

BILLIONTM

BiGuard *S10*

SSL VPN Security Gateway



Administration Guide

Version Release: v101_08302006

Powering communications
with Security

Declaration of Conformity

Konformitätserklärung

in accordance with the **Radio and Telecommunications Terminal Equipment Act (FTEG)**
and **Directive 1999/5/EC (R&TTE Directive)**
gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG)
und der Richtlinie 1999/5/EG (R&TTE)

The Manufacturer: *Billion Electric Co., Ltd.*
Hersteller:
*8F, No. 192, Sec. 2, Chung Hsing Rd.,
Hsin Tien City, Taipei Hsien
Taiwan*

declares that the product: *BiGuard S10*
erklärt, dass das Produkt:
*Telecommunications terminal equipment
Telekommunikations(Tk-)endeinrichtung*

Intended purpose: *SSL VPN Security Gateway*

Verwendungszweck:

complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.

Harmonised standards: Health and Safety requirements contained in §3 (1) 1. (Article 3 (1) a))
Harmonisierte Normen: Gesundheit und Sicherheit gemäß §3 (1) 1. (Artikel 3 (1) a))

EN 60950-1: 2001+A11

Harmonised standards: Protection requirements with respect to EMC §3 (1) 2, (Article 3 (1) b))
Harmonisierte Normen: Schutzanforderungen in Bezug auf die EMV §3 (1) 2, Artikel 3 (1) b))

EN 55022: 1998+A1: 2000+A2: 2003 Class B, EN 61000-3-2: 2000+A2: 2005

EN 61000-3-3: 1995+A1: 2001, EN 55024: 1998+A1: 2001+A2: 2003

IEC 61000-4-2: 1995+A1: 1998+A2: 2000, IEC 61000-4-3: 1995+A1: 1998+A2: 2000

IEC 61000-4-4: 2004, IEC 61000-4-5: 1995+A1: 2000,

IEC 61000-4-6: 1996+A1: 2000, IEC 61000-4-8: 1993+A1: 2000, IEC 61000-4-11: 2004

This declaration is issued by:

Diese Erklärung wird verantwortlich abgegeben durch:

Mettmann
(Place)

03. Aug. 2006
(Date)

Gary Lin

President

Power Partnership GmbH


Power Partnership GmbH
Mozartstraße 78
40822 Mettmann - Germany
Tel. +49 (2104) 801005-Fax 801006

Copyright Information

© 2006 Billion Electric Corporation, Ltd.

The contents of this publication may not be reproduced in whole or in part, transcribed, stored, translated, or transmitted in any form or any means, without the prior written consent of Billion Electric Corporation.

Published by Billion Electric Corporation. All rights reserved.

Version 1.0, September 2006

Disclaimer

Billion does not assume any liability arising out of the application of use of any products or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Billion reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Mac OS is a registered trademark of Apple Computer, Inc.

Windows 98, Windows NT, Windows 2000, Windows Me and Windows XP are registered trademarks of Microsoft Corporation.

FCC Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

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 commercial environment.

If this equipment does cause harmful interference to radio/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 the 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.

Notice:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Safety Information

The BiGuard S10 is built for reliability and long service life. For your safety, be sure to read and follow the following safety warnings.

Read this installation guide thoroughly before attempting to set up the BiGuard S10.

- The BiGuard S10 is a complex electronic device. DO NOT open or attempt to repair it yourself. Opening or removing the covers can expose you to high voltage and other risks. In the case of malfunction, turn off the power immediately and have it repaired at a qualified service center. Contact your vendor for details.
- Connect the power cord to the correct supply voltage.
- Carefully place connecting cables to avoid people from stepping or tripping on them. DO NOT allow anything to rest on the power cord and DO NOT place the power cord in an area where it can be stepped on.
- DO NOT use the BiGuard S10 in environments with high humidity or high temperatures.
- DO NOT use the same power source for the BiGuard S10 as other equipment.
- DO NOT use the BiGuard S10 and any accessories outdoors.
- If you wall mount the BiGuard S10, make sure that no electrical, water or gas pipes will be damaged during installation.
- DO NOT install or use the BiGuard S10 during a thunderstorm.
- DO NOT expose the BiGuard S10 to dampness, dust, or corrosive liquids.
- DO NOT use the BiGuard S10 near water.
- Be sure to connect the cables to the correct ports.
- DO NOT obstruct the ventilation slots on the BiGuard S10 or expose it to direct sunlight or other heat sources. Excessive temperatures may damage your device.
- DO NOT store anything on top of the BiGuard S10.
- Only connect suitable accessories to the BiGuard S10.
- Keep packaging out of the reach of children.
- If disposing of the device, please follow your local regulations for the safe disposal of electronic products to protect the environment.

Table of Contents

Getting Started

| | |
|-----------------------------------------------------------------------------|----|
| About this guide | 1 |
| Unpacking the BiGuard S10 | 2 |
| Front and rear view of the BiGuard S10 | 3 |
| Setting up the BiGuard S10 | 3 |
| Rackmounting the BiGuard S10 | 4 |
| Connecting to a WAN | 4 |
| Connecting to a LAN | 5 |
| Connecting power | 6 |
| Turning on the power and checking LED status | 6 |
| Network deployment/applications | 6 |
| Network environment scenarios | 6 |
| <i>All in one solution: firewall, remote and Internet access</i> | 6 |
| <i>Installing behind a gateway/firewall</i> | 8 |
| <i>Fitting into a DMZ zone behind an existing firewall router</i> | 8 |
| <i>All in one: public servers on DMZ zone, private servers on LAN</i> | 9 |
| SSL VPN Applications | 10 |
| <i>Network Extender</i> | 10 |
| <i>Transport Extender</i> | 10 |
| <i>Network Places</i> | 11 |
| <i>Application Proxy</i> | 11 |
| SSL VPN Features | 11 |
| <i>Granular Access Control</i> | 12 |
| <i>SSL VPN Certification</i> | 13 |
| <i>SSL VPN Portals</i> | 14 |
| <i>Authentication Domain Scenarios</i> | 15 |
| Firewall Settings | 16 |
| Intrusion detection | 16 |
| Block WAN request | 16 |
| WAN settings | 16 |
| Static IP | 16 |
| PPPoE | 16 |
| DHCP | 16 |

Administration Guide

| | |
|------------------------------------------------------------|----|
| Basic Configuration with the Quick Start Menu | 17 |
| Logging in to the BiGuard S10 Web Manager | 17 |
| Navigating in the Web Manager | 21 |
| Quick start to configuring the WAN | 22 |
| <i>Configuring the WAN for Static IP</i> | 22 |
| <i>Configuring the WAN for PPPoE</i> | 22 |
| <i>Configuring the WAN for DHCP</i> | 23 |
| Quick start to configuring SSL VPN | 24 |
| Monitoring Configuration Status | 25 |
| Status submenus | 25 |
| <i>Changing the device name</i> | 27 |
| <i>Changing time and time zone parameters</i> | 28 |

| | |
|----------------------------------------------------------------|-----------|
| Changing the default LAN IP address | 29 |
| DHCP server settings | 29 |
| SSL User Status | 32 |
| ARP Table | 32 |
| Routing Table | 33 |
| DHCP Table | 33 |
| System Log | 34 |
| SSL VPN Log | 35 |
| Configuring the BiGuard S10 | 36 |
| Configuring the Interface | 36 |
| Configuring the LAN | 36 |
| Configuring WAN settings | 39 |
| Configuring the DMZ | 43 |
| Configuring Network Objects | 44 |
| Configuring IP address Network Objects | 44 |
| Creating Address Groups Network Objects | 45 |
| Allowing Services | 46 |
| Creating Service Group Network Objects | 47 |
| Scheduling BiGuard S10 operation | 48 |
| Managing Bandwidth Network Objects | 49 |
| Setting Content Blocking parameters | 50 |
| Setting Policy parameters | 53 |
| Enabling Packet Filtering | 53 |
| Configuring the Virtual Server | 54 |
| Configuring Quality of Service (QoS) parameters | 55 |
| Configuring Ethernet MAC Filtering | 56 |
| Configuring Content Filtering policies | 57 |
| Configuring the System | 59 |
| Setting the Time Zone | 59 |
| Enabling Remote Access | 60 |
| Upgrading the BiGuard S10 Firmware | 60 |
| Backing up and restoring configurations | 61 |
| Configuring and changing passwords | 63 |
| Restarting the system | 63 |
| Configuring Advanced Features | 64 |
| Creating Static Routes | 64 |
| Enabling Dynamic DNS | 65 |
| Configuring SNMP | 66 |
| Configuring Firewall Parameters | 67 |
| Managing Device Parameters | 67 |
| Configuring SSL VPN Parameters | 68 |
| Configuring User Access menus | 68 |
| Portal Layout | 68 |
| Authentication Domain | 68 |
| Group/Application | 71 |
| SSL VPN Applications Overview | 72 |
| Managing accounts | 74 |
| Managing Network Extender IP address and client routes | 77 |
| Modifying the Network Extender IP address range | 77 |
| Creating client routes | 77 |
| Managing Transporter Extender application and host names | 78 |
| Adding a tunneled Transport Extender application | 78 |
| Configuring host names for Transport Extender | 78 |

| | |
|------------------------------------------------|----|
| Managing SSL Certification | 79 |
| <i>Importing a certificate</i> | 79 |
| SSL VPN Portal | 83 |
| <i>Using SSL VPN Portal Access</i> | 83 |
| <i>Installing the Network Extender</i> | 84 |
| <i>Installing the Transport Extender</i> | 86 |
| <i>Accessing Network Place</i> | 87 |
| <i>Using Applications</i> | 87 |
| Log and E-mail Alerts | 92 |
| <i>Log Configuration</i> | 92 |
| <i>Syslog Server</i> | 93 |
| <i>E-mail Alert Notification</i> | 94 |
| Save Configuration to flash | 94 |

Troubleshooting

| | |
|---------------------------------------------------------|-----|
| Before you begin | 95 |
| Network settings | 95 |
| <i>Determining the type of IP network address</i> | 95 |
| Hardware problems | 96 |
| LAN interface problems | 97 |
| <i>Disabling pop-up windows</i> | 98 |
| <i>JavaScripts</i> | 98 |
| <i>Java permissions</i> | 99 |
| WAN interface problems | 99 |
| Internet service provider problems | 100 |
| Recovery | 101 |
| Troubleshooting sequence | 101 |

BiGuard S10 FAQ

| | |
|-----------------------------------------------------|-----|
| DMZ | 107 |
| Firewall | 108 |
| Remote Access | 130 |
| SNMP | 132 |
| SSL Knowledge | 133 |
| SSL Applications | 134 |
| Adding an application proxy | 135 |
| Using Network Extender | 138 |
| Using Transport Extender | 142 |
| Importing a certificate | 146 |
| Registering the BiGuard S10 | 150 |
| Configuring an Active Directory server | 151 |

Networking Basics

| | |
|------------------------------------------------|-----|
| IP Addresses | 161 |
| Net Mask | 161 |
| Subnet Addressing | 161 |
| Private IP Addresses | 162 |
| Network Address Translation (NAT) | 162 |

| | |
|---------------------------------------------------------|-----|
| Dynamic Host Configuration Protocol (DHCP) | 162 |
| Router Basics | 162 |
| What is a Router? | 162 |
| Why use a Router? | 163 |
| Routing Information Protocol (RIP) | 163 |
| Firewall Basics | 163 |
| What is a Firewall? | 163 |
| Stateful Packet Inspection | 163 |
| Denial of Service (DoS) Attack | 163 |
| Why Use a Firewall? | 164 |
| | |
| Specifications | |
| SSL VPN | 165 |
| Access Connection | 165 |
| Application & Management | 165 |
| Compatible Web Browsers | 165 |
| Security | 165 |
| Firewall & Content Filter | 166 |
| Web-Based Management | 166 |
| Quality of Service Control | 166 |
| Logging and Monitoring | 166 |
| Network Protocols and features | 166 |
| Hardware Specification | 167 |
| Physical Interface | 167 |
| Physical Specification | 167 |
| Power Requirement | 167 |
| Operating Environment | 167 |
| | |
| Glossary | |
| | |
| Warranty | |
| Limited Warranty | 173 |

Table of figures

| | | |
|------------------|----------------------------------------------------------------------|----|
| FIGURE 1 | BiGuard S10 front and rear views | 3 |
| FIGURE 2 | Connecting the BiGuard S10 to a WAN | 5 |
| FIGURE 3 | Connecting the BiGuard S10 to a LAN | 5 |
| FIGURE 4 | Connecting the power adapter | 6 |
| FIGURE 5 | All in one solution: firewall, remote and Internet access | 7 |
| FIGURE 6 | Behind a gateway/firewall | 8 |
| FIGURE 7 | Fitting into a DMZ zone behind an existing firewall router | 8 |
| FIGURE 8 | All in one: public servers on DMZ zone, private servers on LAN | 9 |
| FIGURE 9 | Network Extender | 10 |
| FIGURE 10 | Transport Extender | 10 |
| FIGURE 11 | Network Places | 11 |
| FIGURE 12 | Application Proxy | 11 |
| FIGURE 13 | Granular Access Control | 12 |
| FIGURE 14 | SSL VPN Certification | 13 |
| FIGURE 15 | SSL VPN Portals | 14 |
| FIGURE 16 | Authentication Domains - local user database | 15 |
| FIGURE 17 | Authentication Domain - remote authentication | 15 |
| FIGURE 18 | Web Manager main screen overview | 21 |
| FIGURE 19 | Monitoring Status screen items | 25 |
| FIGURE 20 | Device Management screen | 27 |
| FIGURE 21 | Time Zone screen | 28 |
| FIGURE 22 | Ethernet screen | 29 |
| FIGURE 23 | DHCP status screen | 29 |
| FIGURE 24 | Mapping MAC address to fixed IP address screen | 30 |
| FIGURE 25 | SSL User Status screen | 32 |
| FIGURE 26 | ARP Table screen | 32 |
| FIGURE 27 | Routing Table screen | 33 |
| FIGURE 28 | DHCP Table screen | 33 |
| FIGURE 29 | System Log screen | 34 |
| FIGURE 30 | SSL VPN Log screen | 35 |
| FIGURE 31 | LAN screen | 36 |
| FIGURE 32 | DHCP status screen | 37 |
| FIGURE 33 | DHCP Server configuration screen | 38 |
| FIGURE 34 | WAN Settings PPPoE screen | 39 |
| FIGURE 35 | WAN Settings Static IP screen | 41 |
| FIGURE 36 | WAN Settings DHCP screen | 42 |
| FIGURE 37 | Setting WAN bandwidth | 43 |
| FIGURE 38 | Enabling the DMZ | 43 |
| FIGURE 39 | Configuring Network Object Addresses | 44 |
| FIGURE 40 | Adding Addresses to the Address Table | 44 |
| FIGURE 41 | Address Group list | 45 |
| FIGURE 42 | Creating an Address Group | 45 |
| FIGURE 43 | Pre-defined and User-defined Service Table | 46 |
| FIGURE 44 | Adding services to the Service Table | 46 |

| | | |
|------------------|------------------------------------------------------------|----|
| FIGURE 45 | The Service Group Table | 47 |
| FIGURE 46 | Schedule table list | 48 |
| FIGURE 47 | Creating a new Schedule Network Object | 48 |
| FIGURE 48 | Bandwidth Control Table | 49 |
| FIGURE 49 | Adding a Bandwidth Control Network Object | 49 |
| FIGURE 50 | Keyword Filter profiles | 50 |
| FIGURE 51 | Adding a keyword filter Network Object profile | 50 |
| FIGURE 52 | Domain Filter profiles | 50 |
| FIGURE 53 | Adding a domain filter Network Object profile | 51 |
| FIGURE 54 | Restrict URL Features Network Object list | 52 |
| FIGURE 55 | Restricting URL features | 52 |
| FIGURE 56 | Packet Filtering table | 53 |
| FIGURE 57 | Creating a Packet Filtering profile | 53 |
| FIGURE 58 | Virtual Server parameters | 54 |
| FIGURE 59 | Adding a Virtual Server | 54 |
| FIGURE 60 | QoS parameters | 55 |
| FIGURE 61 | Adding a QoS profile | 55 |
| FIGURE 62 | Ethernet MAC Filtering profiles | 56 |
| FIGURE 63 | Adding an Ethernet MAC filter | 56 |
| FIGURE 64 | Configuring Content Filtering Policies | 57 |
| FIGURE 65 | Creating a Content Filtering Profile | 58 |
| FIGURE 66 | Adding an IP Exception | 59 |
| FIGURE 67 | Setting the Time Zone | 59 |
| FIGURE 68 | Enabling Remote Access | 60 |
| FIGURE 69 | Upgrading the firmware | 60 |
| FIGURE 70 | Backing up and restoring configurations | 61 |
| FIGURE 71 | Backing up a configuration | 62 |
| FIGURE 72 | Restoring a configuration | 62 |
| FIGURE 73 | Changing passwords | 63 |
| FIGURE 74 | Restarting the system | 63 |
| FIGURE 75 | The Static Routing List | 64 |
| FIGURE 76 | Adding a static route | 64 |
| FIGURE 77 | Enabling DDNS | 65 |
| FIGURE 78 | Setting DDNS parameters | 65 |
| FIGURE 79 | Enabling SNMP | 66 |
| FIGURE 80 | Setting SNMP parameters | 66 |
| FIGURE 81 | Configuring the firewall | 67 |
| FIGURE 82 | Changing parameters | 67 |
| FIGURE 83 | Portal Layout | 68 |
| FIGURE 84 | Authentication Domain table | 68 |
| FIGURE 85 | Domain authentication types screen | 69 |
| FIGURE 86 | Group/Application table screen | 71 |
| FIGURE 87 | SSL VPN Application choices | 72 |
| FIGURE 88 | Account management screen | 74 |
| FIGURE 89 | Admin account settings screen | 74 |
| FIGURE 90 | Network Extender Client IP Address Assignment screen | 77 |

| | | |
|-------------------|-----------------------------------------------------------------|----|
| FIGURE 91 | Transport Extender configured applications screen | 78 |
| FIGURE 92 | Adding tunneled applications to Transport Extender screen | 78 |
| FIGURE 93 | Transport Extender configured host name resolution screen | 78 |
| FIGURE 94 | Transport Extender add host name resolution screen | 79 |
| FIGURE 95 | SSL Certificate current certificates screen | 79 |
| FIGURE 96 | SSL Certificate generate certificate screen | 79 |
| FIGURE 97 | Downloading the CSR | 80 |
| FIGURE 98 | Signing a certificate | 81 |
| FIGURE 99 | Opening the CSR | 81 |
| FIGURE 100 | SSL Certificate import certificates screen | 82 |
| FIGURE 101 | Current Certificates | 82 |
| FIGURE 102 | Inputting the CSR password | 82 |
| FIGURE 103 | New certificate | 82 |
| FIGURE 104 | Log Configuration screen | 92 |
| FIGURE 105 | Syslog Server screen | 93 |
| FIGURE 106 | E-mail Alert screen | 94 |
| FIGURE 107 | Save Config to Flash screen | 94 |

Getting Started

Welcome to the BiGuard S10 Administration Guide. This manual provides information on using the BiGuard S10 rackmountable device integrated with cutting-edge security technology including VPN and Firewall that enable you to connect your network to the Internet securely without the worry of intruder attacks.



NOTE: CHECK [HTTP://WWW.BIGUARD.COM/](http://www.biguard.com/) FOR THE LATEST VERSION OF THE *BiGuard S10 SERVICES DOCUMENTATION*.

About this guide

This manual describes how to install and operate the BiGuard S10. Please read this manual before you install the product.

This manual includes the following topics:

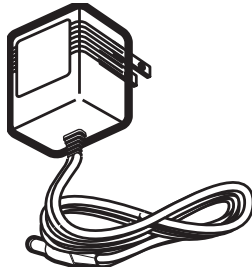
- Product description, features and specifications
- Hardware installation procedure
- Software configuration information
- Quick Setup instructions
- Technical Specifications
- Troubleshooting procedures
- Networking glossary



WARNING: BE SURE TO READ THE **SAFETY INFORMATION** ON PAGE III BEFORE INSTALLING THE **BiGuard S10**.

Unpacking the BiGuard S10

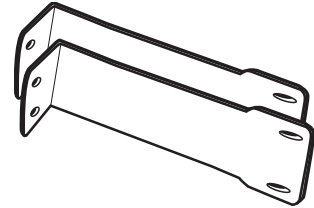
Unpack the BiGuard S10 and check that the following items are in the package:



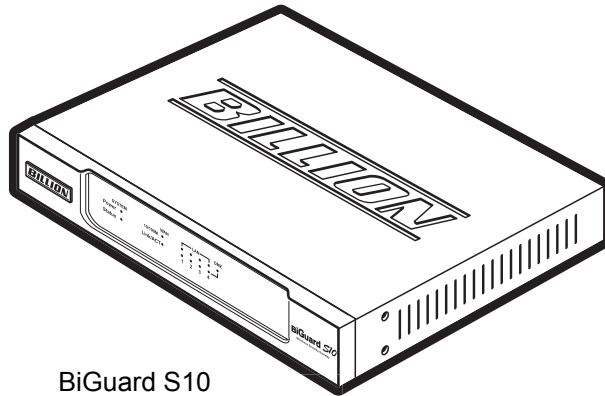
Power adapter



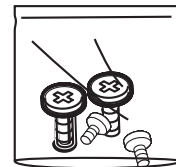
Warranty card x 1



Mounting brackets x 2



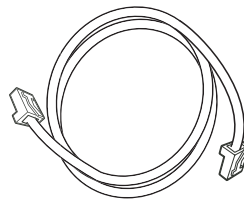
BiGuard S10



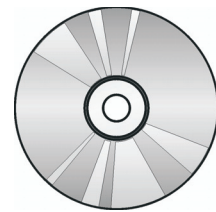
Mounting bracket screws x 4



Quick Start Guide x 1



Ethernet cable x 1



Software CD x 1

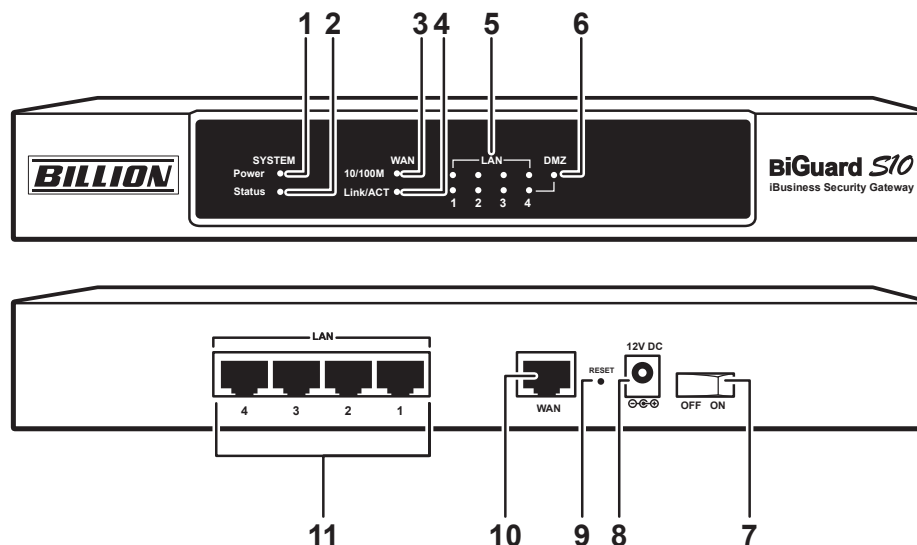


NOTE: If any item is missing or appears damaged, repack the BiGuard S10 and return it to your reseller.

Front and rear view of the BiGuard S10

Figure 1 shows the front and rear components on the BiGuard S10.

FIGURE 1 BiGUARD S10 FRONT AND REAR VIEWS



- | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> 1. Power LED On: Power is turned on 2. Status LED Blinking: Device is in use 3. WAN 10/100 LED Green: Connected at 100 Mbps Off: Connected at 10 Mbps 4. LINK/ACT LED On: Corresponding port (on rear) is connected Blinking: Data is being transmitted or received 5. LAN 1~4 LEDs 10/100M Green: Connected at 100 Mbps Off: Connected at 10 Mbps LINK/ACT On: Corresponding port (on rear) is connected | <ol style="list-style-type: none"> 6. DMZ LED On: DMZ is enabled 7. ON/OFF switch Turns the BiGuard S10 on or off 8. DC 12V connector Connect the power adapter here 9. RESET button Press to reset the BiGuard S10 to the factory default settings. 10. WAN RJ-45 connector 10/100M autosensing Ethernet port for xDSL/cable modem connection 11. LAN 1~4 RJ-45 connectors Use UTP Ethernet cables (CAT5 or CAT5e) to connect PCs to the network. |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

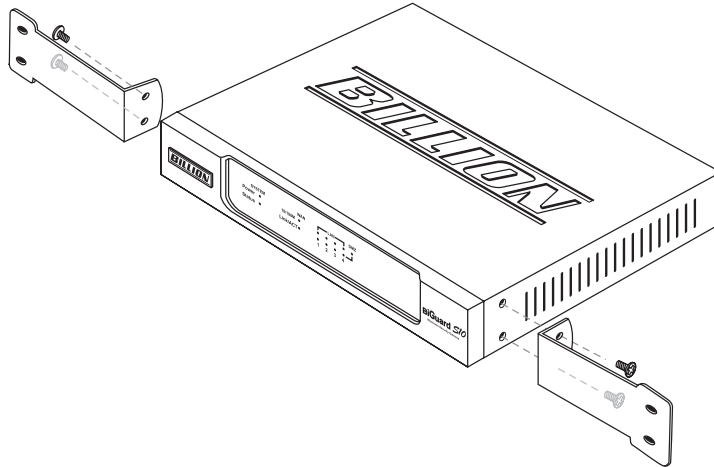
Setting up the BiGuard S10

This section provides a step-by-step guide in the hardware setup (rackmounting and power connection) and installation (LAN and WAN) of the BiGuard S10.

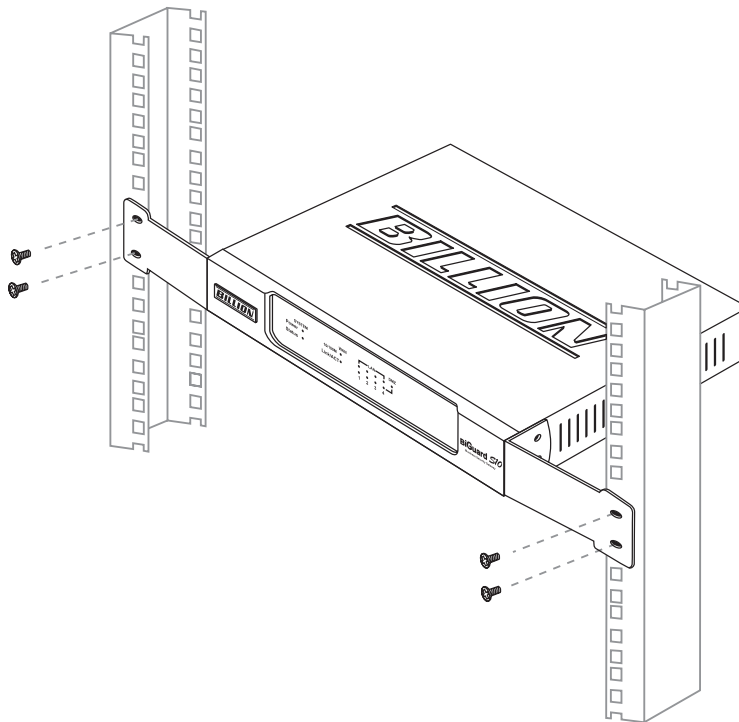
Rackmounting the BiGuard S10

Follow the steps below to install the BiGuard S10 in a rack case.

1. Align one bracket with the holes on one side of the BiGuard S10 and secure it with the bracket screws.
2. Repeat step 1 to attach the other bracket.



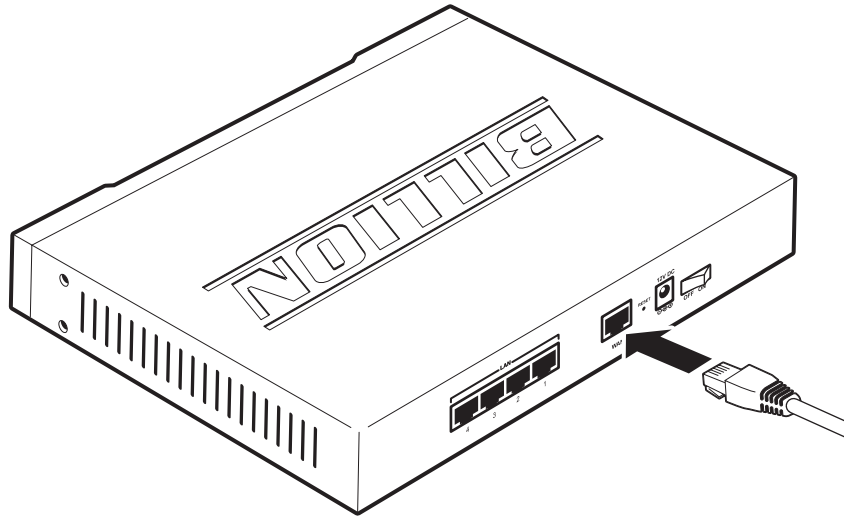
3. After attaching both mounting brackets, position the BiGuard S10 in the rack by lining up the holes in the brackets with the appropriate holes in the rack.
4. Secure the BiGuard S10 to the rack with the remaining rack-mounting screws.



Connecting to a WAN

Connect an RJ-45 Ethernet cable to the WAN port on the BiGuard S10, connect the other end to an ADSL modem, cable modem, or another router.

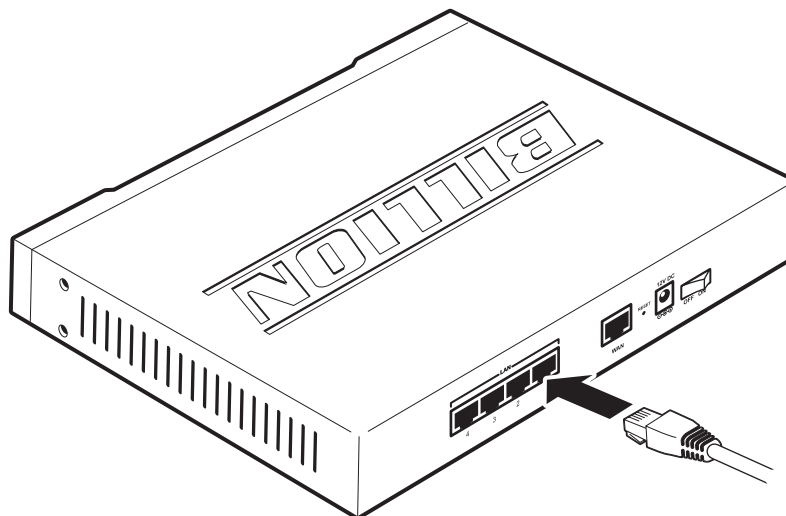
FIGURE 2 CONNECTING THE BiGUARD S10 TO A WAN



Connecting to a LAN

Connect switches, hubs, and servers to the four LAN connectors on the BiGuard S10.

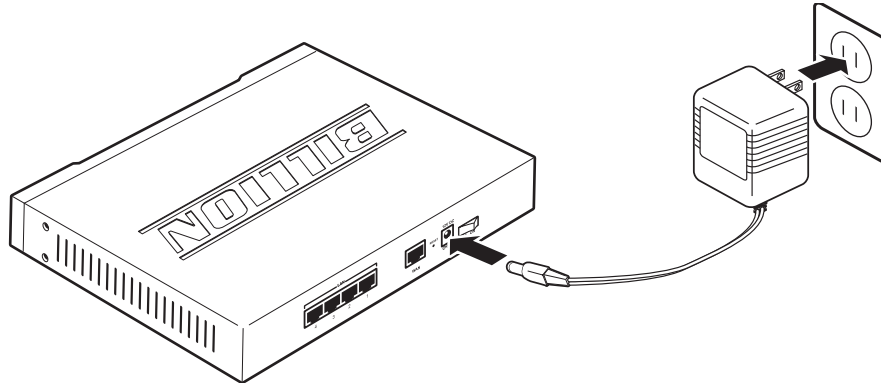
FIGURE 3 CONNECTING THE BiGUARD S10 TO A LAN



Connecting power

Connect the power adapter cable to the DC 12V connector on the BiGuard S10. Connect the power adapter to an electrical outlet.

FIGURE 4 CONNECTING THE POWER ADAPTER



Turning on the power and checking LED status

Press the power switch on the rear of the BiGuard S10. The LEDs all blink once. The LEDs blink in sequence from LAN to WAN. Then all LEDs blink once again. In about thirty (30) seconds, the status LED turns off to indicate the system is operational.

Network deployment/applications

The purpose of this section is to help you set up the BiGuard S10 device in your network, and to introduce the different networking environment scenarios available to you for designing the layout and connectivity of your organization's network.

Before starting to configure the BiGuard S10 for your network, you need to decide on the number of devices that you will need and to choose the type of functionality (router, firewall, or gateway) that they will use. The number of devices that you need to configure depends on the number of networks you want to interconnect, the type of network connection, and on the level of activity on the connected networks.

The following illustrations represent real-world network deployment examples, SSL VPN Applications, and SSL VPN Features for the use of the BiGuard S10 for easy integration of the BiGuard S10 into your existing network.

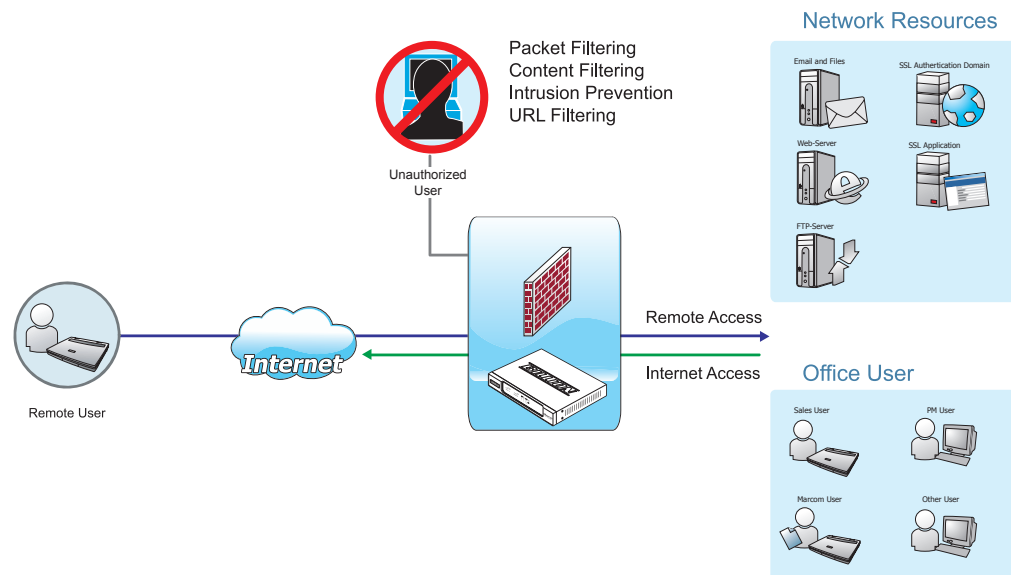
Network environment scenarios

The following tables show different scenarios for deploying the BiGuard S10.

All in one solution: firewall, remote and Internet access

The BiGuard S10 provides the ideal solution for secure remote access to corporate networks, small branch offices and small/medium sized businesses. The BiGuard S10 also provides Internet access and firewall functionality for the organization. A typical setup for users and small businesses alike is to have a single BiGuard S10 device connected to the Internet as a secure gateway to provide an all-in-one secure remote and Internet access solution.

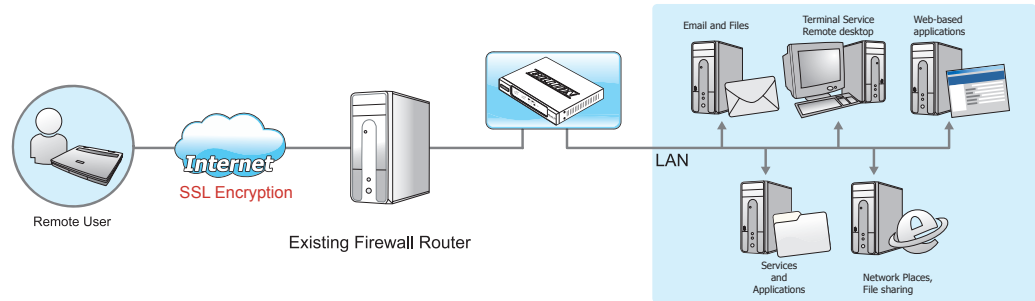
FIGURE 5 ALL IN ONE SOLUTION: FIREWALL, REMOTE AND INTERNET ACCESS



Installing behind a gateway/firewall

The BiGuard S10 can be successfully placed behind any well established network and firewall infrastructure to provide a secure remote access solution to the organization with minimal changes to your existing network topology.

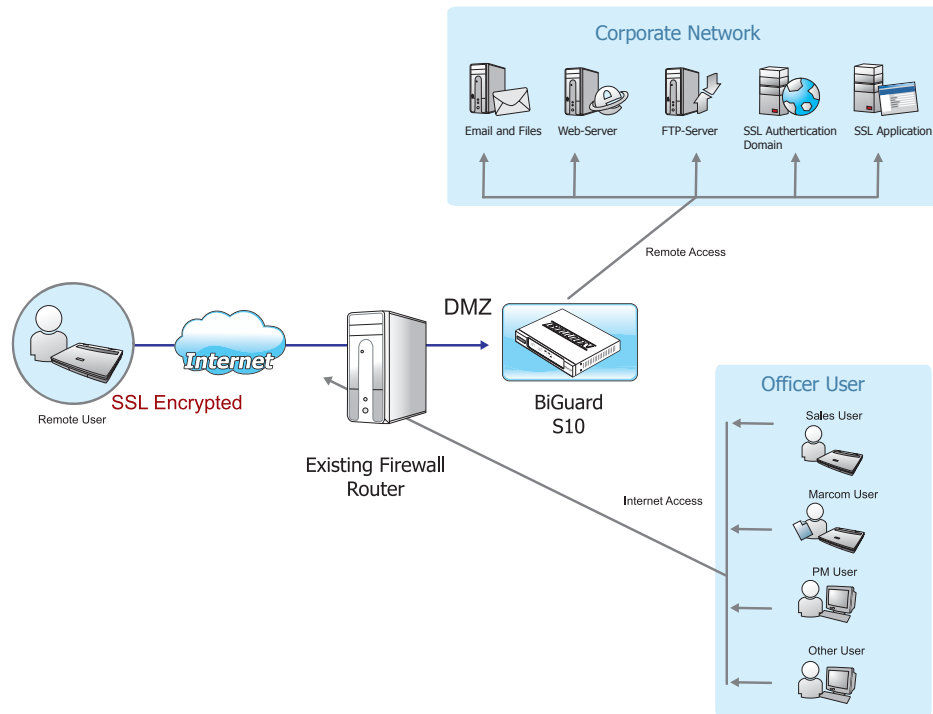
FIGURE 6 BEHIND A GATEWAY/FIREWALL



Fitting into a DMZ zone behind an existing firewall router

The following illustration demonstrates how the BiGuard S10 can be connected to the DMZ zone of an existing firewall router to provide secure remote access to the servers in the office.

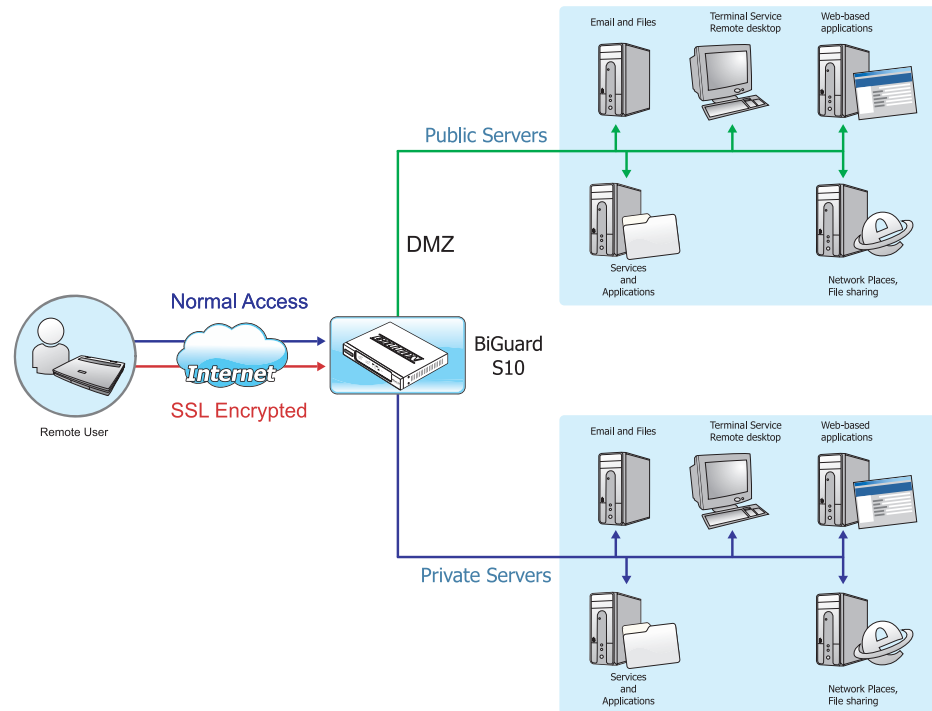
FIGURE 7 FITTING INTO A DMZ ZONE BEHIND AN EXISTING FIREWALL ROUTER



All in one: public servers on DMZ zone, private servers on LAN

The BiGuard S10 above is configured to support secure remote access, firewall and internet access functionality. Public servers are placed on DMZ zone while private servers for secure remote access are placed on the LAN side.

FIGURE 8 ALL IN ONE: PUBLIC SERVERS ON DMZ ZONE, PRIVATE SERVERS ON LAN



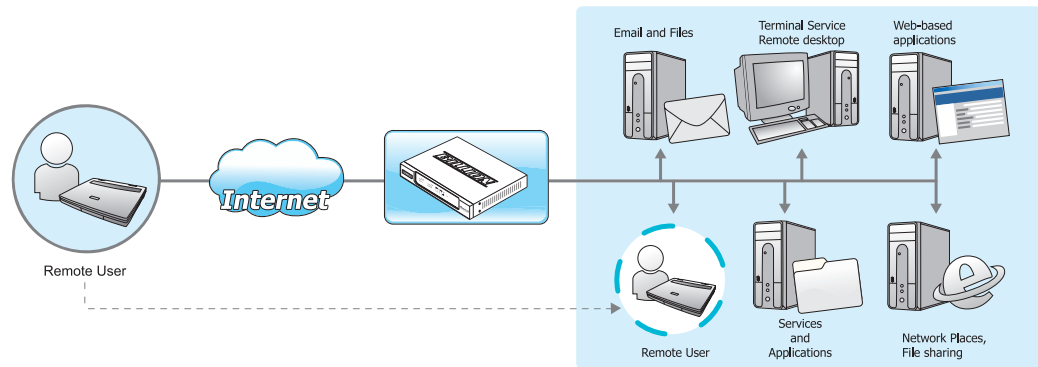
SSL VPN Applications

The BiGuard S10 provides advanced routing functionality along with SSL VPN capability. The BiGuard S10 uses internal routing tables to read each incoming packet and decide how to forward it.

Network Extender

The BiGuard S10 simplifies secure remote communication by combining IP-based access with full connectivity to a company's private network resources in the form of Network Extender. This functionality allows employees and trusted individuals to easily and securely connect to a corporate network over SSL VPN.

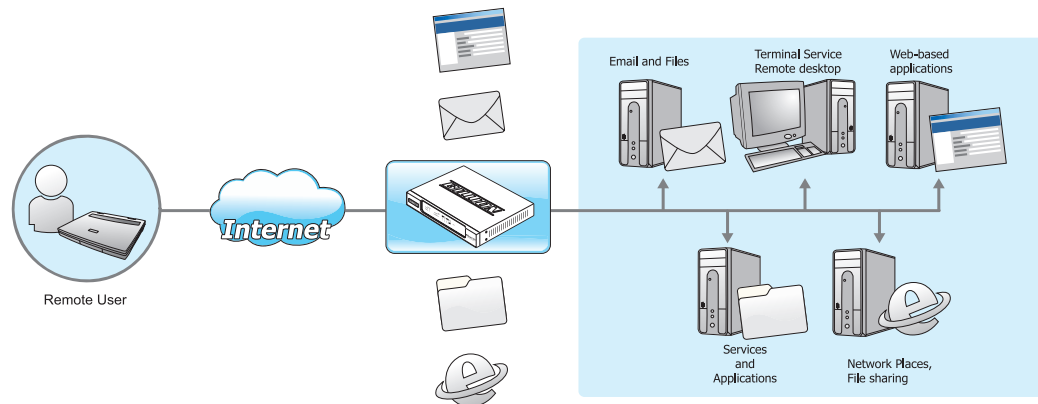
FIGURE 9 NETWORK EXTENDER



Transport Extender

Another application that makes the BiGuard S10 an ideal device for any organization is the Transport Extender technology (non-Web). By using the Transport Extender, an organization can allow remote access to designated services and applications, and the specified network applications are only accessible by designated users.

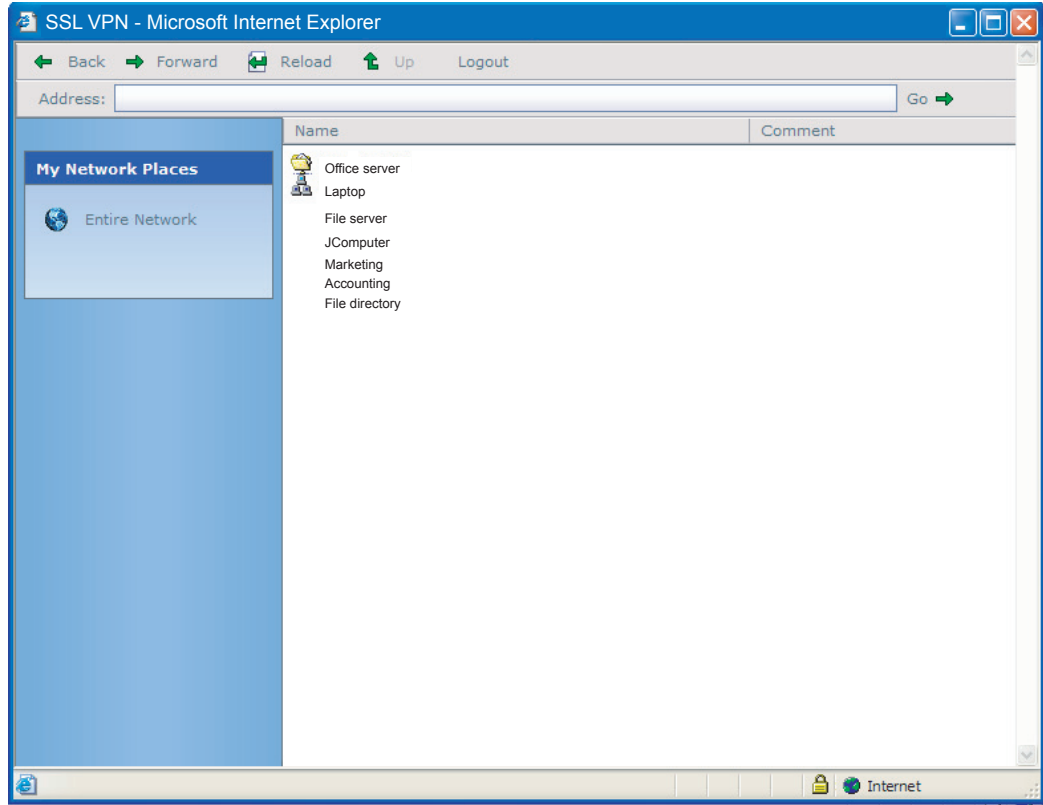
FIGURE 10 TRANSPORT EXTENDER



Network Places

Network Places allows secure, simplified, and transparent user access within the corporate network to the network resources from anywhere.

