

***Billion Electric Co., Ltd.***

***BiGuard S20***

***Gigabit Dual-WAN SSL/IPSec VPN Security Gateway***

***Administration Guide***

## **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 S20*  
erklärt, dass das Produkt:  
*Telecommunications terminal equipment  
Telekommunikations(Tk-)endeinrichtung*

**Intended purpose:** *SSL/IPSec 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))

*IEC 60950-1: 2001*

**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: 2002 / A1: 2002*

*IEC 61000-4-4: 2004, IEC 61000-4-5: 1995 / A1: 2000,*

*IEC 61000-4-6: 2003 / A1: 2004, 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)

*19. Jan 2007*  
(Date)

*Gary Lin*  
President  
Power Partnership GmbH  
Mozartstraße 78  
40622 Mettmann - Germany  
Tel +49 (2104) 801005 Fax 801005

## Copyright Information

© 2008 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 3.17, October 2008

## 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.

UNIX is a registered trademark of The Open Group.

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

All other trademarks are the property of their respective owners.

## 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 S20 is built for reliability and long service life. For your safety, be sure to read and follow these guidelines and safety warnings:

- Read this installation guide thoroughly before attempting to set up the BiGuard S20.
- The BiGuard S20 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 S20 in environments with high humidity or high temperatures.
- DO NOT use the same power source for the BiGuard S20 as other equipment.
- DO NOT use the BiGuard S20 and any accessories outdoors.
- If you wall mount the BiGuard S20, make sure that no electrical, water or gas pipes will be damaged during installation.
- Without surge protection, installation of the BiGuard S20 during a thunderstorm is not recommended.
- DO NOT expose the BiGuard S20 to dampness, dust, or corrosive liquids.
- DO NOT use the BiGuard S20 near water.
- Be sure to connect the cables to the correct ports.
- DO NOT obstruct the ventilation slots on the BiGuard S20 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 S20.
- Only connect suitable accessories to the BiGuard S20.
- 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.
- Please unplugged the router's power cord from the wall outlet when the power cord is damaged.
- Please unplugged the router's power cord from the wall outlet when liquid substance has leaked or spilled on the router.
- Please unplugged the router's power cord from the wall outlet when the router had been dropped or got damaged.
- Please unplugged the router's power cord from the wall outlet when the router isn't operating under the suggested instruction or environment.



*For the latest documentation and updates for the BiGuard S20 visit  
<http://www.biguard.com>*



**About this guide 13****Unpacking the BiGuard S20 14****Front and rear view of the BiGuard S20 15****Setting up the BiGuard S20 16**

Rackmounting the BiGuard S20 16

Connecting to a WAN 17

Connecting to a LAN 17

Connecting power 18

Turning on the power and checking LED status 18

**Network deployment/applications 19**

Network environment scenarios 19

All in one solution: firewall, remote and Internet access 19

Installing behind a gateway/firewall 19

Fitting into a DMZ zone behind an existing firewall router 20

All in one: public servers on DMZ zone, private servers on LAN 21

Load Balancing 22

Auto Fail Over 23

SSL VPN Applications 24

Network Extender 24

Transport Extender 24

Network Place 25

Application Proxy 25

SSL VPN Features 26

Granular Access Control 26

SSL VPN Certification 26

SSL VPN Portals 27

Authentication Domain Scenarios 28

**Firewall Settings 30**

Intrusion detection 30

Block WAN request 30

**WAN settings 30**

Static IP 30

PPPoE 30

DHCP 30

**Logging in to the BiGuard S20 Web Manager 32****Navigating in the Web Manager 38****Basic Configuration with the Quick Start Menu 39**

Quick start to configuring the Dual WAN 39

Configuring the Dual WAN for Static IP 39

Configuring the WAN for PPPoE 40

Configuring the WAN for DHCP 41

Quick start to configuring SSL VPN 42

Adding predefined applications 43

Quick start to configuring IPsec 44

LAN to LAN 44

LAN to LAN (Mobile LAN) 45

LAN to Host 45

LAN to Host (Mobile Client) 45

LAN to Host (for BiGuard VPN Client) 46

The IPSec Configuration Summary screen 47

### **Monitoring Configuration Status 48**

Status submenus 48

Changing the device name 51

Changing time and time zone parameters 54

Changing the default LAN IP address 55

DHCP server settings 56

### **Mapping a MAC address to a fixed IP address 56**

SSL user status 58

ARP table 58

Routing table 59

Session table 59

DHCP table 60

IPSec Status 60

System Log 61

### **Configuring the BiGuard S20 63**

Configuring the Interface 63

Configuring the LAN 63

### **Configuring the Ethernet 63**

### **Configuring the Alias IP 64**

### **Configuring DHCP server settings 65**

### **Disabling DHCP server 65**

65

### **Configuring DHCP server parameters 66**

68

### **Configuring the DHCP relay agent 68**

Configuring WAN settings 69

### **ISP Settings 69**

### **Bandwidth Settings 74**

Dual WAN 76

### **General Settings 76**

Load Balance 77

### **Outbound Load Balance 77**

### **Protocol Binding 78**

Configuring the DMZ 80

Multiple NAT/Subnet 81

Configuring Network Objects 82

Configuring IP address Network Objects 82

### **Creating IP address network objects 82**

### **Editing IP address Network Objects 83**

### **Deleting IP address Network Objects 84**

Creating Address Groups Network Objects 85

### **Creating an address group Network object 85**

- Editing Address Group Network Objects 86**
- Deleting Address Group Network Objects 87**
- Allowing Services 88
- Creating User-defined Services 88**
- Editing User-defined Services 89**
- Deleting User-defined Services 90**
- Creating Service Group Network Objects 91
- Creating Service Group Network Objects 91**
- Editing Service Group Network Objects 92**
- Deleting Service Group Network Objects 93**
- Scheduling BiGuard S20 operation 94
- Creating a Schedule Network Object 94**
- Editing Schedule Network Objects 95**
- Deleting Schedule Network Objects 95**
- Managing Bandwidth Network Objects 96
- Creating Bandwidth Control Network Objects 96**
- Editing Bandwidth Control Network Objects 97**
- Deleting Bandwidth Control Network Objects 97**
- Setting Content Blocking parameters 98
- Creating Keyword Filter Network Objects 98**
- Editing Keyword Filter Network Object 99**
- Deleting Keyword Filter Network Objects 99**
- Creating Domain Filter Network Objects 101**
- Editing Domain Filter Network Objects 101**
- Deleting Domain Filter Network Objects 102**
- Creating Restrict URL Features Network Objects 104**
- Editing Restrict URL Feature Network Objects 104**
- Deleting Restrict URL Feature Network Objects 105**
- Setting Policy parameters 106
- Enabling Packet Filtering 106
- Creating Packet Filtering Parameters 106**
- Editing Packet Filtering Parameters 108**
- Deleting Packet Filtering Parameters 109**
- Configuring the Virtual Server 110
- Creating Virtual Server parameters 110**
- Editing Virtual Server parameters 112**
- Deleting Virtual Server Parameters 113**
- Configuring Quality of Service (QoS) Parameters 114
- Creating QoS Parameters 114**
- Editing QoS parameters 116**
- Deleting QoS Parameters 117**
- Configuring SIP QoS Profile 118**
- Configuring Ethernet MAC Filtering 120
- Creating Ethernet MAC Filters 120**
- Editing Ethernet MAC Filters 121**
- Deleting Ethernet MAC Filters 122**

Configuring Content Filtering policies	123
<b>Creating Content Filtering Parameters</b>	<b>123</b>
<b>Editing Content Filtering Parameters</b>	<b>125</b>
<b>Deleting Content Filtering Parameters</b>	<b>126</b>
<b>Creating a Content Filtering Exception IP Profile</b>	<b>127</b>
Configuring IPsec	128
Creating and Enabling IPsec Tunnels	128
Configuring the System	132
Setting the Time Zone	132
Enabling Remote Access	133
Upgrading the BiGuard S20 Firmware	134
Backing up and restoring configurations	135
<b>Backing up the configuration</b>	<b>135</b>
<b>Restoring a Saved Configuration</b>	<b>136</b>
Configuring and changing passwords	137
Restarting the system	138
Configuring Advanced Features	139
Configuring Static Routes	139
<b>Creating Static Route Parameters</b>	<b>139</b>
<b>Editing Static Route Parameters</b>	<b>139</b>
<b>Deleting Static Routes</b>	<b>140</b>
Configuring Static ARP	141
<b>Creating ARP Entry</b>	<b>141</b>
Enabling Dynamic DNS	144
Configuring SNMP	148
Configuring Firewall Parameters	149
Configuring Proxy	150
Configuring L2TP Parameters	152
Managing Device Parameters	154
<b>Configuring SSL VPN Parameters</b>	<b>157</b>
Configuring User Access menus	157
Portal Layout	157
Authentication Domain	159
<b>Creating a Domain</b>	<b>159</b>
<b>Editing a Domain</b>	<b>160</b>
<b>Deleting a Domain</b>	<b>161</b>
Group/ Application	162
<b>Group</b>	<b>162</b>
<b>Applications</b>	<b>165</b>
SSL VPN Applications Overview	169
<b>Adding the Terminal Service (RDP) application</b>	<b>171</b>
<b>Adding Other Listed Applications</b>	<b>171</b>
Managing accounts	173
<b>Editing the Admin Account</b>	<b>173</b>
<b>Creating a New User Account</b>	<b>176</b>
<b>Editing User Account Parameters</b>	<b>176</b>

**Deleting User Accounts 178**

Account Move 179

Password Policy 181

Configuring Host Checking 184

Advance Setting for Network Extender Service 188

**Packet Filter 189**

189

**Client Address 190****Client Route 190****Standalone 191**

192

**SNE Script and IE Proxy Setting 192****SNE Setting on Client-side 195**

Advance Setting for Transport Extender Service 196

Managing Network Extender IP address and client routes 199

Modifying the Network Extender IP address range 199

Modifying the Network Extender client routes 200

**Creating Client Routes 200****Editing Network Extender Client Routes 200****Deleting Network Extender Client Routes 201**

Configuring Network Extender Host Name Resolution 202

**Creating Network Extender Host Name Resolutions 202**

Managing Transport Extender application and host names 204

Modifying the Transport Extender 204

**Creating a tunneled Transport Extender application 204****Editing Transport Extender Applications 204****Deleting Transport Extender applications 205**

Configuring host names for Transport Extender 206

**Creating Transport Extender Host Name Resolutions 206****Editing Transport Extender Host Name Resolutions 206****Deleting Transport Extender Host Name Resolutions 207**

Managing SSL Certification 208

Importing a certificate 208

SSL VPN Portal 214

Using SSL VPN Portal Access 214

Installing the Network Extender 217

Installing the Standalone Network Extender 221

**Standalone Network Extender Features 223**

Installing the Transport Extender 225

Accessing Network Place 229

Using Applications 230

Using FTP 230

**Administrator FTP Configuration 230****Remote User 235**

Using Telnet/SSH 238

**Administrator Telnet Configuration 238**

**Remote User 242**

Using HTTP(S) 246

**Administrator HTTP(S) Configuration 246**

**Remote User 250**

Using RDP 252

**Administrator Terminal Service (RDP) Configuration 252**

**Remote User 256**

Using VNC 259

**Administrator VNC Configuration 259**

**Remote User 263**

Using CIFS 266

**Administrator CIFS configuration 266  
269**

**Remote User 270**

Additional Applications 272

Mail server (Network Extender) 272

**Administrator Mail Server Configuration 272**

**Remote User 276**

Mail server (Transport Extender) 281

**Administrator Mail Server Configuration 281**

**Host Name Resolution 283**

**Remote User 284**

SSL VPN Concentrator 288

Only connect WAN interface of SSL VPN device 288

Only connect LAN interface of SSL VPN device 295

SSL VPN Connection Verification 303

Common certificate-related problems and their solutions 303

**The certificate was issued by an untrustworthy authority 303  
303**

**The name referred in the certificate does not match  
with the server's name 303**

**Date of the certificate is not valid 303**

**The security certificate has changed since the last check 304**

**Log and E-mail Alerts 305**

Log Configuration 305

Syslog Server 307

E-mail Alert Notification 308

**Save Configuration to Flash 309**

**Language 310**

**Product Registration 311**

VPN Status Page Registration 311

Web Site Registration 319

**Before you begin 325**

Network settings 325

Determining the type of IP network address 325

**Hardware problems 326**

**LAN interface problems 328**

Disabling pop-up windows 329

**Disabling all pop-ups 329****Enabling pop-up blockers with exceptions 329**

Java scripts 329

Java permissions 330

**WAN interface problems 331****Internet service provider problems 332****Troubleshooting Q&A 334**

Performing a hardware reset 335

Performing a software reset 336

**DMZ 339**

Firewall 339

Remote Access 360

**SNMP 363****SSL Knowledge 364**

SSL Applications 365

Adding an application proxy 367

Remote user access 371

Using Network Extender 374

How to configure Network Extender? 374

Remote SSL VPN Portal 377

Using Transport Extender 382

How to configure Transport Extender? 382

Remote SSL VPN Portal 385

**Importing a certificate 389**

Registering the BiGuard S Series 394

**Configuring an Active Directory server 400****IP Addresses 409****Netmask 409****Subnet Addressing 409****Private IP Addresses 410****Network Address Translation (NAT) 410****Dynamic Host Configuration Protocol (DHCP) 410****Router Basics 410**

