tab allows you to specify a local file or a TFTP address to update the firmware.



FIRMWARE

To upgrade the firmware, click **Browse** to locate the firmware file or use remote TFTP server and click **Apply**.

Local PC File Path:

Remote TFTP Server IP Address:

File Name:

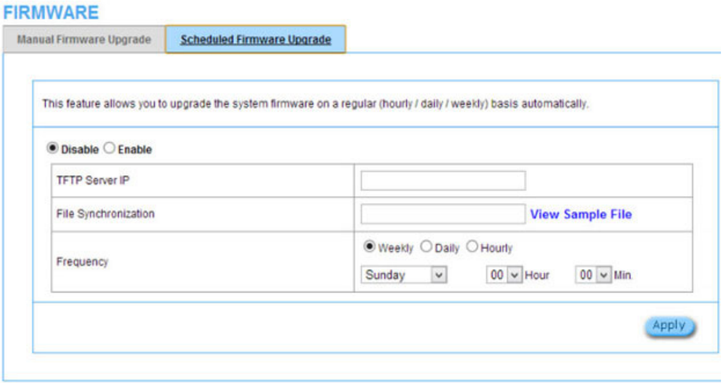
To upgrade the control board firmware, click **Browse** to locate the firmware file and click **Apply**.

Local PC File Path:

Item	Default	Description
Local PC File Path	-	Click Choose File to select a file from your local PC
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.
Control board firmware	-	Click Choose File to select a file from your local PC

Scheduled Firmware Upgrade Tab

The Scheduled Firmware Upgrade tab allows you to specify a file location and frequency for automated firmware upgrades.



FIRMWARE

Manual Firmware Upgrade | Scheduled Firmware Upgrade

This feature allows you to upgrade the system firmware on a regular (hourly / daily / weekly) basis automatically.

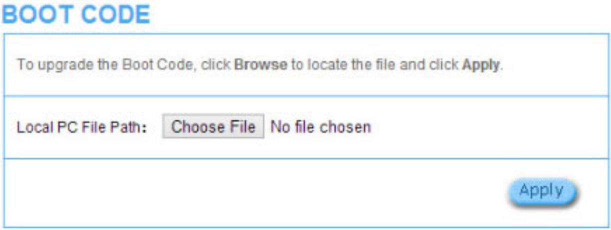
● Disable ○ Enable

TFTP Server IP	
File Synchronization	View Sample File
Frequency	● Weekly ○ Daily ○ Hourly Sunday 00 Hour 00 Min

Item	Default	Description
Disable/Enable	Disable	Disables or enables the scheduled firmware upgrade function.
TFTP Server IP	Empty	Enter the IP address of the TFTP Server.
File Synchronization	Empty	Enter the file name and location in the File Synchronization field.
View Sample File	-	Click the button to display synchronization file example.
Frequency	Weekly	Set the firmware upgrade frequency.

Boot Code

The Boot Code menu allows you to upload a new boot code file should an update become available.



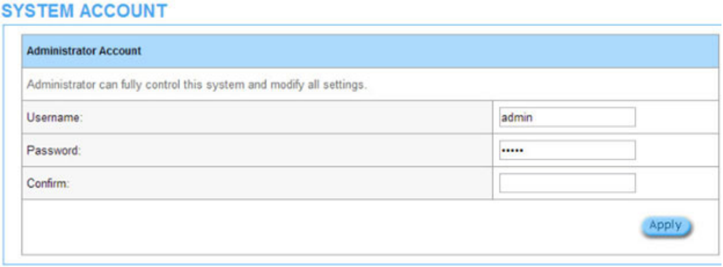
BOOT CODE

To upgrade the Boot Code, click **Browse** to locate the file and click **Apply**.

Local PC File Path: Choose File No file chosen

System Account

The System Account menu allows you to change the administration account for the device.



SYSTEM ACCOUNT

Administrator Account

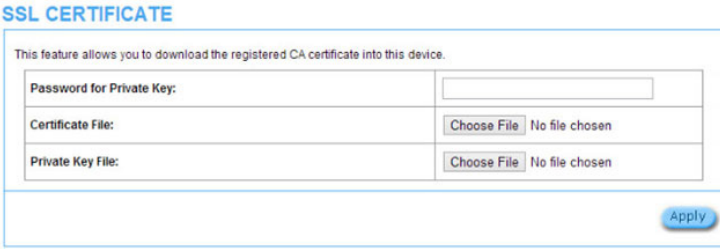
Administrator can fully control this system and modify all settings.

Username:	admin
Password:	•••••
Confirm:	

Item	Description
Username	Enter a username up to 20, case-sensitive alphanumeric characters.
Password	Enter a password up to 20, case-sensitive alphanumeric characters.
Confirm	Re-enter the same password to confirm.

SSL Certificate

The SSL Certificate menu allows you to add your certificate files to the device.