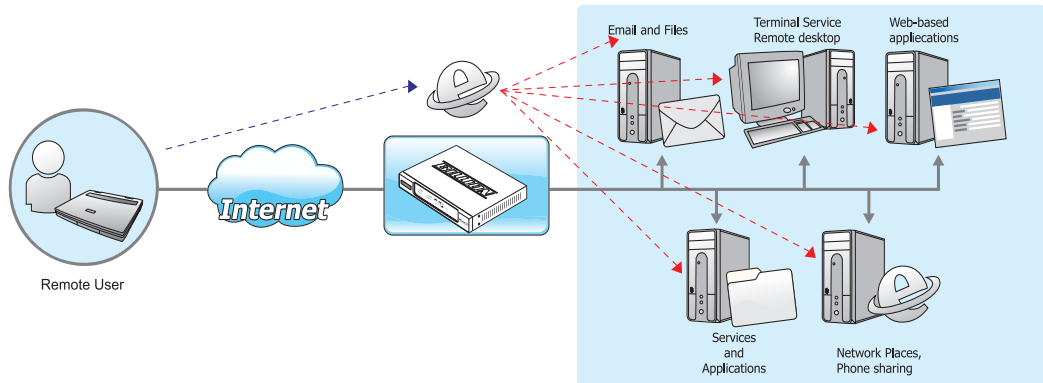
FIGURE 11 NETWORK PLACES



Application Proxy

Application Proxy, supports most commonly used applications through a web-based interface. Supported applications include: VNC (Virtual Network Control), RDP5 (Terminal Service), Telnet, SSH, FTP, HTTP, and HTTPS.

FIGURE 12 APPLICATION PROXY



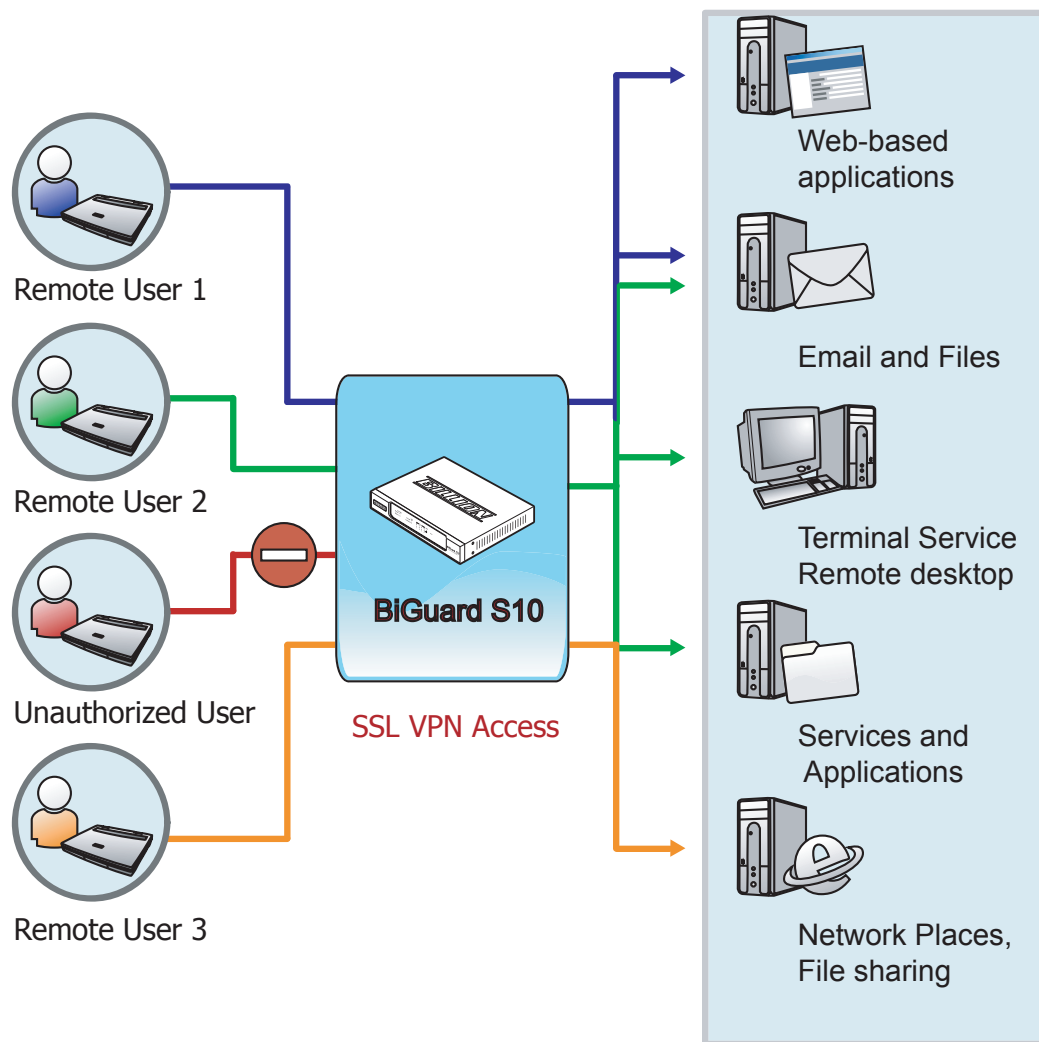
SSL VPN Features

The following sections describe some of the advanced features of the BiGuard S10.

Granular Access Control

With granular policy access control, remote users are granted different privileges and allowed only access to specific applications.

FIGURE 13 GRANULAR ACCESS CONTROL

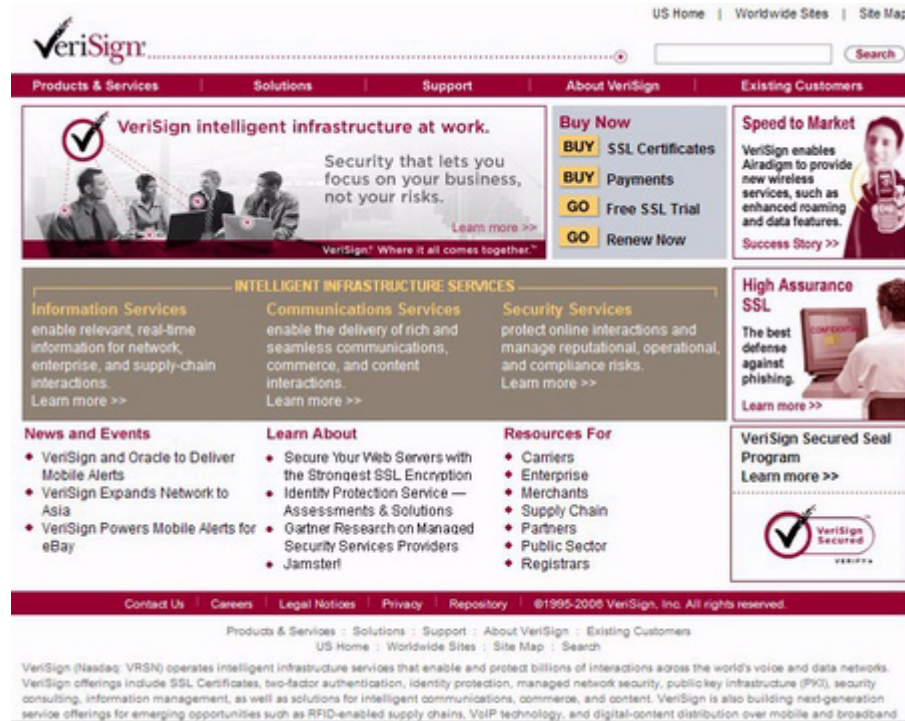


SSL VPN Certification

Manage, generate, and obtain security certificates from the Certificate Authority (CA). For the strongest possible SSL encryption, we recommend only trusted Certificate Authorities to secure network traffic and the strongest SSL encryption.

Remember to import the Certificate to the BiGuard S10. See [Importing a certificate](#) on page 79.

FIGURE 14 SSL VPN CERTIFICATION



SSL VPN Portals

The SSL Portal is the interface with which SSL VPN users interact. The components of your network to which you will be providing remote access through the SSL VPN, such as Application Proxy, Network Places, Network Extender, and Transport Extender, will be presented to them through the portal. The components presented to users through the portal can be customized by defining a portal layout.

See [Configuring SSL VPN Parameters](#) on page 68.

FIGURE 15 SSL VPN PORTALS

BiGuard S10 - SSL VPN Security Gateway

Welcome to SSL VPN Security Gateway

Due to inactivity, your connection will timeout in 58 minutes. [RESET](#)

Network Extender

Click the Network Extender icon to connect to the remote network. Keep your browser open to maintain the connection. If you reload your browser, Network Extender will disconnect and reconnect.

Transport Extender

Click the Transport Extender icon to use the service. It creates an encrypted tunnel to the corporate network, and you can access pre-defined applications as if you were on the corporate network.

Network Place

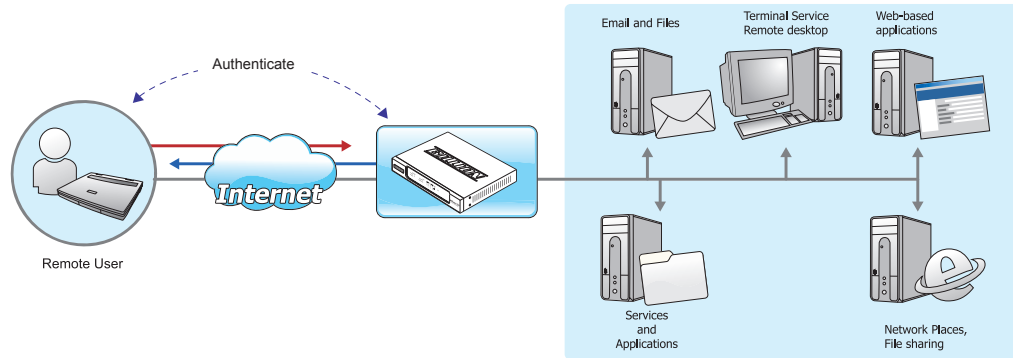
Click the Network Place icon to use the service. It is similar in style to Microsoft's familiar Network Neighborhood. It allows users to browse network shares, rename, delete, retrieve, and upload files.

| Application Name | Host Address | Service | Connection |
|------------------|------------------|---------|-------------------------|
| FTP | 192.168.1.102 | FTP | Connect |
| telnet | 192.168.1.102 | Telnet | Connect |
| SSH | 192.168.1.102 | SSH | Connect |
| Web | 192.168.1.102 | HTTP | Connect |
| WebSSL | 192.168.1.102 | HTTPS | Connect |
| RDP | 192.168.1.102 | RDP5 | Connect |
| VNC | 192.168.1.102 | VNC | Connect |
| FolderGHOST | \\pppsrver1ghost | CIFS | Connect |

Authentication Domain Scenarios

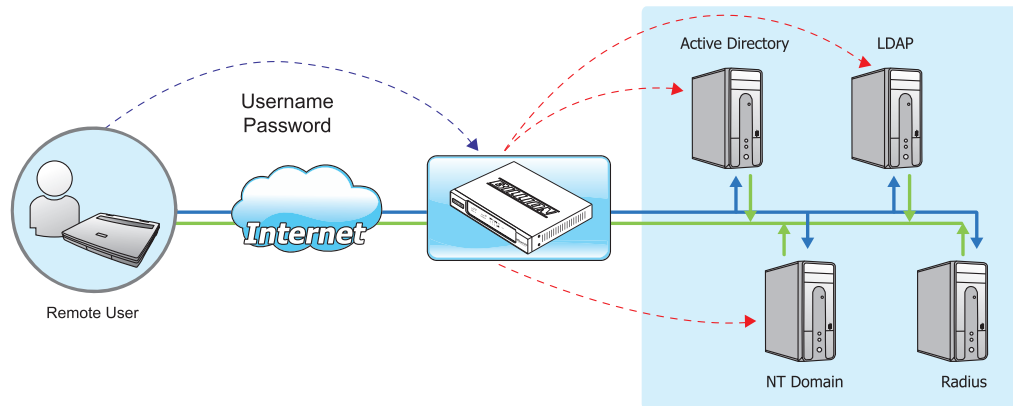
The following illustration demonstrates how a BiGuard S10 can be setup in a small organization to allow administrators the flexibility to manage user authentication simply and without the need of an authentication server.

FIGURE 16 AUTHENTICATION DOMAINS - LOCAL USER DATABASE



The BiGuard S10 provides not only local authentication, but provides clientless identity-based security and flexible centralized management through its support for multiple authentication domains, such as: NT domain, Active Directory, RADIUS and LDAP. Access to resources is provided to technical and non-technical users.

FIGURE 17 AUTHENTICATION DOMAIN - REMOTE AUTHENTICATION



See [Authentication Domain](#) on page 68.

Firewall Settings

The BiGuard S10 has a built-in firewall that provides an extra layer of protection from malicious or unauthorized access to the network. Firewalls are the primary method for keeping a computer secure from intruders. The BiGuard S10 firewall prevents harmful data from coming into and out of a private network or a single computer. The firewall not only provides secure access to the Internet, it also separates your company's public Web server from the company's internal network. The firewall also keeps internal network segments secure from internal unauthorized activity. See [Configuring Firewall Parameters](#) on page 67.

Intrusion detection

The BiGuard S10 firewall features intrusion detection capability. Intrusion detection alerts the administrator when there has been unauthorized access to the network and provides intrusion prevention features.

Block WAN request

The BiGuard S10 firewall can be set to block WAN requests from IP addresses that the router determines are unauthorized.

WAN settings

The BiGuard S10 enables connection to an ISP using a static IP address, PPPoE protocol, or by automatically obtaining an IP address using DHCP. The BiGuard S10 enables you to connect using via the router or by using NAT (Network Address Translation). See [Configuring WAN settings](#) on page 39.

Static IP

A Static WAN connection will be configured according to the IP properties defined by your ISP. In order to configure the BiGuard S10 for a Static WAN connection, you will need a static IP address, subnet mask, default IP gateway, and DNS information from your ISP. See [Configuring the WAN for Static IP](#) on page 22.

PPPoE

Point-to-point protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames in Ethernet frames. It is used mainly with cable modem and DSL services. It offers standard PPP features such as authentication, encryption, and compression. See [Quick start to configuring the WAN](#) on page 22.

DHCP

By configuring DHCP settings, the device is able to get the IP settings automatically from the ISP. See [Configuring the WAN for DHCP](#) on page 23.

Administration Guide

This chapter explains how to perform administration tasks for the BiGuard S10. The Quick Start Menu helps you configure the WAN, LAN, and SSL VPN quickly to get up and running as soon as possible.

This section helps you monitor configuration status and perform housekeeping duties such as changing the time and date and configuring DHCP server settings. Advanced administration tasks include mapping MAC addresses, configuring the Demilitarized Zone (DMZ), enabling and assigning services, creating operation schedules, configuring filtering policies and enabling the Firewall. Other advanced tasks include configuring SSL VPN applications, creating client routes for SSL VPN, managing the Transporter Extender application and host names, managing SSL certifications, and creating system logs.

You can also enable remote access, upgrade the firmware, and back up and restore configurations.

Basic Configuration with the Quick Start Menu

The Quick Start Menu enables you to quickly get the BiGuard S10 configured and running by configuring the WAN and Secure Socket Layer Virtual Private Network (SSL VPN) and configuring a user account.

Logging in to the BiGuard S10 Web Manager

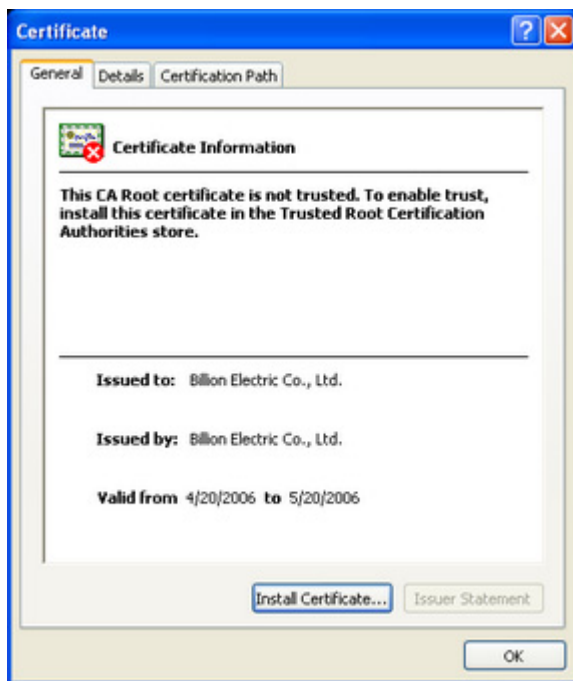
You configure and manage the BiGuard S10 with the Web Manager. The Web Manager is a Web-based interface that you can access from any Web browser.

1. In the Address field of your Web browser, type the default IP address: **192.168.1.254**
A **Security Alert** screen appears.



NOTE: To install the certificate for the BiGuard S10 continue with step 2 by selecting Yes. Otherwise, click on No to disconnect.

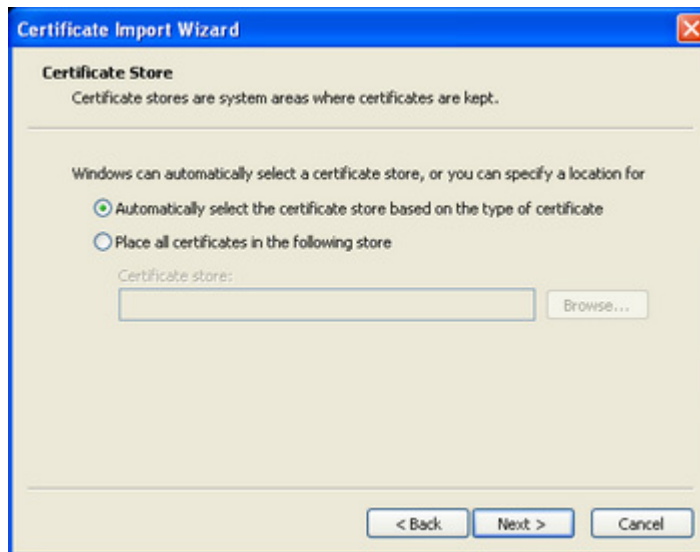
2. Click **View Certificate**. You are prompted to install a certificate.



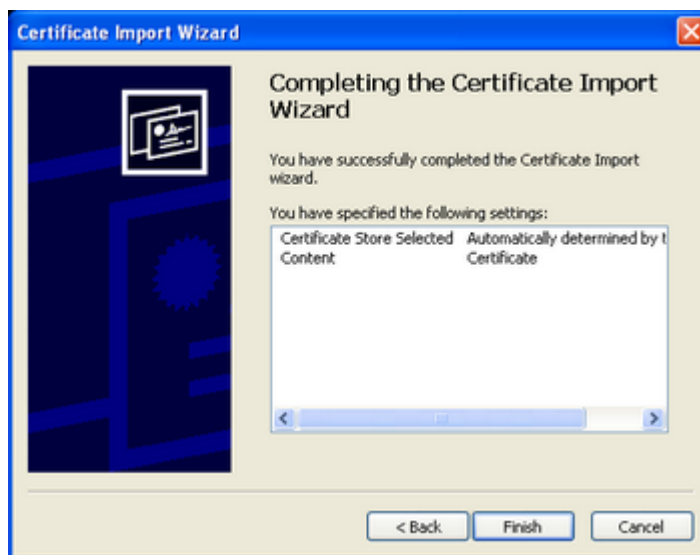
3. Click **Install Certificate**. The Certificate Import Wizard appears.



- Click **Next**. You are prompted to choose the certificate location.



- Select **Automatically select the certificate store based on the type of certificate**, and click **Next**. The wizard completes the installation.



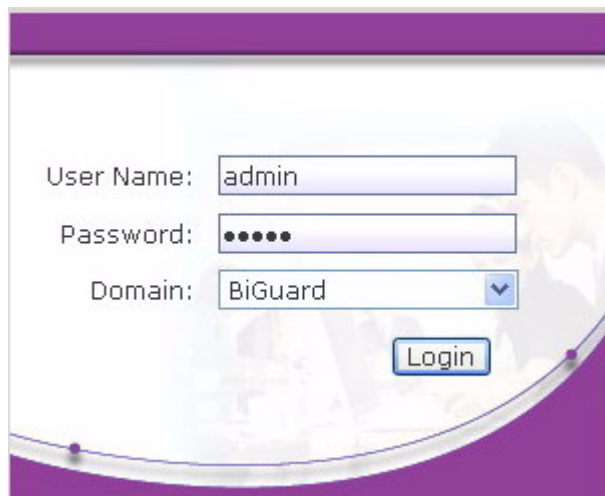
- Click **Finish**. A security warning appears.



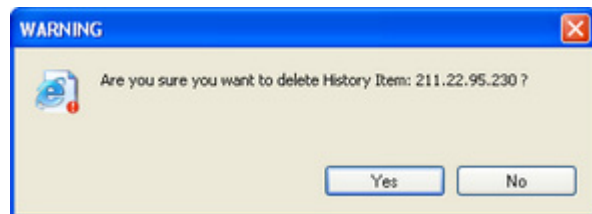
7. Click **Yes** to continue. A screen is displayed showing that the import was successful.
8. Click **OK** to return to the **Certificate** screen and click **OK** again to return to the **Security Alert** screen.



9. Click **Yes** to continue. The login screen appears.



10. Type the default user name and password:
User Name: admin
Password: admin
 Then click **Login**. The Web Manager opens on the Status menu.
 (See [Navigating in the Web Manager](#) on page 21.)
11. To log out of Web Manager, click **LOGOUT**. The **Warning** screen appears.
12. Click **Yes** if you do not want the BiGuard S10 IP address to remain in browser history.





WARNING: NOT CLEARING THE IP ADDRESS OF THE BiGUARD S10 FROM BROWSER HISTORY IS A POTENTIAL SECURITY THREAT. IF YOU HAVE ENABLED REMOTE ADMINISTRATION OF THE BiGUARD S10, BE SURE TO CHANGE THE USER NAME AND PASSWORD.



WARNING: WHEN EXITING THE WEB MANAGER, ALWAYS USE THE LOGOUT BUTTON. IF YOU CLOSE THE WEB MANAGER WITHOUT LOGGING OUT, YOU WILL NOT BE ABLE TO LOG IN WITH THE SAME USER NAME FROM A DIFFERENT COMPUTER UNTIL THE ACCOUNT IDLE TIMEOUT PERIOD HAS PASSED.

Navigating in the Web Manager

Click the items in the **Menu bar** to open a submenu for that item. Click **blue text** (indicates a link) in the main window to open additional submenus or dialog boxes.

FIGURE 18 WEB MANAGER MAIN SCREEN OVERVIEW

Menu bar Blue text opens submenu Sitemap view

SAVE CONFIG RESTART LOGOUT

Save current configuration Restart the router Log out

Click **LOGOUT** to exit the Web Manager without saving any changes. Click **RESTART** to restart the Web Manager with the new configuration. Click **SAVE CONFIG** to save the configuration to the flash memory without restarting.

Quick start to configuring the WAN

This section describes how to configure the BiGuard S10 with basic settings to get your network up and running. There are three protocols for the router's WAN settings: PPPoE, Static IP, and Obtain an IP Address Automatically (DHCP).

Configuring the WAN for Static IP

To configure the WAN for static IP, you will need the following information from your ISP:

- IP address
- Subnet mask
- Gateway
- DNS

Refer to the following to configure the connection:

1. Click **Quick Start** in the **Menu bar**.
2. Click **WAN**. The **Quick Start WAN** screen appears.

The screenshot shows the 'Quick Start WAN' configuration interface. At the top, it says 'Static IP'. Below this, there are several fields for configuration:

| | |
|-------------|------------------------------|
| Protocol | Static IP |
| IP Address | 211.22.95.230 |
| Subnet Mask | 255.255.255.248 |
| Gateway | 211.22.95.225 |
| DNS | Primary DNS: 168.95.1.1 |
| | Secondary DNS: (empty field) |

At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

3. Select **Static IP** from the **Protocol** drop-down menu.
4. Type the IP address in the **IP Address** field.
5. Type the subnet mask in the **Subnet Mask** field.
6. Type the gateway in the **Gateway** field.
7. Type the primary/secondary DNS in the **DNS** fields.

Click **Apply** to confirm the settings.

Configuring the WAN for PPPoE

To configure the WAN for PPPoE, you will need the following information from your ISP:

- User name
- Password
- DNS if necessary (contact your ISP for more information)

Refer to the following to configure the connection:

1. Click **Quick Start** in the **Menu bar**.

- Click **WAN**. The **Quick Start WAN** screen appears.

The screenshot shows the 'Quick Start WAN' configuration window. The title is 'Quick Start WAN'. Below the title is a section for 'PPPoE'. The fields are as follows:

| | |
|-----------------|--------------------------------------------------------------|
| Protocol | PPPoE |
| User Name | |
| Password | |
| Retype Password | |
| Connection | Always On |
| Idle Timeout | 10 minutes |
| DNS | <input checked="" type="checkbox"/> Obtain DNS Automatically |
| | Primary DNS |
| | Secondary DNS |

At the bottom of the window are two buttons: 'Apply' and 'Cancel'.

- Select **PPPoE** from the **Protocol** drop-down menu.
- Type the user name in the **Username** field.
- Type and confirm the password in the **Password** and **Retype Password** fields.
- Select **Always On** or **Connect on Demand** from the **Connection** drop-down menu. If you select **Connect on Demand**, the following **Idle Timeout** field is available.
- Type the number (of minutes) in the **Idle Timeout** field. If your connection is **Connect on Demand**, you are disconnected after the idle timeout period.
- Check **Obtain DNS Automatically** if your ISP provides this with the assigned IP. Otherwise, enter the Primary and Secondary DNS provided by your ISP.
- Click **Apply** to confirm the settings.

Configuring the WAN for DHCP

Configure the WAN for DHCP to enable the BiGuard S10 to automatically assign IP addresses to client stations.

Refer to the following to configure the connection:

- Click **Quick Start** in the **Menu bar**.
- Click **WAN**. The **Quick Start WAN** screen appears.

The screenshot shows the 'Quick Start WAN' configuration window. The title is 'Quick Start WAN'. Below the title is a section for 'Obtain an IP Address Automatically (DHCP Client)'. The fields are as follows:

| | |
|----------|--------------------------------------------------------------|
| Protocol | Obtain an IP Address Automatically |
| DNS | <input checked="" type="checkbox"/> Obtain DNS Automatically |
| | Primary DNS |
| | Secondary DNS |

At the bottom of the window are two buttons: 'Apply' and 'Cancel'.

- Select **Obtain an IP Address Automatically** from the **Protocol** drop-down menu.
- Check **Obtain DNS Automatically** if your ISP provides this with the assigned IP. Otherwise, enter the Primary and Secondary DNS provided by your ISP.
- Click **Apply** to confirm the settings.

Quick start to configuring SSL VPN

This section describes how to configure the BiGuard S10 with basic settings so that the SSL VPN default group is accessible from outside your network. Before a user can access the SSL VPN, a Group user account must be set up for them.

1. Click **Quick Start** → **SSL VPN** in the **Menu bar**. The Quick Start SSL VPN screen appears.

| Quick Start SSL VPN | | |
|------------------------------------------------------------------|------------------|-------------------|
| Please select an "Application Group" from the below Group option | | |
| Group | BiGuard | |
| The information of the selected Group's "Authentication Domain" | | |
| Authentication Domain Name | BiGuard | |
| Authentication Type | local | |
| Authentication Server | Local Machine | |
| The pre-defined Applications of the selected Group | | |
| Application Name | Application Type | IP Address / Path |
| FTP | FTP | 192.168.1.20 |
| Next | | |

2. If you have created new Groups, you can select one from the **Group** drop-down menu. Otherwise, leave the default Group selected and click **Next** to open an account screen. See [Creating Address Groups Network Objects](#) on page 45.

| Quick Start SSL VPN | |
|-------------------------------------------|-----------------------------------------------------------------------|
| Create the account user name and password | |
| User Name | <input type="text"/> |
| Password | <input type="password"/> |
| Retype Password | <input type="password"/> |
| Enable or disable services | |
| Network Places | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Network Extender Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Select available applications | |
| Group | BiGuard |
| Applications | <input type="checkbox"/> FTP |
| Apply Cancel | |

3. Type a user name in the **User Name** field.
4. Type and confirm a password in the **Password** and **Retype Password** fields.
5. Enable access services for the account.

Network Places: account has access to Network Places on the SSL VPN Security Gateway. Network Places is similar to Microsoft's familiar Network Neighborhood, allowing users associated with the account to browse network shares, rename, delete, retrieve, and upload files.

Network Extender: account has access to Network Extender Services on the SSL VPN Security Gateway. Network Extender is a transparent SSL VPN client that runs in the Windows environment enabling users to run applications securely on remote networks.
6. Select applications that the user will have access to.

- Click **Apply** to confirm the settings.

Monitoring Configuration Status

The **Status Menu** enables you to check the status of various router functions. You can view general information about the device including the model name, change the device name, set the current time, monitor the number of active users, and review configuration information related to the LAN and WAN. You can also check tables which show tables displaying ARP, routing, and DHCP information. Also, you can view and save log files showing system and SSL VPN status.

Status submenus

Click **Status** in the **Menu bar** to open the **Status** main screen.

FIGURE 19 MONITORING STATUS SCREEN ITEMS



Registration Click to open a web page on Billion's BiGuard Series website to register the BiGuard S10. Registration enables users to access new firmware, a user's manual, latest product news, quick customer support, and a FAQ.

Model Name Displays the model name.

Device Name Displays the device name. See [Changing the device name](#) on page 27.

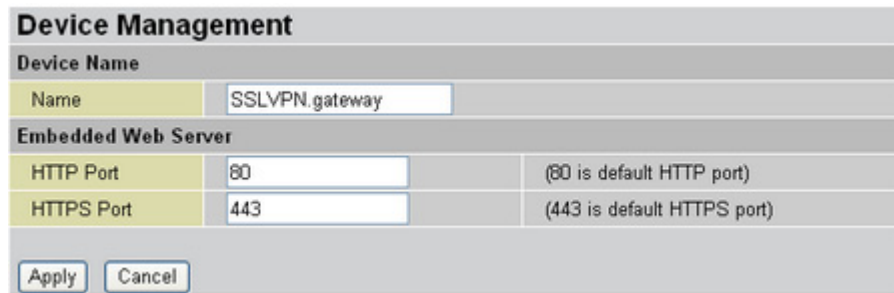
System Up-Time System uptime enables a user to determine how long has the system being online or the time that an unexpected restart or fault occurred. The system up-time is restarted when there is a power failure or upon software or hardware reset.

| | |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Current Time | Displays the current time. See Since you can have two servers sharing the same listening port under the same IP address you can use this item to distinguish the servers. on page 27. |
| Software version | Displays the current firmware version; check the version before upgrading. |
| Bootrom version | Displays the current bootrom version; check the version before upgrading. |
| LAN MAC Address | Displays the LAN MAC address for the LAN ports. |
| WAN MAC Address | Displays the WAN MAC address. |
| Home URL | Displays the manufacturer's website. |
| Active Users | Displays the number of active users who are logged on through the SSL VPN Portal, including the administrator (1). |
| IP Address | Displays the IP address for the LAN. See Changing the default LAN IP address on page 29. |
| Subnet Mask | Displays the Subnet Mask for the LAN. |
| DHCP Server | Displays DHCP server status for the LAN. See DHCP server settings on page 29. |
| Connection Method | Displays the connection method for the WAN. See Configuring WAN settings on page 39. |
| Connection | Displays the connection status for the WAN. |
| IP Address | Displays the IP address for the WAN. |
| Subnet Mask | Displays the Subnet Mask for the LAN. |
| Gateway | Displays the Gateway for the LAN. |
| DNS | Displays the DNS for the LAN. |

Changing the device name

Click **Device Name** in the **Status** screen. The **Device Management** dialog appears.

FIGURE 20 DEVICE MANAGEMENT SCREEN



| Device Management | | |
|---------------------|----------------|-----------------------------|
| Device Name | | |
| Name | SSLVPN.gateway | |
| Embedded Web Server | | |
| HTTP Port | 80 | (80 is default HTTP port) |
| HTTPS Port | 443 | (443 is default HTTPS port) |
| Apply Cancel | | |

Since you can have two servers sharing the same listening port under the same IP address you can use this item to distinguish the servers.

| | |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Name | Type a descriptive name for this device to distinguish it from other gateway devices on the network. |
| Embedded Web Server | Type the port number for HTTP and HTTPS services. Use HTTPS (HyperText Transport Protocol Secure) to access a secure Web server. By typing HTTPS instead of HTTP in the URL, the message is directed to a secure port number rather than the default HTTP Web port number of 80. The session is then managed SSL. |

Changing time and time zone parameters

Click **Current Time** in the **Status** screen. The **Time Zone** dialog appears.

FIGURE 21 TIME ZONE SCREEN

| | |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Time Zone | Enable or disable the time zone function. If you disable time zone, the other fields are unavailable. |
| Local Time Zone (+GMT Time) | Click the drop-down arrow to choose the time zone for your location. |
| SNTP Server IP Address | Four SNTP time synchronization server addresses are defined by default. Change these fields to your preferred SNTP servers. |
| Daylight Saving | Select the check box to automatically update the time based on your location's daylight saving settings. |
| Resync Period | Type the time in minutes to sync the BiGuard S10 internal clock with an SNTP time server. |

Click **Apply** to update new settings.

Changing the default LAN IP address

Click **IP Address** in the **Status** screen. The Ethernet screen lets you change default LAN IP address settings.

FIGURE 22 ETHERNET SCREEN

| Ethernet | |
|----------------------------------------------------------------------------|---------------|
| Parameters | |
| IP Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |
| RIP | Disabled |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

| | |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address | Type the preferred IP address. |
| Subnet Mask | Type the preferred Subnet Mask. |
| RIP | Click the drop-down arrow to enable Routing Information Protocol (RIP). The options are: RIPv1; RIPv2; RIPv1 + RIPv2; RIPv2 Multicast; and RIPv1 + RIPv2 Multicast. |

Click **Apply** to update the new settings.

DHCP server settings

Click **DHCP Server** in the **Status** screen. The DHCP Server screen shows the current settings.

FIGURE 23 DHCP STATUS SCREEN

| DHCP Server | |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Configuration | |
| DHCP Server Mode | <input type="radio"/> Disable <input checked="" type="radio"/> DHCP Server <input type="radio"/> DHCP Relay Agent |
| <input type="button" value="Next"/> | |
| DHCP Server Status | |
| Status | DHCP Server Running |
| Subnet Definitions | |
| Subnet Value | 192.168.1.0 |
| Subnet Mask | 255.255.255.0 |
| Domain Name | SSLVPN.gateway |
| DNS Server | 192.168.1.254 |
| Maximum/Default Lease Time | 86400 / 43200 seconds |
| IP Range | 192.168.1.100 - 192.168.1.199 |

The BiGuard S10 is enabled to act as a DHCP server for your network. Disable this function if the stations that connect to the BiGuard S10 LAN ports use static IP addresses. To change DHCP settings, see [Configuring DHCP server settings](#) on page 37.

MAPPING A MAC ADDRESS TO A FIXED IP ADDRESS

You can map the MAC address for stations that you want to always be assigned the same IP address. Mapped IP addresses must be outside the DHCP start/end IP range. The default start/end IP range is 192.168.1.100 to 192.168.1.199.

FIGURE 24 MAPPING MAC ADDRESS TO FIXED IP ADDRESS SCREEN

| DHCP Server | |
|----------------------------------------------------------------------------|---------------------------------------------------|
| Fixed MAC Address Mapping to fixed IP Address | |
| Host Name | <input type="text"/> |
| MAC Address | <input type="text"/> Candidates ▶ |
| IP Address | <input type="text"/> |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

Refer to the following to map a MAC address to a fixed IP address:

1. Ensure the computer that you are mapping is connected to the LAN and is online.
2. In the **Menu bar**, click **Status**.
3. On the **Status** page, click **DHCP Server**.

| DHCP Server | |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Configuration | |
| DHCP Server Mode | <input type="radio"/> Disable <input checked="" type="radio"/> DHCP Server <input type="radio"/> DHCP Relay Agent |
| <input type="button" value="Next"/> | |
| DHCP Server Status | |
| Status | DHCP Server Running |
| Subnet Definitions | |
| Subnet Value | 192.168.1.0 |
| Subnet Mask | 255.255.255.0 |
| Domain Name | SSLVPN.gateway |
| DNS Server | 192.168.1.254 |
| Maximum/Default Lease Time | 86400 / 43200 seconds |
| IP Range | 192.168.1.100 - 192.168.1.199 |

4. Click **DHCP Server** in **DHCP Server Mode**.

- Click **Next**.

| DHCP Server | | |
|----------------------------------------------------------------------------|---------------------------------------------|---------------------|
| Parameters | | |
| Domain Name | <input type="text" value="SSLVPN.gateway"/> | |
| Use Router as DNS Server | <input checked="" type="checkbox"/> | |
| Primary DNS Server Address | <input type="text" value="192.168.1.254"/> | |
| Secondary DNS Server Address | <input type="text"/> | |
| Default Lease Time | <input type="text" value="43200"/> | seconds |
| Maximum Lease Time | <input type="text" value="86400"/> | seconds |
| Range Start | <input type="text" value="192.168.1.100"/> | |
| Range End | <input type="text" value="192.168.1.199"/> | |
| Specify fixed MAC Address Mapping to fixed IP Address (optional) | | Add |
| Host Name | MAC Address | IP Address |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | |

- Click **Add**.

| DHCP Server | | |
|----------------------------------------------------------------------------|----------------------|----------------------------|
| Fixed MAC Address Mapping to fixed IP Address | | |
| Host Name | <input type="text"/> | |
| MAC Address | <input type="text"/> | Candidates |
| IP Address | <input type="text"/> | |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | |

- In the **Host Name** field, type a name to identify the computer.
- Click **Candidates** to display a list of active PCs on the LAN and then select the computer you want to map from the list.
The MAC address for the computer you select is added to the MAC Address field.
- In the IP Address field, type an IP address that is outside the DHCP start/end IP range
The default DHCP IP range is 192.168.1.100 ~ 192.168.1.199.
- Click **Apply** to complete the mapping.
- Click **Apply** to save the settings.
- Click **SAVE CONFIG** to write the new settings to the router's configuration file.

SSL User Status

The SSL User Status screen lists users that are currently logged onto the BiGuard S10. You can monitor user activity and disconnect specific users.

FIGURE 25 SSL USER STATUS SCREEN

| SSL User Status | | | | |
|-----------------|---------|-----------------|--------------------------|----------------------------|
| Status | | | | |
| Name | Group | From IP Address | Login Time | |
| admin | BiGuard | 211.22.95.226 | Sat Jul 15 03:51:43 2006 | Disconnect |

| | |
|-----------------|-------------------------------------------------------|
| Name | Displays the name of the user. |
| Group | Displays the Group name that the user belongs to. |
| From IP address | Displays the IP address of the user. |
| Login Time | Displays the time the user logged in. |
| Disconnect | Click Disconnect to disconnect specific users. |
| Refresh | Click Refresh to update the screen. |

ARP Table

ARP (Address Resolution Protocol) is a TCP/IP protocol used to obtain a node's physical address. The ARP Table screen shows the mapping of IP addresses to MAC addresses, and provides a way for administrators to monitor system status.

FIGURE 26 ARP TABLE SCREEN

| ARP Table | | | |
|----------------|-------------------|-----------|--------|
| IP <> MAC List | | | |
| IP Address | MAC Address | Interface | Static |
| 211.22.95.226 | 00:A0:C5:D9:19:87 | WAN | no |
| 211.22.95.225 | 00:D0:59:5F:6B:7A | WAN | no |

| | |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address | Displays the IP address of the station. |
| MAC Address | Displays the MAC address of the station. |
| Interface | Displays the interface (LAN or WAN) related to the IP address. |
| Static | Yes indicates that the IP address is assigned and referenced from the fixed MAC address in the DHCP server setting. No indicates that the IP address is not referenced. |

Routing Table

The Routing Table provides administrators with a database in the router that contains current network topology such as current paths for transmitted packets. Both static and dynamic routes are displayed.

FIGURE 27 ROUTING TABLE SCREEN

| Routing Table | | | |
|-----------------|-----------------|-------------------|------|
| Routing Table | | | |
| Destination | Subnet Mask | Gateway/Interface | Cost |
| 211.22.95.224 | 255.255.255.248 | 0.0.0.0/WAN | 0 |
| 192.168.1.0 | 255.255.255.0 | 0.0.0.0/LAN | 0 |
| Default Gateway | 0.0.0.0 | 211.22.95.225/WAN | 0 |

| | |
|-------------------|------------------------------------------------------------------------------------|
| Destination | Displays the IP address of the destination network. |
| Subnet Mask | Displays the destination netmask address. |
| Gateway/Interface | Displays the IP address of the gateway or existing interface that this route uses. |
| Cost | Displays the number of hops counted as the cost of the route. |

DHCP Table

The DHCP Table lists stations on the LAN that have been assigned IP addresses via the DHCP functionality of the BiGuard S10.

FIGURE 28 DHCP TABLE SCREEN

| DHCP Table | | | |
|--------------|-------------|------------------|---------------|
| Leased Table | | | |
| IP Address | MAC Address | Client Host Name | Register Time |

| | |
|------------------|-----------------------------------------------------|
| IP Address | Displays the IP address of the station. |
| MAC Address | Displays the MAC address of the station. |
| Client Host Name | Displays the host name of the station. |
| Register Time | Displays the time that the station has been leased. |

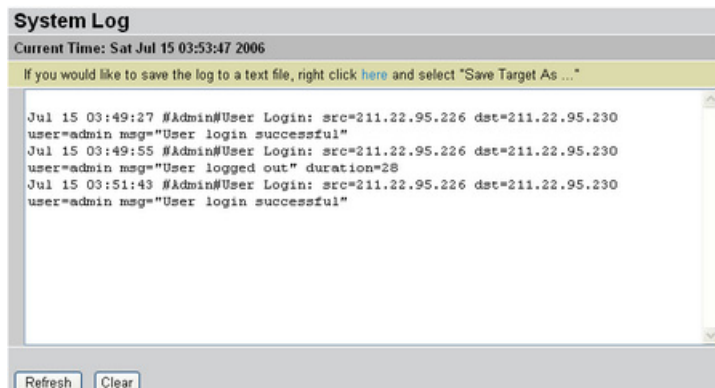
System Log

The System Log dialog logs system events for the BiGuard S10.



NOTE: You can modify parameters for the information that is saved to the log. See [Log and E-mail Alerts](#) on page 92.

FIGURE 29 SYSTEM LOG SCREEN



..right click [here](#)... To save the log, right click where indicated, and then save the log.

Refresh Click to update the system log.

Clear Click to clear the current log from the screen.

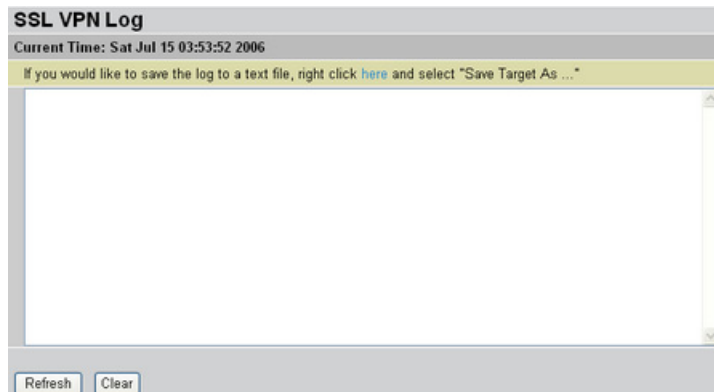
SSL VPN Log

The SSL VPN Log dialog logs SSL VPN events for the BiGuard S10.



NOTE: YOU CAN MODIFY PARAMETERS FOR THE INFORMATION THAT IS SAVED TO THE LOG. SEE [Log and E-mail Alerts](#) ON PAGE 92.

FIGURE 30 SSL VPN LOG SCREEN



..right click here... To save the log, right click where indicated, and then save the log.

| | |
|---------|----------------------------------|
| Refresh | Click to update the SSL VPN log. |
|---------|----------------------------------|

| | |
|-------|-------------------------------------------------|
| Clear | Click to clear the current log from the screen. |
|-------|-------------------------------------------------|

Configuring the BiGuard S10

This section explains how to configure router settings including the LAN, WAN, DMZ, how to create network objects such as addresses, services, address and service groups, schedules, bandwidth control items, and content blocking scenarios. You can also set up security policies which includes configuring packet filtering, virtual servers, quality of service (QoS), and MAC and content filters.

Additionally, you can perform system maintenance and configuration including configuring the time zone, enabling remote access, upgrading the firmware, backing up and restoring configurations, setting the log on password, and restarting the system.

Finally, you configure advanced features including setting up static routing, enabling DDNS and SNMP, configuring the firewall, and managing router device parameters.

Configuring the Interface

Click **Interface** to configure the **LAN**, **WAN**, and **DMZ**.

Configuring the LAN

Click **LAN** to display the LAN submenu items: **Ethernet** and **DHCP Server**.

CONFIGURING THE ETHERNET

The Ethernet dialog lets you change default LAN IP address settings.

FIGURE 31 LAN SCREEN

The screenshot shows the 'Ethernet' configuration window. It has a title bar 'Ethernet' and a 'Parameters' section. The parameters are: IP Address (192.168.1.254), Subnet Mask (255.255.255.0), and RIP (RIPv1). There are 'Apply' and 'Cancel' buttons at the bottom.

| | |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address | Type the preferred IP address. (default 192.168.1.254). |
| Subnet Mask | Type the preferred IP address. |
| RIP | Click the drop-down arrow to enable Routing Information Protocol (RIP). The options are: Disabled; RIPv1; RIPv2; RIPv1 + RIPv2; RIPv2 Multicast; and RIPv1 + RIPv2 Multicast. |

CONFIGURING DHCP SERVER SETTINGS

The BiGuard S10 is enabled to act as a DHCP server for your network. Disable this function if the stations that connect to the BiGuard S10 LAN ports use static IP addresses.