What is a Router? 410

Why use a Router? 411

Routing Information Protocol (RIP) 411

**Firewall Basics 411**

What is a Firewall? 411

Stateful Packet Inspection 411

Denial of Service (DoS) Attack 411

Why Use a Firewall? 412

**SSL VPN 413**

Capabilities 413

Access Connection 413



Application & Management 413

Security 413

**Compatible Web Browsers 414**

**Supported Operating System 414**

**Firewall & Content Filter 414**

**Quality of Service Control 414**

**Web-Based Management 414**

**Two-Factor Authentication 414**

**IPSec VPN 415**

**Availability and Resilience 415**

**Logging and Monitoring 415**

**Network Protocols and features 415**

**Hardware Specifications 416**

Physical Interface 416

Physical Specifications 416

Power Requirements 416

**Operating Environment 416**

**Support and Services 416**

Limited Warranty 431

## Table of figures

<b>FIGURE 1</b>	BiGuard S20 front and rear views .....	15
<b>FIGURE 2</b>	Connecting the BiGuard S20 to a WAN .....	17
<b>FIGURE 3</b>	Connecting the BiGuard S20 to a LAN .....	17
<b>FIGURE 4</b>	Connecting the power cable .....	18
<b>FIGURE 5</b>	LED Status Display .....	18
<b>FIGURE 6</b>	All in one solution: firewall, remote and Internet access .....	19
<b>FIGURE 7</b>	Behind a gateway/firewall .....	20
<b>FIGURE 8</b>	Fitting into a DMZ zone behind an existing firewall router .....	20
<b>FIGURE 9</b>	All in one: public servers on DMZ zone, private servers on LAN .....	21
<b>FIGURE 10</b>	Load Balancing .....	22
<b>FIGURE 11</b>	Auto Fail Over .....	23
<b>FIGURE 12</b>	Network Extender .....	24
<b>FIGURE 13</b>	Transport Extender .....	24
<b>FIGURE 14</b>	Network Place .....	25
<b>FIGURE 15</b>	Application Proxy .....	25
<b>FIGURE 16</b>	Granular Access Control .....	26
<b>FIGURE 17</b>	SSL VPN Certification .....	27
<b>FIGURE 18</b>	SSL VPN Portals .....	28
<b>FIGURE 19</b>	Authentication Domains - local user database .....	28
<b>FIGURE 20</b>	Authentication Domain - remote authentication .....	29
<b>FIGURE 21</b>	Web Manager main screen overview .....	38
<b>FIGURE 22</b>	Monitoring Status screen items .....	48
<b>FIGURE 23</b>	Device Management screen .....	51
<b>FIGURE 24</b>	Time Zone screen .....	54
<b>FIGURE 25</b>	Ethernet screen .....	55
<b>FIGURE 26</b>	DHCP Status screen .....	56
<b>FIGURE 27</b>	Mapping MAC Address to Fixed IP Address screen .....	56
<b>FIGURE 28</b>	SSL User Status screen .....	58
<b>FIGURE 29</b>	ARP Table screen .....	58
<b>FIGURE 30</b>	Routing Table screen .....	59
<b>FIGURE 31</b>	Session Table screen .....	59
<b>FIGURE 32</b>	DHCP Table screen .....	60
<b>FIGURE 33</b>	IPSec Table screen .....	60
<b>FIGURE 34</b>	Traffic Statistics screen .....	61
<b>FIGURE 35</b>	System Log screen .....	62
<b>FIGURE 36</b>	LAN screen .....	63
<b>FIGURE 37</b>	Alias IP screen .....	64
<b>FIGURE 38</b>	DHCP status screen .....	65
<b>FIGURE 39</b>	DHCP Disable Server and Relay Agent .....	65
<b>FIGURE 40</b>	DHCP Server Parameters screen .....	66
<b>FIGURE 41</b>	DHCP Relay Parameters screen .....	68
<b>FIGURE 42</b>	WAN Settings screen .....	69
<b>FIGURE 43</b>	WAN Settings DHCP screen .....	70
<b>FIGURE 44</b>	WAN Settings PPPoE screen .....	71

<b>FIGURE 45</b>	WAN Settings Static IP screen .....	73
<b>FIGURE 46</b>	Bandwidth Settings screen .....	74
<b>FIGURE 47</b>	WAN Alias IP screen .....	75
<b>FIGURE 48</b>	General Setting screen .....	76
<b>FIGURE 49</b>	Outbound Load Balance screen .....	77
<b>FIGURE 50</b>	Protocol Binding screen .....	78
<b>FIGURE 51</b>	Enabling the DMZ .....	80
<b>FIGURE 52</b>	DMZ Transparent Mode .....	80
<b>FIGURE 53</b>	DMZ NAT Mode .....	80
<b>FIGURE 54</b>	Multiple NAT/Subnet Table .....	81
<b>FIGURE 55</b>	Configuring Network Object Addresses .....	82
<b>FIGURE 56</b>	Adding Addresses to the Address Table .....	82
<b>FIGURE 57</b>	Confirmed Addresses in the Address Table .....	83
<b>FIGURE 58</b>	Address Group list .....	85
<b>FIGURE 59</b>	Pre-defined and User-defined Service Table .....	88
<b>FIGURE 60</b>	Adding services to the Service Table .....	88
<b>FIGURE 61</b>	The Service Group Table .....	91
<b>FIGURE 62</b>	Schedule Table list .....	94
<b>FIGURE 63</b>	Adding a Schedule network object profile .....	94
<b>FIGURE 64</b>	Bandwidth Control Table .....	96
<b>FIGURE 65</b>	Adding a Bandwidth Control Network Object .....	96
<b>FIGURE 66</b>	Keyword Filter profiles .....	98
<b>FIGURE 67</b>	Adding a Keyword Filter Network Object Profile .....	98
<b>FIGURE 68</b>	Domain Filter profiles .....	101
<b>FIGURE 69</b>	Adding a domain filter Network Object profile .....	101
<b>FIGURE 70</b>	Restrict URL Features Network Object list .....	104
<b>FIGURE 71</b>	Restricting URL features .....	104
<b>FIGURE 72</b>	Packet Filtering table .....	106
<b>FIGURE 73</b>	Creating a Packet Filtering profile .....	106
<b>FIGURE 74</b>	Virtual Server parameters .....	110
<b>FIGURE 75</b>	Adding a Virtual Server .....	110
<b>FIGURE 76</b>	Moving a Virtual Server rule .....	111
<b>FIGURE 77</b>	QoS parameters .....	114
<b>FIGURE 78</b>	Adding a QoS profile .....	114
<b>FIGURE 79</b>	Moving a QoS rule .....	115
<b>FIGURE 80</b>	Ethernet MAC Filtering profiles .....	120
<b>FIGURE 81</b>	Adding an Ethernet MAC Filter profile .....	120
<b>FIGURE 82</b>	Content Filtering Policies .....	123
<b>FIGURE 83</b>	Creating a Content Filtering Profile .....	123
<b>FIGURE 84</b>	Adding an IP Exception .....	127
<b>FIGURE 85</b>	Deleting an IP Exception .....	127
<b>FIGURE 86</b>	IPSec Tunnels screen .....	128
<b>FIGURE 87</b>	Setting the Time Zone .....	132
<b>FIGURE 88</b>	Enabling Remote Access .....	133
<b>FIGURE 89</b>	Upgrading the Firmware .....	134
<b>FIGURE 90</b>	Backing up and restoring configurations .....	135

<b>FIGURE 91</b>	Backing Up a Configuration .....	136
<b>FIGURE 92</b>	Restoring a configuration .....	136
<b>FIGURE 93</b>	Changing Passwords .....	137
<b>FIGURE 94</b>	Restarting the system .....	138
<b>FIGURE 95</b>	The Static Routing List .....	139
<b>FIGURE 96</b>	Adding a static route .....	139
<b>FIGURE 97</b>	The Static ARP Table .....	141
<b>FIGURE 98</b>	Dynamic DNS Table .....	144
<b>FIGURE 99</b>	Enabling SNMP .....	148
<b>FIGURE 100</b>	Setting SNMP Parameters .....	148
<b>FIGURE 101</b>	Configuring the Firewall .....	149
<b>FIGURE 102</b>	L2TP Table .....	152
<b>FIGURE 103</b>	L2TP Configuration Screen .....	152
<b>FIGURE 104</b>	Changing Parameters .....	154
<b>FIGURE 105</b>	Portal Layout .....	158
<b>FIGURE 106</b>	Authentication Domain table .....	159
<b>FIGURE 107</b>	Domain authentication types screen .....	159
<b>FIGURE 108</b>	Group/Application Table screen .....	162
<b>FIGURE 109</b>	SSL VPN Application choices .....	169
<b>FIGURE 110</b>	Account Management screen .....	173
<b>FIGURE 111</b>	Admin Account Settings screen .....	173
<b>FIGURE 112</b>	Web Portal screen .....	183
<b>FIGURE 113</b>	Network Extender Client IP Address Assignment screen .....	199
<b>FIGURE 114</b>	Network Extender Client Routing Table .....	200
<b>FIGURE 115</b>	Adding Network Extender Client Routes .....	200
<b>FIGURE 116</b>	Network Extender Host Name Resolution screen .....	202
<b>FIGURE 117</b>	Adding a Host Resolution to Network Extender 202	
<b>FIGURE 118</b>	Transport Extender Configured Applications screen .....	204
<b>FIGURE 119</b>	Adding tunneled applications to Transport Extender .....	204
<b>FIGURE 120</b>	Transport Extender Configured Host Name Resolution screen .....	206
<b>FIGURE 121</b>	Transport Extender Add an host name resolution screen .....	206
<b>FIGURE 122</b>	SSL Certificate Current Certificate screen .....	208
<b>FIGURE 123</b>	Generate CSR/CRT screen .....	208
<b>FIGURE 124</b>	Downloading the CSR .....	209
<b>FIGURE 125</b>	CSR files .....	209
<b>FIGURE 126</b>	Opening the CSR .....	210
<b>FIGURE 127</b>	Certificate signing request .....	211
<b>FIGURE 128</b>	Certificate text .....	211
<b>FIGURE 129</b>	Inputting the CSR password .....	212
<b>FIGURE 130</b>	New certificate .....	213
<b>FIGURE 131</b>	Installation proceeding .....	218
<b>FIGURE 132</b>	Installation complete .....	219
<b>FIGURE 133</b>	FTP login .....	236
<b>FIGURE 134</b>	FTP session .....	237
<b>FIGURE 135</b>	Logon message .....	257

<b>FIGURE 136</b> VNC loading .....	264
<b>FIGURE 137</b> CIFS application log in .....	271
<b>FIGURE 138</b> SSL Certificate screen .....	303
<b>FIGURE 139</b> Log Configuration screen .....	305
<b>FIGURE 140</b> Syslog Server screen .....	307
<b>FIGURE 141</b> E-mail Alert screen .....	308
<b>FIGURE 142</b> Save Config to Flash screen .....	309
<b>FIGURE 143</b> Language Menu .....	310

# Getting Started

Welcome to the BiGuard S20 Administration Guide. This manual provides information on using the BiGuard S20 rackmountable device integrated with cutting-edge security technology including VPN and Firewall, enabling you to connect your network to the Internet securely without the worry of intruder attacks.



## Register Your BiGuard Gateway!

**NOTE:** Once you have established an Internet connection, please register your BiGuard gateway at [www.biguard.com](http://www.biguard.com) for firmware updates, the latest information and technical support. It is crucial that you register as soon as possible to enjoy the benefits of possessing a BiGuard gateway.

## About this guide

This manual describes how to install and operate the BiGuard S20. 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 ii before installing the BiGuard S20.