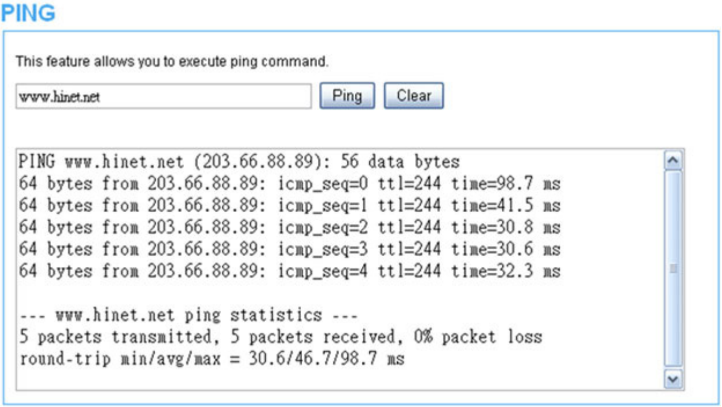
SSL CERTIFICATE

This feature allows you to download the registered CA certificate into this device.

Password for Private Key:	
Certificate File:	Choose File No file chosen
Private Key File:	Choose File No file chosen

PING

The PING menu will issue the ping command to your specified IP address or URL.



PING

This feature allows you to execute ping command.

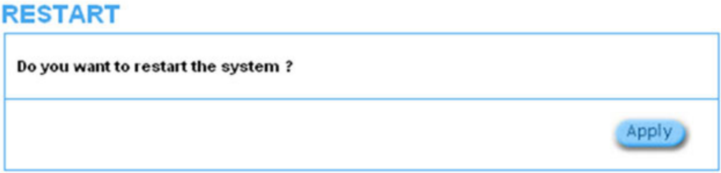
www.hinet.net

```
PING www.hinet.net (203.66.88.89): 56 data bytes
64 bytes from 203.66.88.89: icmp_seq=0 ttl=244 time=98.7 ms
64 bytes from 203.66.88.89: icmp_seq=1 ttl=244 time=41.5 ms
64 bytes from 203.66.88.89: icmp_seq=2 ttl=244 time=30.8 ms
64 bytes from 203.66.88.89: icmp_seq=3 ttl=244 time=30.6 ms
64 bytes from 203.66.88.89: icmp_seq=4 ttl=244 time=32.3 ms

--- www.hinet.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 30.6/46.7/98.7 ms
```

Item	Description
IP or URL	Enter the IP address or the URL link.

Restart

The Restart menu will reboot the device.

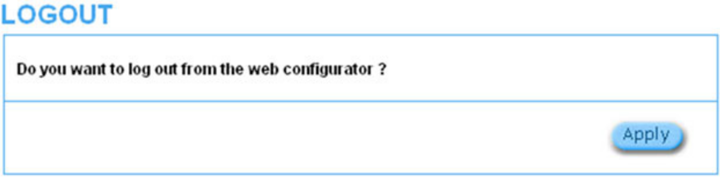


RESTART

Do you want to restart the system ?

Logout

The Logout menu will exit from the configuration screen.



LOGOUT

Do you want to log out from the web configurator ?

Specifications

Supported Wireless Standards	IEEE802.11b/g/n
Chipset	Ralink – RT3052
Connectors	5 x RJ45 Ethernet Female
Antenna Configuration	2x2:2 (TxR:s)
Wireless Frequency Range	2.400 – 2.484
Wireless Bandwidth	20/40MHz

Wireless Encryption Supported	WPA(TKIP with IEEE 802.1x)
	WPA2(AES with IEEE 802.1x)
	WPA -PSK

Maximum Wireless Distance	30m
Maximum Data Transfer Rate	300Mbps (Wireless-N) 10/100 Mbps (RJ45 Ethernet)
Enclosure Material	Plastic
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-10°C to 60°C (14°F to 140°F)
Humidity	20~90% Non-Condensing
Dimensions	223 x 143 x 36 mm

Technical Support

StarTech.com's lifetime technical support is an integral part of our commitment to provide industry-leading solutions. If you ever need help with your product, visit **www.startech.com/support** and access our comprehensive selection of online tools, documentation, and downloads.

For the latest drivers/software, please visit **www.startech.com/downloads**

Warranty Information

This product is backed by a two year warranty.

In addition, StarTech.com warrants its products against defects in materials and workmanship for the periods noted, following the initial date of purchase. During this period, the products may be returned for repair, or replacement with equivalent products at our discretion. The warranty covers parts and labor costs only. StarTech.com does not warrant its products from defects or damages arising from misuse, abuse, alteration, or normal wear and tear.

Limitation of Liability

In no event shall the liability of StarTech.com Ltd. and StarTech.com USA LLP (or their officers, directors, employees or agents) for any damages (whether direct or indirect, special, punitive, incidental, consequential, or otherwise), loss of profits, loss of business, or any pecuniary loss, arising out of or related to the use of the product exceed the actual price paid for the product. Some states do not allow the exclusion or limitation of incidental or consequential damages. If such laws apply, the limitations or exclusions contained in this statement may not apply to you.

StarTech.com

Hard-to-find made easy®

Hard-to-find made easy. At StarTech.com, that isn't a slogan. It's a promise.

StarTech.com is your one-stop source for every connectivity part you need. From the latest technology to legacy products — and all the parts that bridge the old and new — we can help you find the parts that connect your solutions.

We make it easy to locate the parts, and we quickly deliver them wherever they need to go. Just talk to one of our tech advisors or visit our website. You'll be connected to the products you need in no time.

Visit www.startech.com for complete information on all StarTech.com products and to access exclusive resources and time-saving tools.

StarTech.com is an ISO 9001 Registered manufacturer of connectivity and technology parts. StarTech.com was founded in 1985 and has operations in the United States, Canada, the United Kingdom and Taiwan servicing a worldwide market.