FIGURE 32 DHCP STATUS SCREEN

| DHCP Server | |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Configuration | |
| DHCP Server Mode | <input type="radio"/> Disable <input checked="" type="radio"/> DHCP Server <input type="radio"/> DHCP Relay Agent |
| <input type="button" value="Next"/> | |
| DHCP Server Status | |
| Status | DHCP Server Running |
| Subnet Definitions | |
| Subnet Value | 192.168.1.0 |
| Subnet Mask | 255.255.255.0 |
| Domain Name | SSLVPN.gateway |
| DNS Server | 192.168.1.254 |
| Maximum/Default Lease Time | 86400 / 43200 seconds |
| IP Range | 192.168.1.100 - 192.168.1.199 |

| | |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP Server Mode | Choose Disable if IP addresses are assigned manually to stations on your network. Choose DHCP Server to have the BiGuard S10 assign IP addresses automatically to stations on your network. Choose DHCP Relay Agent if you want to place DHCP servers and clients on different networks, making DHCP management easier when there is more than one subnet on the network. |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The **DHCP Server Status** and **Subnet Definitions** screen displays current settings. These items are display only. To change these settings, click **Next**.

FIGURE 33 DHCP SERVER CONFIGURATION SCREEN

| DHCP Server | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|----------------------|
| Parameters | | |
| Domain Name | <input type="text" value="SSLVPN.gateway"/> | |
| Use Router as DNS Server | <input checked="" type="checkbox"/> | |
| Primary DNS Server Address | <input type="text" value="192.168.1.254"/> | |
| Secondary DNS Server Address | <input type="text"/> | |
| Default Lease Time | <input type="text" value="43200"/> | seconds |
| Maximum Lease Time | <input type="text" value="86400"/> | seconds |
| Range Start | <input type="text" value="192.168.1.100"/> | |
| Range End | <input type="text" value="192.168.1.199"/> | |
| Specify fixed MAC Address Mapping to fixed IP Address (optional) Add  | | |
| Host Name | MAC Address | IP Address |
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | |

| | |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain Name | Type the desired domain name. If you are using the BiGuard S10 to replace another device and do not want to change the original networking environment, type the domain name for the previous device. |
| Use Router as DNS Server | When this checkbox is selected, the DNS address that you type in the Primary DNS Server Address field is assigned to stations on the LAN. |
| Primary DNS Server Address | Type the primary DNS address that was provided by your ISP. |
| Secondary DNS Server Address | Type the secondary DNS address that was provided by your ISP. |
| Default Lease Time | Type the number of seconds (from 1 to 999999999) you want for the default lease time. This is the time that the router can use an IP address assigned by the DHCP server. |
| Maximum Lease Time | Type the number of seconds (from 1 to 999999999) you want for the maximum lease time. This is the maximum time that the router can use an IP address assigned by the DHCP server. |
| Range Start | Type the start IP address that the BiGuard S10 assigns to stations on the LAN. |
| Range End | Type the end IP address that the BiGuard S10 assigns to stations on the LAN. |
| Specify fixed MAC Address Mapping to fixed IP Address | This option lets you map a MAC address to a specific IP address; once mapped the router assigns the same IP address to that station every time it logs on to the LAN. See Mapping a MAC address to a fixed IP address on page 30. |

Configuring WAN settings

This menu item enables you to configure WAN settings and also to set WAN outbound and inbound bandwidth parameters.

CONFIGURING THE WAN

You can select one of three protocols for the router's WAN settings: **PPPoE**, **Static IP**, and **Obtain an IP Address Automatically**.

PPPoE protocol. Select this item if your ISP uses the PPPoE (Point-to-Point Protocol Over Ethernet) protocol.

FIGURE 34 WAN SETTINGS PPPoE SCREEN

| WAN Settings | |
|-------------------------|-------------------------------------------------------------------|
| PPPoE | |
| Protocol | PPPoE |
| Mode | <input checked="" type="radio"/> NAT <input type="radio"/> Router |
| Username | <input type="text"/> |
| Password | <input type="text"/> |
| Retype Password | <input type="text"/> |
| Service Name | <input type="text"/> |
| IP Address | 0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically') |
| Authentication Protocol | Auto |
| Connection | Always On |
| Idle Timeout | 10 minutes |
| DNS | <input checked="" type="checkbox"/> Obtain DNS Automatically |
| | Primary DNS <input type="text"/> |
| | Secondary DNS <input type="text"/> |
| RIP | Disable |
| MTU | 1492 |

Apply Cancel

Protocol Displays the current protocol. Click the drop-down arrow to change the protocol.

Mode There are two modes for the connection: NAT (Network Address Translation) and Router. NAT converts private IP addresses (such as in the 192.168.0.0 range) of the machine on the internal private network to one or more public IP addresses for the Internet. Select NAT to add an extra layer of security when user on the internal network need to access the Internet. Select Router for an internal network.

Username Type the user name that your ISP provided.

Password Type the password that your ISP provided.

Retype Confirm the password that your ISP provided.

Service Name Type the name of the ISP.

| | |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address | This field displays the IP address assigned by the PPPoE service provider (0.0.0.0 indicates that the IP address is automatically assigned. If your ISP assigned you a static IP address, type it in this field. |
| Authentication Protocol | Select the authentication protocol from the drop-down menu. Auto: automatically configures the access protocol. This is the default option. CHAP: (Challenge Handshake Authentication Protocol) select this access protocol for dialing into a network that provides a moderate degree of security. PAP: (Password Authentication Protocol) select this access protocol for dialing into a network that provides only basic functionality. |
| Connection | Connection options are Always On and Connect on Demand . If you select Connect on Demand , the following field Idle Timeout is available. If your ISP charges a fee for connection time, select Connect on Demand . |
| Idle Timeout | This field is only available when the Connection field is set to Connect on Demand . Type the number in minutes that you want the connection to disconnect when idle. |
| DNS | Check Obtain DNS Automatically to enable the router to configure this value, or type in the Primary and Secondary DNS values provided by your ISP. |
| RIP | Select the RIP version from the drop-down menu. If you are not sure which version to choose, select Disable . |
| MTU | MTU (Maximum Transmission/Transfer Unit) refers to the largest frame size that can be transmitted over the network. Messages longer than the MTU must be divided into smaller frames. The default value is sufficient for most scenarios. |

Static IP protocol. Select this item if your DSL provides you with a static IP address.

FIGURE 35 WAN SETTINGS STATIC IP SCREEN

The screenshot shows the 'WAN Settings Static IP' configuration screen. It includes the following fields and options:

- Protocol:** Static IP (selected in a dropdown menu)
- Mode:** NAT (selected with a radio button), Router (unselected)
- IP Address:** 211.22.95.230
- Subnet Mask:** 255.255.255.248
- Gateway:** 211.22.95.225
- MAC Address:** Default MAC Address (selected with a radio button), Specify a MAC Address (MAC Clone) (unselected). Below this, there is a text input field containing '00:00:00:00:00:00' and a 'Candidates' button.
- DNS:** Primary DNS: 168.95.1.1, Secondary DNS: (empty text input field)
- RIP:** Disable (selected in a dropdown menu)

At the bottom of the screen, there are 'Apply' and 'Cancel' buttons.

| | |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol | Displays the current protocol. Click the drop-down arrow to change the protocol. |
| Mode | There are two modes for the connection: NAT (Network Address Translation) and Router. NAT converts private IP addresses (such as in the 192.168.0.0 range) of the machine on the internal private network to one or more public IP addresses for the Internet. Select NAT to add an extra layer of security when user on the internal network need to access the Internet. Select Router for an internal network. |
| IP Address | Type the IP address that your ISP provided. |
| Subnet Mask | Type the Subnet Mask that your ISP provided. |
| Gateway | Type the Gateway address that your ISP provided. |
| MAC Address | Select Specify a MAC Address (MAC Clone) if your ISP requires a defined MAC address to access their service or to allow the BiGuard S10 to accommodate the MAC filter from the ISP. Otherwise, click Default MAC Address . |
| DNS | Type the Primary/Secondary DNS address that your ISP provided. |
| RIP | Select the RIP version from the drop-down menu. If you are not sure which version to choose, select Disable . |

DHCP protocol. Select this item if the BiGuard S10 is connected to a router that has DHCP functionality enabled.

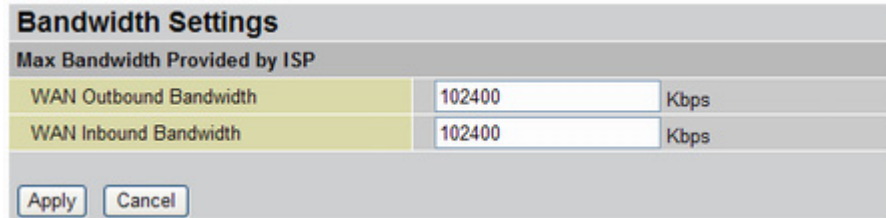
FIGURE 36 WAN SETTINGS DHCP SCREEN

| | |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol | Displays the current protocol. Click the drop-down arrow to change the protocol. |
| Mode | There are two modes for the connection: NAT (Network Address Translation) and Router. NAT converts private IP addresses (such as in the 192.168.0.0 range) of the machine on the internal private network to one or more public IP addresses for the Internet. Select NAT to add an extra layer of security when user on the internal network need to access the Internet. Select Router for an internal network. |
| MAC Address | Select Specify a MAC Address (MAC Clone) if your ISP requires a defined MAC address to access their service or to allow the BiGuard S10 to accommodate the MAC filter from the ISP. Otherwise, click Default MAC Address . |
| DNS | Check Obtain DNS Automatically to enable the router to configure this value, or type in the Primary and Secondary DNS values provided by your ISP. |
| RIP | Select the RIP version from the drop-down menu. If you are not sure which version to choose, select Disable . |

CONFIGURING WAN BANDWIDTH PARAMETERS

This menu item enables you to set the maximum WAN outbound and inbound bandwidth that your ISP can provide.

FIGURE 37 SETTING WAN BANDWIDTH



WAN Outbound Bandwidth Type the maximum outbound bandwidth that is provided by your ISP.

WAN Inbound Bandwidth Type the maximum inbound bandwidth that is provided by your ISP.

Configuring the DMZ

Click **DMZ** to enable or disable the DeMilitarized Zone:

FIGURE 38 ENABLING THE DMZ



The DMZ is a section of the network that is located between an organization's trusted internal network and an untrusted external network such as the Internet. The DMZ is a subnet that is located between firewalls or off one leg of a firewall.

Click the **DMZ** drop-down menu to select **Disable** or **Transparent**.

When set to transparent mode, all interfaces behave as though they are part of the same network, and the firewall filters packets pass through the firewall without modifying any of the source or destination information in the IP packet header

Configuring Network Objects

A Network Object can be a single IP address on your LAN or a group of IP addresses. Network Objects can also be services, schedules, bandwidth control settings, or filter profiles. The Network Objects you create are then available in the drop-down menus of their respective category.

Creating Network Objects makes managing your policy settings easier. For example, you can configure complex filter rules and save the parameters as a Network Object. The next time you want to apply those settings to an account, you just select the Network Object from the respective drop-down menu.

Click **Network Object** to display the Network Object menu items.

Configuring IP address Network Objects

Click **Address** to display the Address screen:

FIGURE 39 CONFIGURING NETWORK OBJECT ADDRESSES

| Address | | |
|------------------|------------------|-------------------|
| Address Table | | |
| Name | IP Address | Subnet Mask/Range |
| **Any | All IP Addresses | |
| **Default WAN IP | WAN IP Address | |

Create ▶

Click **Create** to add a new IP address to the **Address Table**:

FIGURE 40 ADDING ADDRESSES TO THE ADDRESS TABLE

| Address | |
|------------|-----------------------------------|
| Create | |
| Name | <input type="text"/> |
| Type | IP Address ▼ |
| IP Address | <input type="text"/> Candidates ▶ |

Apply Cancel

| | |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name you want to assign to this address Network Object. |
| Type | Select the type of address from the drop-down menu: <ul style="list-style-type: none"> • IP Address • IP Address / Subnet Mask • IP Address Range |
| IP Address | Type the IP address or click Candidates to display a list of active PCs on the LAN and then select the computer you want. |
| Subnet Mask | When IP Address / Subnet Mask is selected from the drop-down menu, this field is displayed. Type the subnet mask associated with the IP address in the IP Address field. |

IP Address Start / End When IP Address Range is selected from the drop-down menu, these two fields are displayed.

- IP Address Start: type the beginning IP address or click **Candidates** to select the starting range from one of the active PCs that are listed on the LAN.
- IP Address End: type the ending IP address.

Click **Apply** to confirm the settings.

Creating Address Groups Network Objects

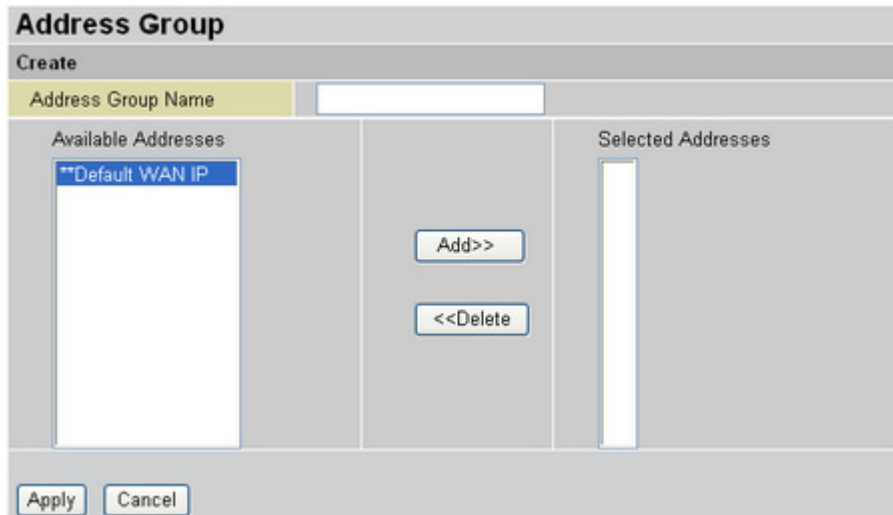
Click **Address Groups** to display the Address Group dialog screen:

FIGURE 41 ADDRESS GROUP LIST



Click **Create** to create a new Address Group:

FIGURE 42 CREATING AN ADDRESS GROUP



| | |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Address Group Name | Type the name that you want this address group Network Object to have. |
| Available Addresses | Displays the list of IP addresses which you can add to this group. Select the addresses you want to add and click Add . |
| Selected Addresses | Displays the list of IP addresses in this group. To delete addresses from this list, select the addresses and click Delete . |

Click **Apply** to confirm the settings.

Allowing Services

Click **Service** to display the list of allowable pre-defined and user-defined services:

FIGURE 43 PRE-DEFINED AND USER-DEFINED SERVICE TABLE

| Service | | | | |
|-----------------------------------|-----------------------|-----------------------|---------------------|---------------------------|
| Pre-defined Service Table | | | | |
| **Any | **HTTP (TCP 80) | **DNS-TCP (TCP 53) | **DNS (UDP 53) | **FTP (TCP 21) |
| **Telnet (TCP 23) | **SMTP (TCP 25) | **POP3 (TCP 110) | **NEWS (TCP 119) | **RealAudio (UDP 7070) |
| **Ping (ICMP) | **H.323 (TCP 1720) | **T.120 (TCP 1503) | **SSH (TCP 22) | **NTP (UDP 123) |
| **HTTPS (TCP 443) | | | | |
| User-defined Service Table | | | | |
| Name | Type | Port/protocol ID | | |
| Create | | | | |

The pre-defined list of services includes all normal networking services such as Telnet and Ping. Click **Create** to add a user-defined service to the **Service Table**:

FIGURE 44 ADDING SERVICES TO THE SERVICE TABLE

| Service | |
|----------------------------------------------------------------------------|----------------------|
| Create | |
| Name | <input type="text"/> |
| Type | TCP |
| Service Port Start | <input type="text"/> |
| Service Port End | <input type="text"/> |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

| | |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name of the service to be added. |
| Type | Select the type of service from the drop-down menu: <ul style="list-style-type: none"> • TCP: services involving transfer control protocol transmission. • UDP: services involving user datagram protocol transmission. • ICMP: services involving internet control message protocol transmission. This option does not require you to set a service port start and end value. • GRE: services involving generic routing encapsulation transmission. This option does not require you to set a service port start and end value. • Others: other protocols. When you select this option, a text box appears enabling you to type the protocol ID. |
| Service Port Start | Type the port number or protocol ID that defines the beginning of the port range that this service is allowed to use. |
| Service Port End | Type the port number or protocol ID that defines the end of the port range that this service is allowed to use. |

Click **Apply** to confirm the settings.

Creating Service Group Network Objects

Click **Service Group** to view the **Service Group Table**.

FIGURE 45 THE SERVICE GROUP TABLE

Service Group Name Type the name that you want this service group Network Object to have.

Available Services Displays the list of available services which you can add to this group. Select the services you want to add and click **Add**.

Selected Services Displays the list of selected services in this group. To delete services from this list, select the services and click **Delete**.

Click **Apply** to confirm the settings.

Scheduling BiGuard S10 operation

Click **Schedule** to view a list of schedule items.

FIGURE 46 SCHEDULE TABLE LIST

| Schedule | | | |
|------------------------|------------------------------------|---------------------|--|
| Schedule Table | | | |
| Name | Day in a week | Time | |
| **Always On | Sun. Mon. Tue. Wed. Thu. Fri. Sat. | From 00:00 To 24:00 | |
| Create | | | |

The **Schedule Table** enables the Administrator or users to set the time for a function or rule to be activated. Schedules are used for many Policy functions.

Click **Create** to create a new schedule.

FIGURE 47 CREATING A NEW SCHEDULE NETWORK OBJECT

| Schedule | |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create | |
| Name | <input type="text"/> |
| Day | <input type="checkbox"/> Sun. <input type="checkbox"/> Mon. <input type="checkbox"/> Tue. <input type="checkbox"/> Wed. <input type="checkbox"/> Thu. <input type="checkbox"/> Fri. <input type="checkbox"/> Sat. |
| Start Time | 08 : 00 |
| End Time | 18 : 00 |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

| | |
|------------|------------------------------------------------------------------|
| Name | Type the name of the schedule Network Object. |
| Day | Check which days you want the schedule to be applicable. |
| Start Time | Select the start time for the schedule from the drop-down menus. |
| End Time | Select the end time for the schedule from the drop-down menus. |

Managing Bandwidth Network Objects

Click **Bandwidth Control** to display the **Bandwidth Table**.

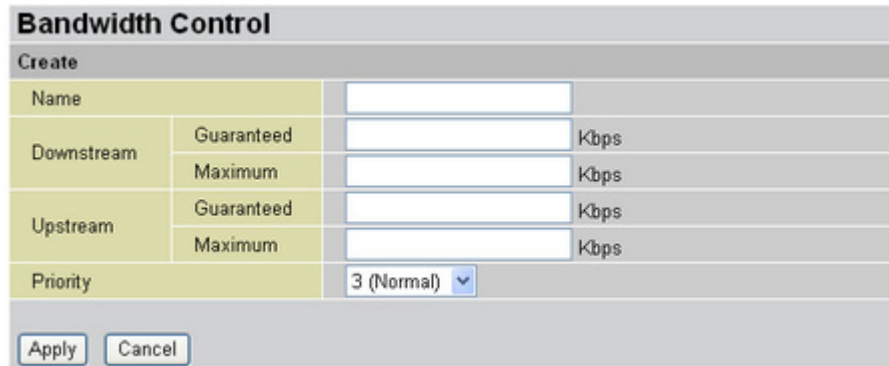
FIGURE 48 BANDWIDTH CONTROL TABLE



Bandwidth control is used in conjunction with QoS functions. Bandwidth Network Objects are selected when setting QoS parameters.

Click **Create** to add a new bandwidth Network Object to the **Bandwidth Control Table**.

FIGURE 49 ADDING A BANDWIDTH CONTROL NETWORK OBJECT



| | |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name for this bandwidth control Network Object. |
| Downstream | Type values for the downstream bandwidth in the text boxes in kilobits per second. <ul style="list-style-type: none"> Guaranteed: type a value that defines the lower limit for downstream bandwidth. Maximum: type a value that defines the upper limit for downstream bandwidth. |
| Upstream | Type values for the upstream bandwidth in the text boxes in kilobits per second. <ul style="list-style-type: none"> Guaranteed: type a value that defines the lower limit for upstream bandwidth. Maximum: type a value that defines the upper limit for upstream bandwidth. |
| Priority | Select the priority to be assigned to this bandwidth control item from the drop-down menu, from 0 (highest) to 6 (lowest). The default is 3 (normal). The value selected here determines which items in the bandwidth control table get priority over the others for bandwidth access. |

Click **Apply** to confirm the settings.

Setting Content Blocking parameters

Content blocking enables you to create filters that disable users from accessing prohibited content. You can create keyword and domain filters, and restrict URL features.

Click **Content Blocking** to display content blocking menu items.

CREATING KEYWORD FILTER NETWORK OBJECTS

Click **Keyword Filtering** to display the keyword filter profile list.

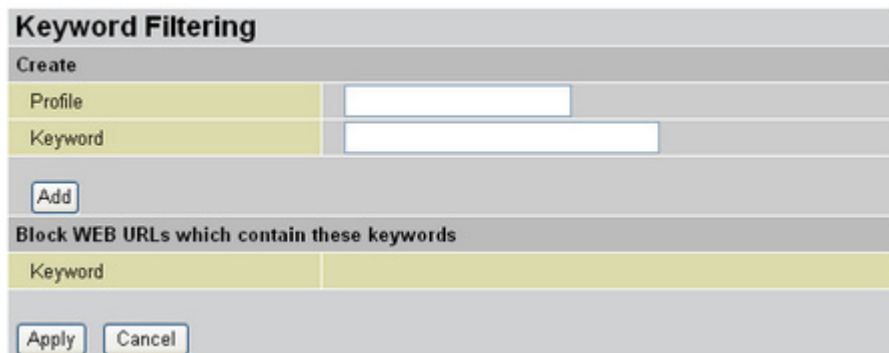
FIGURE 50 KEYWORD FILTER PROFILES



Keyword filters prohibit users from accessing Web sites that contain words specified in these profiles.

Click **Create** to add a new Network Object profile.

FIGURE 51 ADDING A KEYWORD FILTER NETWORK OBJECT PROFILE



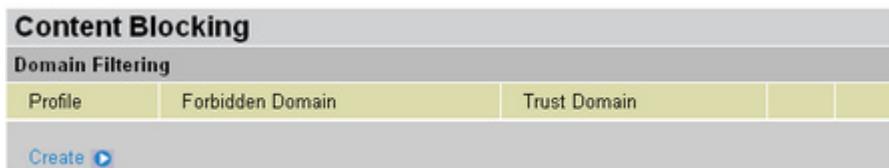
| | |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profile | Type the name of this Network Object profile |
| Keyword | Type the keyword to be filtered and click Add to add this to the content filtering keyword list. The word is displayed under Block WEB URLs which contain these keywords . |

Click **Apply** to confirm the settings.

CREATING DOMAIN FILTER NETWORK OBJECTS

Click **Domain Filtering** to display the domain filter profile list.

FIGURE 52 DOMAIN FILTER PROFILES



Domain filters prohibit users from accessing specific domains (such as .ORG, .COM, or .GOV). Click **Create** to add a new filter Network Object profile.

FIGURE 53 ADDING A DOMAIN FILTER NETWORK OBJECT PROFILE

| | |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profile | Type the name of this profile. |
| Domain | Type the domain to be added to the forbidden or trusted domain lists. |
| Type | Select the domain type from the drop-down menu. <ul style="list-style-type: none"> • Forbidden Domain: users will not be allowed access to Web sites in this domain. Select this and click Add to add the domain to the Block WEB URLs which contain these domains list. • Trusted Domain: users will be allowed access to Web sites in this domain. Select this and click Add to add the domain to the UnBlock WEB URLs which contain these domains list. |

Click **Apply** to confirm the settings.

CREATING RESTRICT URL FEATURES NETWORK OBJECTS

Click **Restrict URL Features** to display the Restrict URL Feature list.

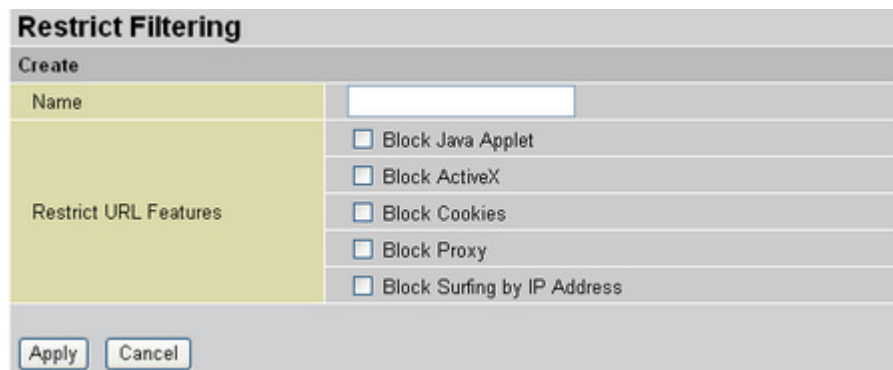
FIGURE 54 RESTRICT URL FEATURES NETWORK OBJECT LIST



The Restrict URL Feature screen enables you to prohibit browser features that constitute a security threat (such as cookies, Java applets, and ActiveX scripts) from being used.

Click **Create** to add a new Network Object profile.

FIGURE 55 RESTRICTING URL FEATURES



| | |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name for this profile. |
| Restrict URL Features | <p>Check which URL features you want disabled.</p> <ul style="list-style-type: none"> • Block Java Applet • Block ActiveX • Block Cookies • Block Proxy • Block Surfing by IP Address |

Click **Apply** to confirm the settings.

Setting Policy parameters

Click **Policy** to set up packet filtering, the virtual server, and Ethernet MAC and content filtering.

Enabling Packet Filtering

Click **Packet Filtering** to display a list of packet filter items.

FIGURE 56 PACKET FILTERING TABLE

| Packet Filtering | | | | | | | | | |
|------------------|------|--------|------|--------|---------|------|----|----------|--|
| Parameters | | | | | | | | | |
| # | Name | Active | Flow | Action | Service | From | To | Schedule | |
| Create ▶ | | | | | | | | | |

Packet filtering enables you to restrict types of data from being transmitted over the network. Click **Create** to add a new parameter to the list.

FIGURE 57 CREATING A PACKET FILTERING PROFILE

| Packet Filtering | |
|----------------------------------------------------------------------------|-------------------------------------------------------|
| Create | |
| Name | <input type="text"/> |
| Active | <input checked="" type="checkbox"/> Enable |
| Packet Flow | LAN to WAN <input type="checkbox"/> Reverse Direction |
| Action | Drop <input type="button" value="v"/> |
| Service | **Any <input type="button" value="v"/> |
| From Address | **Any <input type="button" value="v"/> |
| To Address | **Any <input type="button" value="v"/> |
| Schedule | **Always On <input type="button" value="v"/> |
| Log | <input type="checkbox"/> Enable |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

| | |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name for this profile. |
| Active | Check Enable to make this profile active. |
| Packet Flow | <p>Select the packet flow direction from the drop-down menu.</p> <ul style="list-style-type: none"> LAN to WAN: filters packets being transmitted to the WAN from the LAN. WAN to LAN: filters packets being transmitted to the LAN from the WAN. <p>Check Reverse Direction to apply the same rule with reverse packet flow. (i.e., both directions)</p> |
| Action | <p>Select the action to be applied to the packets from the drop-down menu.</p> <ul style="list-style-type: none"> Drop: discards the packets. Forward: sends the packets to a specified address. |
| Service | Select which services this filter will be applied to from the drop-down menu. |

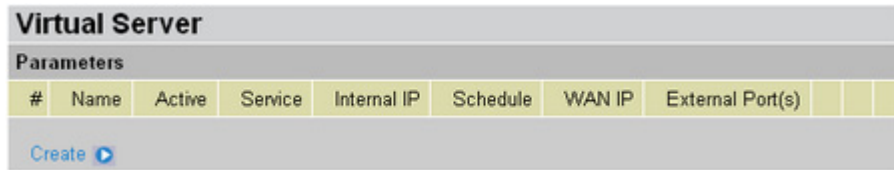
| | |
|--------------|-------------------------------------------------------------------------------------------|
| From Address | Select the origin IP address this filter will be applied to from the drop-down menu. |
| To Address | Select the destination IP address this filter will be applied to from the drop-down menu. |
| Schedule | Select the schedule for when you want this profile to be applicable. |
| Log | Check Enable to have the system create a log file when this filter is run. |

Click **Apply** to confirm the settings.

Configuring the Virtual Server

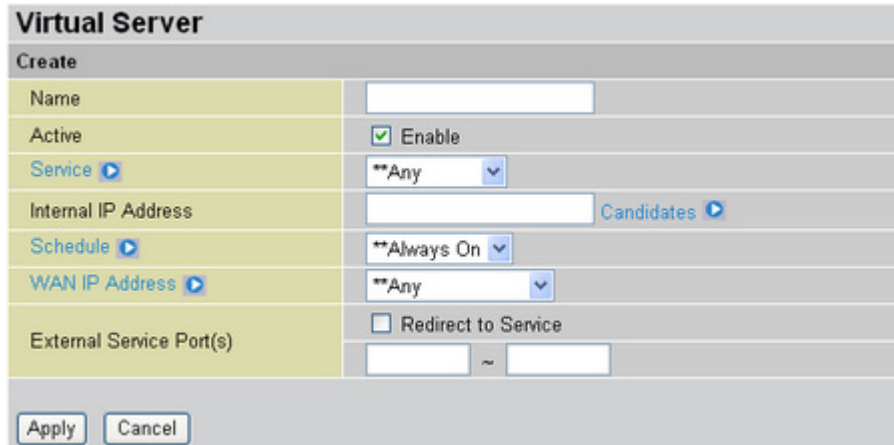
Click **Virtual Server** to view a list of virtual servers and their parameters.

FIGURE 58 VIRTUAL SERVER PARAMETERS



Click **Create** to add a virtual server profile to the list.

FIGURE 59 ADDING A VIRTUAL SERVER



| | |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name of the virtual server. |
| Active | Click Enable to activate this virtual server. |
| Service | Select the service you want to assign to this virtual server. |
| Internal IP Address | Type the IP address you want to assign to the virtual server or click Candidates to see a list of available internal IP addresses you can assign. |
| Schedule | Select the schedule for this virtual server to be active from the drop-down menu. |
| WAN IP Address | Select the WAN IP address from the drop-down menu. |

External Service Port(s) Check **Redirect to Service** if you need to use port redirecting instead of port forwarding and type the range of ports to assign to the virtual server.

Click **Apply** to confirm the settings.

Configuring Quality of Service (QoS) parameters

Click **QoS** to view a list of QoS items and parameters.

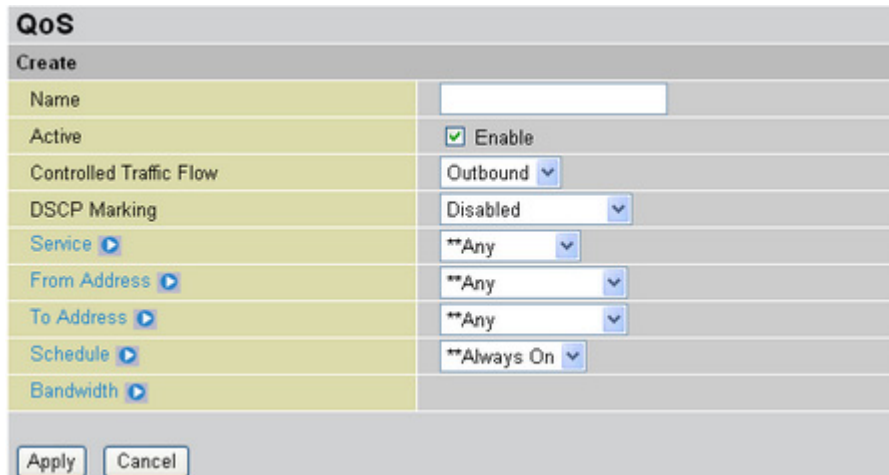
FIGURE 60 QoS PARAMETERS



QoS refers to a defined level of performance in a data communications system for assigned applications. Since some applications such as realtime voice and video need a guaranteed bandwidth to function properly, QoS can ensure that this bandwidth is provided.

Click **Create** to add a new QoS profile.

FIGURE 61 ADDING A QoS PROFILE



| | |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name for this QoS item. |
| Active | Check Enable to activate this QoS profile. |
| Controlled Traffic Flow | Select an option from the drop-down menu. <ul style="list-style-type: none"> • Outbound: QoS profile only applies to outbound traffic • Inbound: QoS profile only applies to inbound traffic |

| | |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DSCP Marking | DSCP Marking, also known as DiffServ enables you to classify traffic based on IP DSCP values. These values can be used to identify traffic within the network. Other interfaces can match traffic based on the DSCP markings. DSCP markings are used to decide how packets should be treated, and is a useful tool to give precedence to varying types of data in QoS scenarios. Select an option from the drop-down menu. The options include Disabled, and various levels of QoS from Bronze to Premium . |
| Service | Select the service you want to assign to this QoS. |
| From Address | Select the origin IP address. |
| To Address | Select the destination IP address. |
| Schedule | Select the schedule for this QoS item to be active from the drop-down menu. |
| Bandwidth | Select a bandwidth Network Object from the Bandwidth drop-down menu. If you have not created bandwidth Network Objects, click Bandwidth to open the Bandwidth Control screen and define bandwidth parameters. (See Managing Bandwidth Network Objects on page 49.) |

Click **Apply** to confirm the settings.

Configuring Ethernet MAC Filtering

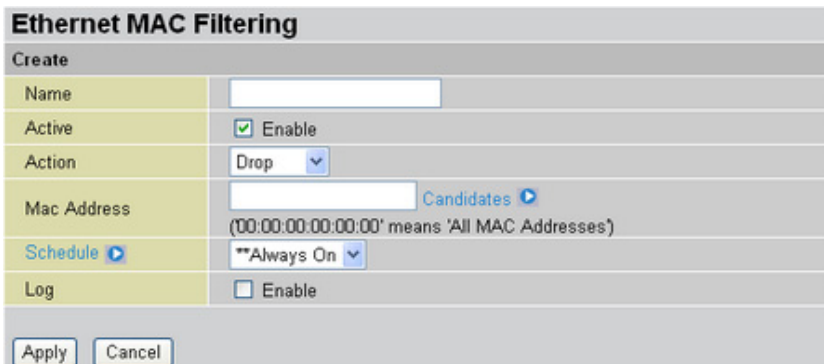
Click **Ethernet MAC Filtering** to view the Ethernet MAC Filtering profile screen.

FIGURE 62 ETHERNET MAC FILTERING PROFILES



Ethernet MAC filtering enables you to prevent Ethernet MAC addresses from being accessed. Click **Create** to add a new Ethernet MAC filter.

FIGURE 63 ADDING AN ETHERNET MAC FILTER



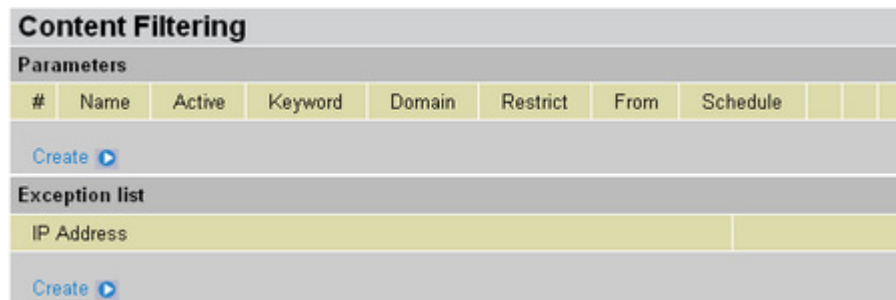
| | |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type a name for the Ethernet MAC filter. |
| Active | Check Enable to activate the filter. |
| Action | Select an action from the drop-down menu. <ul style="list-style-type: none"> • Drop: discards the packets. • Forward: sends the packets to a specified address. |
| Mac Address | Type the MAC address you want to assign to the filter or click Candidates to see a list of available MAC addresses you can assign. |
| Schedule | Select the schedule for this filter to be active from the drop-down menu. |
| Log | Check Enable if you want a log file to be created when this filter is activated. |

Click **Apply** to confirm the settings.

Configuring Content Filtering policies

Click **Content Filtering** to configure content filtering.

FIGURE 64 CONFIGURING CONTENT FILTERING POLICIES



Content filtering policies enable and disable keyword filtering, domain filtering, and restricted URL feature profiles. You can define these parameters now or use parameters that are already defined in Network Objects under Content Blocking.

You can also create an IP address exception list, which allows specified IP addresses to be accessed.

SETTING CONTENT FILTERING PARAMETERS

Under **Parameters**, click **Create** to set up a new content filtering profile.

FIGURE 65 CREATING A CONTENT FILTERING PROFILE



NOTE: YOU MUST FIRST SET UP KEYWORD FILTERING, DOMAIN FILTERING, AND RESTRICT URL FEATURE PROFILES BEFORE YOU CAN ENABLE THESE ITEMS IN THIS SCREEN.

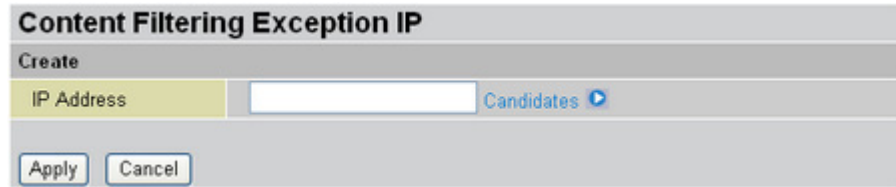
| | |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type a name to be given to this profile. |
| Active | Check Enable to activate this profile. |
| Keywords Filtering | Check Enable to activate keyword filtering and select a Keyword Filtering Network Object from the drop-down menu. (See Creating Keyword Filter Network Objects on page 50.) |
| Domains Filtering | Check Enable to activate domain filtering and select a Domain Filtering profile from the drop-down menu. (See Creating Domain Filter Network Objects on page 50.) Check Disable all WEB traffic except for Trusted Domains to only allow those domains that have been designated as trusted to have access. |
| Restrict Feature | Check Enable to activate the Restrict URL Feature and select a Restrict URL Feature profile from the drop-down menu. (See Creating Restrict URL Features Network Objects on page 52.) |
| From Address | Select the IP address which this filter will apply to from the drop-down menu. |
| Schedule | Select the schedule for this filter to be active from the drop-down menu. |
| Log | Check Enable if you want a log file to be created when this filter is activated. |

Click **Apply** to confirm the settings.

CREATING A CONTENT FILTERING EXCEPTION IP PROFILE

You can exclude specified IP address from the Content Filtering profiles you have set up. Click **Create** under the **Exception List** to add an IP address exception.

FIGURE 66 ADDING AN IP EXCEPTION



Type in the IP address or click **Candidates** and select from available internal IP addresses. Click **Apply** to add the IP address to the exception list.

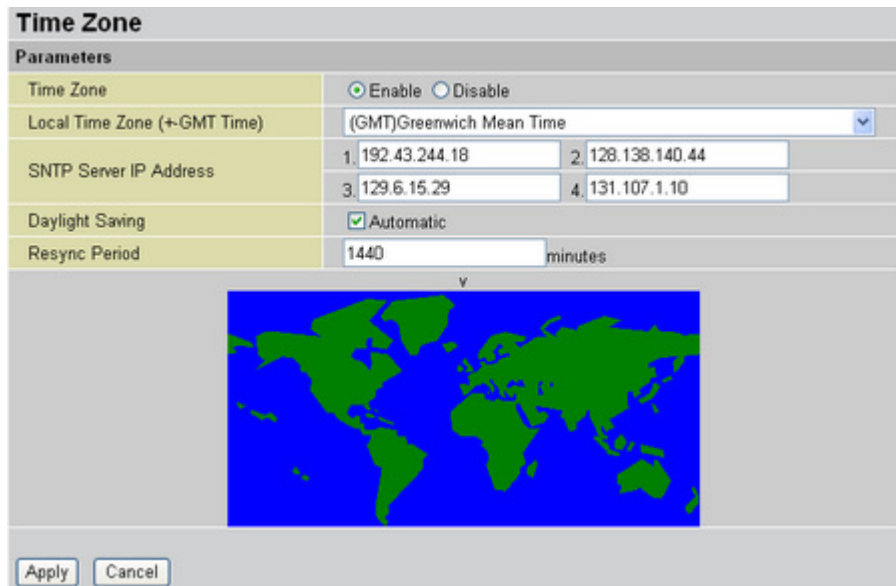
Configuring the System

Use the System menu to set the time zone, configure remote access, set up passwords, upgrade the BiGuard S10 firmware, backup and restore configuration profiles, and restart the system.

Setting the Time Zone

Click **Time Zone** to open the Time Zone screen.

FIGURE 67 SETTING THE TIME ZONE



| | |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Zone | Click Enable to allow the BiGuard S10 to automatically update the time from the network time server. Click Disable to disable automatic updates. |
| Local Time Zone | Select your time zone from the drop-down menu. The time zone is set according to Greenwich Mean Time (GMT). |
| SNTP Server IP Address | Type the IP address or URL (for example <i>time.windows.com</i>) of the SNTP (Simple Network Time Protocol) server. |

| | |
|-----------------|-------------------------------------------------------------------------------------------|
| Daylight Saving | Check this box to allow the BiGuard S10 to automatically adjust for daylight saving time. |
| Resync Period | Type the number of minutes that will elapse before the BiGuard S10 adjusts the time. |

Enabling Remote Access

Click **Remote Access** to enable the remote access feature.

FIGURE 68 ENABLING REMOTE ACCESS

Remote Access Control Select the remote access scenario you want from the list.

Remote Address Select the remote IP address which will be allowed access from the drop-down menu.



WARNING: IT'S RECOMMENDED IF YOU ALLOW REMOTE CONFIGURATION, THAT YOU CONFIGURE IT ONLY FOR A SPECIFIC IP ADDRESS. THE SPECIFIED IP ADDRESS SHOULD ONLY BE AVAILABLE TO YOUR ADMINISTRATOR. SEE [Modifying the Network Extender IP address range](#) ON PAGE 77.

Upgrading the BiGuard S10 Firmware

Periodic firmware updates are available from the BiGuard registration web site: www.biguard.com.

Click **Firmware Upgrade** to upgrade the firmware.

FIGURE 69 UPGRADING THE FIRMWARE

To upgrade the firmware:

1. Download the firmware image from the company Web site.
2. Click **Factory Default Settings** or **Current Settings** to determine how the router will restart after the upgrade.
3. Click **Browse** to go to the location of the downloaded image.
4. Click **Upgrade** to apply the firmware patch.
5. Do **NOT** perform any more actions while the firmware is being upgraded.



WARNING: IT'S RECOMMENDED THAT YOU ALLOW THE FIRMWARE TO COMPLETELY UPGRADE BEFORE ATTEMPTING TO USE THE **BiGuard S10**. ANY INTERRUPTION DURING THE UPGRADE PROCESS (INCLUDING POWER LOSS) MAY RENDER THE DEVICE INOPERABLE.

Backing up and restoring configurations

You can back up different configurations and restore them for flexible network management.

Open the Backup/Restore page by clicking on the **Backup/Restore** button, then select backup all configurations or select only certain objects to your computer. Next click the **Backup** to save your configuration.

FIGURE 70 BACKING UP AND RESTORING CONFIGURATIONS

Backup/Restore
Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Backup Configuration

Backup all configuration to your computer.
 Export the checked objects to your computer

| | | | |
|----------------|-------------------------------------------------|--------------------------------------------|-------------------------------------------------|
| Network Object | <input type="checkbox"/> Address/Group | <input type="checkbox"/> Service/Group | <input type="checkbox"/> Schedule |
| | <input type="checkbox"/> Keyword Filtering | <input type="checkbox"/> Domains Filtering | <input type="checkbox"/> Restrict URL Filtering |
| | <input type="checkbox"/> Bandwidth Control | | |
| Policy | <input type="checkbox"/> Packet Filtering | <input type="checkbox"/> Virtual Server | <input type="checkbox"/> Qos |
| | <input type="checkbox"/> Ethernet MAC Filtering | <input type="checkbox"/> Content Filtering | |
| SSL VPN | <input type="checkbox"/> Certificate | <input type="checkbox"/> User Access | |

Restore Configuration

Configuration File

"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.

To restore configurations, click the **Browse** button to select your backup file. The file address will display in the Configuration File text box. Then click **Restore** to use the backup configurations.



NOTE: YOU MUST CLICK THE **SAVE CONFIG** BUTTON ON THE BOTTOM OF THE SCREEN TO MAKE YOUR CURRENT CONFIGURATION PERMANENT, SEE [Restoring a saved configuration ON PAGE 62](#).

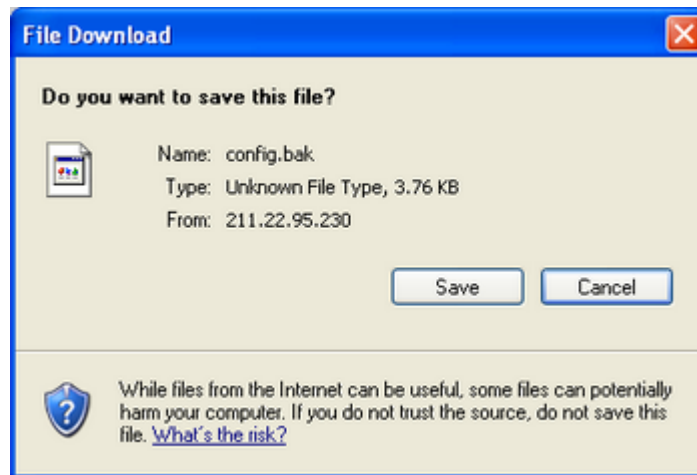
NOTE: TO RESTORE YOUR CONFIGURATIONS. YOU MUST HAVE AN EXISTING BACKUP FILE BEFORE STARTING.

BACKING UP THE CONFIGURATION

You can choose between two backup scenarios.

| | |
|----------------------------|------------------------------------------------------------------------------------------------------------------------|
| Backup all configuration | Click Backup all configuration to your computer to save all current configuration information to the computer. |
| Export the checked objects | Click Export the checked objects to your computer and then check which items you want to include in the backup. |

After you have made your selection, click **Backup** to begin. You are prompted to save the backup file to your computer.