## Unpacking the BiGuard S20

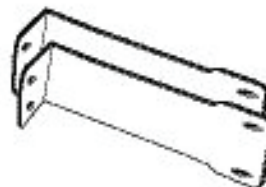
Carefully unpack the BiGuard S20 and check that the following items are included:



Power cable



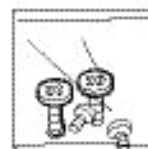
Warranty card x 1



Mounting brackets x 2



BiGuard S20



Mounting bracket screws x 4



Quick Start Guide x 1  
Administration Guide x 1



Ethernet cable x 1



Software CD x 1

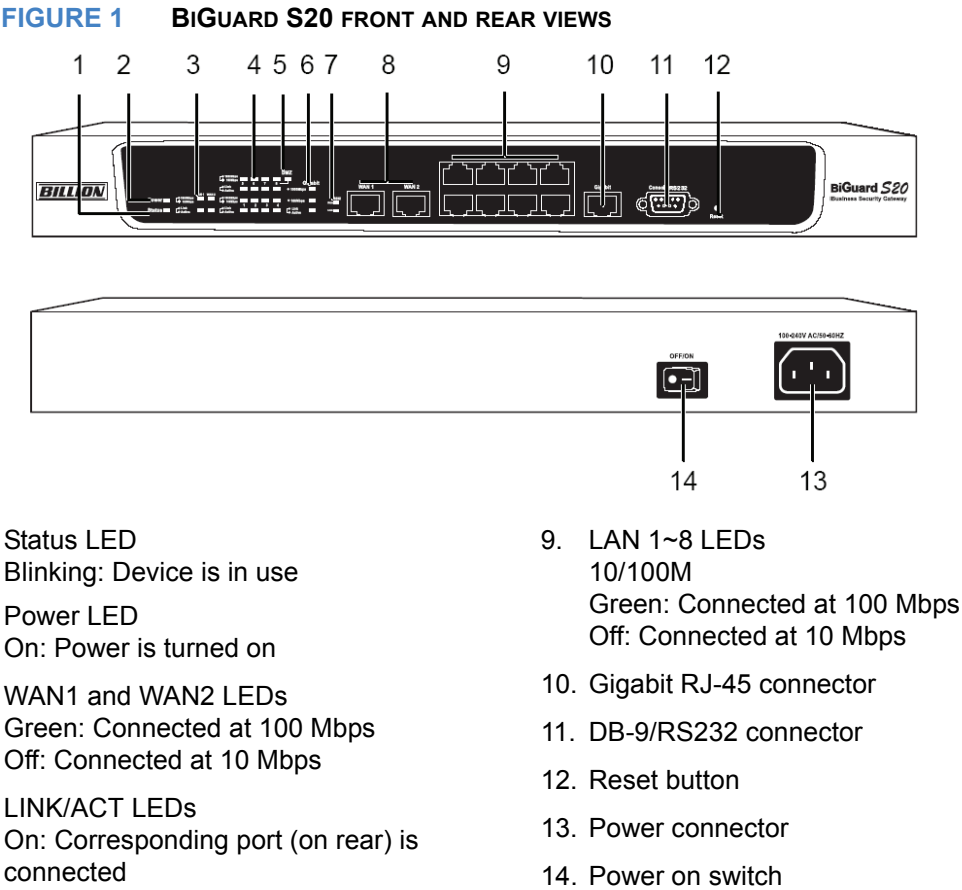


**NOTE:** If any item is missing or appears damaged, repack the BiGuard S20 and return it to your reseller.



Front and rear view of the BiGuard S20

Figure 1 shows the front and rear components on the BiGuard S20.



**NOTE:** Ensure that the BiGuard S20 is turned off before beginning setup.

## Setting up the BiGuard S20

This section provides a step-by-step guide in the hardware setup (rackmounting and power connection) and installation (LAN, WAN, and Gigabit) of the BiGuard S20.

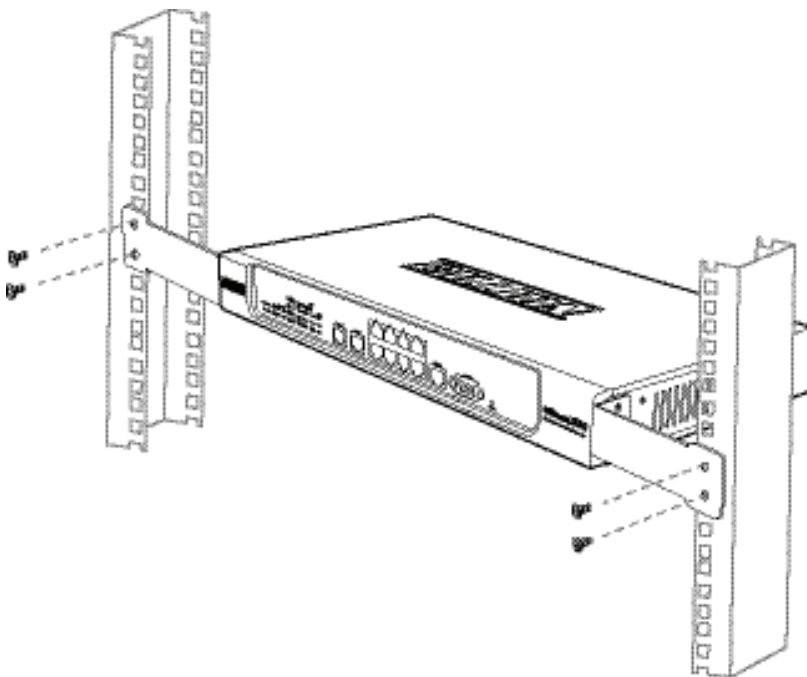
### Rackmounting the BiGuard S20

Follow the steps below to install the BiGuard S20 in a rack case.

1. Align one bracket with the holes on one side of the BiGuard S20 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 S20 in the rack by lining up the holes in the brackets with the appropriate holes in the rack.
4. Secure the BiGuard S20 to the rack with the remaining rack-mounting screws.

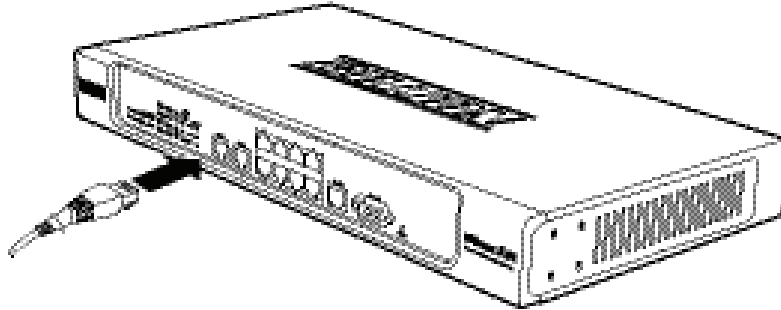


## Connecting to a WAN

Ensure that your hardware is powered off, including the BiGuard S20.

1. Connect an RJ-45 Ethernet cable to the WAN1 port and/or the WAN2 on the BiGuard S20.
2. Connect the other end to an ADSL or cable modem or another router.

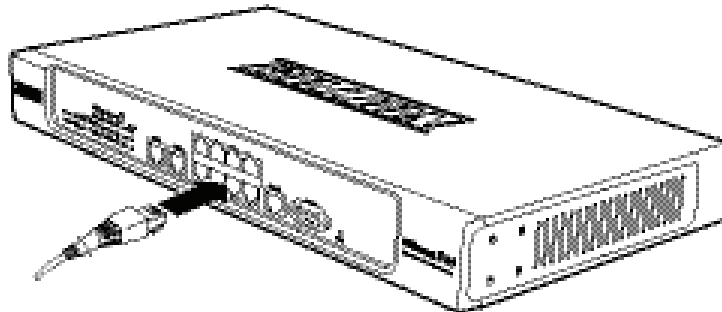
**FIGURE 2** CONNECTING THE BiGUARD S20 TO A WAN



## Connecting to a LAN

1. Connect switches, hubs, and servers to the eight LAN connectors on the BiGuard S20.

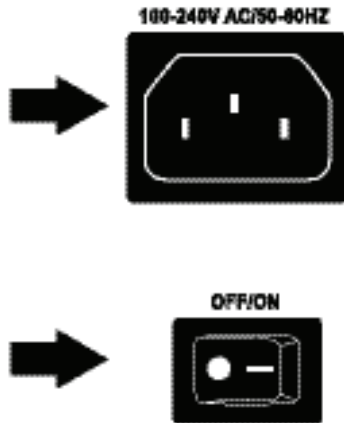
**FIGURE 3** CONNECTING THE BiGUARD S20 TO A LAN



## Connecting power

1. Connect the power cable to the connector on the BiGuard S20 and to an electrical outlet.
2. Turn the power button to the **On** position.

**FIGURE 4** CONNECTING THE POWER CABLE

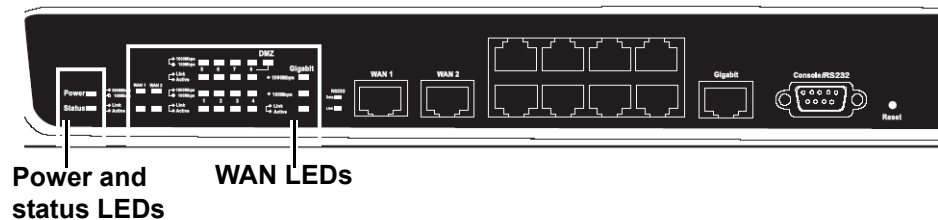


## Turning on the power and checking LED status

Press the power switch on the rear of the BiGuard S20. The LED sequence for powering on the BiGuard S Series is as follows:

- ALL LEDs flash in sequence three times.
- Power, status and connected port LEDs light.
- The status LED turns off to indicate the system is operational.

**FIGURE 5** LED STATUS DISPLAY



## Network deployment/applications

The purpose of this section is to help you set up the Dual WAN BiGuard S20 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 configuring the BiGuard S20 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/IPSec VPN Applications and SSL VPN Features for the use of the BiGuard S20 for easy integration of the BiGuard S20 into your existing network.

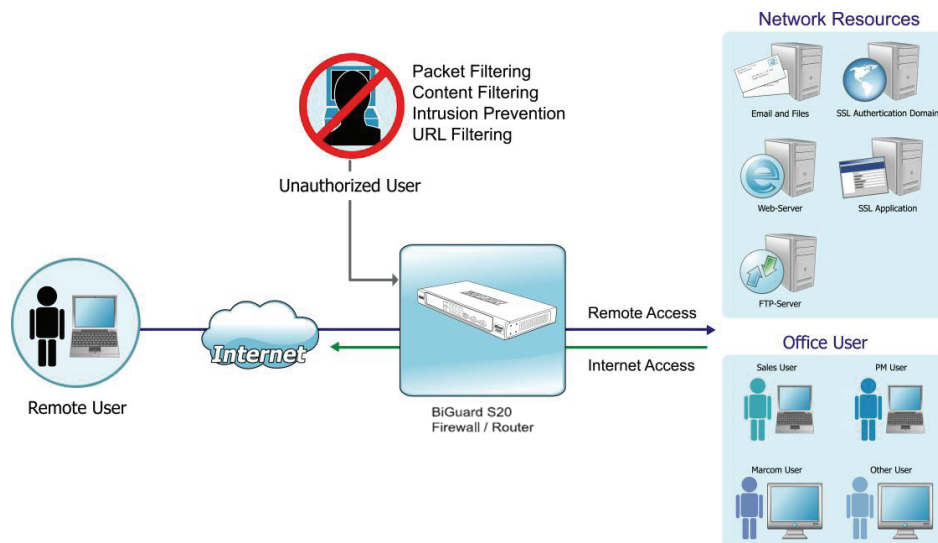
### Network environment scenarios

The following tables show different scenarios for deploying the BiGuard S20.

#### All in one solution: firewall, remote and Internet access

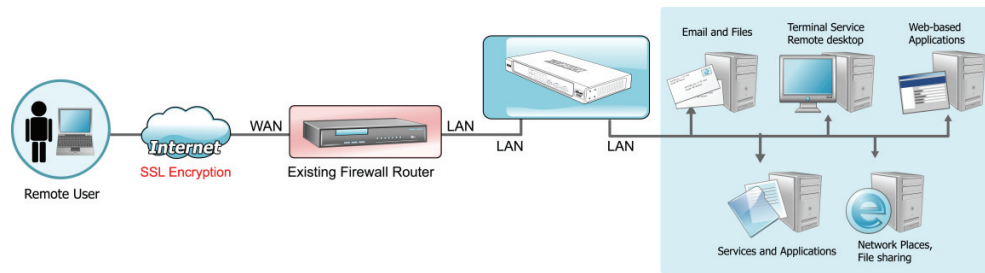
The BiGuard S20 provides the ideal solution for secure remote access to corporate networks, small branch offices and small/medium sized businesses. The BiGuard S20 also provides Internet access and firewall functionality for the organization. A typical setup for users and small businesses alike is to have a single BiGuard S20 device connected to the Internet as a secure gateway to provide an all-in-one secure remote and Internet access solution.

**FIGURE 6 ALL IN ONE SOLUTION: FIREWALL, REMOTE AND INTERNET ACCESS**



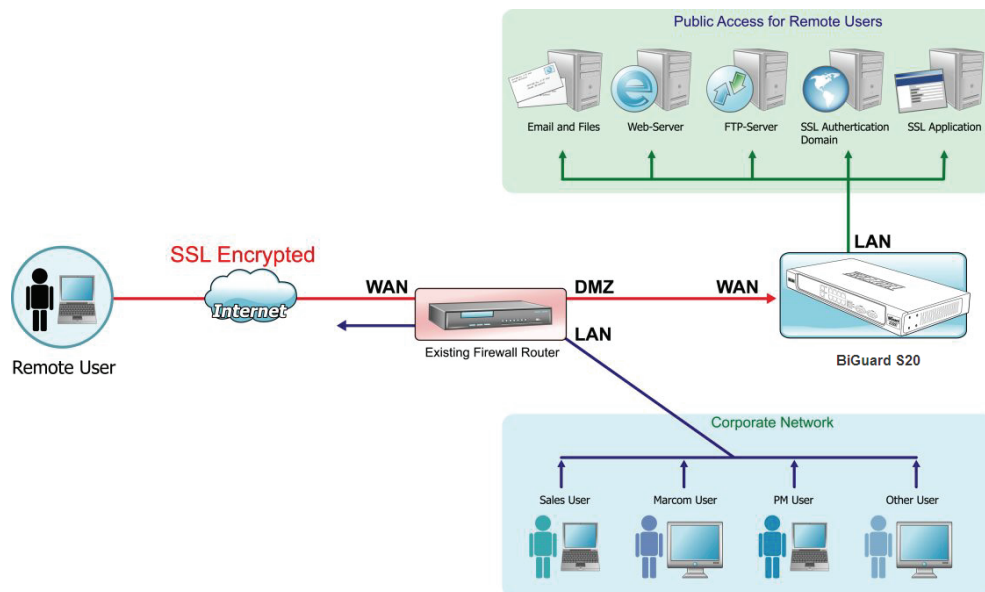
#### Installing behind a gateway/firewall

The BiGuard S20 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 7** BEHIND A GATEWAY/FIREWALL

### Fitting into a DMZ zone behind an existing firewall router

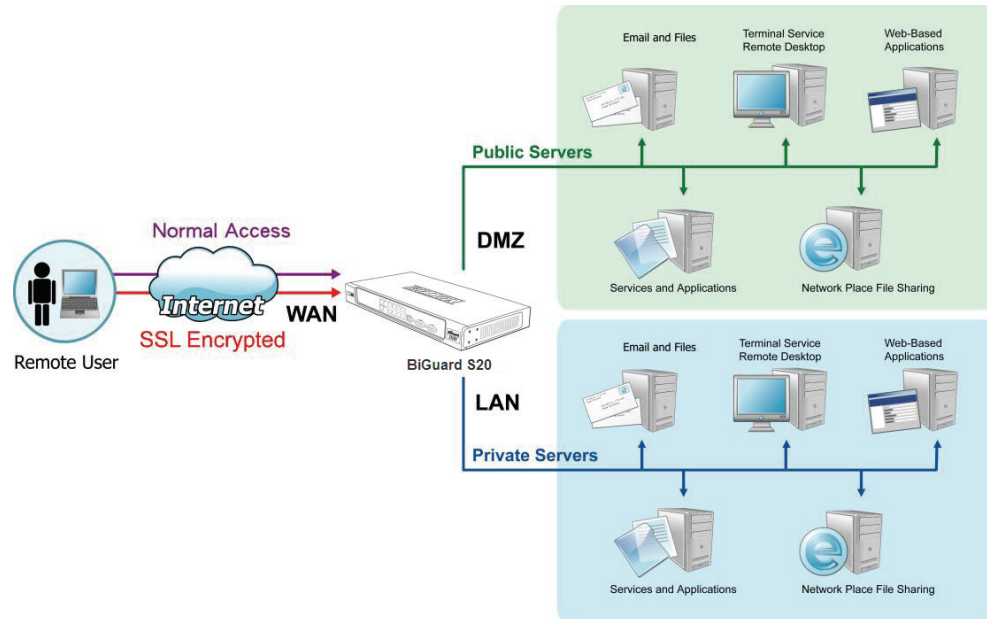
The following illustration demonstrates how the BiGuard S20 can be connected to the DMZ zone of an existing firewall router to provide secure remote access to the servers in the office.

**FIGURE 8** FITTING INTO A DMZ ZONE BEHIND AN EXISTING FIREWALL ROUTER

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

The BiGuard S20 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 9** ALL IN ONE: PUBLIC SERVERS ON DMZ ZONE, PRIVATE SERVERS ON LAN

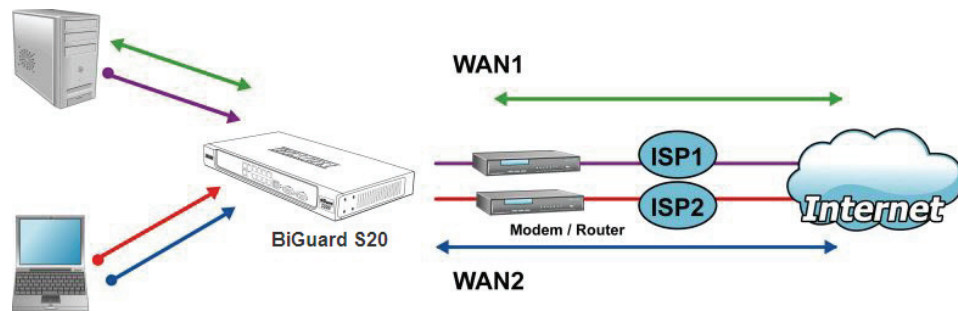




## Load Balancing

With integrated Dual WAN ports, the BiGuard S20 combines two broadband lines such as DSL or Cable into one Internet connection, providing optimal bandwidth sharing for multiple PCs on your network, or allowing maximum reliability with network redundancy. Load Balancing the BiGuard S20 to efficiently balance network traffic across two connections, ideal for small-to-medium businesses that require increased bandwidth, network scalability, and resilience for mission-critical network and Internet applications.

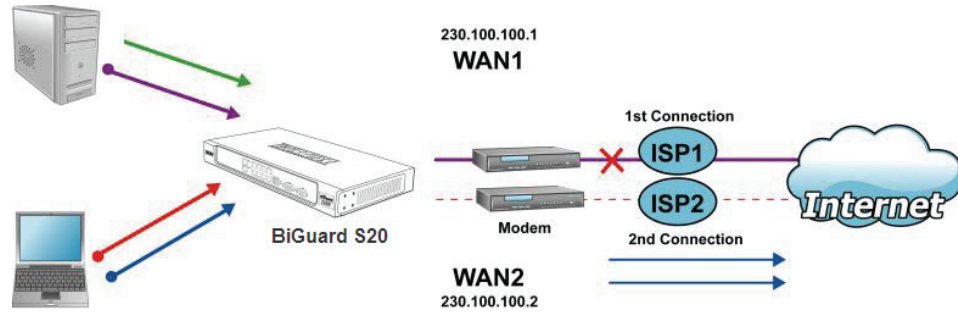
**FIGURE 10** LOAD BALANCING



## Auto Fail Over

In addition to Load Balancing, the integrated Dual WAN ports reliably provide Auto failover. It can be configured to ensure smooth, continuous service should one connection fail, providing maximum business uptime and productivity, plus uninterrupted service for you and your customers.

**FIGURE 11** AUTO FAIL OVER



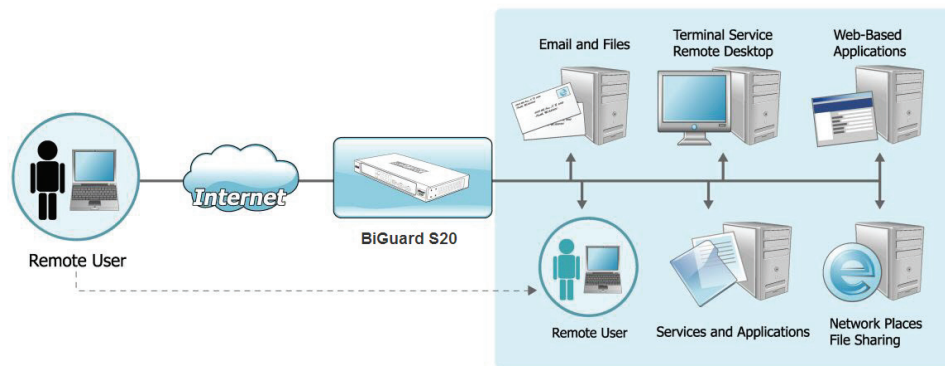
## SSL VPN Applications

The BiGuard S20 provides advanced routing functionality along with SSL VPN capability. The BiGuard S20 uses internal routing tables to read each incoming packet and decide how to forward it.

### Network Extender

The BiGuard S20 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.

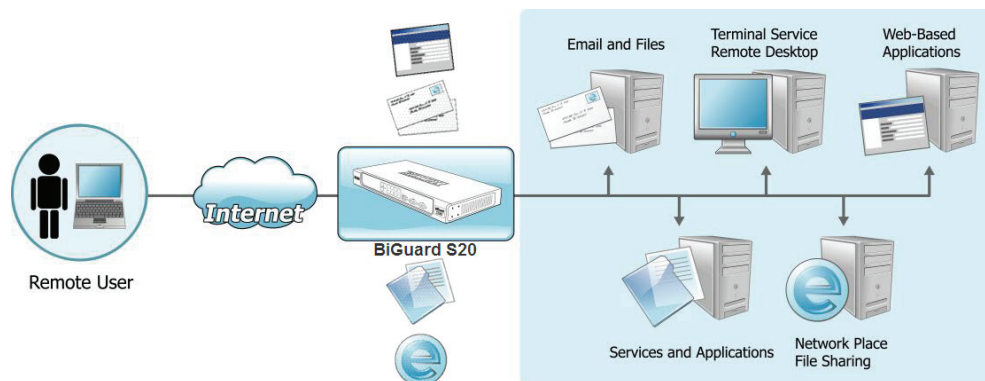
**FIGURE 12 NETWORK EXTENDER**



### Transport Extender

Another application that makes the BiGuard S20 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.