FIGURE 71 BACKING UP A CONFIGURATION**RESTORING A SAVED CONFIGURATION**

To restore a saved configuration, click **Browse** and go to the location of the configuration file. Click **Restore** to begin restoring the configuration.

FIGURE 72 RESTORING A CONFIGURATION

Wait for the router to restart before performing any actions.

Configuring and changing passwords

Select Password to change the password needed to access the BiGuard S10 web configuration interface.

FIGURE 73 CHANGING PASSWORDS

| Password | |
|----------------------------------------------------------------------------|-------|
| Parameters | |
| User Name | admin |
| Password | ***** |
| Retype Password | ***** |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

Type the new password in the Password text box. Retype the password to confirm and click **Apply** to save the new password.

Restarting the system

Click **Restart** to view the Restart screen.

FIGURE 74 RESTARTING THE SYSTEM

| Restart | |
|------------------------------------------------------------------------------|---------------------------------------------------|
| After restarting. Please wait for several seconds to let the system | |
| Restart Router with | <input type="radio"/> Save Config to Flash |
| | <input checked="" type="radio"/> Current Settings |
| | <input type="radio"/> Factory Default Settings |
| <input type="button" value="Restart"/> <input type="button" value="Cancel"/> | |

You can restart the system using the following options:

- Save Config to Flash: saves any recent configuration changes to flash before restarting.
- Current Settings: restarts using the last saved configuration.
- Factory Default Settings: restarts using factory default settings.

Click **Restart** to restart the system with the selected option.

Configuring Advanced Features

The Advanced Features menu enables you to set up static routing, configure DDNS (dynamic domain name server) settings, set up the firewall and SNMP (simple network management protocol), and manage device settings.

Creating Static Routes

Click **Static Route** to view the Static Routing List.

FIGURE 75 THE STATIC ROUTING LIST

| Static Route | | | | | | |
|---------------------|-------|-------------|---------|-------------------|--|--|
| Static Routing List | | | | | | |
| # | Valid | Destination | Netmask | Gateway/Interface | | |
| Create | | | | | | |

Click **Create** to add a new static route to the list.

FIGURE 76 ADDING A STATIC ROUTE

| Static Route | |
|----------------------------------------------------------------------------|----------------------|
| Create | |
| Destination | <input type="text"/> |
| Netmask | <input type="text"/> |
| Gateway | <input type="text"/> |
| Interface | Please Select |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

| | |
|-------------|-------------------------------------------------------|
| Destination | Type the destination IP address for the static route. |
|-------------|-------------------------------------------------------|

| | |
|---------|--------------------------------------------------------------|
| Netmask | Type the netmask associated with the destination IP address. |
|---------|--------------------------------------------------------------|

| | |
|---------|------------------------------|
| Gateway | Type the IP address gateway. |
|---------|------------------------------|

| | |
|-----------|-----------------------------------------------------------|
| Interface | Select the appropriate interface from the drop-down menu. |
|-----------|-----------------------------------------------------------|

Enabling Dynamic DNS

Click **Dynamic DNS** to enable and disable Dynamic DNS (DDNS).

FIGURE 77 ENABLING DDNS

The screenshot shows a 'Dynamic DNS' configuration window. Under the 'Parameters' section, the 'Dynamic DNS' option is selected, and the 'Disable' radio button is chosen. There are 'Apply' and 'Cancel' buttons at the bottom.



NOTE: YOU NEED TO REGISTER AND ESTABLISH AN ACCOUNT WITH THE DYNAMIC DNS PROVIDER USING THEIR WEB SITE BEFORE USING DDNS. THE BIGUARD S10 SUPPORTS SEVERAL DYNAMIC DNS PROVIDERS.

Click **Enable** to open a screen which allows you to set DDNS parameters.

FIGURE 78 SETTING DDNS PARAMETERS

The screenshot shows the 'Dynamic DNS' configuration window with the following settings: 'Dynamic DNS' is set to 'Enable'; 'Dynamic DNS Server' is set to 'www.dyndns.org (dynamic)'; 'Wildcard' is set to 'Enable'; 'Domain Name', 'User Name', and 'Password' fields are empty; 'Retype Password' field is empty; and 'Period' is set to '28' with 'Day(s)' selected in the dropdown menu. 'Apply' and 'Cancel' buttons are at the bottom.

| | |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dynamic DNS Server | Select a DDNS server from the drop-down menu. |
| Wildcard | Click Enable to allow the DDNS wildcard. The Wildcard Alias enables you to point a URL (*.yourdomain.com - set in the Domain Name field) to your dynamic IP address. |
| Domain Name | Type the domain name for the DDNS server. |
| Username | Type the username for accessing the DDNS server. |
| Password | Type the password for accessing the DDNS server. |
| Retype Password | Retype the password for confirmation. |
| Period | Type the period of time and select the units (days or hours) from the drop-down menu. |

Configuring SNMP

Click **SNMP** to enable and disable Simple Network Management Protocol.

FIGURE 79 ENABLING SNMP

The screenshot shows a configuration window titled 'SNMP'. Under the 'Parameters' section, there is a row for 'SNMP' with two radio buttons: 'Enable' (which is selected) and 'Disable'. At the bottom of the window are 'Apply' and 'Cancel' buttons.

Click **Enable**. A screen appears allowing you to set SNMP parameters.

FIGURE 80 SETTING SNMP PARAMETERS

The screenshot shows a configuration window titled 'SNMP'. Under the 'Parameters' section, there is a row for 'SNMP' with two radio buttons: 'Enable' (which is selected) and 'Disable'. Below this, there are three sections: 'SNMP V1 and V2', 'SNMP V3', and 'Access Right'. The 'SNMP V1 and V2' section has three rows: 'Read Community' with 'public' in the text box and '0.0.0.0' in the IP Address box; 'Write Community' with 'password' in the text box and '0.0.0.0' in the IP Address box; and 'Trap Community' with an empty text box and an empty IP Address box. The 'SNMP V3' section has two rows: 'User Name' with an empty text box and 'Password' with an empty text box; and 'Access Right' with two radio buttons: 'Read' (which is selected) and 'Read/Write'. At the bottom of the window are 'Apply' and 'Cancel' buttons.

SNMP V1 and V2 This section enables you to set parameters for SNMP versions 1 and 2. The following information is entered:

- **Read Community:** type the name of the read community and the IP address associated with it.
- **Write Community:** type the name of the write community and the IP address associated with it.
- **Trap Community:** type the name of the trap community and the IP address associated with it.

SNMP V3 This section enables you to set parameters for SNMP version 3. The following information is entered:

- **Username and Password:** type the user name and password for accessing SNMP sites.
- **Access Right:** click **Read** if you only want users to have read access rights. Click **Read/Write** if you want users to have read and write access rights.

Configuring Firewall Parameters

Click **Firewall** to set firewall parameters.

FIGURE 81 CONFIGURING THE FIREWALL

| Firewall | |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Parameters | |
| Intrusion Detection | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Block WAN Request | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

Intrusion Detection Click **Enable** to activate intrusion detection.

Block WAN Request Click **Enable** to activate the Block WAN Request feature.

Managing Device Parameters

Click **Device Management** to change device parameters.

FIGURE 82 CHANGING PARAMETERS

| Device Management | | |
|----------------------------------------------------------------------------|---------------------------------------------|-----------------------------|
| Device Name | | |
| Name | <input type="text" value="SSLVPN.gateway"/> | |
| Embedded Web Server | | |
| HTTP Port | <input type="text" value="80"/> | (80 is default HTTP port) |
| HTTPS Port | <input type="text" value="443"/> | (443 is default HTTPS port) |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | |

Device Name Type the name for the BiGuard S10.

Embedded Web Server Type the port number for the HTTP and HTTPS ports.

Configuring SSL VPN Parameters

This chapter covers the configuration of SSL VPN parameters, including setting user accounts and assigning users to groups, creating applications for the groups, and authenticating domains. Other topics include assigning the client IP address range for the Network Extender, setting applications and the host name resolution for the Transport Extender, and importing and enabling SSL certificates. You can also launch the SSL VPN portal from the SSL VPN menu.

Configuring User Access menus

Use the User Access menu to add authenticated domains to the domain table, establish groups and assign applications to the groups, and create user accounts.

Portal Layout

The Portal Layout is provided to create a personalized layout, including portal banner and the default greeting text string. To use the Portal Layout features, click on **Portal Layout** under the User Access menu. Then select the default logo or change to a new logo by selecting the **Uploaded Logo** option, and click Browse to choose your image or icon. Next, click the **Apply** button.

The default greeting string can also be changed. Just type the desired text string into the Default Greeting String, and click the **Apply** button.

FIGURE 83 PORTAL LAYOUT

Authentication Domain

The **Authentication Domain** item enables you to add domains to the domain table that will be authenticated by the server. The BiGuard S10 verifies that users who log on to the system are in an authenticated domain.

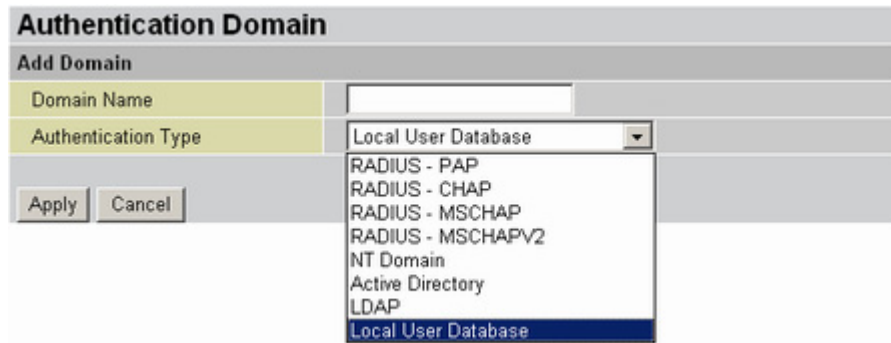
Click **Authentication Domain** to view the **Authentication Domain Table**.

FIGURE 84 AUTHENTICATION DOMAIN TABLE

| Authentication Domain | | | | |
|-----------------------|---------------------|-------------------------|--------------------------|----------|
| Domain Table | | | | |
| Domain Name | Authentication Type | Auth. Server IP Address | | |
| BiGuard | local | Local Machine | Machine's Default Domain | |
| BIGUARD-JANE | local | Local Machine | Edit ▶ | Delete ▶ |
| Create ▶ | | | | |

Click **Create** to add a new domain. The **Add Domain** screen appears.

FIGURE 85 DOMAIN AUTHENTICATION TYPES SCREEN



| | |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain Name | Type a name for the domain. |
| RADIUS - PAP | PAP (Password Authentication Protocol) is an access control protocol for dialing into a network that provides only basic functionality. Passwords are sent over the line unencrypted from the client, it provides password checking, but is not secure from eavesdropping. |
| RADIUS - CHAP | MSCHAP (Microsoft Challenge Handshake Authentication Protocol) is an access control protocol for dialing into a network that provides a moderate degree of security. The CHAP server encrypts the challenge with the password stored in its database for the user and matches its results with the response from the client. If they match, it indicates the client has the correct password, but the password itself never leaves the client's machine. |
| RADIUS - MSCHAP | MSCHAP (Microsoft Challenge Handshake Authentication Protocol) is Microsoft's version of CHAP and provides authentication for PPP connections between a Windows-based computer and an Access Point or other network access device. |
| RADIUS - MSCHAPV2 | MSCHAPV2 (Microsoft Challenge Handshake Authentication Protocol) is Microsoft's second version of CHAP. |
| NT Domain | Select this item if you the domain is being used on a Windows NT server. |
| Active Directory | Active Directory is an advanced, LDAP compliant, hierarchical directory service that comes with Windows 2000 servers. Because it is built on the Internet's Domain Naming System (DNS), workgroups can be given domain names, just like Web sites, and any LDAP-compliant client (Windows, Mac, Unix, etc.) can gain access to it. Active Directory can function in a heterogeneous, enterprise network and encompass other directories including NDS and NIS+. |
| LDAP | LDAP (Lightweight Directory Access Protocol) is a directory listing access protocol. LDAP support is being implemented in Web browsers and e-mail programs, which can query an LDAP-compliant directory. LDAP is a sibling protocol to HTTP and FTP and uses the ldap:// prefix in its URL. LDAP is a simplified version of the DAP protocol, which is used to gain access to X.500 directories. It is easier to code the query in LDAP than in DAP, but LDAP is less comprehensive. |

| | |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local User Database | Choose this option to have authentication performed by checking names in a local user database. Local Database stores the user's data in the BiGuard S10, for the users that do not have any Authentication Domain in their environment. |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



NOTE: RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE) IS THE DE FACTO STANDARD PROTOCOL FOR AUTHENTICATION SERVERS (AAA SERVERS). RADIUS USES A CHALLENGE/RESPONSE METHOD FOR AUTHENTICATION.

Group/Application

This menu item enables you to establish groups and assign allowed applications to the group. When you create a group, you assign the group to an authenticated domain, and then add only the applications that you want group members to access.

Click **Group/Application** to view the **Group Table**.

FIGURE 86 GROUP/APPLICATION TABLE SCREEN

| Group/Application | | | | |
|------------------------|-----------------------|------------------------|----------------------|--|
| Group Table | | | | |
| Name | Authentication Domain | Domain's Default Group | | |
| ftp1 | ftp1 | Yes | Edit | |
| BiGuard | BiGuard | Yes | Edit | |
| Create | | | | |

Figure 86 shows the current groups that have been created, the domain to which the group has been assigned, and whether group is the domain's default group.

To edit a current group, click **Edit**. To create a new group, click **Create**.

CREATING A NEW GROUP

Refer to the following to create a new group:

1. In the Group/Application table (Figure 86), click **Create**. The **Add Group** screen appears.

| Add Group | | | |
|----------------------------------------------|---------------------------------|-------------------|--|
| General Settings | | | |
| Group Name | <input type="text"/> | | |
| Domain | BiGuard | | |
| Application Table | Add Application | | |
| Name | Application | IP Address / Path | |
| | | | |
| Apply Cancel | | | |

2. Type a descriptive name for the group in the **Group Name** field.
3. Select the domain that the group will belong to from the **Domain** drop-down menu.
4. Click **Add Application** to make applications available to the group.

| SSL VPN Application | |
|----------------------------------------------|--------------------------------------|
| Add Application | |
| Application Name | <input type="text"/> |
| Application | Terminal Service (RDP5) |
| IP Address | <input type="text"/> |
| Screen Size | 640 x 480 |
| | 640 x 480 800 x 600 1024 x 768 |
| Apply Cancel | |

5. Type a name in the **Application Name** field.
6. Select an application from the **Application** drop-down menu. See [SSL VPN Applications Overview](#) on page 72.
7. Click **Apply** to confirm the settings.

SSL VPN Applications Overview

The SSL Applications menu item enables you to add applications to be made available to users, and to define application parameters such as the type of application assigned and the IP address.



NOTE: THE APPLICATION NAME YOU CHOOSE CAN BE THE SAME AS THE NAME OF THE APPLICATION ITSELF. OR YOU CAN CHOOSE MORE DESCRIPTIVE OR SHORTENED NAMES.

The **SSL VPN Application** screen lets you add the following applications:

FIGURE 87 SSL VPN APPLICATION CHOICES

| | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Terminal Service (RDP5) | Windows Terminal Server enables an application to be run simultaneously by multiple users at different Windows PCs. Microsoft's RDP (Remote Desktop Protocol) is its native protocol, which works only with Windows clients. RDP5 (ActiveX) - RDP5 is the current version and provides session sound and full-screen mode. RDP5 is only available in an ActiveX client. |
| Virtual Network Computing (VNC) | VNC open source software can be installed on most server or workstations for remote access. When the remote user wants to access the server, the VNC client is delivered through the user's Web browser as a Java client. |
| File Transfer Protocol (FTP) | The FTP protocol is used to transfer files over a TCP/IP network (Internet, Unix, etc.). FTP includes functions to log onto the network, list directories and copy or upload files. FTP operations can be performed by typing commands at a command prompt or via an FTP utility running under a graphical interface such as Windows. |
| Telnet | Telnet is a terminal emulation protocol commonly used on the Internet and TCP/IP-based networks. It allows a user at a terminal or PC to log onto a remote computer and run a program from the command line. |
| Secure Shell (SSH) | SSH (Secure SHell) provides secure logon for Windows and Unix clients and servers. SSH replaces telnet, FTP and other remote logon utilities with an encrypted alternative, and allows a user at a terminal or PC to log onto a remote computer and run a program from the command line. |
| Web (HTTP) | Web browsers communicate with Web servers using TCP/IP protocol. The browser sends HTTP requests to the server, which responds by returning headers (a record sent by clients and servers communicating with each other via the HTTP protocol) and files (HTML pages, Java applets, etc.). |

| | |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Web (HTTPS) | HTTPS (HyperText Transport Protocol Secure) is the protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The session is then managed by a security protocol such as SSL. |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

ADDING THE TERMINAL SERVICE (RDP5) APPLICATION

Refer to the following to add the application:

1. Type a name in the **Application Name** field.

The screenshot shows the 'SSL VPN Application' dialog box with the 'Add Application' section. The 'Application' dropdown menu is open, displaying a list of screen resolutions: 640 x 480, 800 x 600, 1024 x 768, and Full-screen. The 'Full-screen' option is currently selected. Other fields include 'Application Name', 'IP Address', and 'Screen Size'.

2. Select **Terminal Service (RDP5)** from the **Application** drop-down list.
3. Type the IP address in the **IP Address** field.
4. Select a screen resolution from the **Screen Size** drop-down menu. The first three items appear in a window. Full-screen adjusts the screen to the maximum size of the display.
5. Click **Apply** to confirm the settings.



NOTE: DIFFERENT USERS MAY HAVE THEIR SCREEN RESOLUTION SET DIFFERENTLY.

ADDING OTHER LISTED APPLICATIONS

All the other applications have the same screen field items. Refer to the following to add any of the other listed applications:

1. Type a name in the **Application Name** field.

The screenshot shows the 'SSL VPN Application' dialog box with the 'Add Application' section. The 'Application' dropdown menu is open, displaying the option 'Virtual Network Computing (VNC)'. Other fields include 'Application Name', 'IP Address', and 'Screen Size'.

2. Select an item from the **Application** drop-down list.
3. Type the IP address in the **IP Address** field.
4. Click **Apply** to confirm the settings.

Managing accounts

The **Accounts** menu item enables you to create user accounts and assign users to groups created in the **Groups/Applications** menu. You can enable and disable access to services such as the Network Extender and Transport Extender, and enable or disable access to applications assigned to the group.

The BiGuard S10 ships with a default Group (BiGuard) and a default account (admin) already set up. All accounts including the admin account are managed from the **Account** screen.

FIGURE 88 ACCOUNT MANAGEMENT SCREEN

| Account | | | |
|---------------|---------|--------|--|
| Account Table | | | |
| Name | Group | | |
| admin | BiGuard | Edit ▶ | |
| Create ▶ | | | |

The **Account Table** shows the account name and the group the user belongs to. You can create and edit account from this screen. To view details for an account, click **Edit**, and then exit the **Edit Account** screen by clicking **Cancel**.

EDITING THE ADMIN ACCOUNT

Click **Edit** in the Account screen to view account settings for the admin account.

FIGURE 89 ADMIN ACCOUNT SETTINGS SCREEN

| Edit Account | |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| General Setting | |
| Name | admin |
| Group | BiGuard |
| Password | •••••• |
| Retype Password | •••••• |
| Inactivity Timeout | 5 Minutes |
| Service | |
| Network Places | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Network Extender Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Transport Extender Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Web Cache Cleaner | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Network Extender IP Assignment | <input checked="" type="radio"/> Dynamic Assign <input type="radio"/> Fix IP 192.168.1.240 |
| Greeting String | Welcome to SSL VPN Se |
| Application Proxy | |
| Applications | This group has no application now. |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

| | |
|------|------------------------------------------------------------------------------------|
| Name | Displays the name of the account. You cannot change the name of the admin account. |
|------|------------------------------------------------------------------------------------|

| | |
|-------|----------------------------------------------------------------------------------------------------------------|
| Group | Displays the group that the account belongs to. You cannot change the group that the admin account belongs to. |
|-------|----------------------------------------------------------------------------------------------------------------|

| | |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password/ Retype Password | These fields are for typing and confirming the account password. |
| Inactivity Timeout | Displays the amount in minutes of inactivity before a user is automatically logged out. The default setting is 5 minutes. |
| Network Places | When enabled, the user can use Network Place to log onto the SSL VPN. See Accessing Network Place on page 6. |
| Network Extender Service | When enabled, the user can use Network Extender to log onto the SSL VPN. See Installing the Network Extender on page 3. |
| Transport Extender Service | When enabled, the user can use Transport Extender to log onto the SSL VPN. See Installing the Transport Extender on page 5. |
| Web Cache Cleaner | When enabled, the user's Web cache is cleared on log out from the SSL VPN. This aids security as no trail to the SSL VPN IP address is left in unmonitored Web browser history folders. |
| Network Extender IP Assignment | Users who log on to the SSL VPN using Network Extender are assigned an IP address for the connection. Select Dynamic Assign to assign a new IP address each time the user logs on. Select Fix IP to assign the same IP address each time the user logs on for better monitoring of network activity. |
| Greeting String | Displays the text users see when they log on. |
| Applications | Lists the applications that are available to the group the user belongs to. See Using Applications on page 6. |

CREATING A NEW USER ACCOUNT

User accounts enable specified users access to services and applications that you define in the **Group/Application** menu item. See [Group/Application](#) on page 71.

Refer to the following to create a new account:

1. On the Menu bar, click **SSL VPN** → **User Access** → **Account**.
2. Click **Create**.

| Add Account | |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| General Setting | |
| User Name | <input type="text"/> |
| Group | BiGuard <input type="button" value="v"/> |
| Password | <input type="password"/> |
| Retype Password | <input type="password"/> |
| Inactivity Timeout | 5 <input type="text"/> Minutes |
| Service | |
| Network Places | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Network Extender Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Transport Extender Service | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Web Cache Cleaner | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Network Extender IP Assignment | <input checked="" type="radio"/> Dynamic Assign <input type="radio"/> Fix IP <input type="text" value="192.168.1.240"/> |
| Greeting String | Welcome to SSL VPN Se |
| Application Proxy | |
| Applications | This group has no application now. |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

3. Type a user name in the **User Name** field.
4. Select the group the user will belong to from the **Group** drop-down menu. See [Group/Application](#) on page 71.
5. Type and confirm a password in the **Password/Retype Password** fields.
6. Type the time to log out inactive users in the **Inactivity Timeout** field.
7. Enable/disable **Network Places**, **Network Extender Services**, and **Transport Extender**.
8. Enable/disable **Web Cache Cleaner**.
9. If **Network Extender Service** is enabled, select **Dynamic Assign** or **Fix IP** in the **Network Extender IP Assignment** field.
10. Modify the **Greeting String** field as desired.
11. Check the applications that will be available to the user in the **Applications** field.
12. Click **Apply** to confirm the settings.

Managing Network Extender IP address and client routes

Use the **Network Extender** menu item to assign client IP addresses to enable client access.

Modifying the Network Extender IP address range

Users who log on using Network Extender are assigned an IP address when they log on. You can change the IP address range in the **Network Extender Client IP Address Assignment** screen.

FIGURE 90 NETWORK EXTENDER CLIENT IP ADDRESS ASSIGNMENT SCREEN

| Network Extender | |
|----------------------------------------------------------------------------|---------------|
| Client IP Address Assignment | |
| Client Address Range Begin | 192.168.1.210 |
| Client Address Range End | 192.168.1.230 |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

Type the new IP address range parameters and click **Apply**.

Creating client routes

The **Client Route** item enables you to set routing rules for the Network Extender client connection. For example, if the client user's internet packet's destination address is specified in Client Route, the packet will be forwarded to the PPP connection passing through the BiGuard S10 through the SSL VPN tunnel.

1. Click **Client Route** to view the Client Routing Table.

| Network Extender | |
|---------------------------------------|-------------|
| Client Routing Table | |
| Destination | Subnet Mask |
| <input type="button" value="Create"/> | |

2. Click **Create** to add a new client route to the table.

| Network Extender | |
|----------------------------------------------------------------------------|----------------------|
| Add Client Route | |
| Destination Address | <input type="text"/> |
| Destination Subnet Mask | <input type="text"/> |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

3. Type the destination address and destination netmask in the **Destination Address** and **Destination Netmask** fields. Click **Apply** to confirm the settings.

Managing Transporter Extender application and host names

Use the Transport Extender menu to configure applications for use with the Transport Extender and to configure host name resolution.

Adding a tunneled Transport Extender application

Click **Application** under the **Transport Extender** menu to configure an application for secure access in the SSL VPN portal.

FIGURE 91 TRANSPORT EXTENDER CONFIGURED APPLICATIONS SCREEN

| Transport Extender | |
|------------------------------------------------|-----------------|
| Configured Applications for Transport Extender | |
| Local Server IP Address | TCP Port Number |
| | |

Create

The Transporter Extender Configured Applications screen lists the local server IP address and the TCP port number for applications that are configured for tunneling via Transport Extender. To add an application for tunneling, click **Create**.

FIGURE 92 ADDING TUNNELED APPLICATIONS TO TRANSPORT EXTENDER SCREEN

| Transport Extender | |
|---------------------------------------------------------|----------------------|
| Add an Application to be Tunneled by Transport Extender | |
| Local Server IP Address | <input type="text"/> |
| TCP Port Number | <input type="text"/> |

Apply Cancel

Type the local server IP address and the TCP port number for the application to be tunneled and then click **Apply**.

Configuring host names for Transport Extender

Click **Host Name Resolution** to configure Transport Extender host names.

FIGURE 93 TRANSPORT EXTENDER CONFIGURED HOST NAME RESOLUTION SCREEN

| Transport Extender | |
|--------------------------------------------------------|-----------------------------|
| Configured Host Name Resolution for Transport Extender | |
| Local Server IP Address | Fully Qualified Domain Name |
| 192.168.1.200 | BIGUARD-JANE |

Create

The Transporter Extender Configured Host Name screen lists the local server IP address and the fully qualified domain name for Transport Extender.

To add a new domain name, click **Create**.

FIGURE 94 TRANSPORT EXTENDER ADD HOST NAME RESOLUTION SCREEN

Transport Extender
 Add an Host Name Resolution to Transport Extender

| | |
|----------------------------|----------------------|
| Local Server IP Address | <input type="text"/> |
| Full Qualified Domain Name | <input type="text"/> |

Apply Cancel

Type the Local Server IP address and the Full Qualified Domain Name for the resolution and then click **Apply**.

Managing SSL Certification

This section describes how to enable, import, and apply SSL certificates.

Importing a certificate

Follow these instructions to import an SSL certificate:

1. Click **SSL Certificate** to view the **Current Certificates** list.

FIGURE 95 SSL CERTIFICATE CURRENT CERTIFICATES SCREEN

SSL Certificate
 Current Certificates

| Enable | Description | Status | Expiration | Password |
|----------------------------------|----------------------|--------|--------------------------|----------|
| <input checked="" type="radio"/> | md5WithRSAEncryption | Active | May 20 11:27:09 2006 GMT | |

Apply Import Certificate Generate CSR

2. Click **Generate CSR**. You are prompted to fill out a CSR (Certificate Signing Request) form.

FIGURE 96 SSL CERTIFICATE GENERATE CERTIFICATE SCREEN

SSL Certificate
 Generate Certificate Signing Request (CSR)

| | |
|---------------------|---------------------------------------------|
| Name | <input type="text" value="Name"/> |
| Organization | <input type="text" value="Org"/> |
| Unit/Department | <input type="text" value="Unit"/> |
| City/Locality | <input type="text" value="City"/> |
| State (Full Name) | <input type="text" value="State"/> |
| Country | <input type="text" value="TW"/> |
| FQDN (Domain Name) | <input type="text" value="www.bgs10.com"/> |
| Email | <input type="text" value="mail@bgs10.com"/> |
| Password | <input type="password" value="*****"/> |
| New Key Pair Length | <input type="text" value="1024"/> |

Apply Cancel

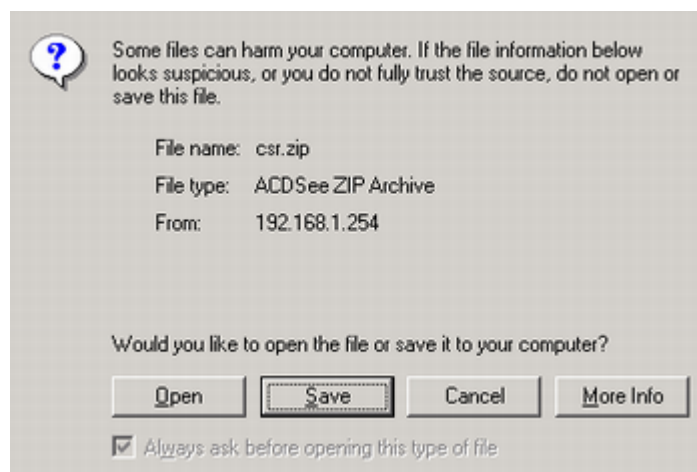
| | |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type your name. |
| Organization | Type your organization. |
| Unit/Department | Type the department you belong to. |
| City/Locality | Type your city. |
| State (Full Name) | If in the US, type the name of your State. |
| Country | Type your two letter country code |
| FQDN (Domain Name) | Type the FQDN (Fully Qualified Domain Name). The FQDN is the complete domain name for a specific host on the Internet, and consists of the host name and domain name (for example, "www.billion.com"). |
| Email | Type your email address. |
| Password | Type a password. Ensure that you write the password in a safe place. |
| New Key Pair Length | This item refers to the strength of the key encryption for the private key (extracted from the zip file). |



NOTE: THE COUNTRY CODE IS TWO ENGLISH CHARACTERS. BE SURE TO WRITE THE PASSWORD DOWN AND PUT IT IN A SAFE PLACE.

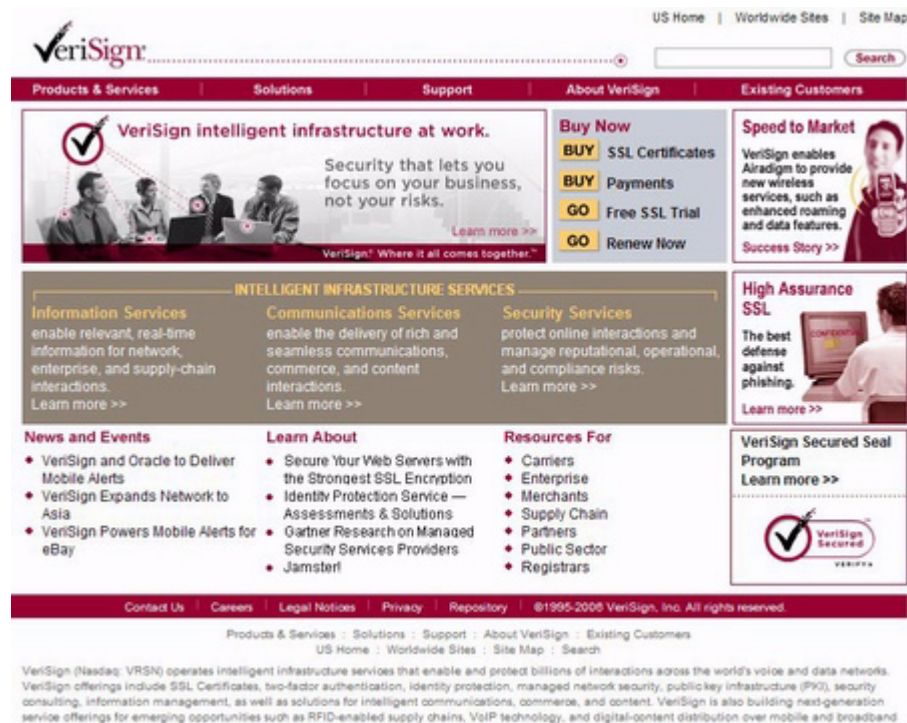
3. Click **Apply**. The browser prompts you to download the zipped CSR file, which includes your private key (server.key) and CSR (csr) files.

FIGURE 97 DOWNLOADING THE CSR



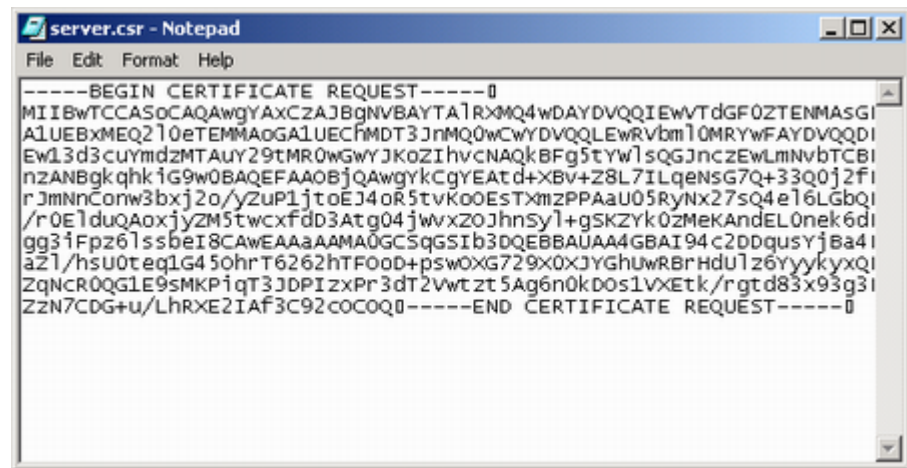
4. Click **Save**. You are prompted for a download location. Save the file to your computer and extract the files to a folder.
5. Next you can sign a certificate (for example from Verisign - www.verisign.com)

FIGURE 98 SIGNING A CERTIFICATE



6. Follow the instructions from the web. You will be prompted to input your CSR.
7. Open your CSR with a text editor such as Windows Notepad (Windows Wordpad and MS Word are not suggested due to compatibility issue).

FIGURE 99 OPENING THE CSR



8. Copy all of the CSR text and paste it in the appropriate field on the certificate provider's website and finish following the certificate provider's instructions for getting a certificate.
The certificate provider will send you the certificate by email.
9. Copy the certificate text and paste into a text editor. Save the file as "server.crt".
10. Zip the files server.crt and server.key into a file (for example, "server.zip").
11. In the **SSL Certificate** screen, click **Import Certificate**.

FIGURE 100 SSL CERTIFICATE IMPORT CERTIFICATES SCREEN

- Click **Browse** and go to the location of the zipped file. When the file is listed in the Certificate File text box, click **Upload**.

The certificate is loaded and added to the Current Certificates list.

FIGURE 101 CURRENT CERTIFICATES

| Enable | Description | Status | Expiration | Password | |
|-------------------------------------|-----------------------|------------|--------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> | sha1WithRSAEncryption | Non-Active | Jul 6 23:59:59 2006 GMT | <input type="button" value="Input"/> | <input type="button" value="Delete"/> |
| <input checked="" type="checkbox"/> | md5WithRSAEncryption | Active | May 20 11:27:09 2006 GMT | | |

Buttons: Apply, Import Certificate, Generate CSR

- Now you must activate the imported certificate. Click **Input** to input the password.

FIGURE 102 INPUTTING THE CSR PASSWORD

Buttons: Apply, Cancel

- In the **Password** text box, type the password that you created when generating the CSR.
- Click **Apply**. The certificate is ready to be used.

FIGURE 103 NEW CERTIFICATE

| Enable | Description | Status | Expiration | Password | |
|-------------------------------------|-----------------------|--------|--------------------------|--------------------------------------|--|
| <input checked="" type="checkbox"/> | sha1WithRSAEncryption | Active | Jul 6 23:59:59 2006 GMT | <input type="button" value="Input"/> | |
| <input type="checkbox"/> | md5WithRSAEncryption | Active | May 20 11:27:09 2006 GMT | | |

Buttons: Apply, Import Certificate, Generate CSR

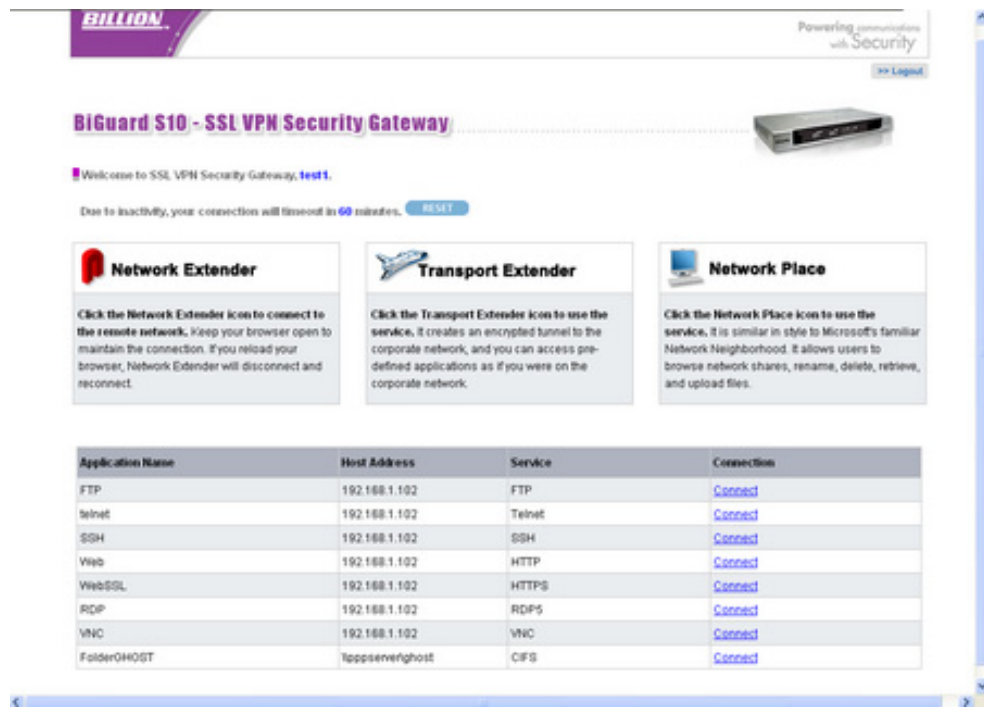
- Click **Enable** to enable the certificate.

SSL VPN Portal

The BiGuard S10 provides a secure and flexible enterprise-wide solution for data and application access anytime and anywhere. By using the BiGuard S10 SSL VPN portal services, organizations with a mobile workforce, a remote office and telecommuters gain available and reliable access to their company's network resources, centralized application control, and critical data management without the sacrifice of user-experience and performance.

Using SSL VPN Portal Access

This chapter deals with the features that make the BiGuard S10 the ideal, secure gateway solution for the novice and the professional alike. From a standard web browser, remote users can access personalized portal pages quickly and easily. Tailored personalized access is managed with the simple click of a mouse.



| Application | Definition |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Extender | Browser based plug-in that simplifies clientless remote access deployments, while delivering full network connectivity for any IP-based application. See Installing the Network Extender on page 84. Click on the icon to connect to the Network Extender. Besides ActiveX control installation, no additional software is required. |
| Transport Extender | Browser based plug-in that allows only specified Protocol and IP addresses with SSL encryption access to pre-defined applications on the network. Click on the icon to connect to the Transport Extender. |
| Network Place | Click on the icon to connect to the Network Place. This application allows users to access designated network places and transfer files between them. Username and password are not required for login. |
| FTP | File Transfer Protocol between network locations. No additional password or log-in required. Click on the connect option to easily access the File Transfer Protocol. |

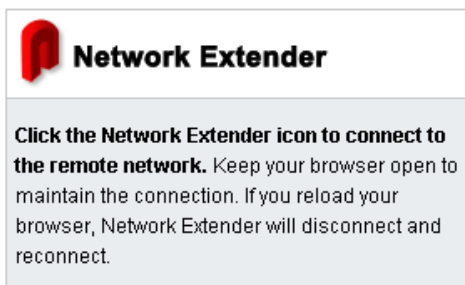
| Application | Definition |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telnet | JAVA based plug-in protocol for accessing remote systems. Click on connect and follow the on-screen instructions to complete the connection. |
| SSH | JAVA based plug-in interface for the secure transfer of files. Click on connect and follow the on-screen instructions. Username and password is required for login. |
| Web | Click the icon to browse to a specified web page on the intranet or Internet. |
| WebSSL | Click the icon to browse to a specified web page on the intranet or Internet with Secure Sockets Layering activated. |
| RDP | Multi-channel protocol that allows users terminal service connection to a computer. Clients exist for Windows 2003 and later versions only. Click on connect and follow the on-screen instructions. ActiveX plug-in must be installed for client to be established. |
| VNC | JAVA based plug-in protocol (Virtual Network Computing) for the remote control of another computer. Click on connect and follow the on-screen instructions. User authentication is required. |

Installing the Network Extender

The Network Extender is a web based plug-in that simplifies clientless remote access while delivering full network connectivity for IP-based applications. The Network Extender enables combined IPSec and SSL VPN in one solution, simplifying remote access deployments while providing maximum flexibility for diverse remote access requirements.

To create a Network Extender connection follow the instructions below:

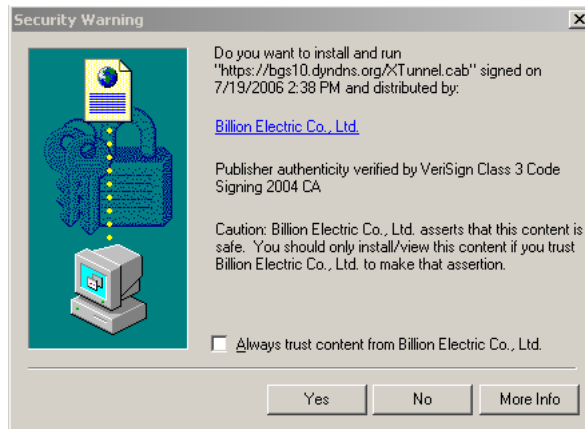
1. Click the **Network Extender** icon.



NOTE: YOU MAY HAVE TO DISABLE POP-UP BLOCKERS TO PROCEED.


2. Click **Install ActiveX Control**.
3. You are prompted to install the adapter.

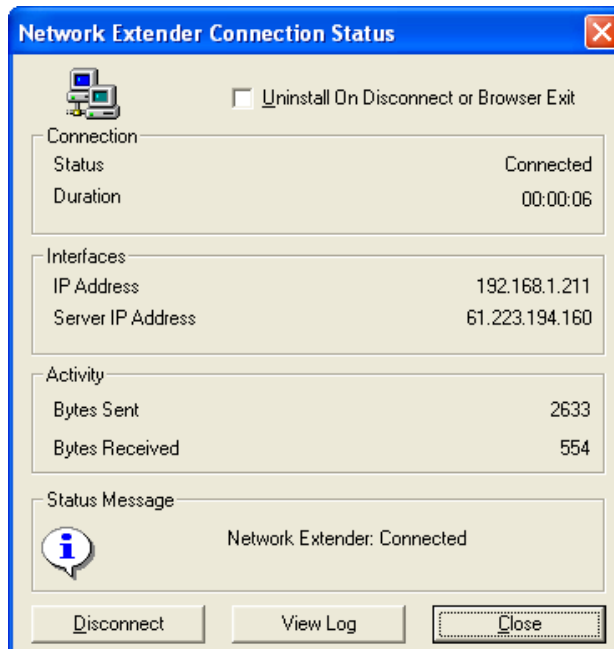
- Click **Yes** when prompted to accept the SSLDrv Adapter.



Setup installs the adapter.



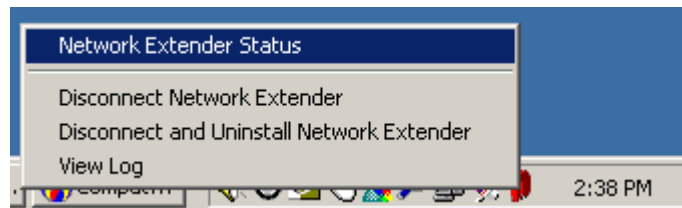
After setup is complete, an icon  appears in the task bar, indicating that the Network Extender is active and the **Connection Status** screen appears.



- Check **Uninstall On Disconnect or Browser Exit** to have the system uninstall the driver every time you disconnect the Network Extender.
- Click **Disconnect** to disconnect the Network Extender.
- Click **View Log** to view a log of Network Extender processes.

- Click **Close** to close the status screen. Network Extender is still active in the status bar.

To view the status screen again, or perform one of the actions above, right-click the Network Extender icon, and select an option from the menu.

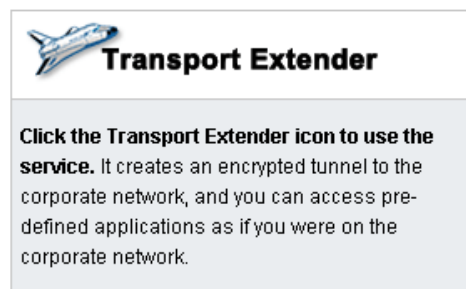


Installing the Transport Extender


The Transport Extender enables you to access an encrypted path to another distant network, and access applications that are on that network.

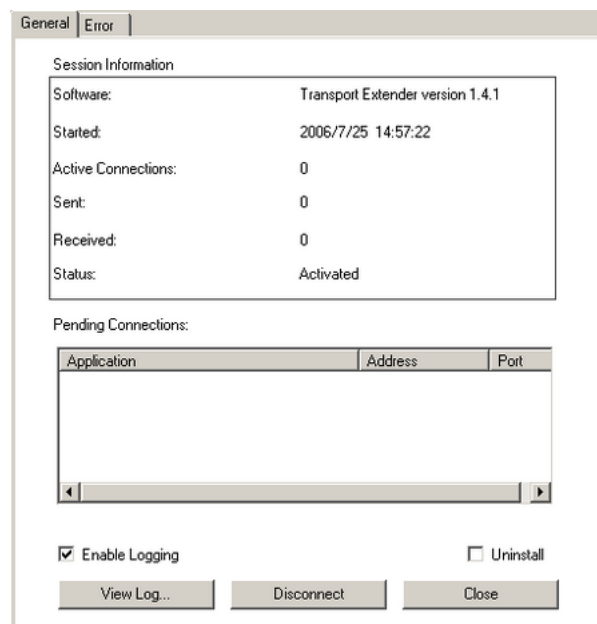
To create a Transport Extender connection follow the instructions below:

1. Click the **Transport Extender** icon.



2. The Transport Extender installs.

After setup is complete, an icon  appears in the task bar, indicating that the Network Extender is active and the **Session Information** appears.



This screen displays the session information and a list of pending connections for applications.

- Click the **Error** tab to view a list of session errors.
- Check **Enable Logging** to allow the system to log all activity for the session.
- Click **View Log** to view a session log.

- Check **Uninstall** if you want to uninstall the driver upon disconnecting.
- Click **Disconnect** to disconnect the Transport Extender.
- Click **Close** to close the Transport Extender screen. Transport Extender is still active in the status bar.