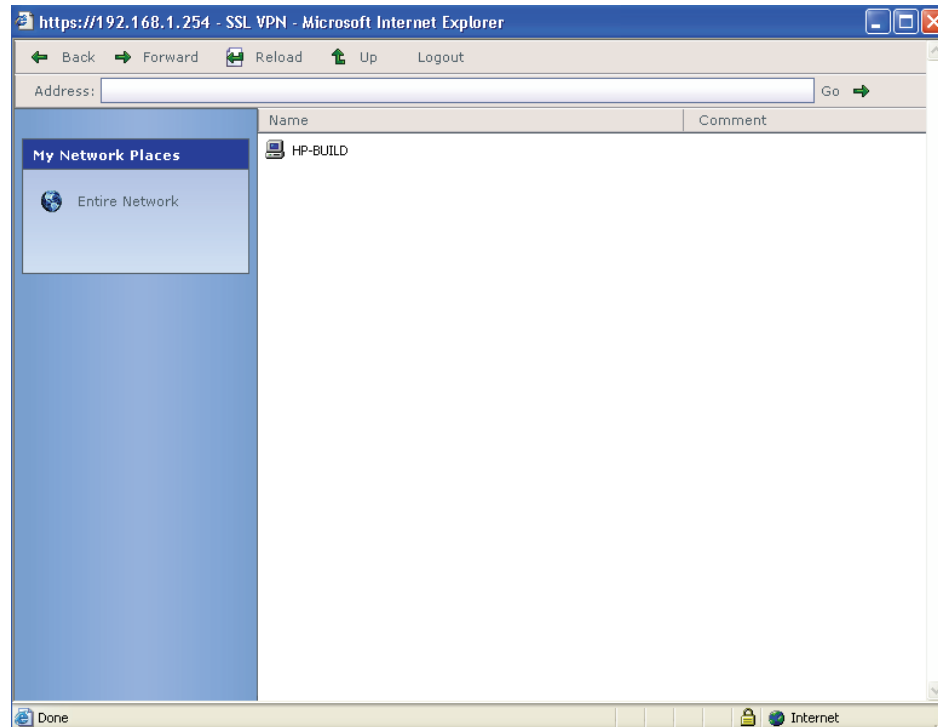
**FIGURE 13 TRANSPORT EXTENDER**



## Network Place

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

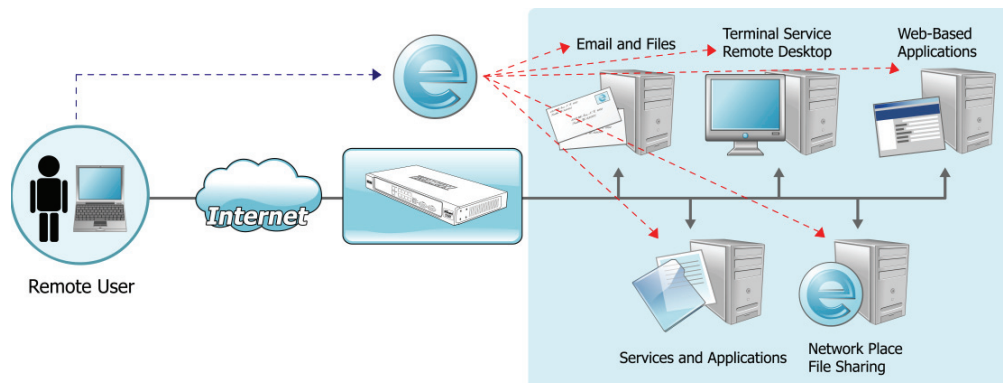
**FIGURE 14 NETWORK PLACE**



## 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 15 APPLICATION PROXY**



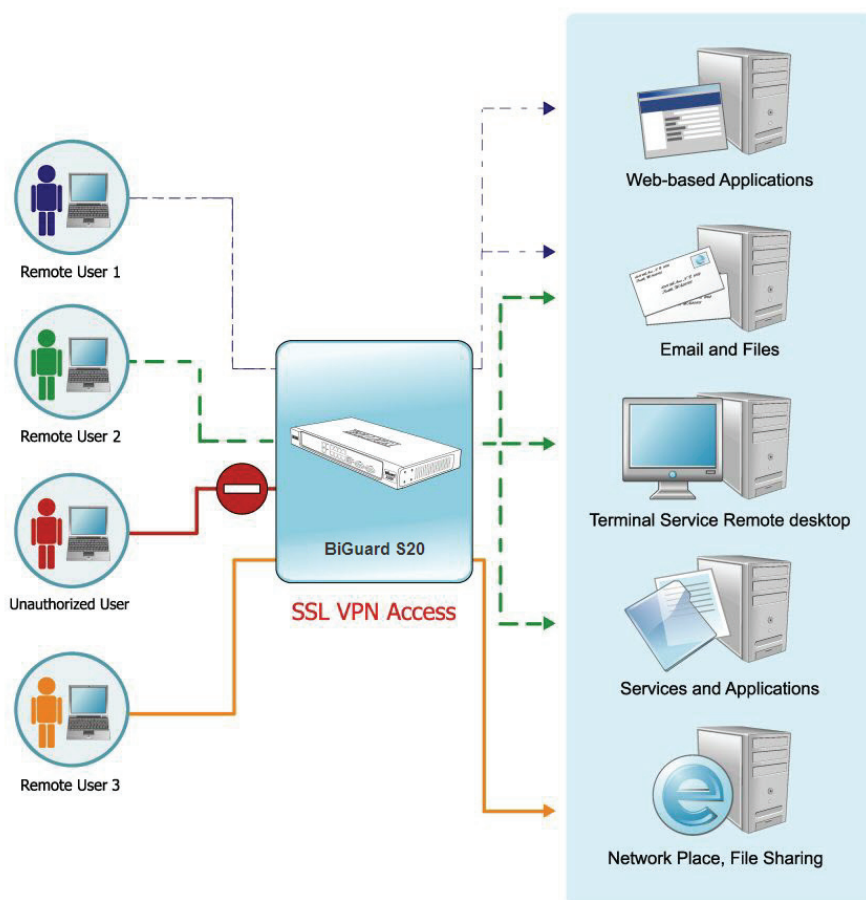
## SSL VPN Features

The following sections describe some of the advanced features of the BiGuard S20.

### Granular Access Control

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

**FIGURE 16** GRANULAR ACCESS CONTROL



### SSL VPN Certification

Manage, generate, and obtain security certificates from the Certificate Authority (CA). The certificate can achieve three purpose, enhanced authentication, encryption, and digital signature. It is recommended to install the certificate from a trusted root CA in the device configuration. This will provide the user a secure network traffic, a stronger SSL encryption, and much higher reliability. 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 S20. See [Importing a certificate](#) on page 208.

**FIGURE 17 SSL VPN CERTIFICATION**

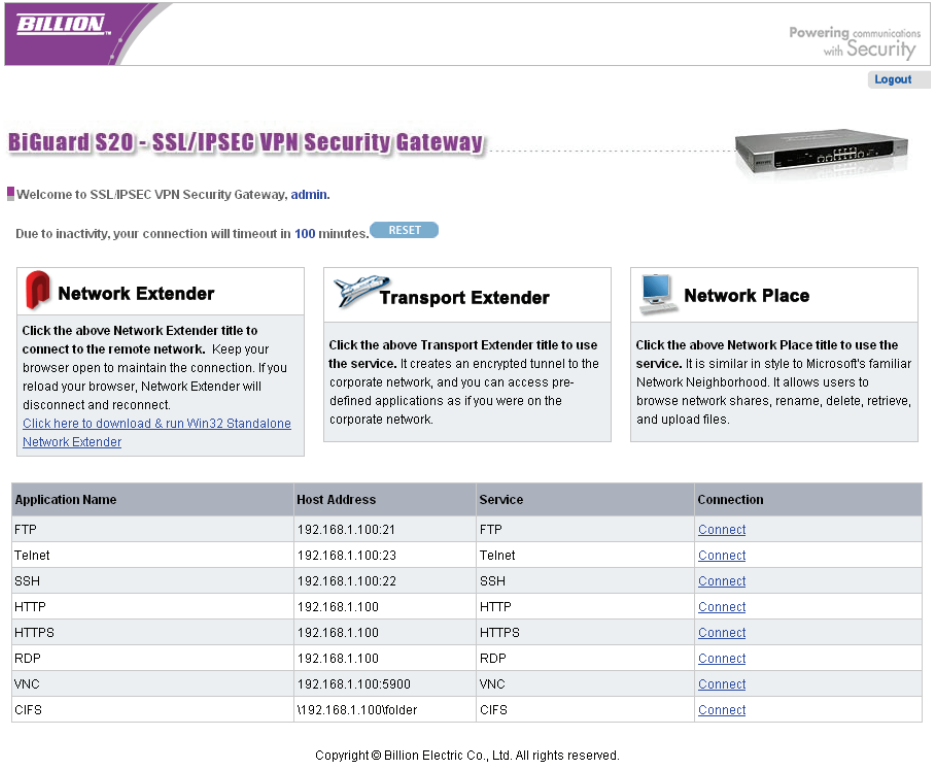
The screenshot shows the VeriSign website with a navigation bar at the top containing links for US Home, Worldwide Sites, Contact Us, and Site Map. Below the navigation bar is a search bar and a main menu with categories: Products & Services, Solutions, Support, About VeriSign, and Existing Customers. The main content area features a large banner for 'VeriSign® Identity Protection' with the tagline 'When consumers trust you, trust VeriSign' and a 'Learn more >>' link. To the right of the banner is a sidebar with 'SSL Certificates' and buttons for 'BUY SSL Certificates', 'BUY Code Signing', 'TRY Free SSL Trial', 'RENEW Renew Now', and 'SIGN IN Certificate Center'. Below the banner is a 'What's New' section mentioning 'VeriSign and Ratepoint' with a 'More News >>' link. The main content area is divided into three columns: 'Featured Product' (VeriSign Identity Protection Fraud Detection Stock Trading Module), 'Industry Solutions' (listing various sectors like Consumer Products, Financial Services, Healthcare, etc.), and 'Quick Links' (listing News and Events, RSS Feeds, Investor Relations, etc.). Below these columns is a 'Customers' section featuring 'ADDISON AVENUE FEDERAL CREDIT UNION' with the tagline 'We Listen. You Prosper.™'. On the right side of the main content area is a 'Try VeriSign SSL FREE for 14 days' offer with a 'Start now >>' link, and a 'VeriSign Secured Seal >>' section. The footer contains a copyright notice for 1995-2008 VeriSign, Inc. and a list of links for Products & Services, Solutions, Support, About VeriSign, Existing Customers, US Home, Worldwide Sites, Site Map, Search, and Feedback. A small disclaimer at the bottom states that VeriSign (Nasdaq: VRSN) is the trusted provider of Internet infrastructure services for the digital world.

## 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 Place, 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 157.

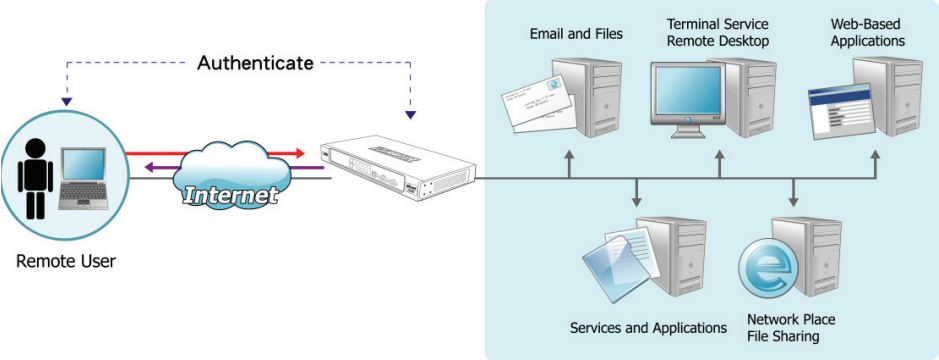
FIGURE 18 SSL VPN PORTALS



Authentication Domain Scenarios

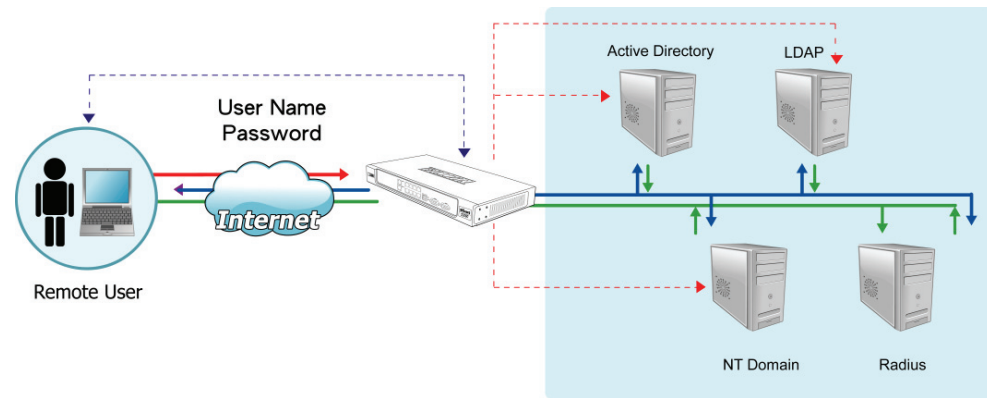
The following illustration demonstrates how a BiGuard S20 can be set up in a small organization to allow administrators the flexibility to manage user authentication simply and without the need of an authentication server.

FIGURE 19 AUTHENTICATION DOMAINS - LOCAL USER DATABASE



The BiGuard S20 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 20 AUTHENTICATION DOMAIN - REMOTE AUTHENTICATION**

See [Authentication Domain](#) on page 159.

## Firewall Settings

The BiGuard S20 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 S20 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 149.

## Intrusion detection

The BiGuard S20 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 S20 firewall can be set to block WAN requests from IP addresses that the router determines are unauthorized.

## WAN settings

The BiGuard S20 enables connection to an ISP using a static IP address, PPPoE protocol, or by automatically obtaining an IP address using DHCP. The BiGuard S20 enables you to connect using via the router or by using NAT (Network Address Translation). See [Configuring WAN settings](#) on page 69.

## Static IP

A Static WAN connection will be configured according to the IP properties defined by your ISP. In order to configure the BiGuard S20 for a Static WAN connection, you will need a static IP address, subnet mask, default IP gateway, and DNS information from your ISP.

## 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.

## DHCP

By configuring DHCP settings, the device is able to obtain IP settings automatically from the ISP.

# Administration Guide

This chapter explains how to perform administration tasks for the BiGuard S20. The Quick Start Menu helps you configure the WAN, LAN and SSL VPN quickly to get up and run as soon as possible.

This section helps you monitor configuration status and perform common tasks 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 Transport Extender application and host names, managing SSL certifications, configuring Dual WAN settings, configuring IPSec, using Dynamic DNS and creating system logs.

This chapter also describes enabling remote access, upgrading the firmware, and backing up and restoring configurations.

## Logging in to the BiGuard S20 Web Manager

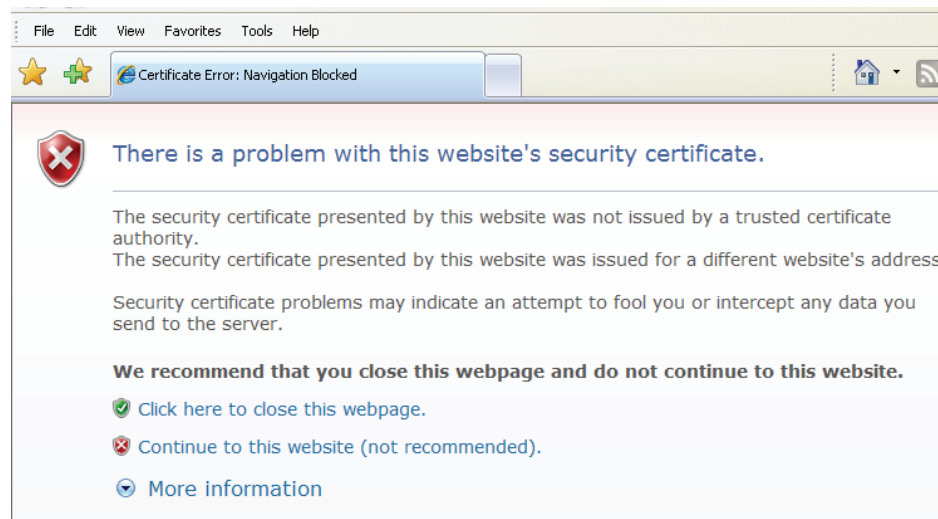
You configure and manage the BiGuard S20 with the Web Manager. The Web Manager is a web-based interface that you can access from any Java-enabled Web browser.