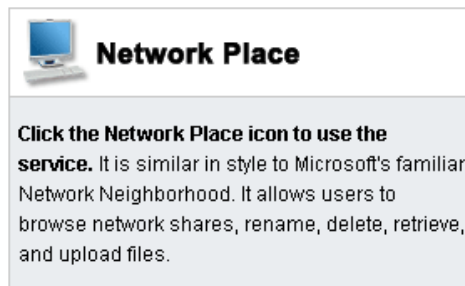
To view the Transport Extender screen again, or disconnect the Transport Extender, right-click the Transport Extender icon and select an option from the menu.



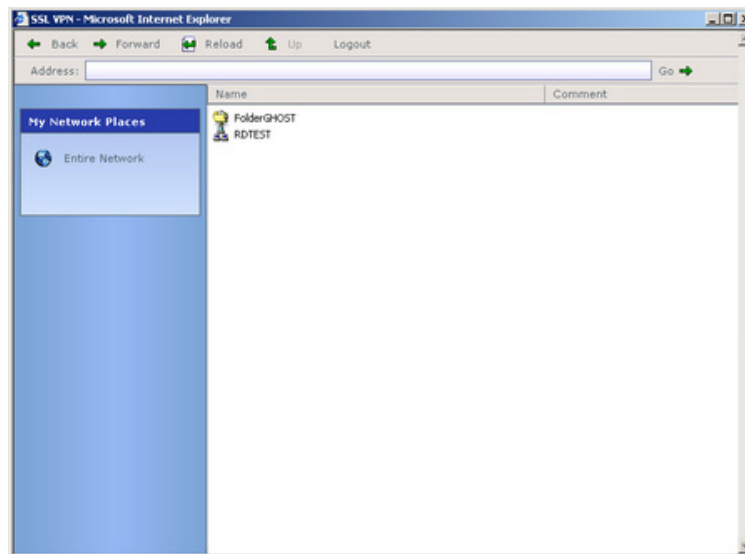
Accessing Network Place

Network Places enables you to access locations on the network to perform typical file related tasks such as browsing shared files, deleting or adding files, and changing file names.

Click the **Network Place** icon.



The local intranet network opens.



Use this screen to perform common file management tasks.

Using Applications

The list of applications in the web portal screen makes them easy to access:

| Application Name | Host Address | Service | Connection |
|------------------|-----------------|---------|-------------------------|
| FTP | 192.168.1.102 | FTP | Connect |
| telnet | 192.168.1.102 | Telnet | Connect |
| SSH | 192.168.1.102 | SSH | Connect |
| Web | 192.168.1.102 | HTTP | Connect |
| WebSSL | 192.168.1.102 | HTTPS | Connect |
| RDP | 192.168.1.102 | RDP5 | Connect |
| VNC | 192.168.1.102 | VNC | Connect |
| FolderOHOST | \\ppserverghost | CIFS | Connect |

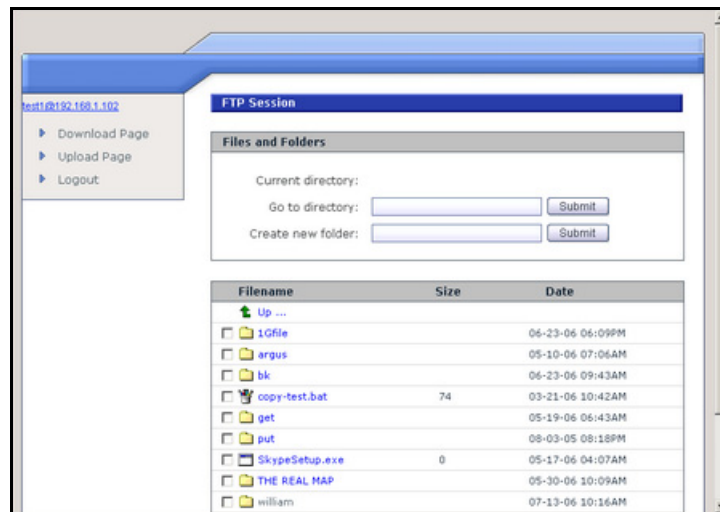
The following sections explain how to access each application.

USING FTP

FTP (File Transfer Protocol) is a protocol used to transfer files over a TCP/IP network. FTP is used for such tasks as uploading HTML pages to the web server. FTP includes functions to log onto the network, list directories and copy files.

FTP operations can be performed by typing commands at a command prompt or using a GUI FTP utility running in a graphical interface such as Windows. FTP transfers can also be started from within a Web browser by entering the URL preceded with **ftp://**.

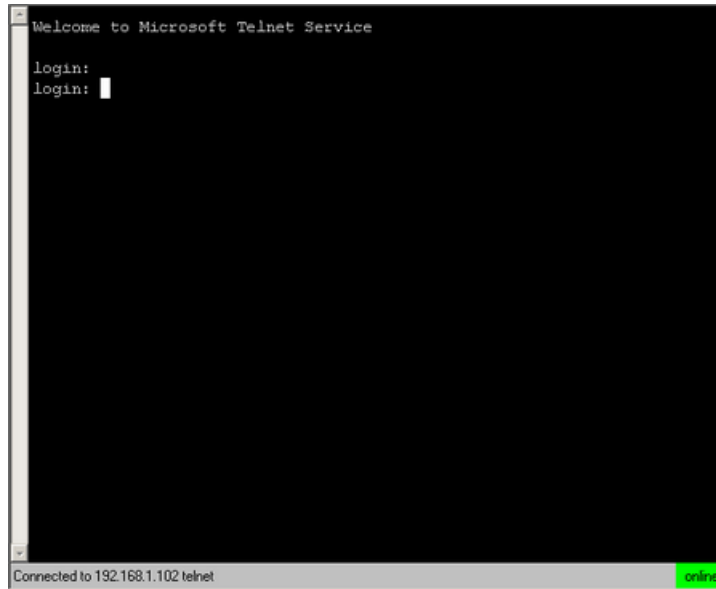
Click **Connect** in the FTP application line. The **FTP Session** screen appears.



USING TELNET

Telnet is a terminal emulation protocol used on the Internet and TCP/IP-based networks that enables users to at a terminal or PC to log onto a remote computer and run a program. Telnet is an inherent component of the TCP/IP communications protocol, and usually requires an account with a password and username to log on.

Click **Connect** in the Telnet application line. The **Telnet Service** screen appears.



Type your login name and press [Enter] to login to Telnet.

Commands may be abbreviated. Supported commands are:

| | |
|----------------|-------------------------------------------|
| close | close current connection |
| display | display operating parameters |
| open | connect to a site |
| quit | exit telnet |
| set | set options (type 'set ?' for a list) |
| status | print status information |
| unset | unset options (type 'unset ?' for a list) |
| ?/help | print help information |

CONNECTING TO SSH

SSH (Secure SHell) provides secure logon for Windows and Unix clients and servers. SSH replaces telnet, ftp and other remote logon utilities with an encrypted alternative.

Click **SSH** to view the login screen.



You are prompted for a user name and password which is provided to you by the network administrator.

USING WEB AND WEB SSL

The Web and Web SSL (Secure Sockets Layering) applications enable you to logon to the company intranet to view web pages.

Click **Web** to display a website on the intranet or Internet.

Click **Web SSL** to open up a secure website on the intranet or Internet.

USING RDP

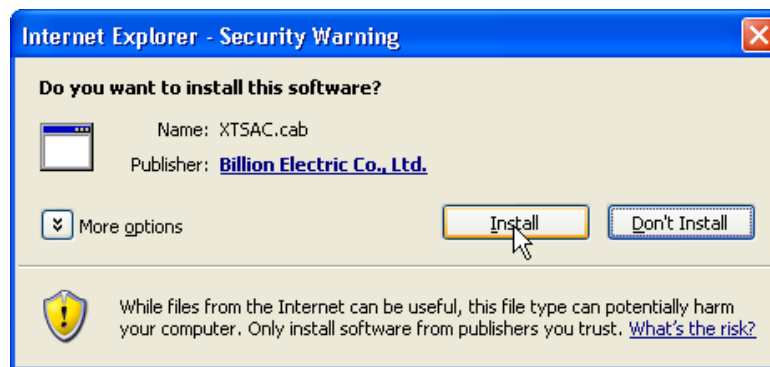
RDP (Remote Desktop Protocol) is a presentation services protocol that controls the input and output between a Windows terminal client and Windows Terminal Server.

The first time you run RDP, you will be prompted to install an ActiveX component and Remote Desktop program file.

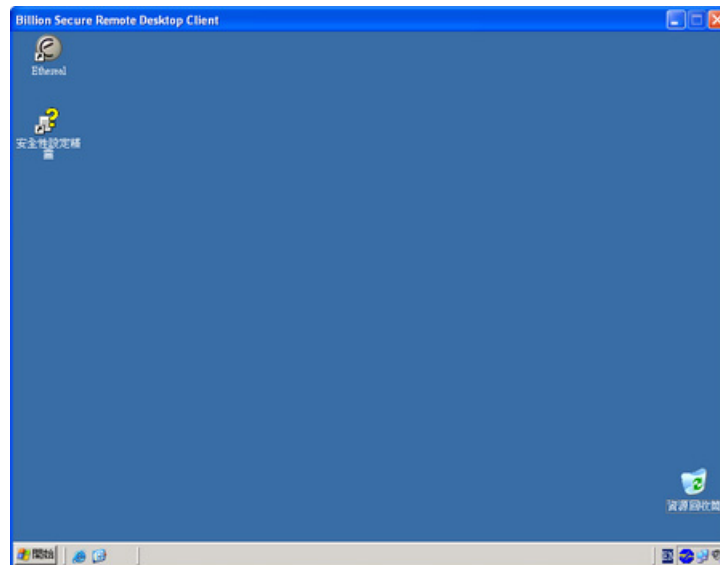
1. Click **RDP**. You are prompted to install an ActiveX component.



2. Click **Install**. The ActiveX Control is installed. You are prompted to install the RDP program file.



Click **Install**. The RDP program file installs and the remote desktop appears.



From here, you can control the remote system.

USING VNC

Virtual Network Computing (VNC) is a desktop sharing system which uses the RFB (Remote FrameBuffer) protocol to remotely control another computer. It transmits the keystrokes and mouse clicks from one computer to another relaying the screen updates back in the other direction, over a network.

Click **VNC**. The remote host is contacted and you are prompted for a password.



Type the password and click **OK**. The remote screen appears.

Log and E-mail Alerts

The BiGuard S10 incorporates industry-standard alert protocols for capturing network activity information. The information can then be written to a log, sent to an external server, or to a selected E-mail address.

Log Configuration

Click **Log Configuration** to open the **Log Configuration** screen.

FIGURE 104 LOG CONFIGURATION SCREEN

| Log Configuration | | | |
|-----------------------|-------------------------------------|--------------------------|--------------------------|
| Parameters | | | |
| Categories | System/SSL VPN Log | Syslog Server | E-mail Alert |
| ISP Connection | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| System Error Messages | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| User Login | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Unauthorized Login | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Configuration Changes | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Packet Filter | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| MAC Filter | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Content Filter | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Firewall | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| SSL VPN | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Debug | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Apply Cancel

| | |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Categories | Select System/SSL VPN Log to capture to a log. Select Syslog Server to capture and send to a specified external server. Select Email Alert to send information log to a pre-specified E-mail account. |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

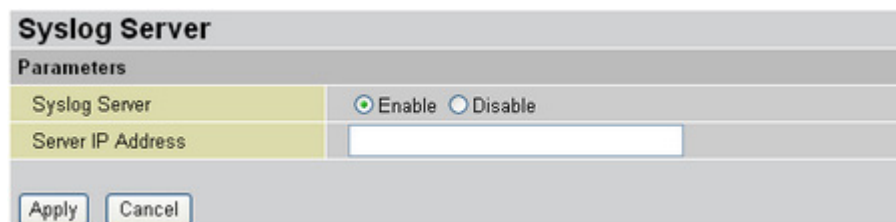
| | |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISP connection | Enable reporting of network connection/traffic information. |
| System error messages | Enable reporting of system or hardware error messages. |
| User login | Enable reporting of user logins. |
| Unauthorized login | Enable reporting of unauthorized users that attempted the task and generated the error message. |
| Configuration changes | Enable reporting of configuration changes. |
| Packet Filter | Enable packet filtering. Note: Packet filtering won't intercept packets that stay within the confines of the LAN. |
| MAC Filter | The MAC Filter enables the administrator to control the access. If the MAC address is denied, the BiGuard S10 will not respond to any request from the MAC address (for example: if the device trying to access the router has a virus). |
| Content Filter | The content filter enables you to prevent unauthorized access to forbidden URLs. |
| Firewall | Enable security alerts for network traffic or program blocking. |
| SSL VPN | Check this item to enable SSL activity logs. |
| Debug | Check this item to enable debug messages to be saved in the system log. |

Click **Apply** to confirm the settings.

Syslog Server

The Syslog (system log) Server enables the router to transmit event and alert messages across the network to a server using the syslog protocol. The operating system sends messages at the start or end of a process to report the process status.

FIGURE 105 SYSLOG SERVER SCREEN



| | |
|-------------------|----------------------------------------------------------------------------------------------------------------------|
| Syslog Server | Enables system logs to be sent to an external syslog server. When enabled, the Server IP Address field is available. |
| Server IP Address | Type the server IP address where the syslog will be saved. |

Click **Apply** to confirm the settings.

E-mail Alert Notification

This item enables the router to send a security event logs by e-mail to a specified recipient.

FIGURE 106 E-MAIL ALERT SCREEN

| | |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------|
| E-mail Alert | Enables a log of security-related events to be sent to a specified e-mail address. When enabled, the following fields are available. |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------|

| | |
|----------------------------|----------------------------------------------------|
| Recipient's E-mail Address | Type the e-mail account to receive the log alerts. |
|----------------------------|----------------------------------------------------|

| | |
|-------------------------|---------------------------------------------------------------------|
| Sender's E-mail Address | Type a sender e-mail name if this is required by the SMTP provider. |
|-------------------------|---------------------------------------------------------------------|

| | |
|------------------|---------------------------------|
| SMTP Mail Server | Type the SMTP mail server name. |
|------------------|---------------------------------|

| | |
|-------------------|--------------------------------------|
| Mail Server Login | Check this box if login is required. |
|-------------------|--------------------------------------|

| | |
|----------|-------------------------------------------|
| Username | Type the user name for the login account. |
|----------|-------------------------------------------|

| | |
|----------|------------------------------------------|
| Password | Type the password for the login account. |
|----------|------------------------------------------|

| | |
|-----------------------------|--------------------------------|
| Period of Send E-mail Alert | Designate frequency of alerts. |
|-----------------------------|--------------------------------|

Click **Apply** to confirm the settings.

Save Configuration to flash

This item enables you to save the current configuration to flash.

FIGURE 107 SAVE CONFIG TO FLASH SCREEN

Click **Apply** to save the configuration.

Troubleshooting

Before you begin

This appendix covers possible problems you may have with the hardware setup and configuration of your BiGuard S10. Before continuing, ensure that you have correctly installed the hardware. See [Setting up the BiGuard S10](#) on page 19.

If you cannot find a solution to your problem here, please login to your registration account and submit your questions through technical support on the registration web site.

Network settings

Many homes have more than one computer. The computers can be connected to each other with a central hub, router, or switch to create a network.

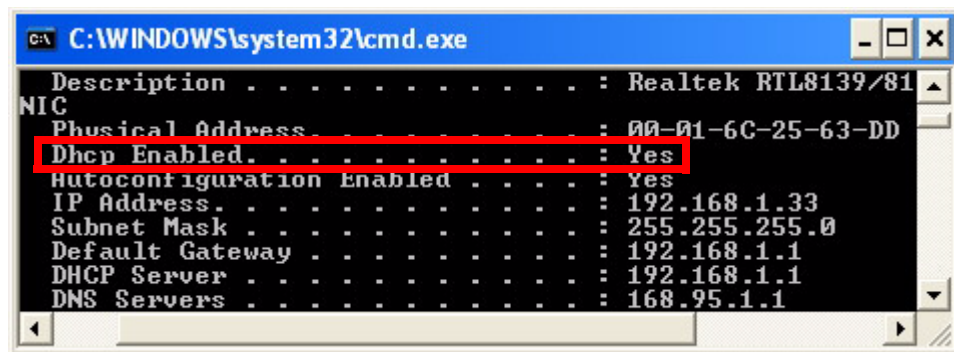
All computers (or any device such as a printer) that are on a network, must have a network IP address. The IP address is either assigned manually (a static IP address), or it is assigned automatically (dynamic IP address) by a DHCP router or server. This is the same for both wired and wireless connections.

Determining the type of IP network address

Refer to the following to determine if your computer is assigned an IP address automatically or manually.

1. From the Windows desktop click **Start** → **Run**.
2. Type **cmd** and click **OK**.
3. At the command prompt, type **ipconfig /all**.

Look for the line **DHCP Enabled**.



```
C:\WINDOWS\system32\cmd.exe
Description . . . . . : Realtek RTL8139/81
NIC
Physical Address . . . . . : 00-01-6C-25-63-DD
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address. . . . . : 192.168.1.33
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 168.95.1.1
```

Note: You may have to scroll up to see it.

If DHCP is enabled, then your router assigns IP addresses automatically. You should use the dynamic settings in the network settings for your type of network.

If DHCP is not enabled, then you have to configure network settings for the BiGuard S10. See [Configuring the WAN for DHCP](#) on page 23.

Hardware problems

This section deals with issues regarding the BiGuard S10 hardware.

My BiGuard S10 won't turn on

If the power, status, WAN, LAN, and DMZ LEDs fail to light up when you turn on the BiGuard S10, check the following:

- Ensure that the power cord is properly connected to your device and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12VDC power adapter supplied by Billion for this product.

If the error persists, you may have a hardware problem. Contact technical support.

The BiGuard S10 LEDs don't turn off after powering on

When your BiGuard S10 is turned on, the LEDs stay on for about 10 seconds and then turn off. If all the LEDs stay on, there may be a hardware problem.

If all LEDs are still on one minute after powering up:

- Cycle the power to see if the router recovers.
- Reset the configuration to factory defaults.

If the error persists, you may have a hardware problem. Contact technical support.

My BiGuard LAN or Internet port LED is not on

If either the LAN LEDs or Internet LED does not light up when the Ethernet connection is established, you should check the following:

- Ensure each Ethernet cable connection is firmly connected at the firewall and at the hub or workstation.
- Ensure that power is turned on to the connected hub or workstation.
- Ensure you are using the correct cable. When connecting the firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

I forgot my password

- First try entering the default user name and password:
User Name: admin
Password: admin

Note that both the User Name and Password are case-sensitive.

If this fails, restore your BiGuard S10 to its factory default settings by holding the reset button on the back of your router until the status LED begins to blink. Then enter the default user name and password to access your router.



NOTE: RESTORING TO FACTORY DEFAULT WILL WIPE OUT ALL THE CONFIGURATIONS YOU HAVE PREVIOUSLY SET. YOU ARE STRONGLY ADVISED TO CREATE A BACKUP COPY OF THE SETTINGS BEFORE RESETTING THE ROUTER.

LAN interface problems

Refer to this section for issues relating to the BiGuard S10's LAN Interface.

I can't access the BiGuard S10 from the LAN

There is no response from my BiGuard S10 connecting from the LAN:

- Check that you have the correct type of Ethernet cable and ensure that the cable connection is plugged in properly at both the PC end and router end.
- Ensure the PC's Ethernet adapter is installed and functioning properly. Refer to your PC's documentation for details.

If the error persists, you may have a hardware problem. Contact technical support.

I can't ping any PC on the LAN

- Check the 10/100M LAN LEDs on the BiGuard S10 front panel. One of these LEDs should be on. If they are both off, check the cable connections between the BiGuard S10 and the hub or PC.
- Ensure that the corresponding LAN LEDs on your PC's Ethernet device are on.
- Ensure that the driver software for your PC's Ethernet adapter and TCP/IP software is correctly installed and configured on your PC.
- Verify that the IP address and the subnet mask of the BiGuard S10 and the PCs connected to it are on the same subnet.

The date and time are not synchronized

If the date and time are not being displayed correctly, set the date and time for your BiGuard S10 using the Web Configuration Interface. Both date and time can be found under **Configuration** → **System** → **Time Zone**.

To synchronize the date and time, open the status page on the Web Configuration Interface, and click **Sync now**.

I can't access the BiGuard S10 Web Configuration Interface

I have trouble accessing BiGuard S10's Web Configuration Interface from a PC connected to the network:

- Check the connection between the PC and the router.
- Ensure your PC's IP address is on the same subnet as the router.
- If your BiGuard S10's IP address has changed and you don't know the current IP address, reset the router to factory defaults by holding the Reset button on the back of your router for 6 seconds. This will reset the router's IP address to 192.168.1.254.
- Check to see if your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to ensure that the Java applet is loaded.
- Try closing the browser and re-launching it.
- Make sure you are using the correct user name and password. User names and passwords are case-sensitive, so make sure that **CAPS LOCK** is not on when entering this information.
- Try clearing your browser's cache. For Internet Explorer, do the following:
 1. Click **Tools** → **Internet Options**.
 2. Under the **General** tab, click **Delete Files**.

3. Make sure that the **Delete All Offline Content** checkbox is checked, and click **OK**.
4. Click **OK** under **Internet Options** to close the dialogue.
 - In DOS, type **arp -d** at the command prompt to clear your computer's ARP (Address Resolution Protocol) table.

Disabling pop-up windows

To use the Web Configuration Interface, you need to disable pop-up blocking. You can either disable pop-up blocking, which is enabled by default in Windows XP Service Pack 2, or create an exception for the BiGuard S10's IP address.



NOTE: THE FOLLOWING INSTRUCTIONS COVER INTERNET EXPLORER. FOR OTHER BROWSERS, REFER TO THE BROWSER'S ONLINE DOCUMENTATION.

DISABLING ALL POP-UPS

In Internet Explorer, select **Tools** → **Pop-up Blocker** and select **Turn Off Pop-up Blocker**.

You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab of the **Internet Options** dialogue.

1. In Internet Explorer, select **Tools** → **Internet Options**.
2. Under the **Privacy** tab, clear the **Block pop-ups** checkbox and click **Apply** to save your changes.

ENABLING POP-UP BLOCKERS WITH EXCEPTIONS

Follow these instructions to allow pop-up blockers with the BiGuard S10:

1. In Internet Explorer, select **Tools** → **Internet Options**.
2. Under the **Privacy** tab, click **Settings** to open the **Pop-up Blocker Settings** dialogue.
3. Enter the IP address of your router (default 192.168.1.254).
4. Click **Add** to add the IP address to the list of **Allowed sites**.
5. Click **Close** to return to the **Privacy** tab of the **Internet Options** dialogue.
6. Click **Apply** to save your changes.

JavaScripts

If the Web Configuration Interface is not displaying properly in your browser, check to make sure that JavaScripts are allowed.

1. In Internet Explorer, click **Tools** → **Internet Options**.
2. Under the **Security** tab, click **Custom Level**.
3. Under **Scripting**, check to see if **Active scripting** is set to **Enable**.
4. Ensure that **Scripting of Java applets** is set to **Enabled**.
5. Click **OK** to close the dialogue.

Java permissions

The following Java Permissions should also be given for the Web Configuration Interface to display properly:

1. In Internet Explorer, click **Tools** → **Internet Options**.
2. Under the **Security** tab, click **Custom Level**.
3. Under **Microsoft VM***, make sure that a safety level for **Java permissions** is selected.
4. Click **OK** to close the dialogue.



NOTE: IF JAVA FROM SUN MICROSYSTEMS IS INSTALLED, SCROLL DOWN TO JAVA (SUN) AND ENSURE THAT THE CHECKBOX IS FILLED.

WAN interface problems

If you are having problems with the WAN Interface, refer to the following tips.

I can't get a WAN IP address from the ISP

My WAN IP address cannot be obtained from the ISP:

- If you are using PPPoE or PPTP encapsulation, you need a user name and password, which is provided by your ISP. Ensure that you have entered the correct **Service Type**, **User Name**, and **Password**. Note that user names and passwords are case-sensitive.
- If your ISP requires MAC address authentication, clone the MAC address from your computer on the LAN as BiGuard S10's WAN MAC address. Click **Specify a MAC Address (MAC Clone)** and type the MAC address in the WAN Settings dialog.
- If your ISP requires host name authentication, configure your computer's name as BiGuard S10's system name.

| WAN Settings | |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Static IP | |
| Protocol | Static IP |
| Mode | <input checked="" type="radio"/> NAT <input type="radio"/> Router |
| IP Address | 211.22.95.230 |
| Subnet Mask | 255.255.255.248 |
| Gateway | 211.22.95.225 |
| MAC Address | <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address (MAC Clone) |
| | <input type="text" value="00 00 00 00 00 00"/> Candidates |
| DNS | Primary DNS 168.95.1.1 Secondary DNS |
| RIP | Disable |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

Internet service provider problems

Unless you have been assigned a static IP address by your ISP, your BiGuard S10 will need to request an IP address from the ISP in order to access the Internet.

I can't access the Internet when connected to the BiGuard S10

If your BiGuard S10 is unable to access the Internet, first determine if your router is able to obtain a WAN IP address from the ISP.

To check the WAN IP address:

1. Open your browser and choose an external site (e.g. www.billion.com).
2. Access the Web Configuration Interface by entering your router's IP address (default is 192.168.1.254). The WAN IP Status is displayed on the first page.
3. Check to see that the WAN port is properly connected to the ISP. If **Connected** in your connection method is not shown, your router has not successfully obtained an IP address from your ISP. Refer to the next section.

| WAN | |
|-------------------|-------------------------------------------------------|
| Connection Method | Static IP |
| Connection | Disconnected <input type="button" value="Ping Test"/> |
| IP Address | 220.128.220.175 |
| Subnet Mask | 255.255.255.0 |
| Gateway | 220.128.220.254 |
| DNS | |

I can't get an IP address from my ISP

If an IP address cannot be obtained:

1. Turn off the power to your cable or DSL modem.
2. Turn off the power to your BiGuard S10.
3. Wait five minutes and power on your cable or DSL modem.
4. When the modem has finished synchronizing with the ISP (generally shown by LEDs on the modem), turn on the power to your router.

If you still can't obtain an IP address:

- Your ISP may require a login program. Contact your ISP and ask them whether they require PPPoE or some other type of login procedure.
- If your ISP requires a login, check to see that your user name and password are entered correctly. The user name and password are case sensitive.
- Your ISP may check for your computer's host name. Assign the computer Host Name of your ISP account as your computer's host name on the router.
- Your ISP may check for your computers MAC address. Inform your ISP that you have purchased a new network device and ask them to use your router's MAC address, or configure your router to spoof your computer's MAC address.

My IP address can be obtained, but my browser cannot load any web pages from the Internet

- Your computer may not recognize DNS server addresses. Configure your computer manually with DNS addresses.
- Your computer may not have the router correctly configured as its TCP/IP gateway.

Recovery

You can restore your BiGuard S10 to its factory settings by performing a recovery of the router. You should perform this procedure in the event a software or hardware reset is not effective.



Performing a recovery of the router will reset all settings and return the router to the settings it has when you first installed it. To reset the router without erasing all your settings, perform a software reset.

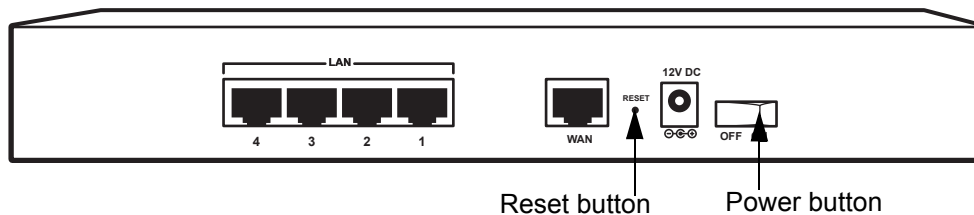
Follow the instructions to perform a hardware reset.

1. Manually setup your administrator PC's IP to the following address:



NOTE: THE IP ADDRESS RANGE IS 192.169.1.0~24

2. Switch off the power on your BiGuard S10 Series.
3. Hold down the reset button and switch on the power



4. When the status LED in the front panel blinks 3 times and then remains lit, release the reset button.
5. Wait for six seconds, then open your browser and enter the IP address 192.168.1.254 in the address bar. You will see the recovery mode page.
6. Follow the on-screen instructions.



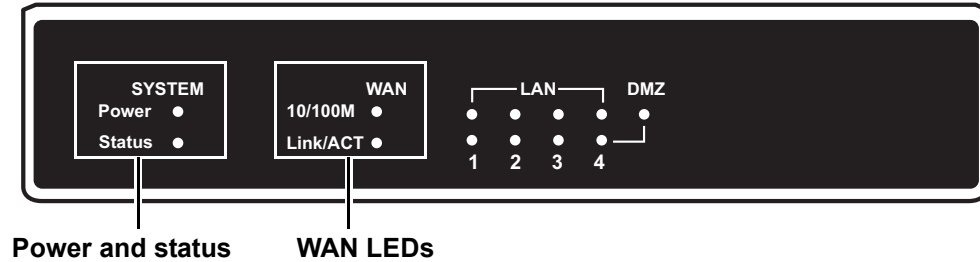
NOTE: IF ALL OF THE ABOVE PROCEDURES STILL DO NOT WORK, CONTACT YOUR DEALER FOR FURTHER INSTRUCTIONS.

Troubleshooting sequence

This section answers some common questions about the BiGuard S10 operation and provides some troubleshooting tips.

QUESTION: What's the LED sequence of the BiGuard S10 Series when powering on?

- ANSWER:** The LED sequence for powering on the BiGuard S10 Series is as follows:
- WAN LEDs flash in sequence twice.
 - Power and status LEDs light.
 - In about thirty (30) seconds, the status LED turns off to indicate the system is operational.



QUESTION: What's the default username and password of the BiGuard S10 Series?

- ANSWER:** The default username and password for the BiGuard S10 Series is as follows:
- **Username:** admin
 - **Password:** admin

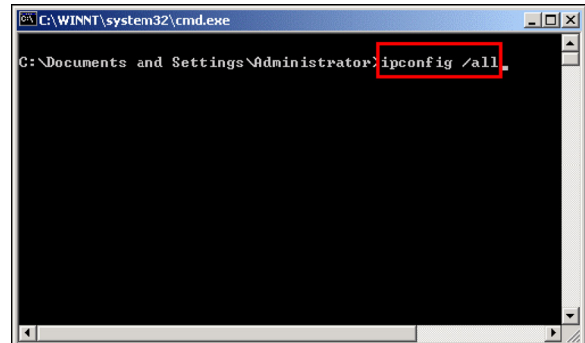
QUESTION: What's the factory default LAN IP address for the BiGuard S10 Series?

- ANSWER:** The factory default LAN IP address for the BiGuard S10 Series is as follows:
- **IP address:** 192.168.1.254
 - **Subnet Mask:** 255.255.255.0

QUESTION: I remember the LAN IP address for my BiGuard S10 Series router is 192.168.1.254, but I can't login in now. What should I do?

ANSWER: Follow these troubleshooting procedures:

1. Check if there is another computer or router using the following IP address: 192.168.1.254.
2. If your computer is automatically assigned an IP address, perform the following steps:
 - a. Click **Start** and then select **Run**.
 - b. Type **cmd** or **command** in the **Run** text box.
 - c. A DOS window opens.
 - d. In the DOS prompt type **C:\>ipconfig /all** (see illustration) to verify that your computer has been assigned an IP address.
3. If your network is setup to use a static IP address, please make sure the IP address is setup correctly.
4. If steps 1,2 and 3 don't work, power off the router, wait a few moments and power on the router and perform steps 1 ~ 3 again.

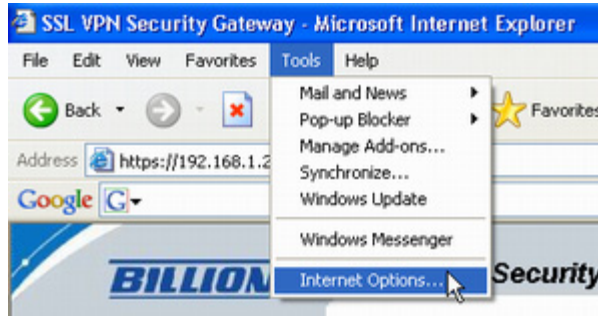


QUESTION: I've just upgraded the router firmware to the latest version, but I found some of the buttons or pages don't display or work properly.

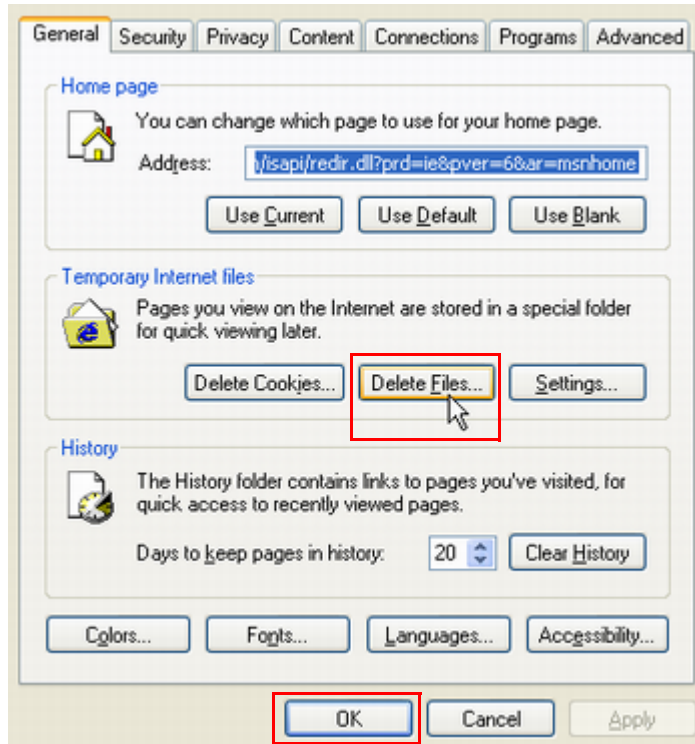
ANSWER: It is possible that the browser is referencing data stored in the cache. Clear the offline browser data in the cache, restart the browser, and try again.

To clear the cache in Internet Explorer, do the following:

1. Open the Internet Explorer browser, select **Tools** → **Internet Options**.



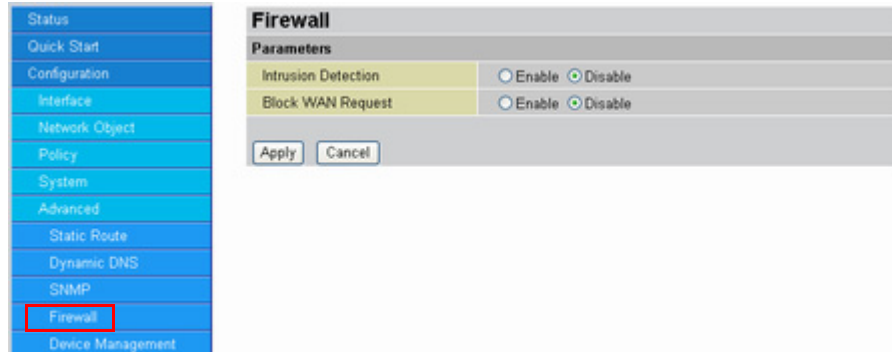
2. In the **General** settings tab, click **Delete Files** and click **OK**.



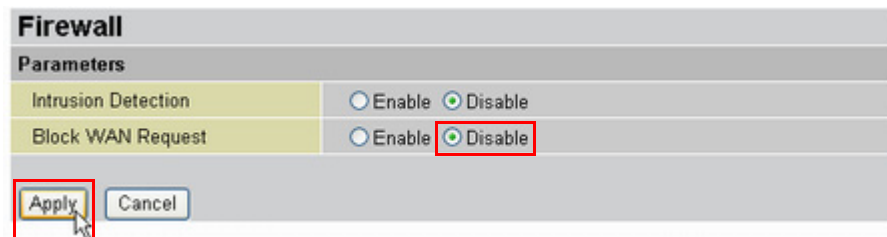
QUESTION: Why can't I ping the WAN IP address of the BiGuard S10 Series from the Internet?

ANSWER: Make sure the Block WAN Request is disabled.

1. Click **Configuration** → **Advanced** → **Firewall**.



2. Next to **Block WAN Request**, click the **Disable** radio button.



3. Click **Apply**.

You can now ping the BiGuard S10 WAN IP address.

BiGuard S10 FAQ

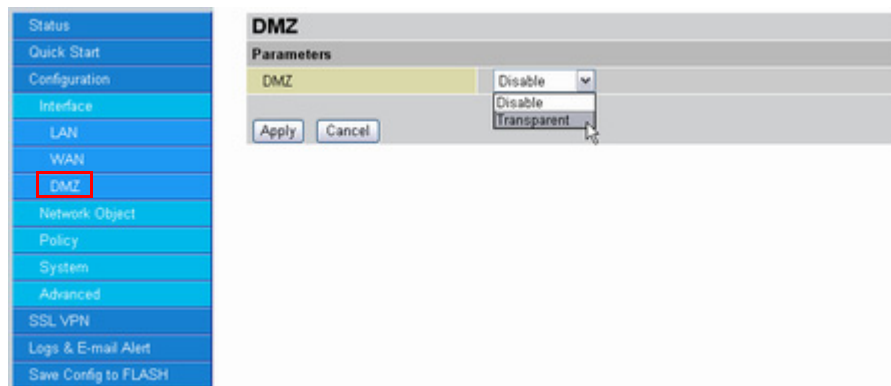
DMZ

QUESTION: What is a DMZ? How do I set one up?

ANSWER: The DeMilitarized Zone (DMZ) port provides a way for public servers (FTP, Mail, Web, etc.) to be visible to the outside world. These public servers can still be accessed from the secure LAN side. It can prevent outside users from getting direct access to a server that has company data.

The BiGuard S10 Series supports hardware DMZ. To set up a DMZ for the BiGuard S10 Series, follow these instructions.

1. From the **Configuration** menu, select **Interface, DMZ**:



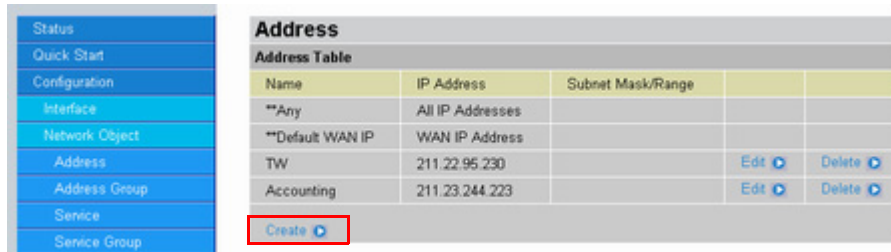
2. From the drop down menu, select **Transparent** and click **Apply**.
The hardware DMZ port is the same as the LAN port number
3. Connect the DMZ server to this port and all internet traffic attempting to access your WAN IP address will be routed through the DMZ server.

Firewall

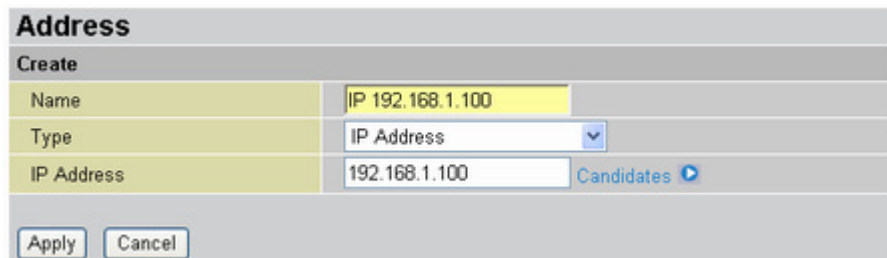
QUESTION: How can I setup the firewall rule to block Internet access to the IP address 192.168.1.100?

ANSWER: Use the packet filtering function in **Configuration** → **Policy** → **Packet Filtering**. First, however, you must add this address to the Address List. Follow these instructions.

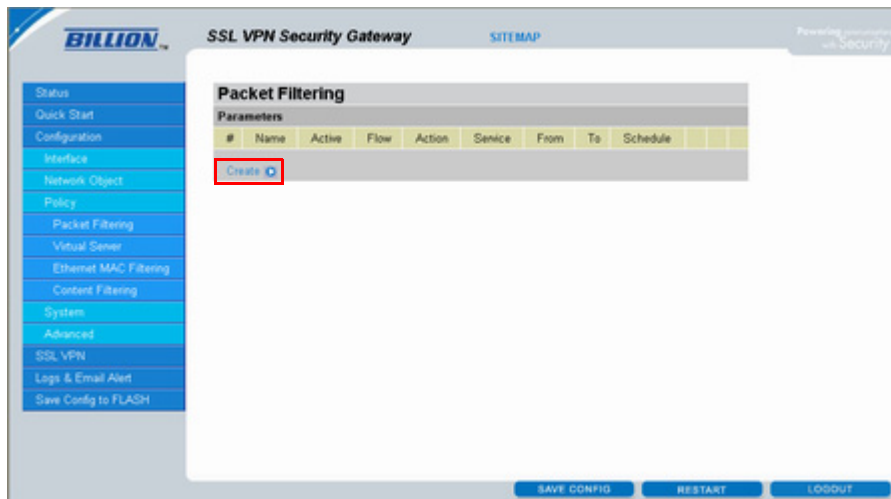
1. Click **Configuration** → **Network Object** → **Address**. The Address Table appears.



2. Click **Create**.



3. Type a descriptive name for this address in the **Name** text box, select **IP Address** from the drop-down list, and type the address (in this case 192.168.1.100) in the **IP Address** text box.
4. Click **Apply** to save the new item.
5. Click **Configuration** → **Policy** → **Packet Filtering**.



6. Click **Create**.

7. Type a descriptive name for this filter, select **LAN to WAN** from the **Packet Flow** drop-down list and check the **Reverse Direction** box.
8. Select **HTTP** from the **Service** drop-down list, and select the newly created address from the **To Address** drop-down list.

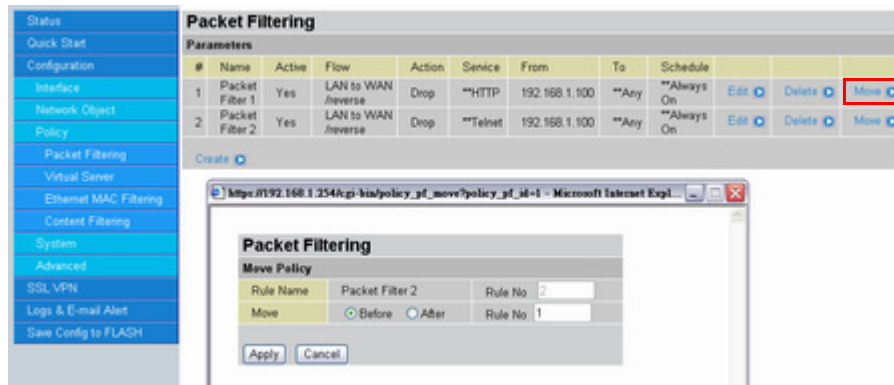
9. Click **Apply**. The new filter appears in the **Packet Filtering Parameters** list.

| Packet Filtering | | | | | | | | | | |
|------------------|---------------|--------|---------------------|--------|---------|------------------|-------|-------------|------|--------|
| Parameters | | | | | | | | | | |
| # | Name | Active | Flow | Action | Service | From | To | Schedule | | |
| 1 | Packet Filter | Yes | LAN to WAN /reverse | Drop | **HTTP | IP 192.168.1.100 | **Any | **Always On | Edit | Delete |

From here, you can click **Edit** to change filter parameters or click **Delete** to remove the filter from the list.

QUESTION: What does the Rule No. mean in Packet Filtering? Is it related to the priority?

ANSWER: Rule No. is the packet filtering identification. It is related to the policy priority. The rule priority can be moved higher or lower by selecting before or after a specified rule number.



QUESTION: What kinds of filters are supported in content filtering?

ANSWER: The following content filters are supported:

- Keyword Filtering
- Domain Filtering
- Restricted Features (including Java Applet, ActiveX, Cookies, Proxy, and surfing by IP Address)

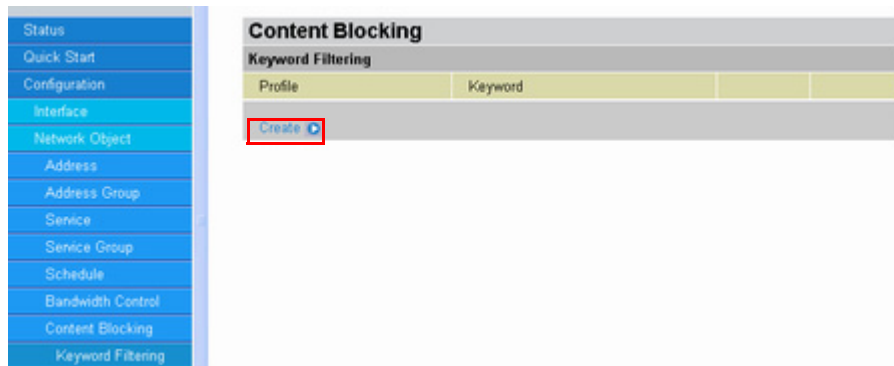
QUESTION: What is Keyword Filtering in Content filter? How do I use it?

ANSWER: Keyword filter is the filtering technology that blocks access to any URL that includes specified keywords defined by the user (see example below).

Example:

The user wants to define the keyword “sex” to block access to sex related web sites. First, the user must set up a keyword filtering profile.

1. Click **Configuration** → **Network Object** → **Content Blocking** → **Keyword Filtering**.



2. Click **Create** to add a new **Keyword Filtering** profile.

Keyword Filtering

Create

| | |
|---------|--------------|
| Profile | Sex-Websites |
| Keyword | sex |

Add

Block WEB URLs which contain these keywords

| | |
|---------|--|
| Keyword | |
|---------|--|

Apply **Cancel**

3. Type a descriptive name for the keyword filtering profile and type the keyword in the text boxes.
4. Click **Add**. The keyword is added to the **Block WEB URLs** list.

Keyword Filtering

Create

| | |
|---------|--------------|
| Profile | Sex-Websites |
| Keyword | |

Add

Block WEB URLs which contain these keywords

| | |
|---------|---------------|
| Keyword | |
| sex | Delete |

Apply **Cancel**

5. Add more keywords to this filter by typing the keyword into the **Keyword** text box and clicking **Add**.

Keyword Filtering

Edit

| | |
|---------|--------------|
| Profile | Sex-Websites |
| Keyword | |

Add

Block WEB URLs which contain these keywords

| | |
|---------|---------------|
| Keyword | |
| sex | Delete |
| porn | Delete |
| sexy | Delete |

Apply **Cancel**

- Click **Apply**. The new profile is listed.

| Content Blocking | | | |
|-------------------|-----------|--------|----------|
| Keyword Filtering | | | |
| Profile | Keyword | | |
| Sex-Websites | sex , ... | Edit ▶ | Delete ▶ |
| Create ▶ | | | |

From here you can **Edit** or **Delete** the profile.



NOTE: BE CAREFUL WHEN EDITING THE PROFILE; YOU MAY ALTER THE POLICY RULE. THE INSTRUCTIONS IN STEP 7 ESTABLISH THE POLICY RULES.

Now that you've created a **Keyword Filtering Profile**, you can activate the filter.

- Click **Configuration** → **Policy** → **Content Filtering**.

- Status
- Quick Start
- Configuration
- Interface
- Network Object
- Policy
- Packet Filtering
- Virtual Server
- Ethernet MAC Filtering
- Content Filtering

Content Filtering

Parameters

| # | Name | Active | Keyword | Domain | Restrict | From | Schedule | | |
|----------|------|--------|---------|--------|----------|------|----------|--|--|
| Create ▶ | | | | | | | | | |

Exception list

| | |
|------------|--|
| IP Address | |
| Create ▶ | |

- Click **Create**.

Content Filtering

Create

| | |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Pornography |
| Active | <input checked="" type="checkbox"/> Enable |
| Keywords Filtering ▶ | <input checked="" type="checkbox"/> Enable Sex-Websites ▼ |
| Domains Filtering ▶ | <input type="checkbox"/> Enable Sex-Websites Gambling Games <small>not for Trusted Domains</small> |
| Restrict Feature ▶ | <input type="checkbox"/> Enable |
| From Address ▶ | **Any ▼ |
| Schedule ▶ | **Always On ▼ |
| Log | <input type="checkbox"/> Enable |

Apply Cancel

- Type a descriptive name for this content filtering profile and check **Active** to enable content filtering.
- In **Keywords Filtering**, check **Enable** and select your new **Keywords Filtering** profile from the drop-down list.



NOTE: IF YOU HAVE NOT CREATED A KEYWORD FILTERING PROFILE, THE DROP-DOWN LIST WILL BE ABSENT.

11. Click **Apply**. The new content filter is listed.

| Content Filtering | | | | | | | | | |
|------------------------|-------------|--------|--------------|----------|----------|-------|-------------|----------------------|------------------------|
| Parameters | | | | | | | | | |
| # | Name | Active | Keyword | Domain | Restrict | From | Schedule | | |
| 1 | Pornography | Yes | Sex-Websites | Disabled | Disabled | **Any | **Always On | Edit | Delete |
| Create | | | | | | | | | |
| Exception list | | | | | | | | | |
| IP Address | | | | | | | | | |
| Create | | | | | | | | | |

From here you can **Edit** or **Delete** the content filter.



NOTE: THE FILTER WILL BLOCK URLS SUCH AS WWW.SEXPICTURE.COM, AND OTHER RELATED URLS THAT HAVE SEX IN THE DOMAIN NAME. HOWEVER IT WILL ALSO BLOCK POTENTIALLY HARMLESS OR USEFUL DOMAINS SUCH AS "WWW.SEXANDHEALTH.COM". YOU CAN STOP THESE DOMAINS FROM BEING FILTERED; REFER TO THE NEXT SECTION REGARDING DOMAIN FILTERING.

If you want some IP address to be exempt from this content filter, click **Create** under **Exception List** and type the IP address in the text box or click **Candidates** to select an IP address from the list.

| Status | Quick Start | Configuration | Interface | Network Object | Address | Address Group | Service |
|------------------------|--------------------|----------------------|----------------------|------------------------|---------|---------------|---------|
| Content Blocking | | | | | | | |
| Domain Filtering | | | | | | | |
| Profile | Forbidden Domain | Trust Domain | | | | | |
| Sex Sites | www.sexpicture.com | www.sexandhealth.com | Edit | Delete | | | |
| Games | www.games.com | | Edit | Delete | | | |
| Billion | | www.billion.com | Edit | Delete | | | |
| Create | | | | | | | |

QUESTION: What is Domains Filtering in Content Filter? How do I use it?

ANSWER: Domain filtering is a firewall function designed to block specific domain addresses (see example below).

Example:

The user wants to block www.sexpicture.com from being accessed. Follow these instructions.

1. Click **Configuration** → **Network Object** → **Content Blocking** → **Domain Filtering**.

| Status | Quick Start | Configuration | Interface | Network Object | Address | Address Group | Service | Service Group | Schedule | Bandwidth Control | Content Blocking | Keyword Filtering | Domain Filtering | Restrict URL Feature |
|------------------------|------------------|---------------|-----------|----------------|---------|---------------|---------|---------------|----------|-------------------|------------------|-------------------|------------------|----------------------|
| Content Blocking | | | | | | | | | | | | | | |
| Domain Filtering | | | | | | | | | | | | | | |
| Profile | Forbidden Domain | Trust Domain | | | | | | | | | | | | |
| Create | | | | | | | | | | | | | | |

2. Click **Create** to add a new **Domain Filter** profile.

Domain Filtering

Create

| | |
|---------|--------------------|
| Profile | Sex Sites |
| Domain | www.sexpicture.com |
| Type | Forbidden Domain |

Add

Block WEB URLs which contain these domains

| | |
|------------------|--|
| Forbidden Domain | |
|------------------|--|

UnBlock WEB URLs which contain these domains

| | |
|----------------|--|
| Trusted Domain | |
|----------------|--|

Apply **Cancel**

3. Type a descriptive name for the domain filtering profile and type the domain name (in this case “www.sexpicture.com”) in the text boxes. Select **Forbidden Domain** from the **Type** drop-down list.
4. Click **Add**. The keyword is added to the Block WEB URLs list.

Domain Filtering

Create

| | |
|---------|------------------|
| Profile | Sex Sites |
| Domain | |
| Type | Forbidden Domain |

Add

Block WEB URLs which contain these domains

| | |
|--------------------|---------------|
| Forbidden Domain | |
| www.sexpicture.com | Delete |

UnBlock WEB URLs which contain these domains

| | |
|----------------|--|
| Trusted Domain | |
|----------------|--|

Apply **Cancel**

As described in the last section, you may wish to allow some sites that may have suspect words in their domain names (for example, “www.sexandhealth.com”).

- Type the name of the domain you want to unblock in the **Domain** text box and select **Trusted Domain** from the drop-down list.

Domain Filtering

Create

| | |
|---------|---------------------------------------------------|
| Profile | Sex Sites |
| Domain | <input type="text" value="www.sexandhealth.com"/> |
| Type | Forbidden Domain ▾ |

Block WEB URLs which contain these domains

| | |
|--------------------|---------------------------------------|
| Forbidden Domain | |
| www.sexpicture.com | <input type="button" value="Delete"/> |

UnBlock WEB URLs which contain these domains

| | |
|----------------|--|
| Trusted Domain | |
|----------------|--|

- Click **Add**. The domain is added to the trusted domain list.

Domain Filtering

Create

| | |
|---------|----------------------|
| Profile | Sex Sites |
| Domain | <input type="text"/> |
| Type | Forbidden Domain ▾ |

Block WEB URLs which contain these domains

| | |
|--------------------|---------------------------------------|
| Forbidden Domain | |
| www.sexpicture.com | <input type="button" value="Delete"/> |

UnBlock WEB URLs which contain these domains

| | |
|----------------------|---------------------------------------|
| Trusted Domain | |
| www.sexandhealth.com | <input type="button" value="Delete"/> |

- Click **Apply**. The new domain filters are listed.

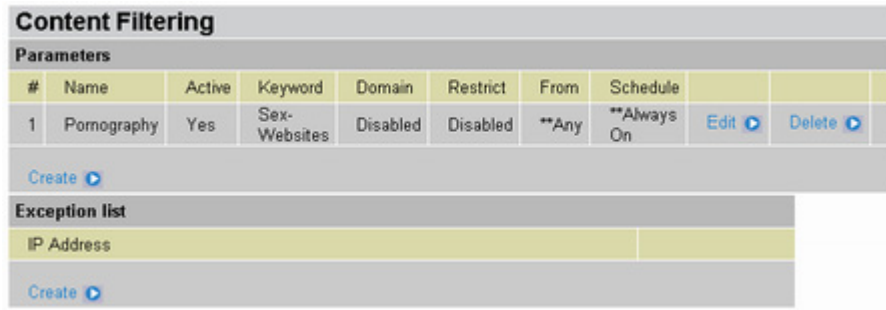
Content Blocking

Domain Filtering

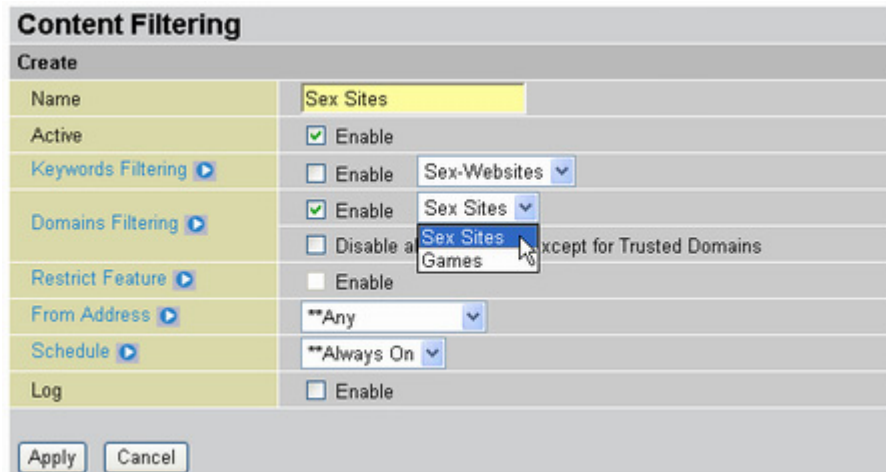
| Profile | Forbidden Domain | Trust Domain | | |
|-----------|--------------------|----------------------|-------------------------------------|---------------------------------------|
| Sex Sites | www.sexpicture.com | www.sexandhealth.com | <input type="button" value="Edit"/> | <input type="button" value="Delete"/> |

From here you can **Edit** or **Delete** the domain filter.
Now you can activate the domain filter.

- Click **Configuration** → **Policy** → **Content Filtering**.



- Click **Create** to add a new content filter policy.



- Type a descriptive name for this content filtering profile and check **Active** to enable content filtering.
- In **Domains Filtering**, check **Enable** and select your new **Keywords Filtering** profile from the drop-down list.

QUESTION: What is “Disable all WEB traffic except for Trusted Domains” in Content Filtering? How do I use it?

ANSWER: **Disable all WEB traffic except for Trusted Domains** blocks all web traffic with the exception of specific URLs selected by the user.

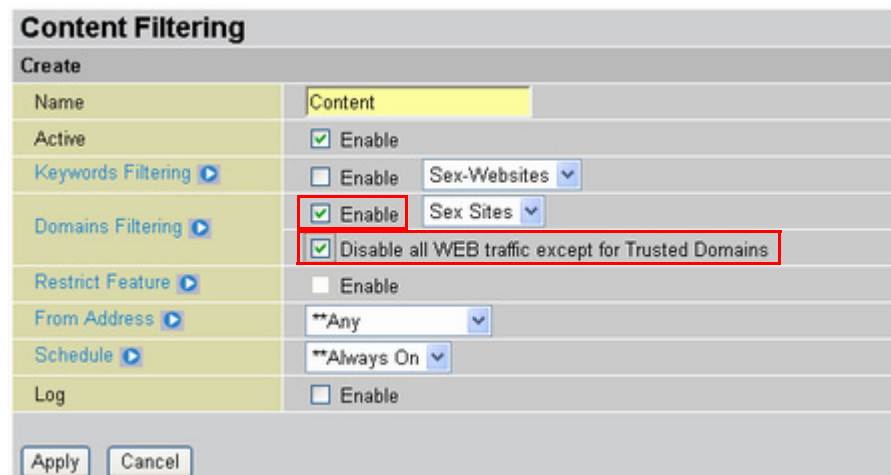
Example:

To allow a user access to only the **www.billion.com** URL, follow the two steps below.

Step 1: Designate the URL **www.billion.com** as a trusted domain as described in Steps 5 ~ 7 in the previous section.



Step 2: Click **Configuration** → **Policy** → **Content Filtering** → **Create** and select both “Domain filter” and “Disable all WEB traffic except for Trusted Domains” options.



QUESTION: What are “Block Java Applet” and “Block ActiveX” in Restrict Features?

ANSWER: Block Java Applet and Block ActiveX blocks HTML access to potentially harmful instructions found in files with extensions such as .js, .class, .ocx or .cab.

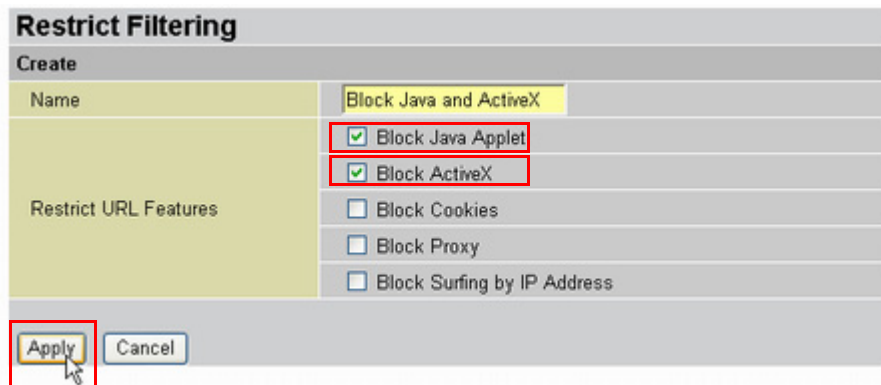
Downloaded malicious Java applets and JavaScript can steal, delete or modify information and compromise security and breach a user’s system. In addition, “buggy” applets hamper performance and needlessly consume network bandwidth. Once this function is enabled, malicious code cannot be executed unless the function is disabled.

Before you can restrict Java applets and JavaScript, you must first create the content blocking profile. Follow these instructions.

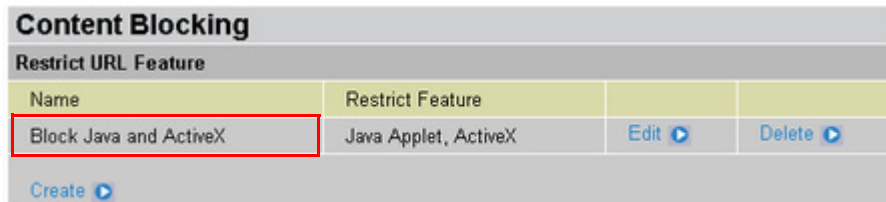
1. Click **Configuration** → **Network Object** → **Content Blocking** → **Restrict URL Feature**.



2. Click **Create** to create a **Restrict Filtering** profile.

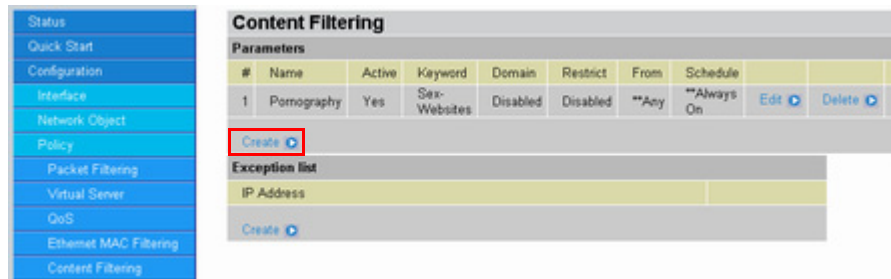


3. Type a descriptive name in the text box and check the **Block Java Applet** and **Block ActiveX** boxes.
4. Click **Apply**. The new profile is added to the list.

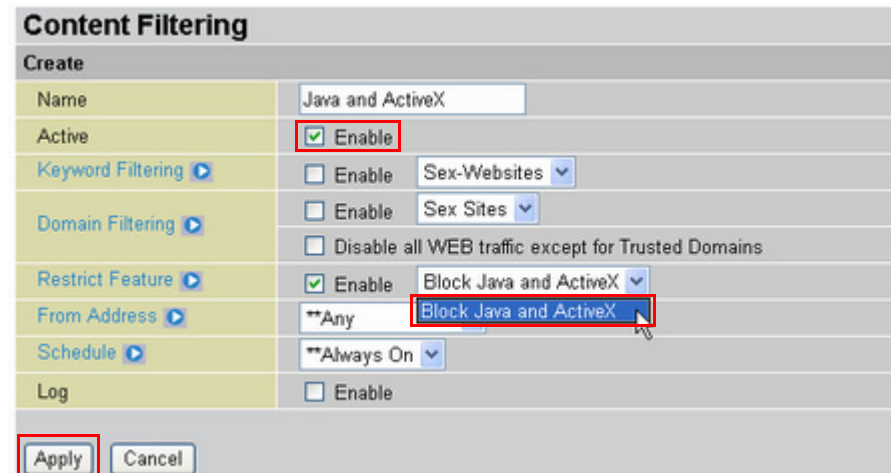


From here you can **Edit** or **Delete** the profile. Now you can enable the **Restrict URL Feature**.

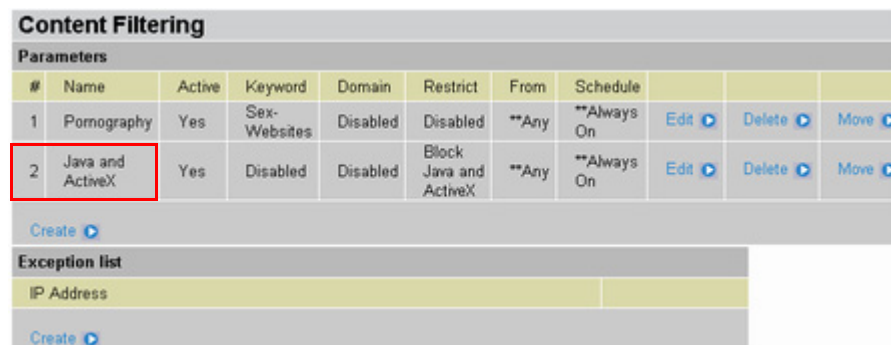
- Click **Configuration** → **Policy** → **Content Filtering**.



- Click **Create** to create a new content filter.



- Type a descriptive name for this content filter, and next to **Active** check **Enable** to activate this content filter.
- Next to **Restrict Feature**, check **Enable** and select the new profile from the drop-down list.
- Click **Apply**. The new content filter is added to the list.



From here you can **Edit** or **Delete** the filter.

You can also **Move** the filter, which changes the policy rule priority. The rule priority can be moved higher or lower by selecting before or after a specified rule number, which changes the order of the rules. See [What does the Rule No. mean in Packet Filtering? Is it related to the priority?](#) on page 110.

QUESTION: What is “Block Web Proxy” in Restrict Features?

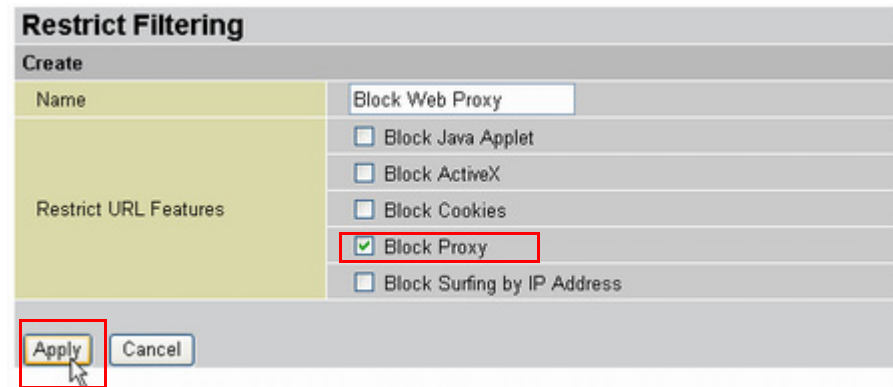
ANSWER: This policy blocks the user access to the Setup Web Proxy function, and prevents the user from circumventing the Restrict Features function for Internet use.

To block the web proxy, follow these instructions.

1. Click **Configuration** → **Network Object** → **Content Blocking** → **Restrict URL Feature**.



2. Click **Create** to create a **Restrict Filtering** profile.

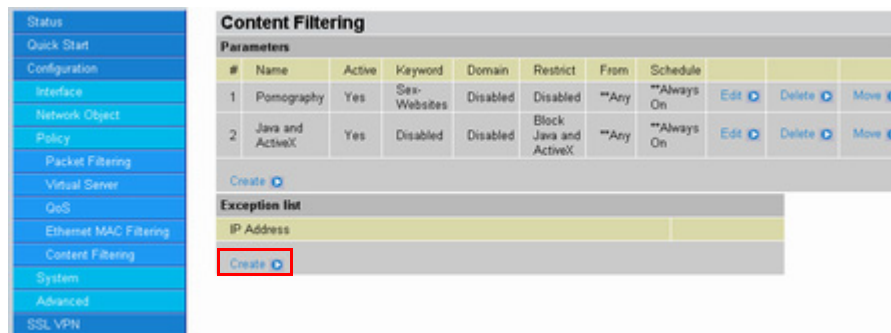


3. Type a descriptive name in the text box and check the **Block Proxy** box.
4. Click **Apply**. The new profile is added to the list.

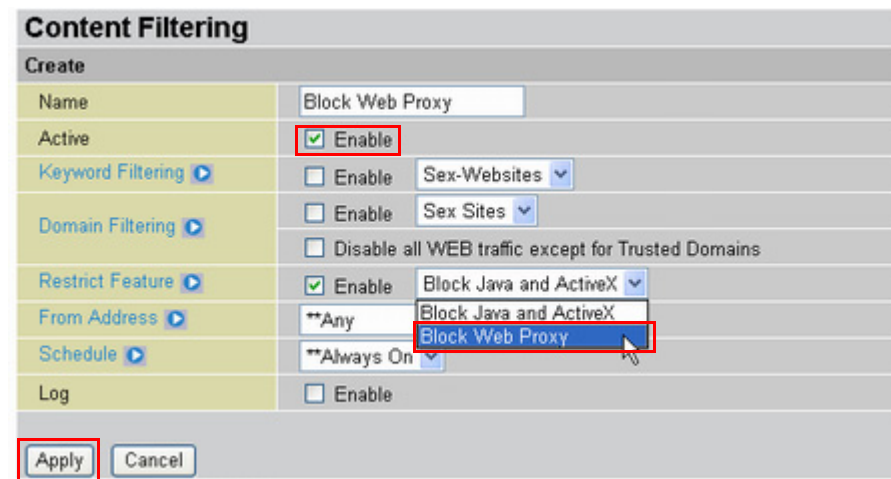


From here you can **Edit** or **Delete** the profile.
Now you can enable the **Restrict URL Feature**.

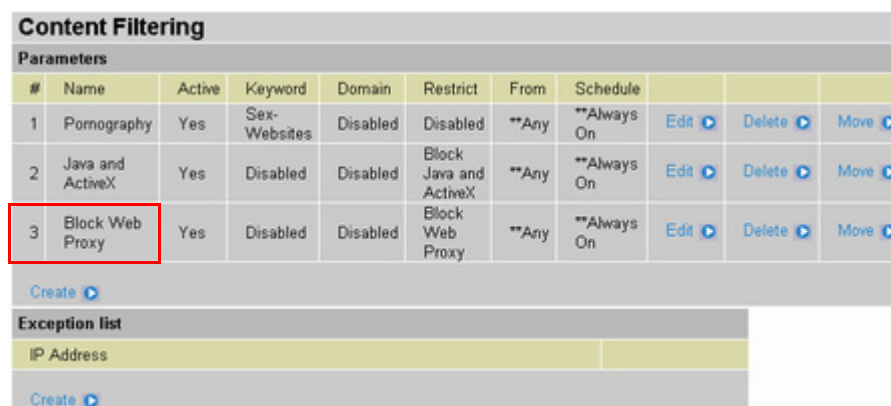
- Click **Configuration** → **Policy** → **Content Filtering**.



- Click **Create** to create a new content filter.



- Type a descriptive name for this content filter, and next to **Active** check **Enable** to activate this content filter.
- Next to **Restrict Feature**, check **Enable** and select the new profile from the drop-down list.
- Click **Apply**. The new content filter is added to the list.



From here you can **Edit** or **Delete** the filter.

You can also **Move** the filter, which changes the policy rule priority. The rule priority can be moved higher or lower by selecting before or after a specified rule number, which changes the order of the rules. See [What does the Rule No. mean in Packet Filtering? Is it related to the priority?](#) on page 110.

QUESTION: What is “Block Cookies” in Restrict Features?

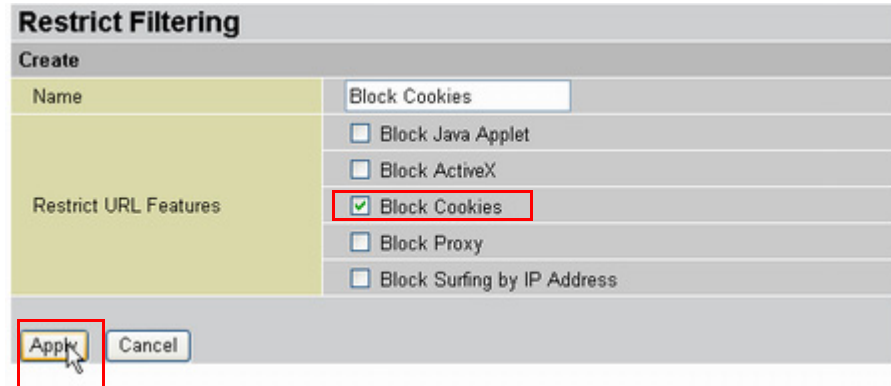
ANSWER: This policy blocks the saving/reading of cookies. Both secure and insecure web-sites are blocked from using this function.

To block cookies, follow these instructions.

1. Click **Configuration** → **Network Object** → **Content Blocking** → **Restrict URL Feature**.



2. Click **Create** to create a **Restrict Filtering** profile.

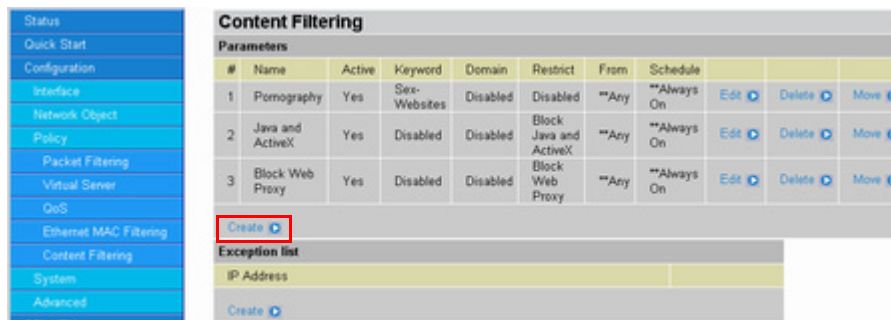


3. Type a descriptive name in the text box and check the **Block Proxy** box.
4. Click **Apply**. The new profile is added to the list.

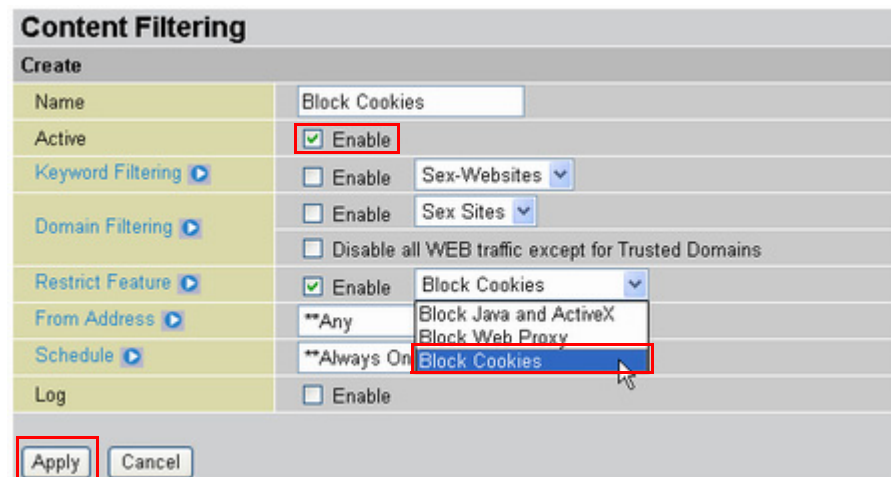


From here you can **Edit** or **Delete** the profile.
Now you can enable the **Restrict URL Feature**.

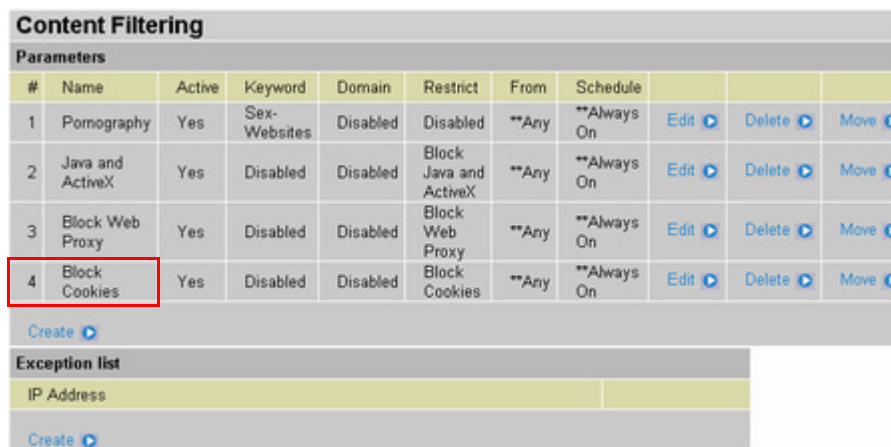
- Click **Configuration** → **Policy** → **Content Filtering**.



- Click **Create** to create a new content filter.



- Type a descriptive name for this content filter, and next to **Active** check **Enable** to activate this content filter.
- Next to **Restrict Feature**, check **Enable** and select the new profile from the drop-down list.
- Click **Apply**. The new content filter is added to the list.



From here you can **Edit** or **Delete** the filter.

You can also **Move** the filter, which changes the policy rule priority. The rule priority can be moved higher or lower by selecting before or after a specified rule number, which changes the order of the rules. See [What does the Rule No. mean in Packet Filtering? Is it related to the priority?](#) on page 110.

QUESTION: What is “Block Surfing by IP Address” in the Restrict Features?

ANSWER: Enabling the Block Surfing by IP Address policy prevents users from bypassing the Domain Filter function by blocking designated IP addresses from accessing the Internet (See example below).

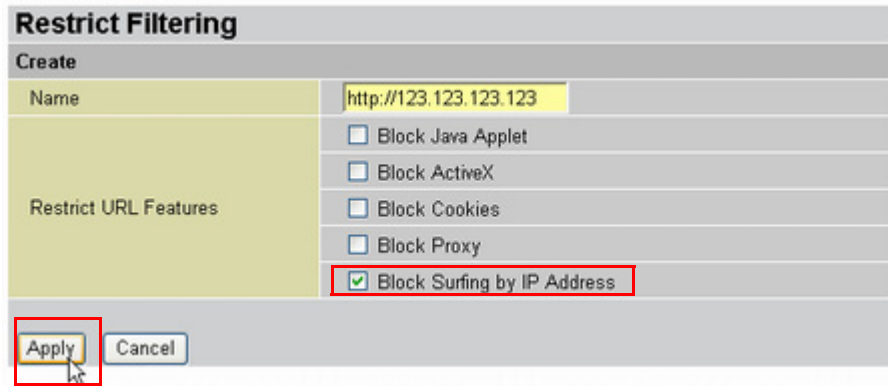
Example:

The IP address http://123.123.123.123 will be blocked if this option is enabled. Follow these instructions.

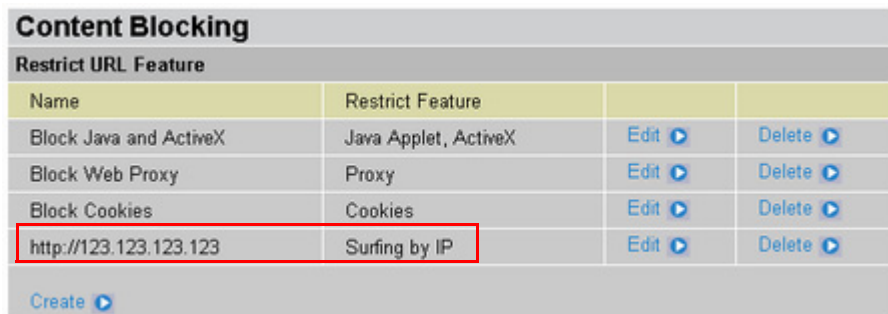
1. Click **Configuration** → **Network Object** → **Content Blocking** → **Restrict URL Feature**.



2. Click **Create** to create a **Restrict Filtering** profile.

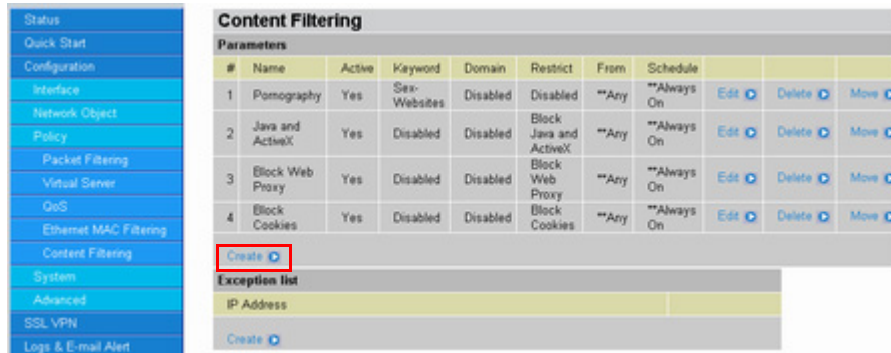


3. Type the IP address (in this case “http://123.123.123.123”) in the text box and check the **Block Surfing by IP Address** box.
4. Click **Apply**. The new profile is added to the list.

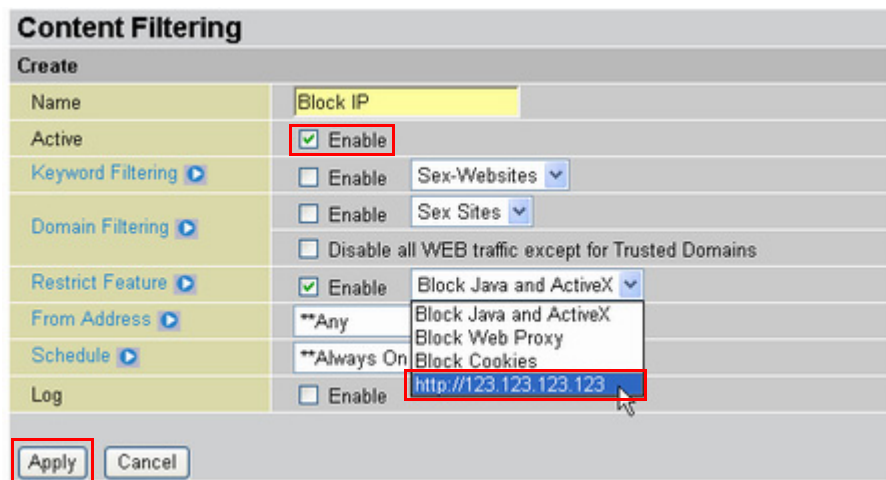


From here you can **Edit** or **Delete** the profile.
 Now you can enable the **Restrict URL Feature**.

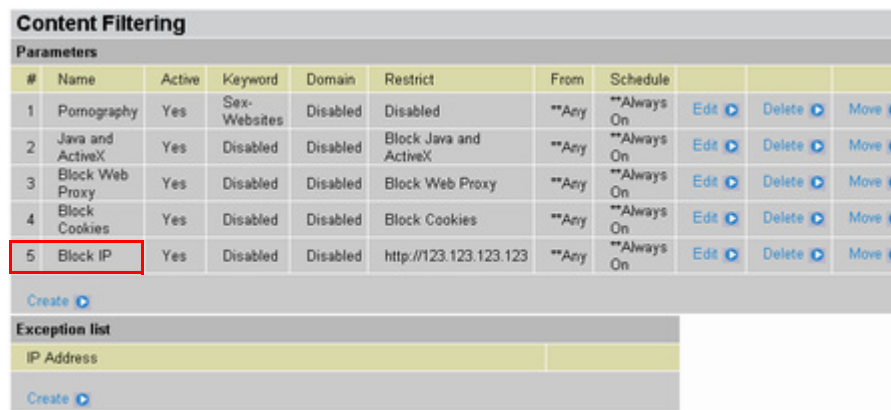
5. Click **Configuration** → **Policy** → **Content Filtering**.



6. Click **Create** to create a new content filter.



7. Type a descriptive name for this content filter, and next to **Active** check **Enable** to activate this content filter.
8. Next to **Restrict Feature**, check **Enable** and select the new profile from the drop-down list.
9. Click **Apply**. The new content filter is added to the list.



From here you can **Edit** or **Delete** the filter.

You can also **Move** the filter, which changes the policy rule priority. The rule priority can be moved higher or lower by selecting before or after a specified rule number, which changes the order of the rules. See [What does the Rule No. mean in Packet Filtering? Is it related to the priority?](#) on page 110.

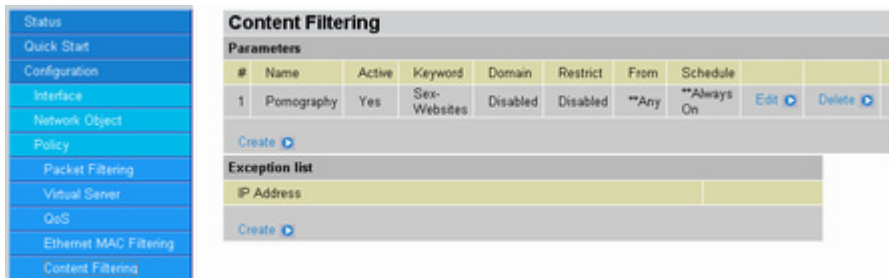
QUESTION: What is “Exception List” in the Content Filtering?

ANSWER: Exception List is an option to exclude an IP address from content filtering policies (See example below).

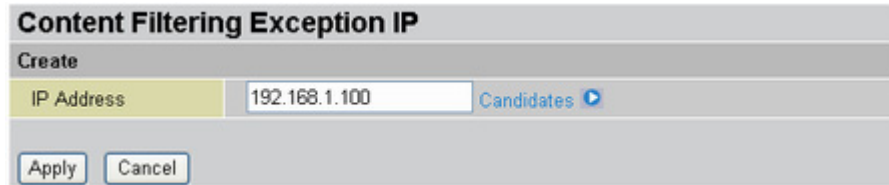
Example:

The user wants to place IP address 192.168.1.100 in the exception list.

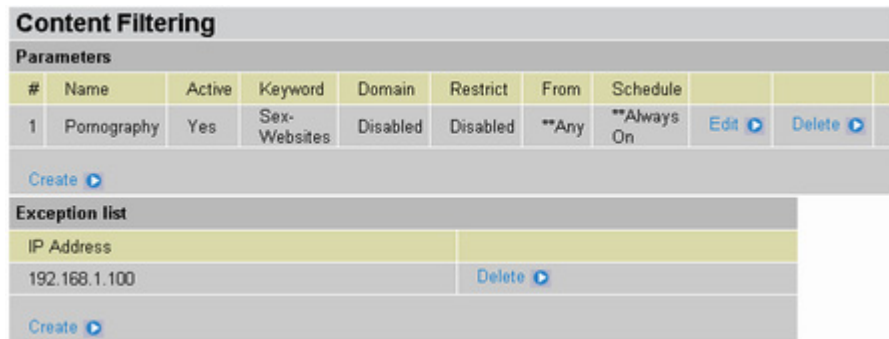
1. Click **Configuration** → **Policy** → **Content Filtering**.



2. Under **Exception List**, click **Create**.



3. Type the IP address you want excepted (in this case “192.168.1.100”), or click **Candidates** and select an available IP address from the list.
4. Click **Apply**. The IP address is added to the **Exception List**.



5. To remove the IP address from the **Exception List**, click **Delete**.

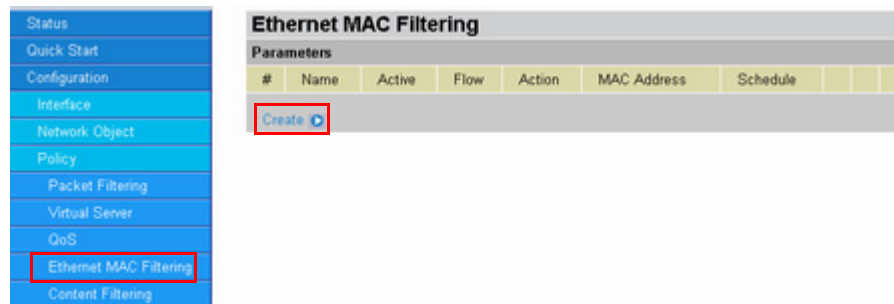
QUESTION: What is Ethernet MAC filtering? How do I use it?

ANSWER: The BiGuard S10 Series checks MAC addresses against a list of allowed or denied addresses before responding to a request. The following examples show a list of MAC filters.

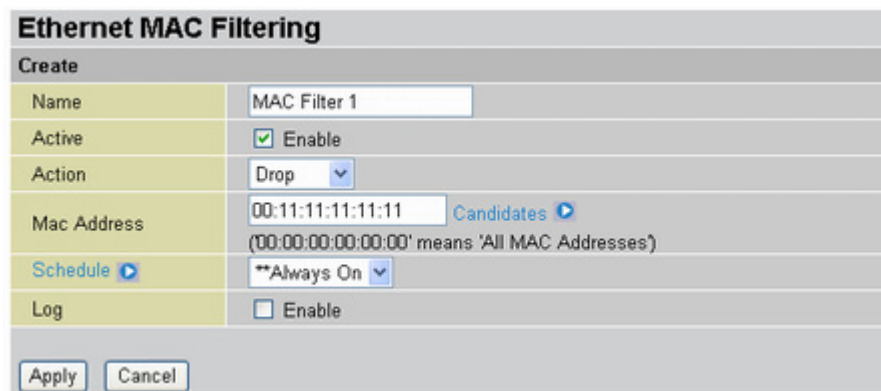
Example 1:

The user wants MAC addresses to be able to access the Internet except 00:11:11:11:11:11.

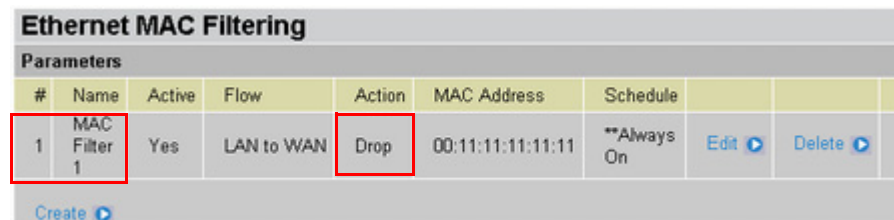
1. Click **Configuration** → **Policy** → **Ethernet MAC Filtering**.



2. Click **Create** to add an Ethernet MAC filter.



3. Type a descriptive name for this filter and check **Enable** next to **Active** to activate the filter.
4. From the Action drop-down list, select Drop.
5. Type the MAC address in the text box or click **Candidates** and select an available MAC address from the list.
6. Click **Apply**. The new filter is added to the list.



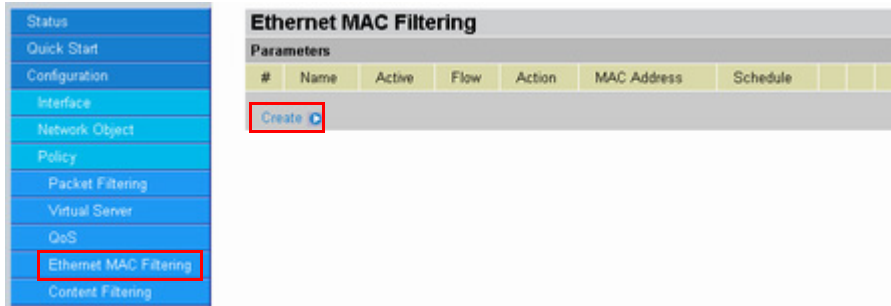
Example 2:

The user wants to block all MAC addresses (computers on the LAN) with the exception of address 00:11:11:11:11:11 from accessing the Internet.

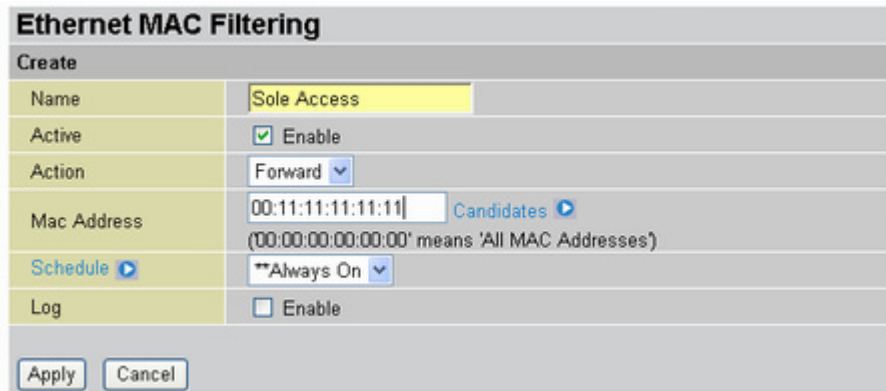


NOTE: 00:00:00:00:00:00 DESIGNATES ALL MAC ADDRESS. THE RULE NO. (#) DESIGNATES PRIORITY.

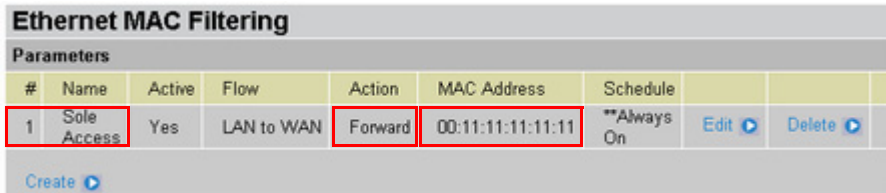
1. Click **Configuration** → **Policy** → **Ethernet MAC Filtering**.



2. Click **Create** to add an Ethernet MAC filter.



3. Type a descriptive name for this filter and check **Enable** next to **Active** to activate the filter.
4. From the **Action** drop-down list, select **Forward**.
5. Type the MAC address in the text box or click **Candidates** and select an available MAC address from the list.
6. Click **Apply**. The new filter is added to the list.



This filter allows the designated MAC address (00:11:11:11:11:11) to have access to the Internet. Now, the user will create a filter that prevents all other MAC addresses from accessing the Internet.

- Click **Create** to add the next MAC filter.

- Type a descriptive name for this filter and check **Enable** next to **Active** to activate the filter.
- From the **Action** drop-down list, select **Drop**.



WARNING: WHEN CONFIGURING THE DEFAULT LAN MAC FILTER RULE TO “DROP”, FIRST ADD THE ADMINISTRATOR’S MAC ADDRESS TO A FORWARD RULE. OTHERWISE, YOU WILL EXPERIENCE PROBLEMS IN CONFIGURING THE BIGUARD S10 SERIES.