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

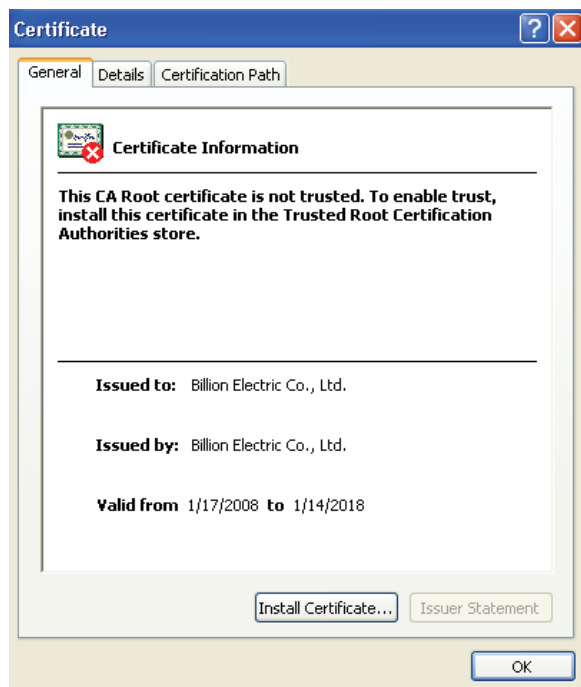


**NOTE:** To install the certificate for the BiGuard S20 continue by selecting **Yes**. Otherwise, click **No** to disconnect.

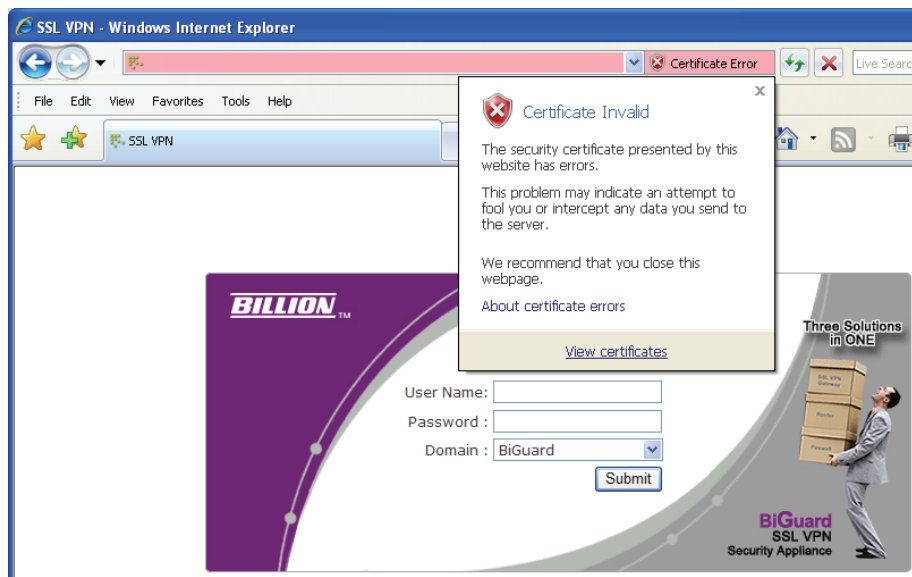
**Note:** Window Vista (Internet Explorer 7)'s version of **Security Alert**.



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



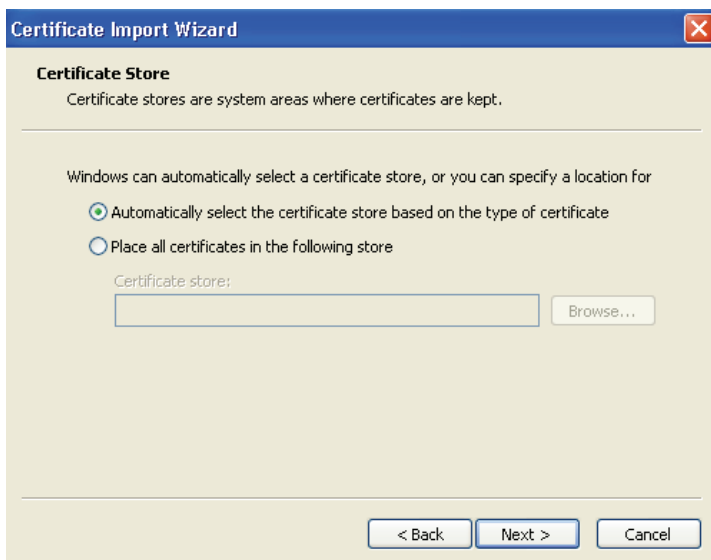
**Note:** Window Vista (Internet Explorer 7)'s version of **Security Alert**.



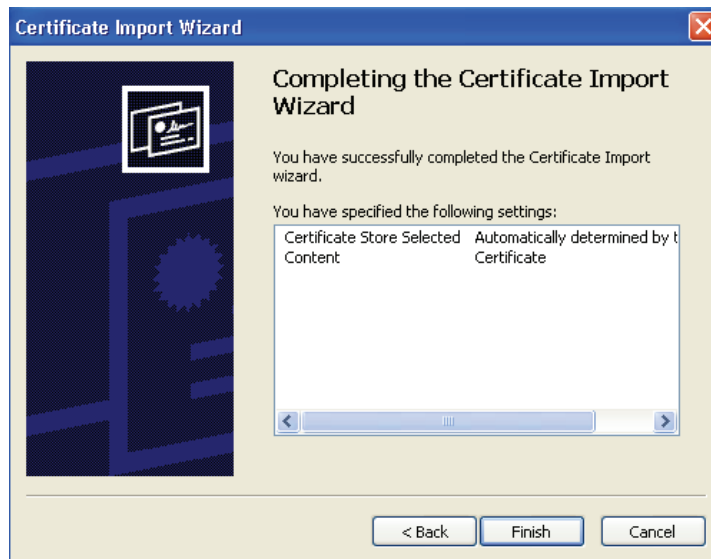
3. Click **Install Certificate**. The Certificate Import Wizard appears.



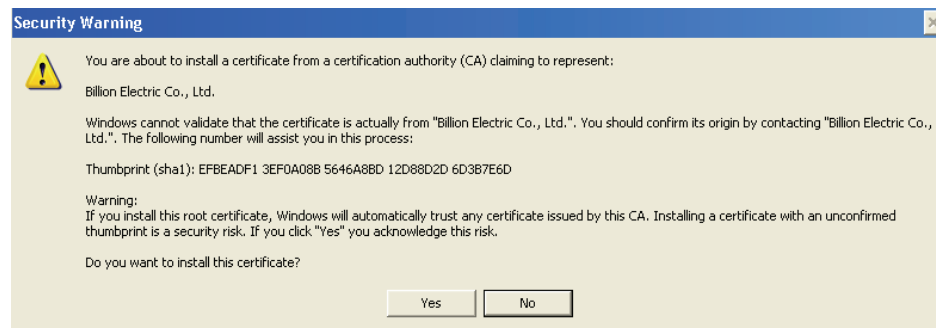
4. Click **Next**. You are prompted to choose the certificate location.



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



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



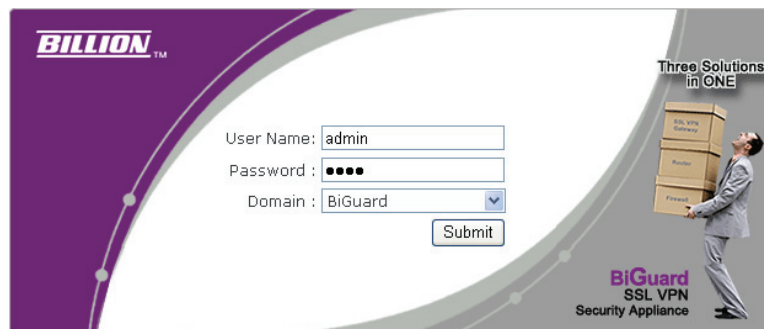
7. Click **Yes** to continue. A screen is displayed showing that the import was successful.



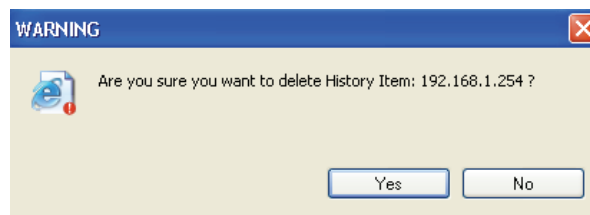
8. Click **OK** to return to the Certificate screen and click **OK** again to return to the Security Alert screen.



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



10. Enter the default user name and password:  
User Name: **admin**  
Password: **admin**  
then click **Submit**. The Web Manager opens on the Status menu.  
(See [Navigating in the Web Manager](#) on page 38.)
11. To log out of Web Manager, click **LOGOUT**. The Warning screen appears.



12. Click **Yes** if you do not want the BiGuard S20 IP address to remain in the browser history.





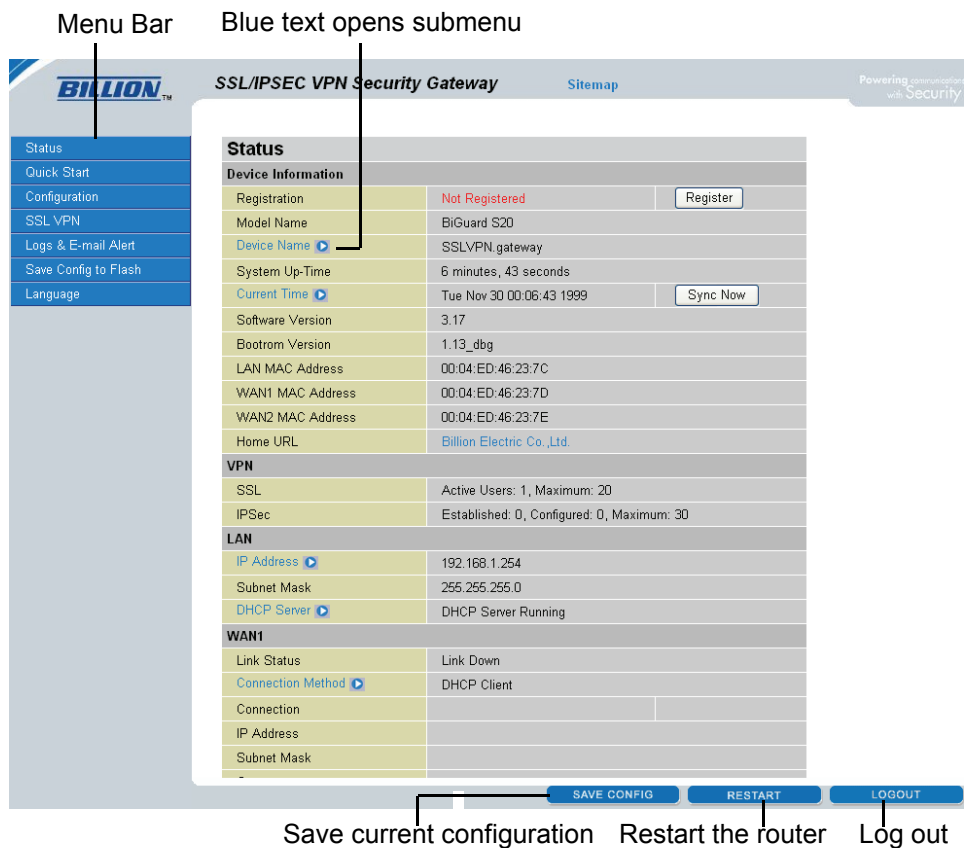
**WARNING:** When exiting the Web Manager, always use the LOGOUT button. If you close the Web Manager without logging out, you will not be able to log in with the same user name from a different computer until the account idle timeout period has passed.

**WARNING:** Not clearing the IP address of the BiGuard S20 from browser history is a potential security threat. If you have enabled remote administration of the BiGuard S20, be sure to change the user name and password.

## 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 21 WEB MANAGER MAIN SCREEN OVERVIEW**



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.

Basic Configuration with the Quick Start Menu

The Quick Start Menu enables you to quickly get the BiGuard S20 set up and run by configuring the WAN and Secure Socket Layer Virtual Private Network (SSL VPN) and assigning a user account.