- Type 00:00:00:00:00:00 in the text box. This designates the filter to be applied to all MAC addresses.
- Click **Apply**. The new filter is added to the list.

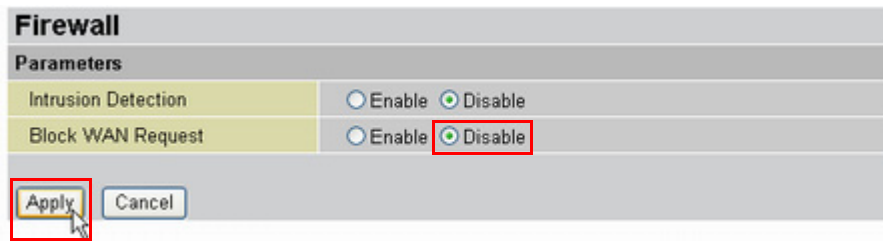
| # | Name | Active | Flow | Action | MAC Address | Schedule | Edit | Delete | Move |
|---|-------------|--------|------------|---------|-------------------|-------------|------|--------|------|
| 1 | Sole Access | Yes | LAN to WAN | Forward | 00:11:11:11:11:11 | **Always On | Edit | Delete | Move |
| 2 | No Access | Yes | LAN to WAN | Drop | 00:00:00:00:00:00 | **Always On | Edit | Delete | Move |

QUESTION: Why can't I ping the WAN IP address of the BiGuard S10 Series from the Internet?

ANSWER: Make sure the Block WAN Request is disabled.

- Click **Configuration** → **Advanced** → **Firewall**.

- Next to **Block WAN Request**, click the **Disable** radio button.



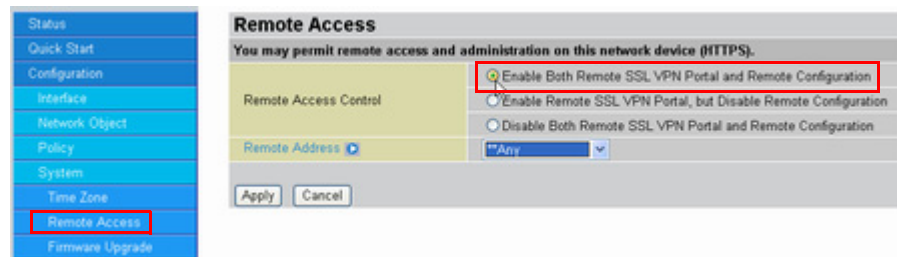
- Click **Apply**.

You can now ping the BiGuard S10 WAN IP address.

Remote Access

QUESTION: How do I remotely configure the BiGuard S10 Series?

ANSWER: Browse to <http://BiGuard-S-WAN-IP-Address> or <https://BiGuard-S-WAN-IP-Address> and ensure that the Remote Access function is enabled in the **System** → **Remote Access** menu.



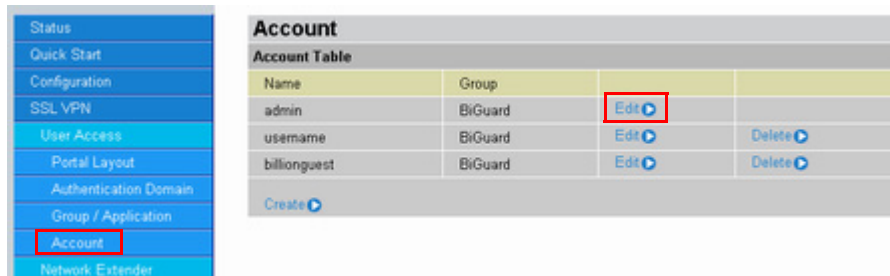
Click **Apply** to save the settings.

QUESTION: What's the Auto log-out timer?

ANSWER: There is an inactivity timeout within the configuration pages. The default value for all the users (including the administrator) is 5 minutes. If there is no activity within the configuration pages after the idle timeout limit is reached, you will be automatically logged out by the BiGuard S10 Series.

You can configure the auto logout timer value in the "Inactivity Timeout" field.

- Click **SSL VPN** → **User Access** → **Account**.



- Click **Edit** next to the account you would like to alter (for example, "admin").

| Edit Account | |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| General Setting | |
| Name | admin |
| Group | BiGuard |
| Password | ***** |
| Retype Password | ***** |
| Inactivity Timeout | 20 Minutes |
| Service | |
| Network Places | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Network Extender Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Transport Extender Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Web Cache Cleaner | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Network Extender IP Assignment | <input checked="" type="radio"/> Dynamic Assign <input type="radio"/> Fix IP 192.168.1.240 |
| Greeting String | <input checked="" type="radio"/> Default <input type="radio"/> Custom Welcome to the BiGuard ! |
| Application Proxy | |
| Applications | <input type="checkbox"/> FTP |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

- In the **Inactivity Timeout** text box, type the number of minutes you would like to change the auto logout timer to be.
- Click **Apply** to save the changes.

QUESTION: Can upgrade firmware remotely from the WAN port?

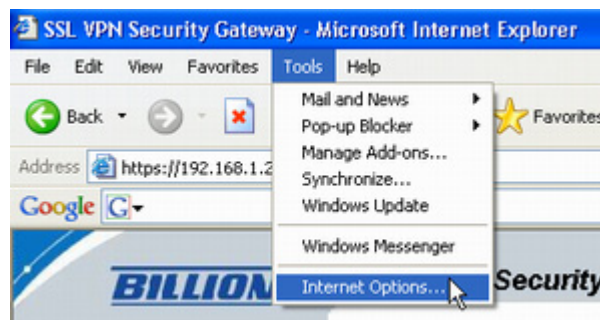
ANSWER: Yes, but we do not recommend doing so as Internet service reliability varies between areas.

QUESTION: I've just upgraded the router firmware to the latest version, but I found some of the buttons or pages don't display or work properly.

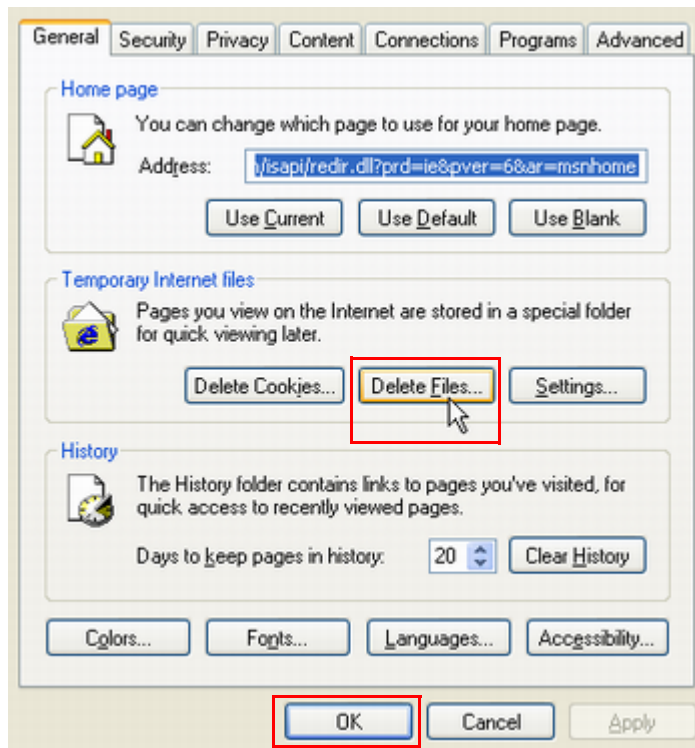
ANSWER: It is possible that the browser is referencing data stored in the cache. Clear the offline browser data in the cache, restart the browser, and try again.

To clear the cache in Internet Explorer, do the following:

- Open the Internet Explorer browser, select **Tools** → **Internet Options**.



2. In the **General** settings tab, click **Delete Files** and click **OK**.



SNMP

QUESTION: What type of SNMP MIBs are supported by the BiGuard S10 Series?

ANSWER: The following MIBs are supported by the BiGuard S10 Series:

- RFC1213(MIB-II);
- System group
- Interfaces group
- Address Translation group
- IP group
- ICMP group
- TCP group
- UDP group
- SNMP group

SSL Knowledge

QUESTION: What browser and version do I need to successfully connect to the BiGuard S10 Series?

ANSWER: It is strongly recommended that the following browsers be used for successful connection:

- Internet Explorer 6.0SP1 (supports Microsoft Internet Explorer 5.01 or newer)
- Mozilla 1.7.1 and newer
- Firefox 1.0.6 and newer
- Opera 8.02 and newer
- Safari 1.3.1 and newer

QUESTION: What needs to be activated on the browser for me to successfully connect to the BiGuard S10 Series?

ANSWER: The following options on the browser need to be enabled for successful connection:

- SSLv2, SSLv3, or TLS
- Cookies
- Pop-ups for the site
- Java
- Javascript
- ActiveX



NOTE: ALTHOUGH SSLV2 IS SUPPORTED, IT IS RECOMMENDED TO USE SSLV3 OR TLS FOR OPTIMUM COMPATIBILITY.

QUESTION: What version of Java do I need?

ANSWER: You will need to install Sun's JRE 1.3.1 or newer (available for download at <http://www.java.com>) to use some of the features on the BiGuard S10 Series, but we recommend using version 1.5 or newer (**Note:** the Sun designation is version 5.0).

If you are experiencing issues with the RDP5 Java component, upgrade to the newest Java version.

SSL Applications

QUESTION: What SSL Applications does the BiGuard S10 Series provide? What do they do?

ANSWER: The Billion BiGuard S10 Series provides clientless, identity-based, secure remote access to your protected internal network. Using the 'SSL VPN Portal' environment, the Billion BiGuard S10 Series can provide users with secure remote access to your entire private network, or to individual components such as file shares, web-servers, FTP servers, remote desktops, or even individual applications hosted on Microsoft Terminal Servers. These various methods of secure remote access are provided by the following components:

- **Network Extender** - Network Extender can provide remote users with full access to your protected internal network. The experience is virtually identical to that delivered by traditional IPSec VPN clients, but Network Extender does not require any manual client installation. Instead, the Network Extender client is automatically installed on remote user's PCs which instantiates a virtual adapter for SSL-secure point-to-point access to permitted hosts and subnets on the internal network.
- **Transport Extender** - Transport Extender is a feature that allows only specified Protocol and IP addresses to be accessible with SSL encryption, which provides a more secure connection during transmission. Transport Extender can be used in services with static listening ports such as a POP3 or SMTP Server.
- **Network Place** - Network Place provides remote users with a secure web-interface to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a web-interface, similar in style to Microsoft's familiar "Network Neighborhood" or "My Network Places", Network Place allows users with appropriate permissions to browse network shares, delete, retrieve, and upload files.
- **Application Proxy** - Application Proxy is the more finely granular components of a trusted network, which can be accessed through the SSL VPN. Network Resources can be pre-defined by the administrator and assigned to users or groups as proxies for remote users. The BiGuard S10 Series utilizes integrated client so all the applications will be shown as web-based, therefore, users do not need to install the client software for each application.

Application Proxy is comprised of the following remote access capabilities:

- **Terminal Service (RDP5)** - Terminal Service (RDP5) is the current version of Microsoft's Remote Desktop Protocol. Because of its increased functionality (such as session sound and full-screen mode) it is only able to operate in conjunction with an ActiveX client (such as Internet Explorer 6.0.2800 or later).
- **Virtual Network Computing (VNC)** - Virtual Network Computing (VNC) was originally developed by AT&T, but is today widely available as open source. Any one of the many variants of VNC server available can be installed on most any workstation or server for remote access. The VNC client to connect to those servers is delivered to remote users through the web-browser as a Java client.

- **File Transfer Protocol (FTP)** - File Transfer Protocol (FTP) Proxy access to an FTP server on the internal network, or any other network segment that can be reached by the SSL VPN, including the Internet. The remote user communicates with the BiGuard S10 Series by HTTPS then FTP allows users with appropriate permissions to upload, download, or create folders in a similar fashion to an FTP client.
- **Telnet (Java)** - A Java based telnet client delivered through the remote user's web-browser. The remote user can access the IP address specified by the administrator of any accessible telnet server via an SSL VPN connection, the proxy then communicates between the user (over SSL) and the server (using native telnet).
- **Secure Shell (SSH)** - A Java based SSH client delivered through the remote user's web-browser. The remote user can access the IP address specified by the administrator of any accessible SSH server via an SSL VPN connection, the proxy then communicates between the user (over SSL) and the server (using native encrypted SSH).
- **Web (HTTP)** - Web (HTTP) Proxy access to an HTTP server on the internal network, or any other network segment that can be reached by the BiGuard S10 Series. The remote user communicates with the BiGuard S10 Series by HTTPS (using an administrator predefined URL), which is retrieved over HTTP by the SSL VPN, through URL request and BiGuard S10 series will redirect the request to a https server in your network. Web-application session authentication is supported, as are many popular web applications or web email systems, including Microsoft Outlook Web Access.
- **Secure Web (HTTPS)** - Proxy access to an HTTPS server on the internal network, or any other network segment that can be reached by the BiGuard S10 Series. The remote user communicates with the BiGuard S10 Series by HTTPS (using an administrator predefined URL), which is retrieved over HTTPS by the SSL VPN, unencrypted, through URL request and BiGuard S10 series will redirect the request to a https server in your network. Web-application session authentication is supported, as are many popular web applications, including Microsoft Outlook Web Access.

Adding an application proxy

QUESTION: How do I add an application proxy for remote users?

ANSWER: You can add applications proxies through the SSL VPN Group/Application menu.

Example:

You want to add an FTP application to the BiGuard group. Follow these instructions:

1. Click **SSL VPN** → **User Access** → **Group/Application**.

The screenshot shows the management interface. On the left is a vertical navigation menu with the following items: Status, Quick Start, Configuration, SSL VPN, User Access, Portal Layout, Authentication Domain, Group / Application (highlighted with a red box), and Account. The main content area is titled 'Group/Application' and contains a 'Group Table' with the following data:

| Name | Authentication Domain | Domain's Default Group | |
|---------|-----------------------|------------------------|------|
| ftp1 | ftp1 | Yes | Edit |
| BiGuard | BiGuard | Yes | Edit |

Below the table is a 'Create' button. The 'Edit' buttons in the table are highlighted with red boxes.

- Click **Edit** to modify the group settings.

Edit Group

General Settings

| | |
|------------|---------|
| Group Name | BiGuard |
| Domain | BiGuard |

Application Table Add Application ▶

| Name | Application | IP Address / Path | | |
|----------------------------------------------------------------|-------------|-------------------|--|--|
| Note! To make application changes, press Apply . | | | | |

Apply Cancel

- Click **Add Application**.

SSL VPN Application

Add Application

| | |
|------------------|---------------------------------|
| Application Name | BiGuard FTP |
| Application | Terminal Service (RDP5) ▼ |
| IP Address | Terminal Service (RDP5) |
| Screen Size | Virtual Network Computing (VNC) |

Apply Cancel

- File Transfer Protocol (FTP) ▶
- Telnet
- Secure Shell (SSH)
- Web (HTTP)
- Secure Web (HTTPS)

- Type a descriptive name for the application, and select the application (FTP in this case) from the **Application** drop down list.
- Type the designated IP address in the **IP Address** text box.
- Click **Apply**. The application is added to the list.

Edit Group

General Settings

| | |
|------------|---------|
| Group Name | BiGuard |
| Domain | BiGuard |

Application Table Add Application ▶

| Name | Application | IP Address / Path | | |
|-------------|-------------|-------------------|------------------------------------------------------------------|--------------------------------------------------------------------|
| BiGuard FTP | FTP | 192.168.1.200 | Edit ▶ | Delete ▶ |

Note! To make application changes, press **Apply**.

Apply Cancel

From here you can **Edit** or **Delete** the application.

- Click **Apply** to save the new settings and exit the **Edit Group** screen. Users can now be added to the FTP server through the SSL VPN menu.
- Select **SSL VPN** → **User Access** → **Account**.

Account

Account Table

| Name | Group | | |
|-------------|---------|---------------------|-----------------------|
| admin | BiGuard | Edit ▶ | |
| username | BiGuard | Edit ▶ | Delete ▶ |
| billonguest | BiGuard | Edit ▶ | Delete ▶ |

Create ▶

- Click **Create** to add an account.

- Type the user name and ensure the correct group is selected from the drop-down list.
- Type a password in the text box, and retype the password for confirmation.
- Check the **Application Proxy Applications** box (in this case “BiGuard FTP”).
- Click **Apply**.
- Log out of the web configuration and log on again as the new user.

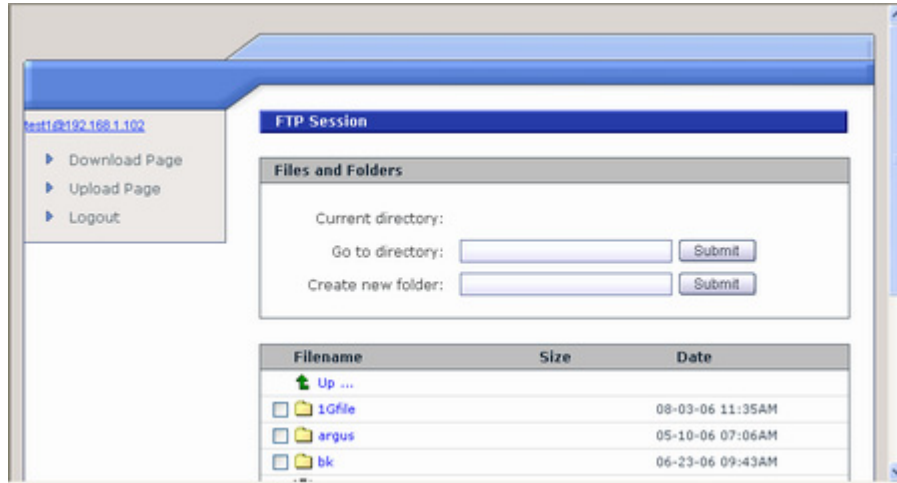
After you click **Login**, the following screen will be displayed.

| Application Name | Host Address | Service | Connection |
|------------------|---------------|---------|-------------------------|
| BiGuard FTP | 192.168.1.200 | FTP | Connect |

The FTP server is now ready for use.

15. Click **Connect** for access.

A new FTP browser screen is displayed for FTP access:



NOTE: THE SINGLE SIGN ON (SSO) FEATURE CAN ONLY BE USED IF THE USER HAS THE SAME USER NAME AND PASSWORD ON THE REMOTE SIGN ON SERVER AND THE FTP SERVER.

Using Network Extender

QUESTION: How do I set up Network Extender?

ANSWER: Use the following guide to set up Network Extender.

1. Click **Quick Start** → **SSL VPN**.

| Quick Start SSL VPN | | |
|------------------------------------------------------------------------|------------------|---------------------------------|
| Please select an "Application Group" from the below Group option | | |
| Group | BiGuard | |
| The information of the selected Group "BiGuard" Authentication Domain" | | |
| Authentication Domain Name | BiGuard | |
| Authentication Type | local | |
| Authentication Server | Local Machine | |
| The pre-defined Applications of the selected Group | | Add Application |
| Application Name | Application Type | IP Address / Path |
| BiGuard FTP | FTP | 192.168.1.200 |
| Next | | |

2. Select the group to add the user account to from the drop-down list and click **Next**.

Quick Start SSL VPN

Create the account user name and password

| | |
|-----------------|----------------------------------------|
| User Name | <input type="text" value="Username"/> |
| Password | <input type="password" value="*****"/> |
| Retype Password | <input type="password" value="*****"/> |

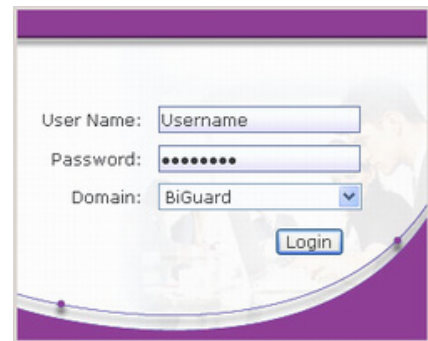
Enable or disable services

| | |
|--------------------------|-----------------------------------------------------------------------|
| Network Places | <input type="radio"/> Enable <input type="radio"/> Disable |
| Network Extender Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |

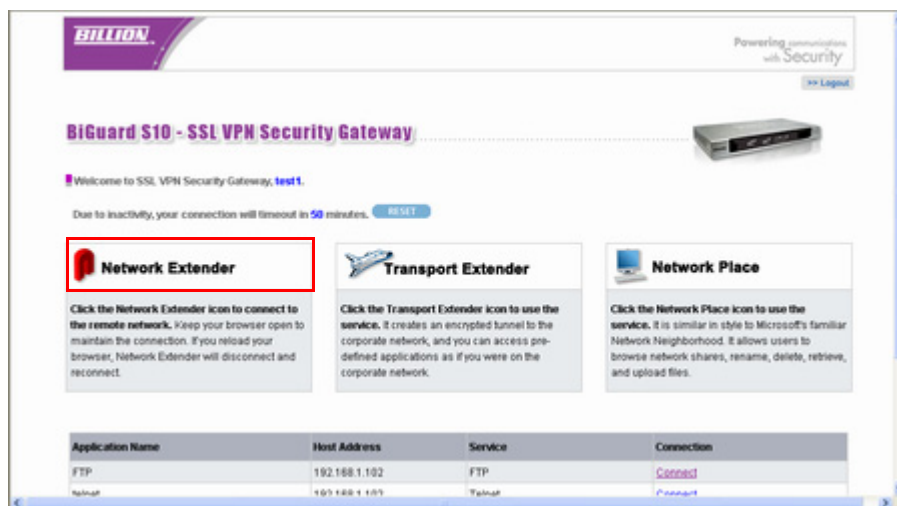
Select available applications

| | |
|--------------|-------------------------------------------------|
| Group | BiGuard |
| Applications | <input checked="" type="checkbox"/> BiGuard FTP |

3. Type the user name and the password. Retype the password for confirmation.
4. Ensure the **Network Extender Service** button is enabled.
5. Click **Apply**:
6. Log out and log in again as the new user.

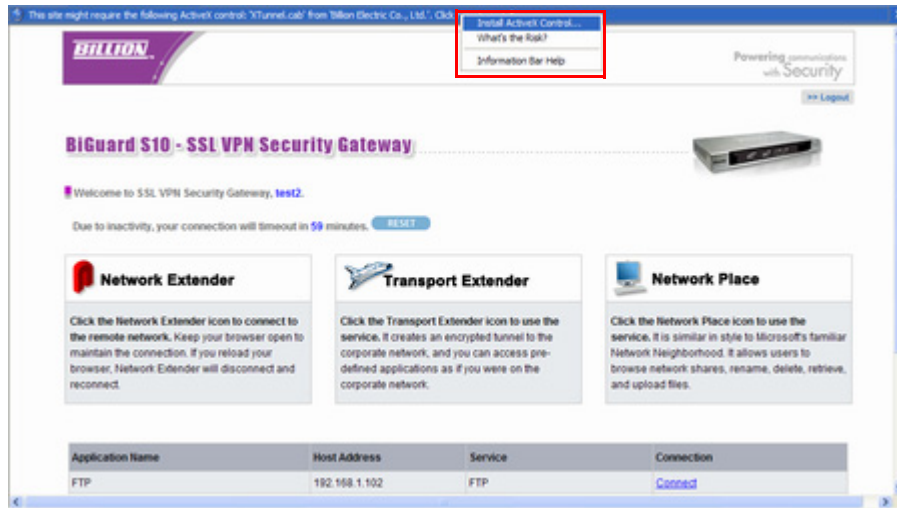


The following screen is displayed

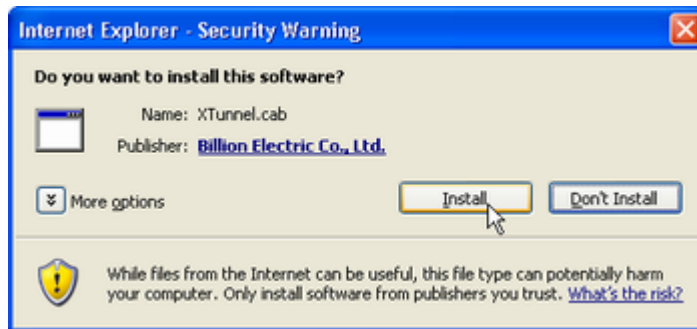


7. Click **Network Extender**.

A drop-down message appears at the top of your browser, prompting you to Install an ActiveX Control.



8. Click **Install ActiveX Control**.
A Security Message is displayed.



9. Click **Install**.
The installation begins and you see this screen.



A Hardware Installation message appears.



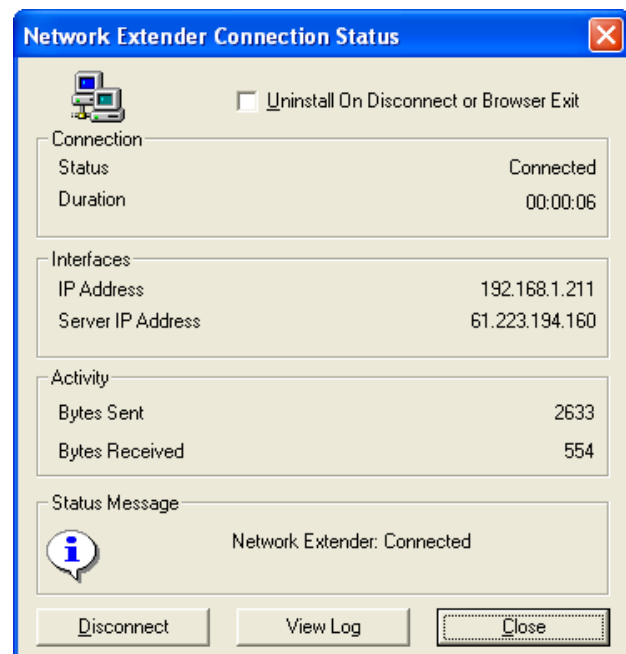
10. Click **Continue Anyway**.

After setup is complete, an icon

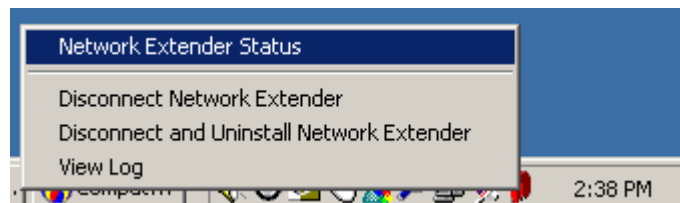


appears in the task bar, indicating that the Network Extender is active and the following screen appears.

- Check **Uninstall On Disconnect or Browser Exit** to have the system uninstall the driver every time you disconnect the Network Extender. If this box is left unchecked, ActiveX Control will not need to be installed when you log on again. If the box is checked, ActiveX will uninstall itself when you log off to prevent unauthorized access, for example, if a public domain terminal was used to access Network Extender.
- Click **Disconnect** to disconnect the Network Extender.
- Click **View Log** to view a log of Network Extender processes.
- Click **Close** to close the status screen. Network Extender is still active in the status bar.



To view the status screen again, or perform one of the actions above, right-click the Network Extender icon, and select an option from the menu.



QUESTION: What is the Client Address in Network Extender?

ANSWER: The Client Address is for an Administrator to set the IP range in order to distribute IP addresses for Network Extender users.

QUESTION: What is the Client Route in Network Extender?

ANSWER: Client Route allows you to set routing rules for the Network Extender client user's connection. For example, if the client user's internet packet's destination address is specified in Client Route, the packet will be forwarded to the PPP connection passing through the BiGuard S10 Series via the SSL VPN tunnel.

QUESTION: I have successfully created a Network Extender connection, but I cannot access my corporation network, what is going on?

ANSWER: Ensure that your Client Address (192.168.1.210~192.168.1.230 by default) is in the same subnet as your BiGuard S10 Series LAN network address (192.168.1.254 by default). Alternatively, if your client address is not the same as your BiGuard S10 Series LAN network address you have to add a client route to your LAN network address as a routing table for Network Extender connection, if you would like to access the LAN network resources.

Using Transport Extender

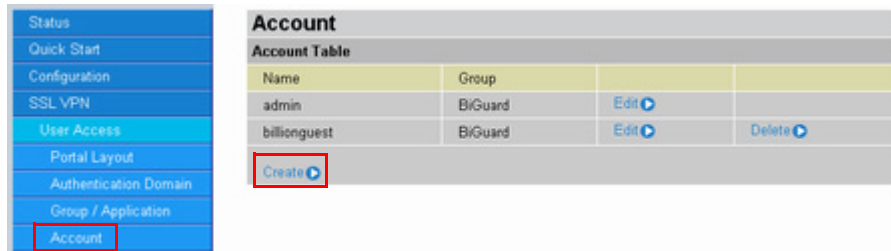
QUESTION: What is Transport Extender?

ANSWER: Transport Extender is a feature that allows only specified Protocol and IP addresses to be accessible with SSL encryption. This will provide more restricted secure connections to only the specified IP address and port number. Transport Extender can be used in services with static listening ports such as a POP3 or SMTP Server.

QUESTION: How do I setup Transport Extender?

ANSWER: Use the following guide to set up Transport Extender.

1. Click **SSL VPN** → **User Access** → **Account**.



2. Click **Create**.

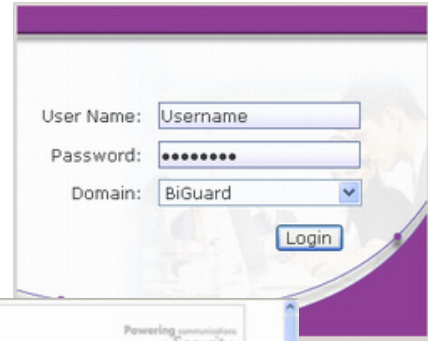
The **Add Account** page is displayed.

3. Type the user name and the password. Retype the password for confirmation.
4. Select the **Group** that you want to assign the user to from the drop-down list.
5. Click the Transport Extender Service **Enable** button.
6. Click **Apply**.
7. Click **SSL VPN** → **Transport Extender** → **Application**.

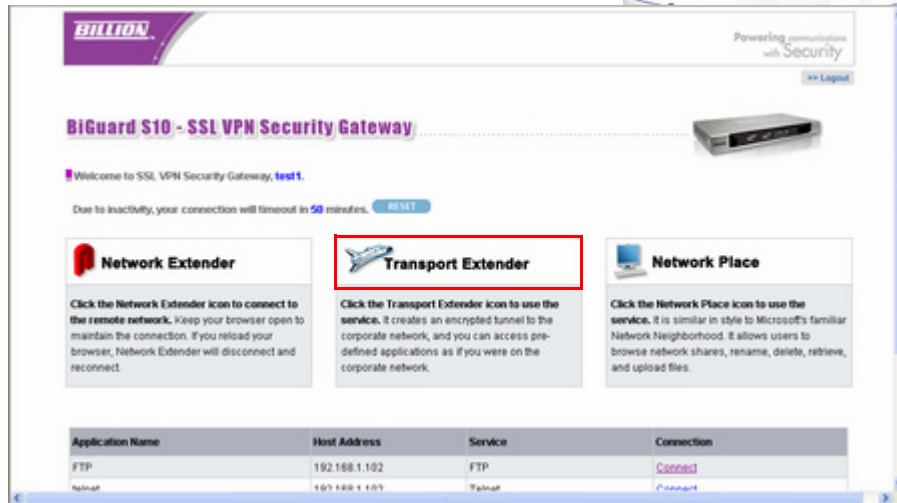
8. Click **Create**.
- The Transport Extender page is displayed.

9. Type the local server Fixed IP address, and TCP Port Number to be used by Transport Extender (192.168.1.254 and 110, in the example) and click **Apply**:

- Log out and log in to the BiGuard S10 as the remote user created.

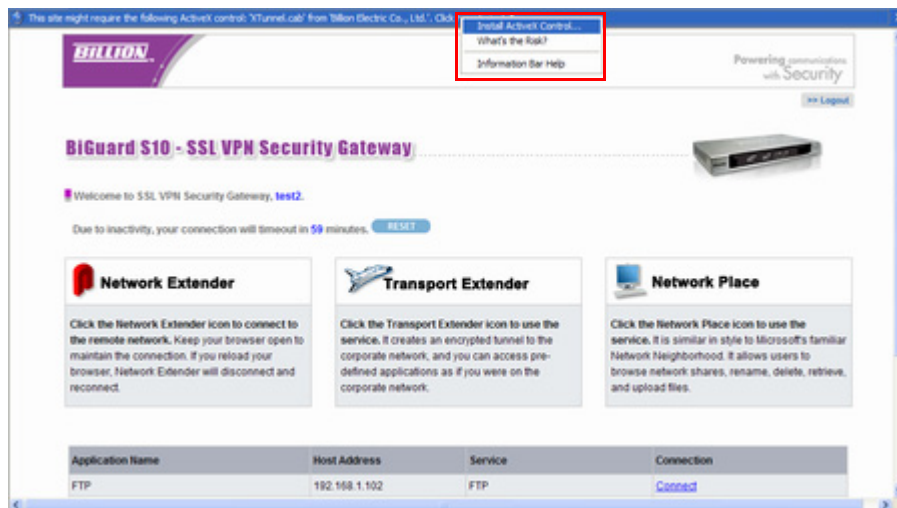


The following screen is displayed



- Click **Transport Extender**.

A drop-down message appears at the top of your browser, prompting you to Install an ActiveX Control.




- Click **Install ActiveX Control**.

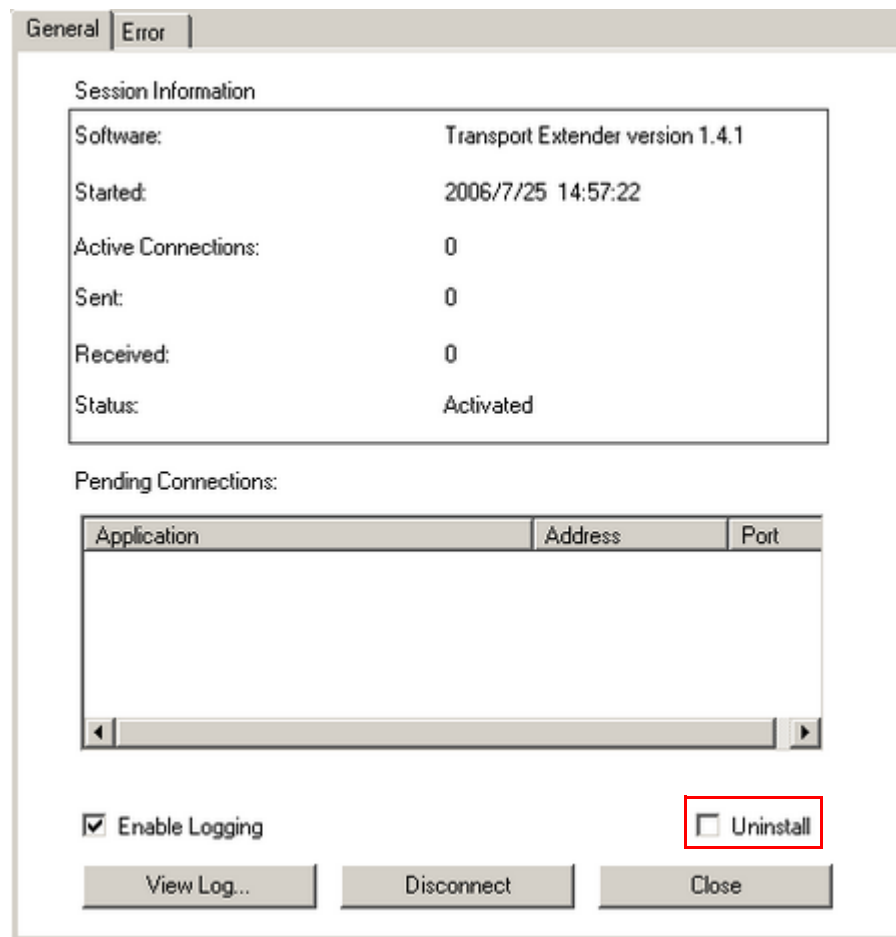
A Security Message will be displayed.



13. Click **Install**.

The Transport Extender installs.

After setup is complete, an icon  appears in the task bar, indicating that the Network Extender is active and the following screen appears.



This screen displays the session information and a list of pending connections for applications.

- Click the **Error** tab to view a list of session errors.
- Check **Enable Logging** to allow the system to log all activity for the session.
- Click **View Log** to view a session log.
- Check **Uninstall** if you want to uninstall the driver upon disconnecting. If this box is left un-checked, ActiveX Control will not need to be installed when you log on again. If the box is checked, ActiveX will uninstall itself when you log off to prevent unauthorized access, for example, if a public domain terminal was used to access Transport Extender.
- Click **Disconnect** to disconnect the Transport Extender.
- Click **Close** to close the Transport Extender screen. Transport Extender is still active in the status bar.

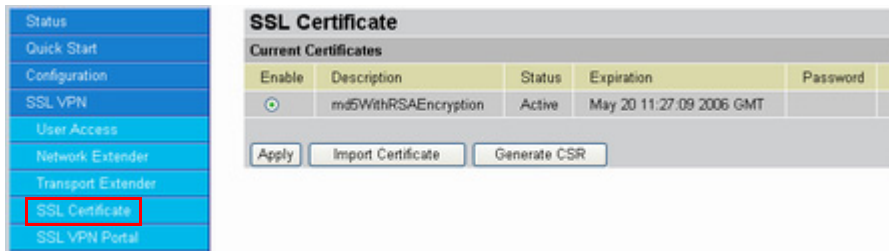
To view the Transport Extender screen again, or disconnect the Transport Extender, right-click the Transport Extender icon and select an option from the menu.



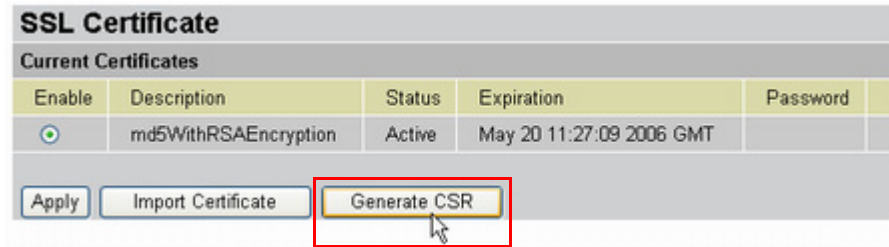
Importing a certificate

Follow these instructions to import an SSL certificate.

1. Click **SSL VPN** → **SSL Certificate**.



2. Click **Generate CSR**.



You are prompted to fill out a CSR (Certificate Signing Request) form.


| SSL Certificate | |
|----------------------------------------------------------------------------|---------------------------------------------|
| Generate Certificate Signing Request (CSR) | |
| Name | <input type="text" value="Name"/> |
| Organization | <input type="text" value="Org"/> |
| Unit/Department | <input type="text" value="Unit"/> |
| City/Locality | <input type="text" value="City"/> |
| State (Full Name) | <input type="text" value="State"/> |
| Country | <input type="text" value="TW"/> |
| FQDN (Domain Name) | <input type="text" value="www.bgs10.com"/> |
| Email | <input type="text" value="mail@bgs10.com"/> |
| Password | <input type="password" value="*****"/> |
| New Key Pair Length | <input type="text" value="1024"/> |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

- **Name:** Type your name.
- **Organization:** Type your organization.
- **Unit/Department:** Type the department you belong to.
- **City/Locality:** Type your city.
- **State (Full Name):** If in the US, type the name of your State.
- **Country:** Type your two letter country code
- **FQDN (Domain Name):** Type the FQDN (Fully Qualified Domain Name). The FQDN is the complete domain name for a specific host on the Internet, and consists of the host name and domain name (for example, "www.billion.com").
- **Email:** Type your email address.
- **Password:** Type a password. Ensure that you write the password in a safe place.
- **New Key Pair Length:** This item refers to the strength of the key encryption for the private key (extracted from the zip file)



NOTE: THE COUNTRY CODE IS TWO ENGLISH CHARACTERS. BE SURE TO WRITE THE PASSWORD DOWN AND PUT IT IN A SAFE PLACE.

3. Click **Apply**. The browser prompts you to download the zipped CSR file, which includes your private key (server.key) and CSR (csr) files.

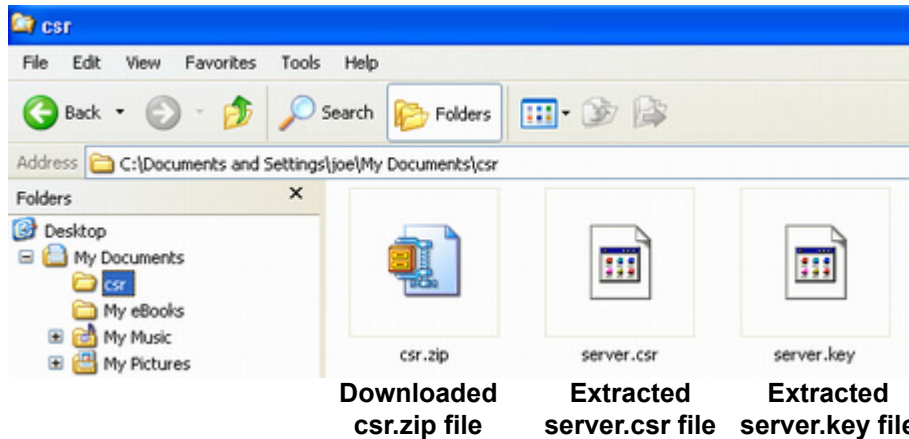
 Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: csr.zip
 File type: ACDSee ZIP Archive
 From: 192.168.1.254

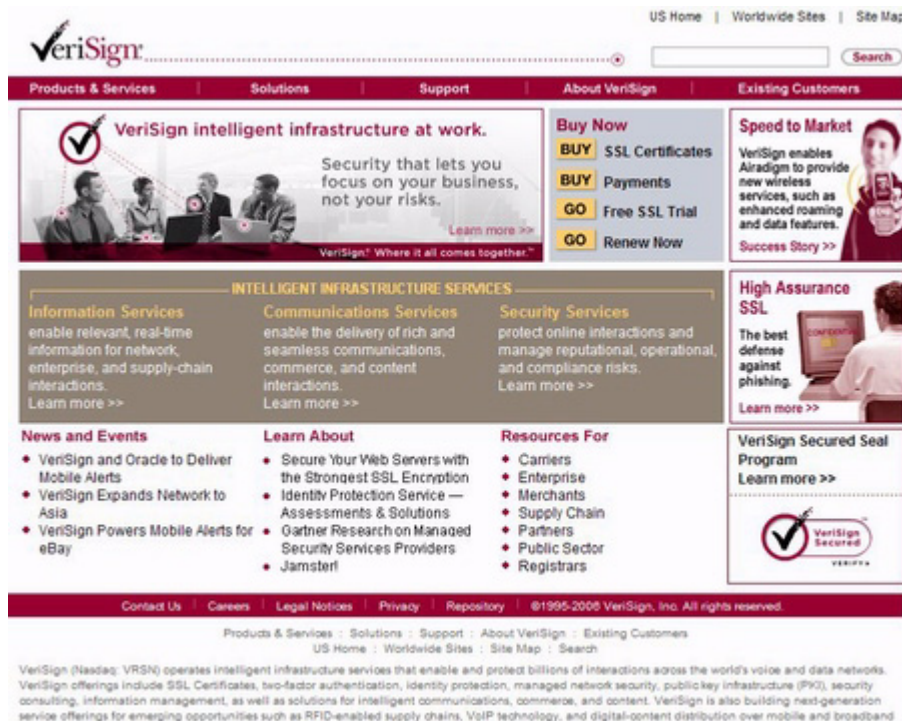
Would you like to open the file or save it to your computer?

Always ask before opening this type of file

- Click **Save**. You are prompted for a download location. Save the file to your computer and extract the files to a folder.

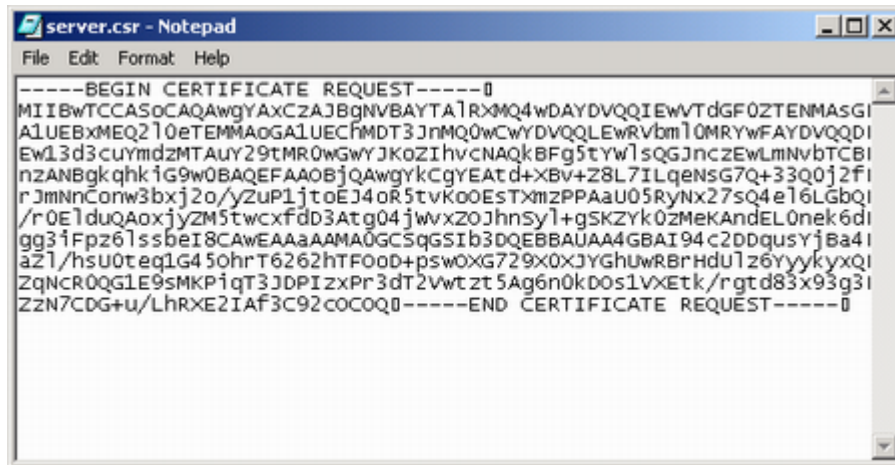


- Next you can sign a certificate (for example from Verisign - www.verisign.com).

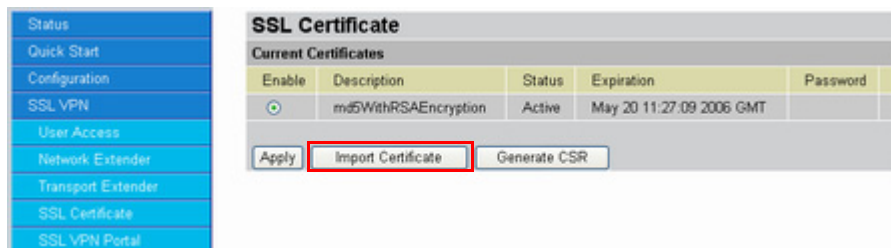


- Follow the instructions from the web. You will be prompted to input your CSR.

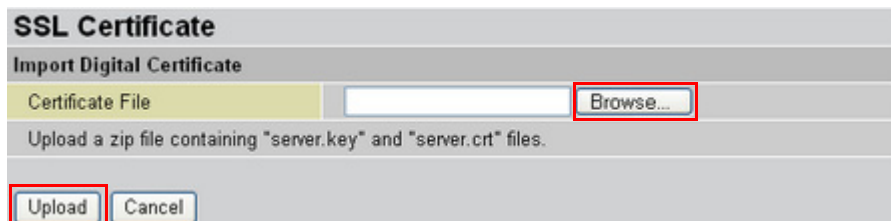
- Open server.csr with a text editor such as Windows Notepad.



- Copy the CSR text and paste it in the appropriate field on the certificate provider's website and finish following the certificate provider's instructions for getting a certificate. The certificate provider will send you the certificate by email.
- Copy the certificate text and paste into a text editor. Save the file as "server.crt".
- Zip the files server.crt and server.key into a file (for example, "server.zip").
- In the **SSL Certificate** screen, click **Import Certificate**.