Quick start to configuring the Dual WAN

This section describes how to configure the BiGuard S20 with basic settings to get your network up and running. There are three protocols for the router's WAN settings:

- Static IP
- PPPoE
- Obtain an IP Address Automatically (DHCP)



**NOTE:** The BiGuard S20 has two WAN connections, WAN1 and WAN2. The configuration steps are identical. In the following example, WAN1 is used.

Configuring the Dual 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 **WAN1**. The Quick Start WAN1 screen appears.
3. Select **Static IP** from the **Protocol** drop-down menu.

Quick Start WAN

Static IP

Protocol	Static IP	
IP Address	<input type="text"/>	
Subnet Mask	<input type="text"/>	
Gateway	<input type="text"/>	
DNS	Primary DNS	<input type="text"/>
	Secondary DNS	<input type="text"/>

4. Select **Static IP** from the **Protocol** drop-down menu.
5. Enter the IP address in the **IP Address** field.
6. Enter the subnet mask in the **Subnet Mask** field.
7. Enter the gateway in the **Gateway** field.
8. Enter the primary/secondary DNS in the **DNS** fields.
9. 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.
2. Click **WAN1**. The Quick Start WAN1 screen appears.
3. Select **PPPoE** from the **Protocol** drop-down menu.

Quick Start WAN1	
PPPoE	
Protocol	PPPoE <input type="button" value="v"/>
User Name	<input type="text"/>
Password	<input type="password"/>
Retype Password	<input type="password"/>
Connection	Always On <input type="button" value="v"/>
Idle Timeout	10 <input type="text"/> minutes
DNS	<input checked="" type="checkbox"/> Obtain DNS Automatically
	Primary DNS <input type="text"/>
	Secondary DNS <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Configuring the WAN for DHCP

Configure the WAN for DHCP to enable the BiGuard S20 to automatically assign IP addresses to client stations.

Refer to the following to configure the connection:

- 1. Click **Quick Start** in the Menu bar.
- 2. Click **WAN1**. The Quick Start WAN1 screen appears.
- 3. Select **Obtain an IP Address Automatically** from the **Protocol** drop-down menu.

Quick Start WAN1

Obtain an IP Address Automatically (DHCP Client)

Protocol

Obtain an IP Address Automatically

DNS

☒ Obtain DNS Automatically

Primary DNS

Secondary DNS

Apply

Cancel

- 4. Check **Obtain DNS Automatically** if your ISP provides this with the assigned IP. Otherwise, enter the Primary and Secondary DNS provided by your ISP.
- 5. Click **Apply** to confirm the settings.

## Quick start to configuring SSL VPN

This section describes how to configure the BiGuard S20 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.

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		<a href="#">Add Application</a>
Application Name	Application Type	IP Address / Path
<input type="button" value="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 85.

Quick Start SSL VPN	
Create the account user name and password	
Group Name	BiGuard
User Name	<input type="text"/>
Password	<input type="password"/>
Retype Password	<input type="password"/> <input type="checkbox"/> Use group default password
<input type="button" value="Add"/>	
Account Table	
admin	
<input type="button" value="Apply"/> <input type="button" value="Back"/>	

3. Enter the user name in the **User Name** field.
4. Enter and confirm a password in the **Password** and **Retype Password** fields. (**Note:** Tick **Use group default password** to use the group's password.)
5. Click **Add** to add the account. Once the account is added, the newly added account will be displayed in the Account Table below (**Note:** Account Table displays all the accounts under the chosen Group).

Quick Start SSL VPN	
Create the account user name and password	
Group Name	BiGuard
User Name	<input type="text"/>
Password	<input type="password"/>
Retype Password	<input type="password"/> <input type="checkbox"/> Use group default password
<input type="button" value="Add"/>	
Account Table	
example	<input type="button" value="Delete"/>
admin	
<input type="button" value="Apply"/> <input type="button" value="Back"/>	

- Click **Apply** to confirm the settings and you will be directed to the Account Table page displaying all the created accounts.

## Adding predefined applications

- In the Quick Start SSL VPN screen, click **Add Applications**. The Add Applications screen appears.

SSL VPN Application	
Add Application	
Application Name	<input type="text"/>
Application	Terminal Service (RDP) <input type="button" value="v"/>
IP Address/Domain Name	<input type="text"/>
Screen Size	640 x 480 <input type="button" value="v"/>
Local Device	<input type="checkbox"/> Drives
	<input type="checkbox"/> Ports
	<input type="checkbox"/> Printers
	<input type="checkbox"/> Smart Cards
Console Mode	<input type="checkbox"/> Active
Single Sign On Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Application and Path	<input type="text"/>
Terminal Server Port	3389 <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Fill in the **Application Name** blank with a given name.
- Select an application from the **Application** drop-down menu.  
See [SSL VPN Applications Overview](#) on page 169.
- Click **Apply** to confirm the settings.

## Quick start to configuring IPSec

This section describes how to set up an IPSec connection using the **IPSec Wizard**. Refer to the following to configure an IPSec connection:

1. Click **Quick Start** → **IPSec** in the Menu bar. The IPSec Wizard screen appears.

IPSec Wizard	
Step 1 of 3: Connection Information	
Connection Name	<input type="text"/>
Interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
PreShared Key	<input type="text"/>
Connection Type	<input checked="" type="radio"/> LAN to LAN
	<input type="radio"/> LAN to LAN (Mobile LAN)
	<input type="radio"/> LAN to Host
	<input type="radio"/> LAN to Host (Mobile Client)
	<input type="radio"/> LAN to Host (For BiGuard VPN Client)
<input type="button" value="Next"/>	

2. Enter the connection name in the **Connection Name** field.
3. Select the **WAN1** or **WAN2** interface to establish an IPSec VPN tunnel connection.
4. Enter a preshared key in the **PreShared Key** field. The preshared key is used by the Internet Key Exchange protocol (IKE) to establish a shared security policy and authenticated keys. Each router must be able to identify its counterpart using the preshared key before any IPSec traffic can be passed.
5. Select a connection type from the **Connection Type** buttons and click **Next**.



**NOTE:** The following steps depend on the choice of connection mode.

### LAN to LAN

LAN to LAN uses an IPSec VPN tunnel to securely establish a connection to a remote router. Selecting LAN to LAN and clicking **Next** displays the Remote Information screen:

IPSec Wizard	
Step 2 of 3: Remote Information	
Remote Secure Gateway Address (or Hostname)	
<input type="text"/>	
Remote Network	IP Address
	Netmask
<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
<input type="button" value="Back"/> <input type="button" value="Next"/>	

1. Type the IP address or Hostname of the remote VPN gateway in the **Remote Secure Gateway Address (or Hostname)** field.
2. Type the **IP Address** and **Netmask** of the **Remote Network** in the supplied fields.
3. Click **Back** to return to the Connection Information screen or click **Next** to proceed to the Configuration Summary screen.



## LAN to LAN (Mobile LAN)

LAN to LAN (Mobile LAN) uses an IPsec VPN tunnel to securely establish a connection to a remote router that is using Dynamic Internet IP.

Selecting LAN to LAN (Mobile LAN) and clicking **Next** displays the Remote Information screen:

IPSec Wizard			
Step 2 of 3: Remote Information			
Remote Identifier		<input type="text"/>	
Remote Network	IP Address	<input type="text"/>	<input type="text"/>
	Netmask	<input type="text"/>	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>			

1. Type the remote identifier of the remote gateway in the **Remote Identifier** field. Depending on the input value, the ID type is auto-defined as IP Address, FQDN(DNS) or FQUN(E-mail).
2. Type an IP address and netmask of the Remote Network in the **IP Address** and **Netmask** field.
3. Click **Back** to return to the Connection Information screen or click **Next** to proceed to the Configuration Summary screen.

## LAN to Host

LAN to Host uses an IPsec VPN tunnel to securely establish a connection to a computer.

Selecting LAN to Host and clicking **Next** displays the Remote Information screen:

IPSec Wizard	
Step 2 of 3: Remote Information	
Remote Secure Gateway Address (or Hostname)	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	

1. Type the IP address or hostname of the remote VPN device in the **Remote Secure Gateway Address (or Hostname)** field to allow a VPN tunnel to be established.
2. Click **Back** to return to the Connection Information screen or click **Next** to proceed to the Configuration Summary screen.

## LAN to Host (Mobile Client)

LAN to Host (Mobile Client) uses an IPsec VPN tunnel to securely establish a connection to a computer that uses Dynamic Internet IP.

Selecting LAN to Host (Mobile Client) and clicking **Next** displays the Remote Information screen:

IPSec Wizard	
Step 2 of 3: Remote Information	
Remote Identifier	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	

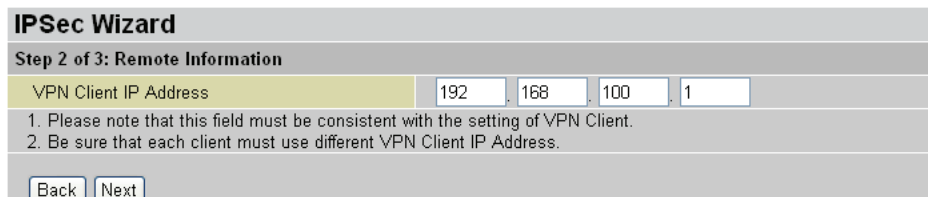
1. Type the remote identifier of the remote gateway in the **Remote Identifier** field. Depending on the input value, the ID type is auto-defined as IP Address, FQDN(DNS) or FQUN(E-mail).

2. Click **Back** to return to the Connection Information screen or click **Next** to proceed to the Configuration Summary screen.

### LAN to Host (for BiGuard VPN Client)

LAN to Host (for BiGuard VPN Client) uses an IPsec VPN tunnel to securely establish a connection to a computer that has BiGuard VPN Client installed.

Selecting **LAN to Host (for BiGuard VPN Client)** and clicking **Next** displays the Remote Information screen:



**IPsec Wizard**

**Step 2 of 3: Remote Information**

VPN Client IP Address: 192 168 100 1

1. Please note that this field must be consistent with the setting of VPN Client.  
2. Be sure that each client must use different VPN Client IP Address.

1. Type the VPN Client IP Address for the BiGuard VPN Client. This value is applied on both remote ID and Remote Network as a single address.



**NOTE:** Ensure that each client uses a different VPN Client Address.

2. Click **Back** to return to the Connection Information screen or click **Next** to proceed to the Configuration Summary screen.

The IPSec Configuration Summary screen

The Configuration Summary screen displays the data input on the selected Connection Type screens.

IPSec Wizard

Configuration Summary

Connection Name		test		
Tunnel		Enabled		
Interface		WAN1		
Local	ID	WAN IP Address	Type	IP Address
	Network	192.168.1.254/255.255.255.0	Type	Subnet
Remote	Secure Gateway	ANY	Type	Dynamic IP
	ID	192.168.100.1	Type	IP Address
	Network	192.168.100.1	Type	Single IP
Proposal	Secure Association	Aggressive Mode		
	Method	ESP		
	Encryption Protocol	3DES		
	Authentication Protocol	MD5		
	Perfect Forward Secure	Enabled		
	Key Group	Group 2		
	PreShared Key	test		
	IKE Life Time	3600 seconds		
Key Life Time	28800 seconds			

Back

Done

Review the connection information on the screen. To make any necessary amendments, click **Back** to return to the Connection Type screen. To complete the IPSec Configuration, click **Done**.

## 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 etc. 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 22** MONITORING STATUS SCREEN ITEMS

Status

Device Information

Registration	Not Registered	Register
Model Name	BiGuard S20	
Device Name	SSLVPN.gateway	
System Up-Time	6 minutes, 43 seconds	
Current Time	Tue Nov 30 00:06:43 1999	Sync Now
Software Version	3.17	
Bootrom Version	1.13_dbg	
LAN MAC Address	00:04:ED:46:23:7C	
WAN1 MAC Address	00:04:ED:46:23:7D	
WAN2 MAC Address	00:04:ED:46:23:7E	
Home URL	Billion Electric Co.,Ltd.	

VPN

SSL	Active Users: 1, Maximum: 20
IPSec	Established: 0, Configured: 0, Maximum: 30

LAN

IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server	DHCP Server Running

WAN1

Link Status	Link Down
Connection Method	DHCP Client
Connection	
IP Address	
Subnet Mask	
Gateway	

WAN2

Link Status	Link Down
Connection Method	DHCP Client
Connection	
IP Address	
Subnet Mask	
Gateway	

---

**Device Information**

Registration	Click to open a web page on Billion's BiGuard S Series website to register the BiGuard S20. Registration enables users to access new firmware, a user's manual, latest product news, quick customer support, and FAQ.
Model Name	Displays the model name.
Device Name	Displays the device name. See <a href="#">Changing the device name</a> on page 51.
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.
Software version	The version number of firmware on the flash. BiGuard S20 dual firmware feature protect upgrade failure by allowing two firmwares on the flash at the same time. The current running firmware is marked as "(Active)"
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 1 MAC Address	Displays the WAN MAC address for WAN 1.
WAN 2 MAC Address	Displays the WAN MAC address for WAN 2.
Home URL	Displays the manufacturer's website.