The following screen appears.



- Click **Browse** and go to the location of the zipped file. When the file is listed in the Certificate File text box, click **Upload**.

The certificate is loaded and added to the Current Certificates list.



- Now you must activate the imported certificate. Click **Input** to input the password.

SSL Certificate

Input Password

| | |
|-------------------------|-----------------------------------------------------------------------------------------------------------------|
| Certificate Description | www.bgs10.com |
| Issuer | C=US, O=VeriSign, Inc., OU=For Test Purposes Only. No assurances., CN=VeriSign Trial Secure Server Test Root CA |
| Subject | C=TW, ST=test, L=test, O=org, OU=Unit, OU=Terms of use at www.verisign.com/cps/testca (c)05, CN=www.bgs10.com |
| Serial Number | ~@ |
| Expiration Date | Jul 6 23:59:59 2006 GMT |
| Password | 123456789 |

Apply Cancel

- In the **Password** text box, type the password that you created when generating the CSR.
- Click **Apply**. The certificate is ready to be used.

SSL Certificate

Current Certificates

| Enable | Description | Status | Expiration | Password |
|----------------------------------|-----------------------|--------|--------------------------|----------|
| <input checked="" type="radio"/> | sha1WithRSAEncryption | Active | Jul 6 23:59:59 2006 GMT | Input |
| <input type="radio"/> | md5WithRSAEncryption | Active | May 20 11:27:09 2006 GMT | |

Apply Import Certificate Generate CSR

- Click **Enable** to enable the certificate.

Registering the BiGuard S10

QUESTION: How do I register my BiGuard S10?

ANSWER: Register the BiGuard S10 as follows.

- On the status page, click **Register**.

Status

- Status
- Quick Start
- Configuration
- SSL VPN
- Logs & E-mail Alert
- Save Config to Flash

Status

Device Information

| | | |
|------------------|--------------------------------|----------|
| Registration | Not Registered | Register |
| Model Name | BiGuard S10 | |
| Device Name | SSLVPN gateway | |
| System Up-Time | 2 days, 35 minutes, 10 seconds | |
| Current Time | Thu Dec 2 00:35:10 1999 | Sync Now |
| Software Version | 1.00h for menu | |
| Bootrom Version | 1.06c | |
| LAN MAC Address | 00:04:ED:00:00:01 | |
| WAN MAC Address | 00:04:ED:00:00:00 | |
| Home URL | Billion Electric Co.,Ltd. | |

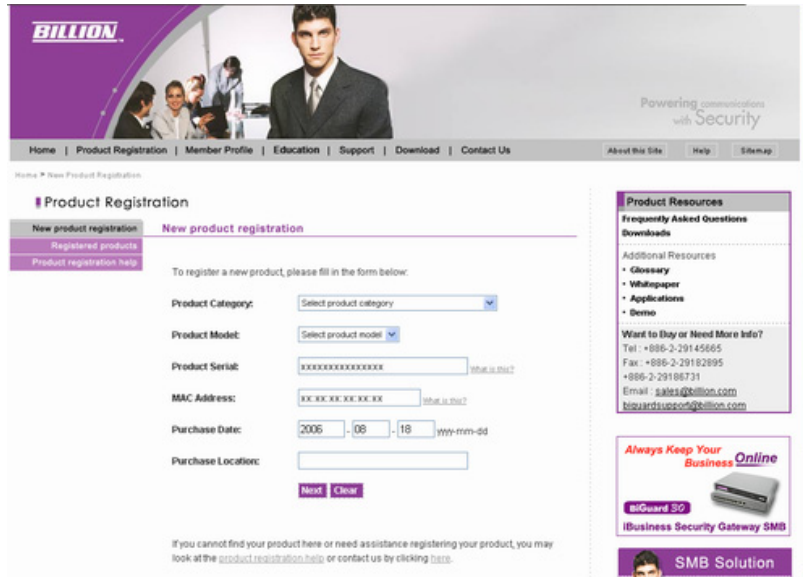
SSL

| | |
|--------------|---|
| Active Users | 1 |
|--------------|---|

LAN

| | |
|-------------|---------------------|
| IP Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |
| DHCP Server | DHCP Server Running |

The manufacturer's website opens a registration page and your BiGuard S10's MAC address is automatically added in the appropriate field. The serial number must be typed in by the user.



2. Follow the instructions to fill out the rest of the form and register your BiGuard S10.



NOTE: To REGISTER THE BIGUARD S10 WITHOUT USING THE WEB CONFIGURATION INTERFACE, GO TO WWW.BIGUARD.COM AND CLICK **PRODUCT REGISTRATION**.



This section describes how to configure an active directory server for use with the BiGuard S10.



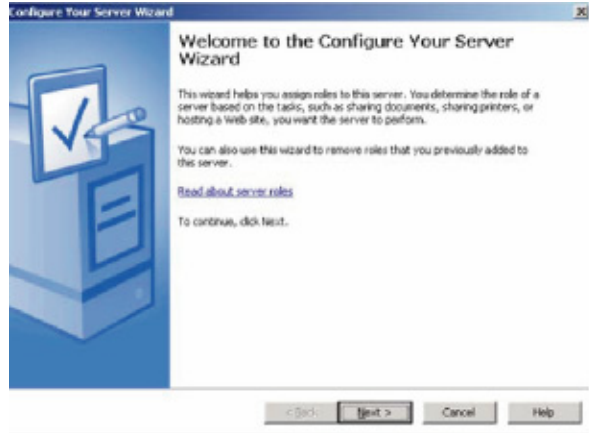
NOTE: Windows Server 2000 and 2003 support the Active Directory server feature.

Configuring an Active Directory server

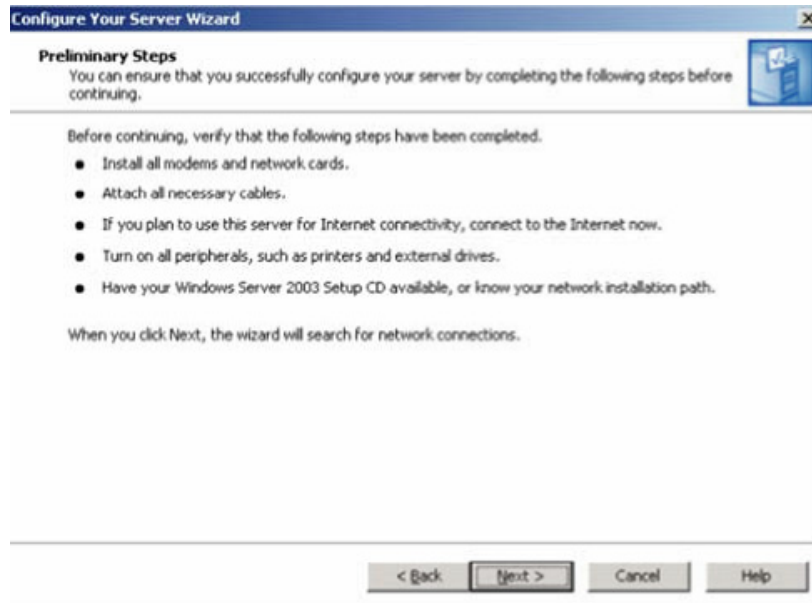
Follow these instructions to configure an Active Directory server.

3. Click the **Start** button of your Windows PC.
4. Click **Settings**.
5. Click **Control Panel**.
6. Double-click **Administrative Tools**.
7. Click **Configure Your Server Wizard**.

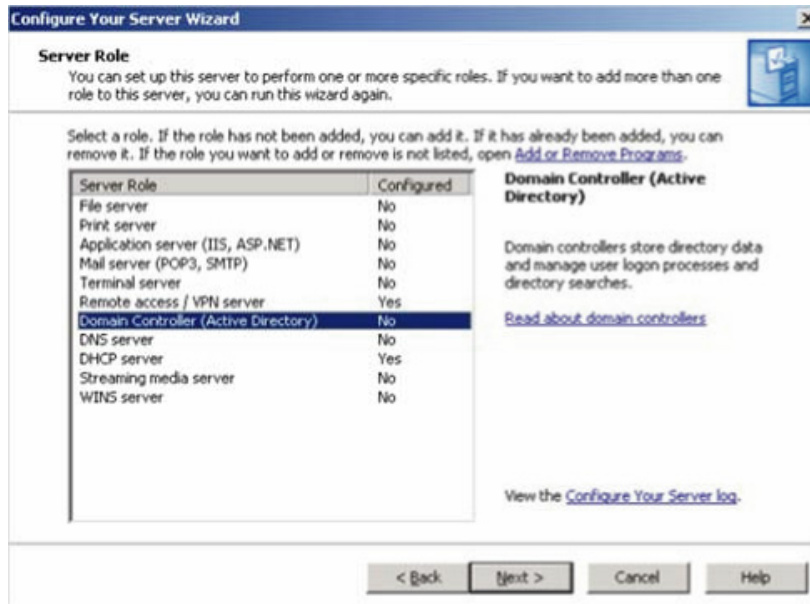
The **Welcome to the Configure Your Server Wizard** screen opens.



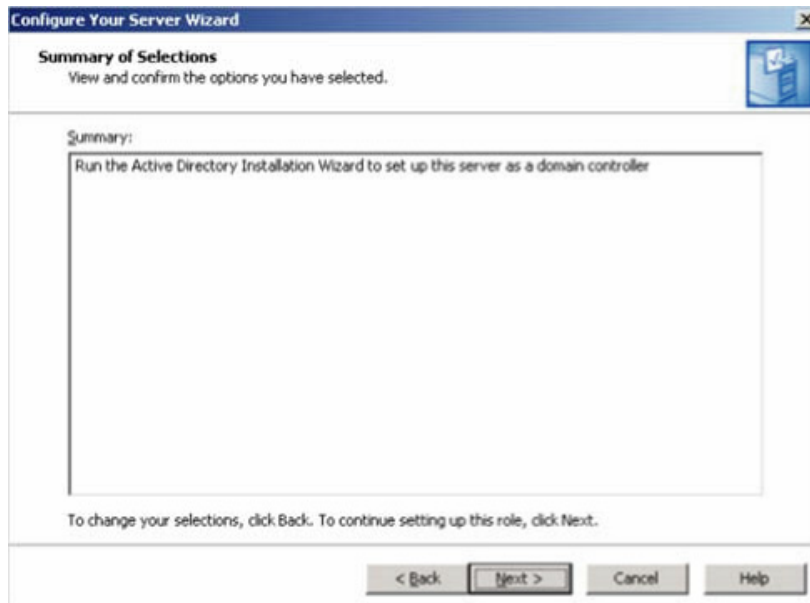
- 8. Click **Next**. The **Preliminary Screen** opens.



- Click **Next**.
The **Server Role** screen opens.



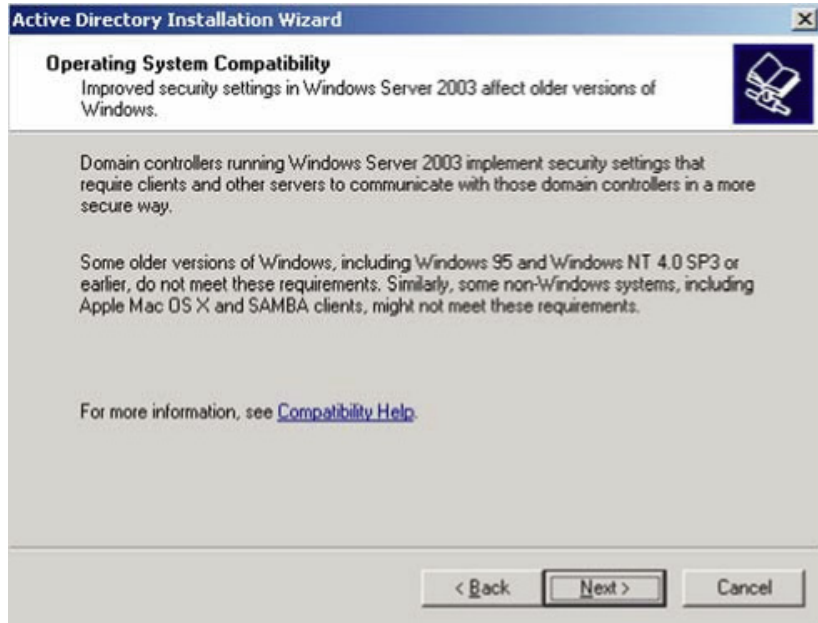
- Select **Domain Controller (Active Directory)**, and then click **Next**.
The **Summary of Selections** screen appears.



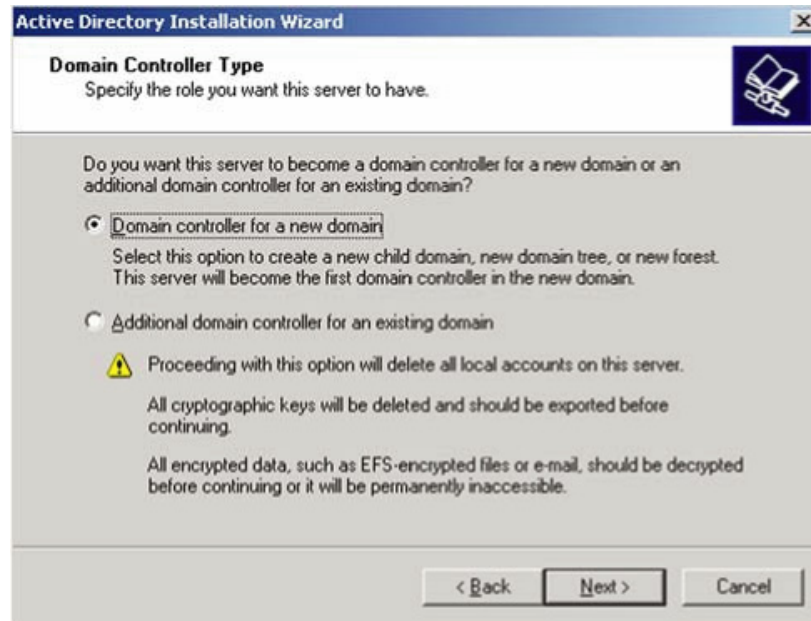
- 11. Click **Next**.
The **Welcome to the Active Directory Installation Wizard** screen appears.



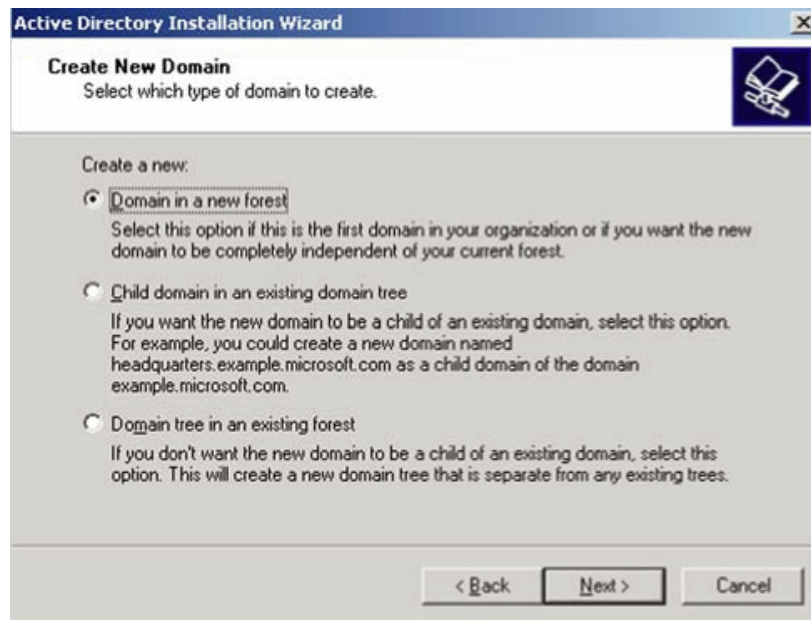
- 12. Click **Next**.
The **Operating System Compatibility** screen appears.



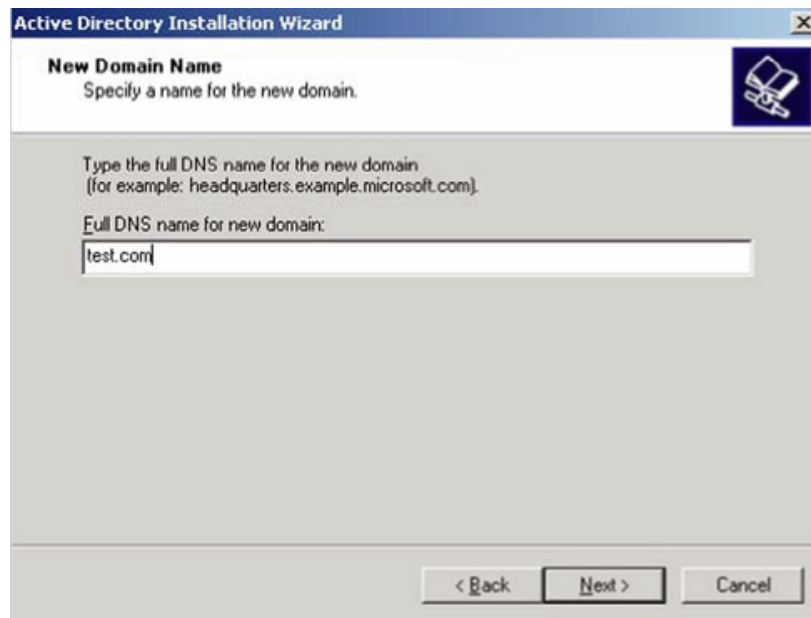
- Click **Next**.
The **Domain Controller Type** screen opens.



- Select **Domain controller for a new domain**, and then click **Next**.
The **Create New Domain** screen appears.

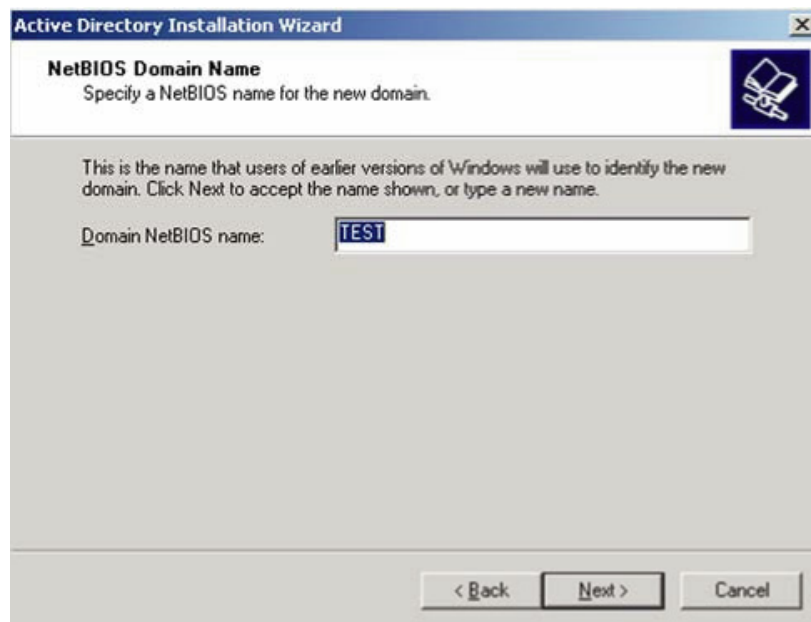


15. Select **Domain in a new forest**, and then click **Next**.
The **New Domain Name** screen opens.



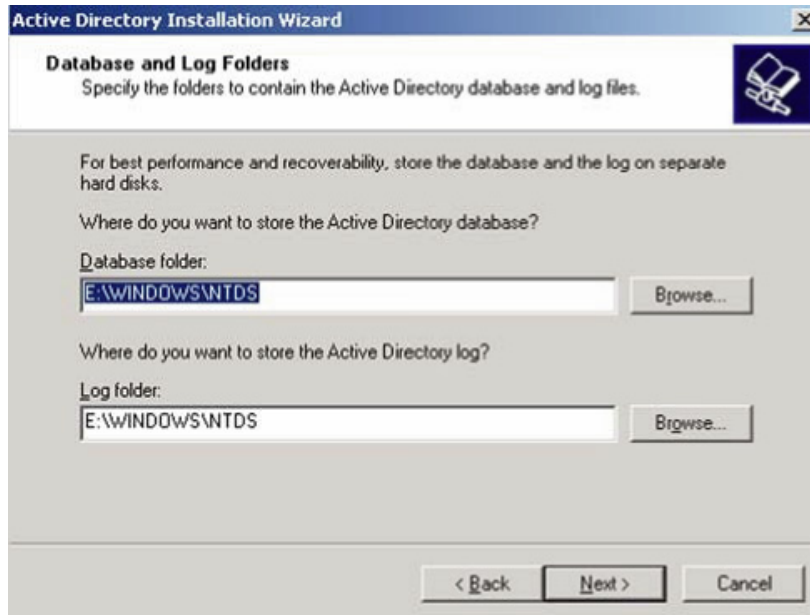
The screenshot shows the 'Active Directory Installation Wizard' window. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'New Domain Name' with the instruction 'Specify a name for the new domain.' Below this, it says 'Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).' A text box labeled 'Full DNS name for new domain:' contains the text 'test.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

16. Enter a domain name, and then click **Next**.
The **NetBIOS Domain Name** screen appears.

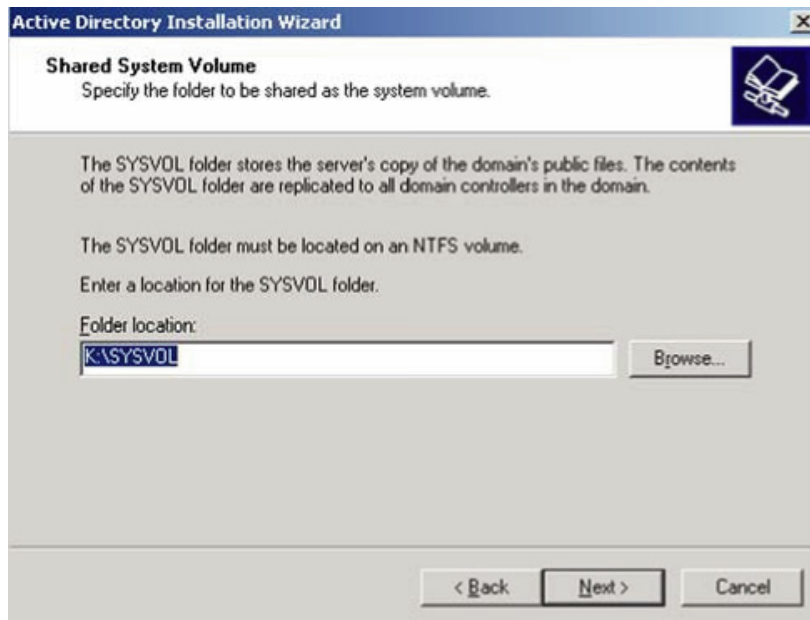


The screenshot shows the 'Active Directory Installation Wizard' window. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'NetBIOS Domain Name' with the instruction 'Specify a NetBIOS name for the new domain.' Below this, it says 'This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.' A text box labeled 'Domain NetBIOS name:' contains the text 'TEST'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

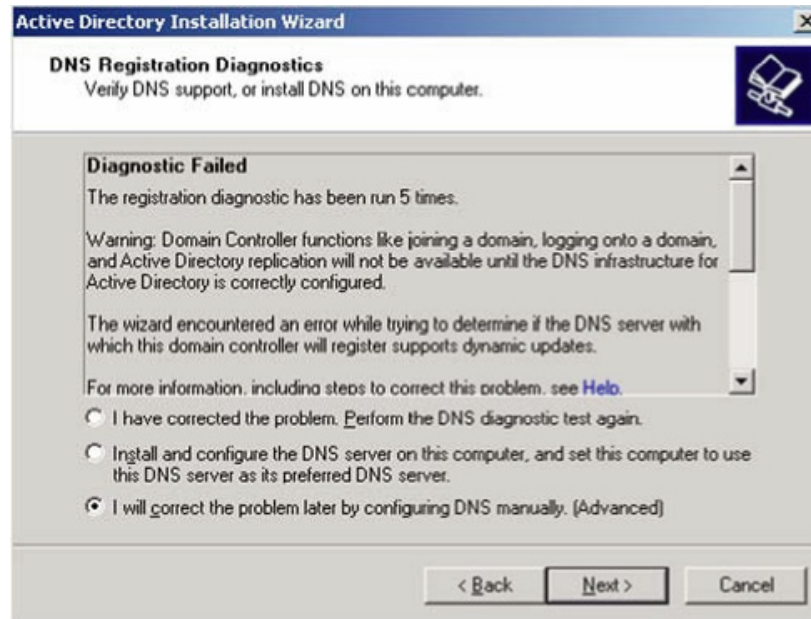
17. Enter a domain NetBIOS name, and then click **Next**. The **Database and Log Folders** screen appears.



18. Select the folders that will store the Active Directory database and log. Then click **Next**. The **Shared System Volume** screen opens.

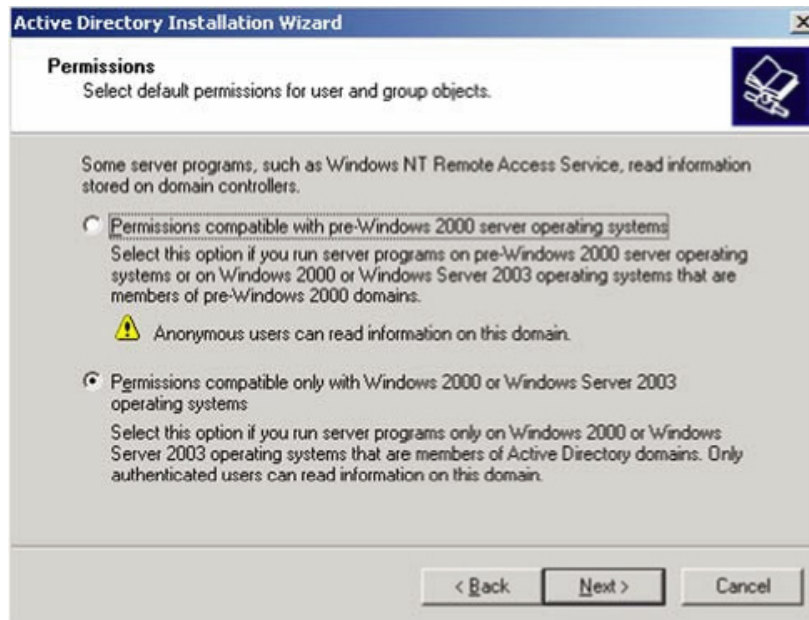


19. Enter a location for the SYSVOL folder, and then click **Next**.
The **DNS Registration Diagnostics** screen appears.



20. Select **I will correct the problem later by configuring DNS manually (Advanced)**, and then click **Next**.

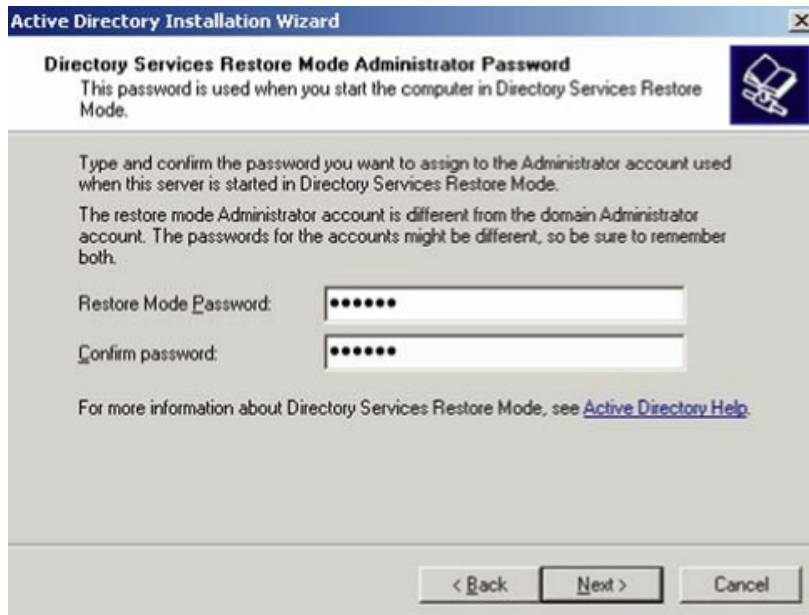
The **Permissions** screen appears.



21. Select **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**.

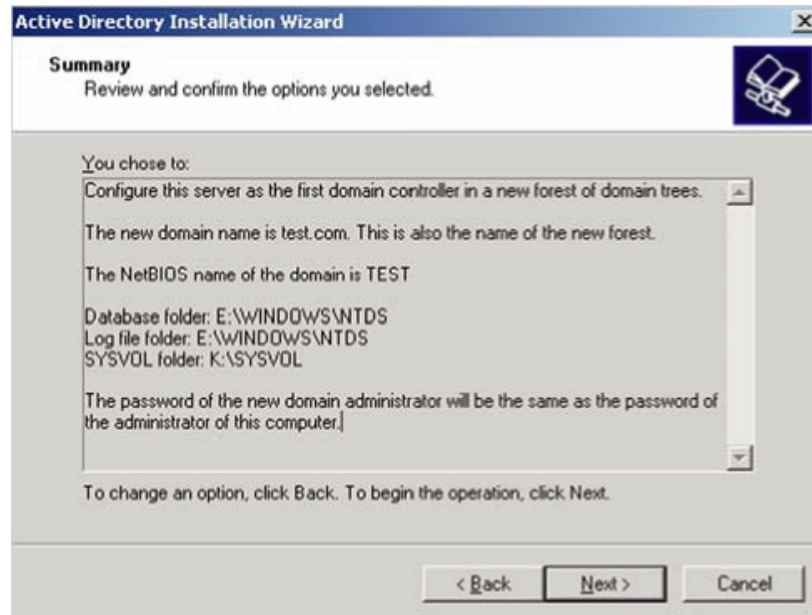
22. Click **Next**.

The **Directory Services Restore Mode Administrator Password** screen appears.



23. Enter your Administrator password for the Active Directory server. Then enter it again in the **Confirm password** field.

24. Click **Next**.
The **Summary** screen appears.



25. Click **Next**.
The wizard will configure Active Directory automatically, and will notify you when the configuration is complete.

Networking Basics

IP Addresses

With the number of TCP/IP networks interconnected across the globe, ensuring that transmitted data reaches the correct destination requires each computer on the Internet to have a unique identifier. This identifier is known as the IP address. The Internet Protocol (IP) uses a 32-bit address structure, and the address is usually written in dot notation.

A typical IP address looks like this: *198.25.12.8*

The 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, while the second part identifies the host node or station on the network. How the address is divided depends on the address range and the application.

The five standard IP address classes each have different methods to determine the network and host sections of the address, which makes multiple hosts on a network possible. TCP/IP software identifies each address class by reading a unique bit pattern that precedes each address type. Once the address class has been recognized, the software can then correctly determine the addresses' host section. With this structure, IP addresses uniquely identify each network and node.

Net Mask

With each address class, the size of the two subdivided parts (network address and host address) is implied by the class. A net mask associated with an IP address can also express this partitioning. A net mask 32-bit quantity yields the network address when combined with an IP address. As an example, the net masks for Class A, B, and C are 255.0.0.0, 255.255.0.0, and 255.255.255.0 respectively.

Instead of dotted-decimal notation, the net mask can also be written in terms of the number of ones from the left. This number is added to the IP address, following a back slash (/). For example, a typical Class C address could be written as 192.168.234.245/24, which means that the net mask is 24 ones followed by 8 zeros. (11111111 11111111 11111111 00000000).

Subnet Addressing

Subnet addressing enables the split of one IP network address into multiple physical networks. These smaller networks are called subnetworks, and these subnetworks can make efficient use of each address when compared to needing a different network number at each end of a routed link. This technique is especially useful in smaller network environments, such as small office LANs.

A Class B address provides 16 bits of node numbers, which enable 65,536 nodes. Since most organizations don't require such a large number of nodes, the free bits can be reassigned with subnet addressing.

Multiple Class C addresses can be made from a Class B address. For example, the IP address of 172.20.0.0 allows eight extra bits to use as a subnet address, since node addresses are limited to a maximum of 255. The IP address of 172.20.52.212 would be read as IP network address 172.20, subnet number 52, and node number 212.

Besides extending the number of available addresses, this technique also allows a network manager to design an address scheme for the network by using different subnets. This can be useful when trying to distinguish other geographical locations in the network or other departments in the organization.

Private IP Addresses

When isolated from the Internet, the hosts on your local network may be assigned IP addresses with no conflicts. However, the Internet Assigned Numbers Authority (IANA) has reserved several blocks of IP addresses for private networks. These include:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.16.255.255 192.168.0.0 - 192.168.255.255

When assigning IP addresses to your private network, be sure to use IP addresses from these ranges.

Network Address Translation (NAT)

Traditionally, multiple computers that needed simultaneous Internet access also required a range of IP addresses from the Internet Service Provider (ISP). Not only was this method very costly, but the number of available IP addresses for computers is limited. Instead, BiGuard S10 uses a type of address sharing called Network Address Translation to grant Internet access to several computers on the same network through the same Internet account. This method translates internal IP addresses to a single address that is unique on the Internet. This unique address can either be fixed or dynamic, depending on the type of Internet account, and the internal LAN IP addresses may also be either private or registered addresses.

NAT also offers firewall-like protection to your network, since internal LAN addresses are shielded from the public Internet. All incoming traffic to the public IP address is handled by the router, which means added security for your network from intruders. If a particular computer on your LAN requires access from outside computers, you can use port forwarding to accomplish this. For information on how to configure port forwarding on BiGuard S10, refer to [Configuring the Virtual Server](#) on page 54

Dynamic Host Configuration Protocol (DHCP)

If the PCs on a LAN require access to the Internet, each PC must be configured with an IP address, a gateway address, and one or more DNS server addresses. Rather than configuring each PC manually, you can instead configure a network device to act as a Dynamic Host Configuration Protocol (DHCP) server. PCs on the network can automatically obtain IP addresses from a list of addresses stored on the DHCP server. In addition, other information such as gateway and DNS address can also be assigned with a DHCP server. When connecting to the ISP, BiGuard S10 also functions as a DHCP client. BiGuard S10 can automatically obtain an IP address, subnet mask, gateway address, and DNS server addresses if the ISP assigns this information using DHCP.

Router Basics

What is a Router?

A router is a device that forwards data packets along networks. A router is connected to at least two networks. Usually, this is a LAN and a WAN that is connected to an ISP network. Routers are located at gateways, the places where two or more networks connect. Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols to communicate with each other and configure the best route between any two hosts.

Routers can vary in performance and scale, the types of physical WAN connection they support, and the number of routing protocols supported. BiGuard S10 offers a convenient and powerful way for small-to-medium businesses to connect their networks.

Why use a Router?

While large bandwidth can easily and inexpensively be provided in a LAN, having high bandwidth between a LAN and the Internet can be prohibitively expensive. Because of this, Internet access is usually done through a slower WAN link, such as a cable or DSL modem. To efficiently use this slower connection, a router acts as a mechanism for selecting and transmitting data meant for the Internet. By using a router, organizations can enjoy relatively inexpensive Internet access, while maintaining a high-speed local area network.

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is an interior gateway protocol that specifies how routers exchange routing table information. Routers periodically update each other with RIP, changing their routing tables when necessary.

BiGuard S10 supports the RIP protocol. RIP also supports subnet and multicast protocols. RIP is not required for most home applications.

Firewall Basics

What is a Firewall?

Firewalls prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. With the functionality of a NAT router, the firewall adds features that deal with outside Internet intrusion and attacks. When an attack or intrusion is detected, the firewall can be configured to log the intrusion attempt, and can also notify the administrator of the incident. With this information, the administrator can work with the ISP to take action against the hacker. Against some types of attacks, the firewall can discard intruder packets, thereby fending off the hacker from the private network.

Stateful Packet Inspection

BiGuard S10 uses Stateful Packet Inspection (SPI) to protect your network from intrusions and attacks. Unlike less sophisticated Internet sharing routers, SPI ensures secure firewall filtering by intercepting incoming packets at the network layer, and analyzing them for state-related information that is associated with all network connections. User-level applications such as Web browsers and FTP can make complex network traffic patterns, which BiGuard S10 analyzes by looking at groups of connection states.

All state information is stored in a central cache. Traffic passing through the firewall is analyzed against these states, and then is either allowed to pass through or rejected.

Denial of Service (DoS) Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Why Use a Firewall?

With a LAN connected to the Internet through a router, there is a chance for hackers to access or disrupt your network. A simple NAT router provides a basic level of protection by shielding your network from the outside Internet. Still, there are ways for more dedicated hackers to either obtain information about your network or disrupt your network's Internet access. Your BiGuard S10 provides an extra level of protection from such attacks with its built-in firewall.

Specifications

SSL VPN

Access Connection

- Network Extender
- Transport Extender
- Application Proxy

Application & Management

- Personalized Web Portal
- Single Sign-On (SSO)
- My Network Places (Web CIFS)
- SSL event log and monitor
- Terminal services (RDP5)
- File Transfer Protocol (FTP)
- Telnet
- Virtual Network Computing (VNC)
- Secure Shell (SSH) support
- Web based data (HTTP, HTTPS)
- Granular User Policy Management

Compatible Web Browsers

- Microsoft Internet Explorer 5.01 or newer versions (Internet Explorer 6.0SP1 is strongly recommended)
- Opera 8.02 and newer versions
- Firefox 1.0.6 and newer versions
- Safari 1.3.1 and newer versions
- Mozilla 1.7.1 and newer versions
- Sun JRE 1.3.1 or newer versions

Security

- SSL encryption
- Web cache cleaner
- Local Database
- Digital Certificate
- User Access Control
- Authentication Domains: RADIUS, LDAP, Active Directory, NT Domain

Firewall & Content Filter

- Stateful Packet Inspection (SPI)
- Denial of Service (DoS) prevention
- Packet Filter
- Intrusion Detection
- URL Filter
- Java Applet/Active X/Cookie Blocking

Web-Based Management

- Easy-to-use web interface
- Firmware upgraded through web-based interface
- Local and remote management through HTTP & HTTPS
- Backup Firmware support

Quality of Service Control

- Support DiffServ approach
- Traffic prioritization and bandwidth management based-on IP protocol, port number and IP address
- Policy control based on IP address or MAC address

Logging and Monitoring

- Centralized Logs
- System Log
- E-mail alert and intrusion log
- System status monitoring

Network Protocols and features

- Static IP, PPPoE and DHCP client connection to ISP
- NAT, static routing and RIP1/2
- Dynamic Domain Name System (DDNS)
- Router Mode
- Virtual Server
- Hardware DMZ
- DHCP Server
- SNTP
- Multi-NAT*
- SNMP
- Transparent Bridging*

Hardware Specification

Physical Interface

- 1 x 10/100Mbps WAN port
- 4 x 10/100Mbps LAN ports
(1 port can be configured to DMZ)
- Power Switch
- Reset button

Physical Specification

- Dimensions: 19" x 6.54" x 1.65"
(482mm x 166mm x 42mm w/ bracket)
(250mm x 166mm x 33.8mm w/o bracket)

Power Requirement

- Input: 12V DC, 1A

Operating Environment

- Operating temperature: 0 ~ 40 C
- Storage temperature: -20 ~ 70 C
- Humidity: 20 ~ 95% non-condensing

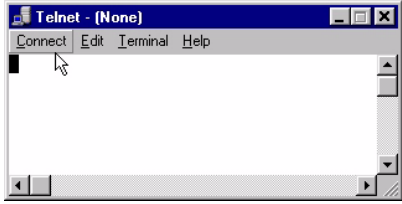
Glossary

The following glossary of networking terms is provided for your convenience.

| Term | Definition |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Point | Access points are way stations in a wireless LAN that are connected to an Ethernet hub or server. Users can roam within the range of access points and their wireless device connections are passed from one access point to the next. |
| Authentication | Authentication refers to the verification of a transmitted message's integrity. |
| DMZ | DMZ (DeMilitarized Zone) A part of the network that is neither part of the internal network nor directly part of the Internet. Basically, a perimeter network established to house public services. |
| Beacon Interval | Refers to the interval between packets sent by access points for the purposes of synchronizing wireless LANs. |
| DHCP | DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses. |
| DNS | DNS stands for Domain Name System. DNS converts machine names to the IP addresses that all machines on the net have. It translates from name to address and from address to name. |
| Domain Name | The domain name typically refers to an Internet site address. |
| DTIM | DTIM (Delivery Traffic Indication Message) provides client stations with information on the next opportunity to monitor for broadcast or multicast messages. |
| Filter | Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses. |
| Firewall | Firewalls are methods used to keep networks secure from malicious intruders and unauthorized access. Firewalls use filters to prevent unwanted packets from being transmitted. Firewalls are typically used to provide secure access to the Internet while keeping an organization's public Web server separate from the internal LAN. |
| Firmware | Firmware refers to memory chips that retain their content without electrical power (for example, BIOS ROM). The router firmware stores settings made in the interface. |
| Fragmentation | Refers to the breaking up of data packets during transmission. |
| FTP | FTP (File Transfer Protocol) is used to transfer files over a TCP/IP network, and is typically used for transferring large files or uploading the HTML pages for a Web site to the Web server. |
| Gateway | Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information. |
| Host Name | The name given to a computer or client station that acts as a source for information on the network. |

| Term | Definition |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP | HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTP establishes a connection with a Web server and transmits HTML pages to client browser (for example Windows IE). HTTP addresses all begin with the prefix 'http://' prefix (for example, <i>http://www.yahoo.com</i>). |
| ICMP | ICMP (Internet Control Message Protocol) is a TCP/IP protocol used to send error and control messages over the LAN (for example, it is used by the router to notify a message sender that the destination node is not available). |
| IP | IP (Internet Protocol) is the protocol in the TCP/IP communications protocol suite that contains a network address and allows messages to be routed to a different network or subnet. However, IP does not ensure delivery of a complete message—TCP provides the function of ensuring delivery. |
| IP Address | The IP (Internet Protocol) address refers to the address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Clients are assigned either a permanent address or have one dynamically assigned to them via DHCP. IP addresses are written as four sets of numbers separated by periods (for example, 211.23.181.189). |
| ISP | An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines. |
| LAN | LANs (Local Area Networks) are networks that serve users within specific geographical areas, such as in a company building. LANs are comprised of servers, workstations, a network operating system, and communications links such as the router. |
| MAC Address | A MAC address is a unique serial number burned into hardware adapters, giving the adapter a unique identification. |
| Metric | A number that indicates how long a packet takes to get to its destination. |
| MTU | MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network. Messages larger than the MTU are divided into smaller packets. |
| NAT | NAT (Network Address Translation - also known as IP masquerading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN. |
| Network Administrator | The network administrator is the person who manages the LAN within an organization. The administrator's job includes ensuring network security, keeping software, hardware, and firmware up-to-date, and keeping track of network activity. |
| NTP | NTP (Network Time Protocol) is used to synchronize the realtime clock in a computer. Internet primary and secondary servers synchronize to Coordinated Universal Time (UTC). |
| Packet | A packet is a portion of data that is transmitted in network communications. Packets are also sometimes called frames and datagrams. Packets contain not only data, but also the destination IP address. |

| Term | Definition |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ping | Ping (Packet INternet Groper) is a utility used to find out if a particular IP address is present online, and is usually used by networks for debugging. |
| Port | Ports are the communications pathways in and out of computers and network devices (routers and switches). Most PCs have serial and parallel ports, which are external sockets for connecting devices such as printers, modems, and mice. All network adapters use ports to connect to the LAN. Ports are typically numbered. |
| PPPoE | PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet. |
| Preamble | Preamble refers to the length of a CRC (Cyclic Redundancy Check) block that monitors communications between roaming wireless enabled devices and access points. |
| Protocol | A protocol is a rule that governs the communication of data. |
| RIP | RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination. |
| RTS | RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data. |
| Server | Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network. |
| SMTP | SMTP (Simple Mail Transfer Protocol) is the standard Internet e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail. |
| SNMP | SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol. SNMP hardware or software components transmit network device activity data to the workstation used to oversee the network. |
| SSID | SSID (Service Set Identifier) is a security measure used in WLANs. The SSID is a unique identifier attached to packets sent over WLANs. This identifier emulates a password when a wireless device attempts communication on the WLAN. Because an SSID distinguishes WLANs from each other, access points and wireless devices trying to connect to a WLAN must use the same SSID. |
| Subnet Mask | Subnet Masks (SUBNETwork masks) are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP address to determine whether to accept or reject the packet. |
| SysLog Server | A SysLog server monitors incoming Syslog messages and decodes the messages for logging purposes. |
| TCP | (Transmission Control Protocol) is the transport protocol in TCP/IP that ensures messages over the network are transmitted accurately and completely. |

| Term | Definition |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TCP/IP | TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in realtime video and audio transmission). |
| Telnet | <p>Telnet is a terminal emulation protocol commonly used on the Internet and TCP- or IP-based networks:</p>  <p>Windows Telnet Client</p> <p>Telnet is used for connecting to remote devices and running programs. Telnet is an integral component of the TCP/IP communications protocol.</p> |
| UDP | (User Datagram Protocol) is a protocol within TCP/IP that is used to transport information when accurate delivery isn't necessary (for example, real-time video and audio where packets can be dumped as there is no time for retransmitting the data). |
| Virtual Servers | Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server). |
| WEP | WEP (Wired Equivalent Privacy) is the de facto security protocol for wireless LANs, providing the "equivalent" security available in hardwired networks. |
| Wireless LAN | Wireless LANs (WLANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN. |
| WLAN | WLANs (Wireless LANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN. |
| WAN | WAN (Wide Area Network) is a communications network that covers a wide geographic area such as a country (contrasted with a LAN, which covers a small area such as a company building). |

Warranty

Limited Warranty

Thank you for purchasing Billion products.

Billion Electric Co., Ltd., (hereinafter referred to as “Billion”) provides a 24-month warranty on the hardware of this product with respect to defects in material and workmanship under normal use and service, and under the conditions set out on this warranty. The warrant, with respect to the proper performance of the product, is limited in conjunction with the other products specified on the packaging and/or the manual of Billion.

Billion does not cover damage or failure caused by accident, misuse, modified, faulty installation, struck by lightning, serial number has been removed or repaired contrary to the instructions given by Billion, or by others than those previously specifically designated for that purpose by Billion. The warranty does not extend to defects resulting from normal wear and tear, nor does it extend to any deviating application relating to local, regional, or national (deviation) technical or safety standards.

The standard software shipped with this product is provided “as is”. Billion does not guarantee that the software will be free of defects. The software supplied may not be suitable for intended use by the end user.

For warranty service the product must be reported to Billion, Billion authorized local agent or Billion authorized distributors to receive an advice of where to send the faulty product.

For claims of warranty, technical support, or customer service, please contact Billion authorized local agent or Billion authorized distributors. In any circumstance, contacting Billion headquarters is welcome via following details:

E-mail: support@billion.com

URL: <http://www.billion.com>