**VPN**

SSL Active Users	Displays the number of active users who are logged on through the SSL VPN Portal, including the administrator.
IPSec	Displays the number of established, configured and the maximum number of tunnels for IPSec.

**LAN**

IP Address	Displays the IP address for the LAN. See <a href="#">Changing the default LAN IP address</a> on page 55.
Subnet Mask	Displays the subnet mask for the LAN.
DHCP Server	Displays DHCP server status for the LAN.( Disable / DHCP Server / DHCP Relay Agent )See <a href="#">DHCP server settings</a> on page 56.

**WAN 1 and WAN 2**


---

---

---

Link Status	It displays WAN link status and the result of autonegotiation. If WAN is connected, it shows "Link Up", with speed (10Mbps/100Mbps/1000Mbps) and mode ( Half duplex / Full duplex ). If WAN is not connected, it shows "Link Down".
Connection Method	Displays the connection method for the WAN1 and WAN2. See <a href="#">Configuring WAN settings</a> on page 69.
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 WAN.
Gateway	Displays the gateway for the WAN.

---

---

## Changing the device name

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

**FIGURE 23** DEVICE MANAGEMENT SCREEN

Device Management		
<b>Device Name</b>		
Name	SSLVPN.gateway	
<b>DNS Backup</b>		
DNS Backup	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
IP Address	192.168.1.254	
<b>Embedded Web Server</b>		
HTTP Port	80	(80 is default HTTP port)
HTTPS Port	443	(443 is default HTTPS port)
Configuration	<input type="checkbox"/> Same subnet is required to access remote configuration	
SSL Protocol	<input checked="" type="checkbox"/> SSL V2 <input checked="" type="checkbox"/> SSL V3 <input checked="" type="checkbox"/> TLS	
SSL Encryption	<input type="checkbox"/> Key length $\geq$ 128 bits	
<b>Central Management Server</b>		
CMS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
IP Address/Domain Name		
CMS Server Port	8443	(8443 is default CMS Server Port)
Resync Period	1	minutes
<b>Telnet Setup</b>		
Telnet Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Telnet Port	23	(23 is default Telnet port)
Interface	LAN	
Configurable Address	**Any	
<b>Dial-In Setup</b>		
Dial-In	<input type="radio"/> Enable Dial-In but Disable CLI <input type="radio"/> Enable CLI but Disable Dial-In <input checked="" type="radio"/> Disable CLI and Dial-In	
Baudrate Setting	57600bps(14.4K/28.8K modem)	
Init-String	ATS0=0Q0&D3&C1	
Server IP Address Assign	10.0.0.1	
Client IP Address Assign	10.0.0.2	
<b>CLI Setup</b>		
CLI Account	<input type="radio"/> User Defined <input checked="" type="radio"/> System Default	
User Name	admin	
Password	*****	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Return"/>		

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

---

### Device Name

**Name** Enter a given name in the Name field to distinguish it from other gateway devices on the network. The value of the field will be shown on the status page so that the administrator can identify the device after login.

### DNS Backup

**DNS Backup** Select the radio button **Enable** to use the DNS Backup feature.

**IP Address** Enter the DNS server's IP Address if you want to use this DNS backup when WAN interface can't connect.

---

---

**Embedded Web Server**

HTTP Port / HTTPS Port	BiGuard S20 allows a user to modify the default port number of HTTP and HTTPS, which are 80 and 443 respectively. Modifying the well-known port numbers can prevent from hacker or internet robot access your site easily.
Configuration	Check the check box if you want to restrict remote configuration access only to people that are within the same subnet as the device.
SSL Protocol	Check the check box to enforce the selection of SSL protocol. Default protocol is auto-negotiation.
SSL Encryption	Check the check box to enforce the higher security of SSL Encryption which key length is more than 128 bits. Default key length is auto-negotiation.

**Telnet Setup**

Telnet Server	You can <b>Enable</b> or <b>Disable</b> the use of Telnet to be used to communicate with the device.
Telnet Port	Enter the Telnet port, the default is 23.
Interface	Check the check box to enable telnet access from WAN. For security concern, the default setting only allows access from LAN.
Configurable Address	Choose the IP Address you want to communicate with other PCs. You could choose from <b>Configurable Address</b> drop-down menu or click <b>Configurable Address</b> to create IP Addresses.

**Dial-In Setup**

Dial-In	With <b>Dial-In</b> enabled, administrator can use dial-in modem to perform router configurations through the terminal and web interface.
Baudrate Setting	The <b>Baudrate Setting</b> can be adjusted according to the speed of the modem that will establish a connection with the router.
Init-String	<b>Init-String</b> are used to configure the modem's options for things like error correction, data compression, flow control and much more. Please look up in your modem manual for the suitable init-string as the incorrect init-string can cause the connection to fail.
Server IP Address Assign	Enter the address in the <b>Server IP Address Assign</b> field that the administrator will access through the modem connection.
Client IP Address Assign	Enter the address in the <b>Client IP Address Assign</b> field that the administrator will be assigned to through the modem connection.

**CLI Setup**

CLI Account	Choose between <b>User Defined</b> and <b>System Default</b> user name and password for the CLI login account.
-------------	--

---



---

User Name	Type the user name you want for the <b>User Defined</b> CLI Account.
-----------	--

Password	Type the password you want for the <b>User Defined</b> CLI Account.
----------	---

---

Click **Apply** to confirm the settings.

### Changing time and time zone parameters

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

**FIGURE 24** TIME ZONE SCREEN

Time Zone

Parameters

Time Zone

☒ Enable ☐ Disable

Local Time Zone (+ -GMT Time)

(GMT)Greenwich Mean Time

SNTP Server IP Address

1192.43.244.18

2128.138.140.44

3129.6.15.29

4131.107.1.10


Daylight Saving

☒ Automatic

Resync Period

1440

minutes



Apply

Cancel

Return

Time Zone	Enable or disable the time zone function. If you disable time zone, the other blanks are unavailable.
Local Time Zone (+GMT Time)	Click the drop-down menu to choose the time zone for your location.
SNTP Server IP Address	Four SNTP time synchronization server addresses are defined by default. Change these blanks to your preferred SNTP servers.
Daylight Saving	Check the check box to automatically update the time based on your location's daylight saving settings.
Resync Period	Type in the period of the time that the device resync internal clock with SNTP 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 25 ETHERNET SCREEN

Ethernet

Parameters

IP Address	192.168.1.254
Subnet Mask	255.255.255.0
RIP	Disabled
LAN IP Subnet Sync	<input checked="" type="checkbox"/> Auto Configure the IP Range of Network Extender

Apply

Cancel

Return

IP Address	Enter the preferred IP address.
Subnet Mask	Enter the preferred subnet mask.
RIP	Click the drop-down menu to enable Routing Information Protocol (RIP). The options are: RIPv1; RIPv2; RIPv1 + RIPv2; RIPv2 Multicast; and RIPv1 + RIPv2 Multicast.
LAN IP Subnet Sync	Check the check box if you want the device to automatically configure the IP range of the Network Extender configuration according to LAN IP subnet (this saves you the worry of manually changing the IP address of Network Extender, everytime you have an IP change).

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 26** DHCP STATUS SCREEN

DHCP Server

Configuration

DHCP Server Mode

☐ Disable

☒ DHCP Server

☐ DHCP Relay Agent

Next

Return

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 S20 enables to act as a DHCP server for your network. Disable this function if the stations that connect to the BiGuard S20 LAN ports use static IP addresses. To change DHCP settings, see [Configuring DHCP server settings](#) on page 65.

### **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 27** MAPPING MAC ADDRESS TO FIXED IP ADDRESS SCREEN

DHCP Server

Fixed MAC Address Mapping to fixed IP Address

Host Name

MAC Address

Candidates

IP Address

Apply

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**. On the **Status** page, click **DHCP Server**.

3. On the DHCP Server Configuration screen, click **Next**.

DHCP Server	
<b>Configuration</b>	
DHCP Server Mode	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Server <input type="radio"/> DHCP Relay Agent
<input type="button" value="Next"/> <input type="button" value="Return"/>	
<b>DHCP Server Status</b>	
Status	DHCP Server Running
<b>Subnet Definitions</b>	
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 **Add**.

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

5. In the **Host Name** field, fill in a name to identify the computer.

DHCP Server	
<b>Fixed MAC Address Mapping to fixed IP Address</b>	
Host Name	
MAC Address	<a href="#">Candidates</a>
IP Address	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- You can either fill in MAC address blank, or click **Candidates** link and pick up the computer you want to map from the MAC address lists of active PCs on the LAN.
- In the **IP Address** field, fill in 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.

## Status Overview

### SSL user status

The SSL User Status screen lists users that are currently logged onto the BiGuard S20. You can monitor user activity and disconnect specific users.

Click **Status** → **SSL User Status** in the Menu bar to open SSL User status screen.

**FIGURE 28** SSL USER STATUS SCREEN

SSL User Status				
Status				
Name	Group	From IP Address	Login Time	
admin	BiGuard	192.168.1.35	Tue Nov 30 00:04:22 1999 (6000s)	<a href="#">Disconnect</a>
<input type="button" value="Refresh"/>				

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 <b>Disconnect</b> to disconnect specific users.
Refresh	Click <b>Refresh</b> 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.

Click **Status** → **ARP Table** in the Menu bar to open ARP table screen.

**FIGURE 29** ARP TABLE SCREEN

ARP Table			
IP <> MAC List			
IP Address	MAC Address	Interface	Static
192.168.1.1	00:1A:4B:39:63:70	LAN	no
172.16.1.254	00:04:ED:CA:05:7E	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	<b>Yes</b> indicates that the IP address is assigned and referenced from the fixed MAC address in the DHCP server setting. <b>No</b> indicates that the IP address is not referred.

## 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.

Click **Status**→ **Routing Table** in the Menu bar to open routing table screen.

**FIGURE 30 ROUTING TABLE SCREEN**

Routing Table			
Routing Table			
Destination	Subnet Mask	Gateway/Interface	Cost
192.168.1.0	255.255.255.0	0.0.0.0/LAN	0

Destination	Displays the IP address of the destination network.
Subnet Mask	Displays the destination subnet mask 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.

## Session table

The NAT Session Table displays a list of current sessions for both incoming and outgoing traffic with protocol type, source IP, source port, destination IP and destination port, each page shows 10 sessions.

Click **Status**→ **Session Table** in the Menu bar to open Session Table screen.

**FIGURE 31 SESSION TABLE SCREEN**

Session Table					
Session Table					
No.	Protocol	Src. IP	Src. Port	Dest. IP	Dest. Port
1	TCP	192.168.1.35	3325	192.168.1.254	443
Session 1 - 1 of 1, 1/1.					
Filter	Src. IP	Src. Port	Dest. IP	Dest. Port	
First	Prev	Next	Last	Jump to session	GO

No	Displays the IP address of the destination network.
Protocol	Displays the destination subnet mask address.
Src.IP	Displays the IP address of the gateway or existing interface that this route uses.
Src.Port	Displays the number of hops counted as the cost of the route.
Dest.IP	Displays the IP address of the destination network.
Dest.Port	Displays the destination subnet mask address.

Table controls	<p><b>Filter:</b> when the presented field is filled, please click Filter button.</p> <p><b>Src.IP:</b> please input the source IP you would like to filter.</p> <p><b>Src.Port:</b> please input the source port you would like to filter.</p> <p><b>Dest.IP:</b> please input the destination IP you would like to filter.</p> <p><b>Dest.Port:</b> please input the destination port you would like to filter.</p> <p><b>First:</b> To the first page.</p> <p><b>Previous:</b> To the previous page.</p> <p><b>Next:</b> To the next page.</p> <p><b>Last:</b> To the last page.</p> <p><b>Jump to the session:</b> please input the session number you would like to see and press the <b>GO</b> button.</p>
----------------	--

## DHCP table

The DHCP Table lists the DHCP lease information for all IP addresses assigned by the DHCP server in the device.

Click **Status**→ **DHCP Table** in the Menu bar to open DHCP table screen.

**FIGURE 32 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.

## IPSec Status

The IPSec Table provides administrators with detailed information regarding the configured IPSec Connections.

Click **Status**→ **IPsec Status** in the Menu bar to open IPsec Status screen.

**FIGURE 33 IPSEC TABLE SCREEN**

IPSec Status							
IPSec Tunnels							
Name	Enable	Status	Local Network	Remote Network	Remote Gateway	SA	Action

Name	Displays the name of the IPSec Tunnel.
Enable	Displays whether this tunnel is enabled (tick) or disabled (cross).
Status	Shows if the device is ready (active) or not ready (inactive) to establish connection.
Local Network	Displays the local network IP address.

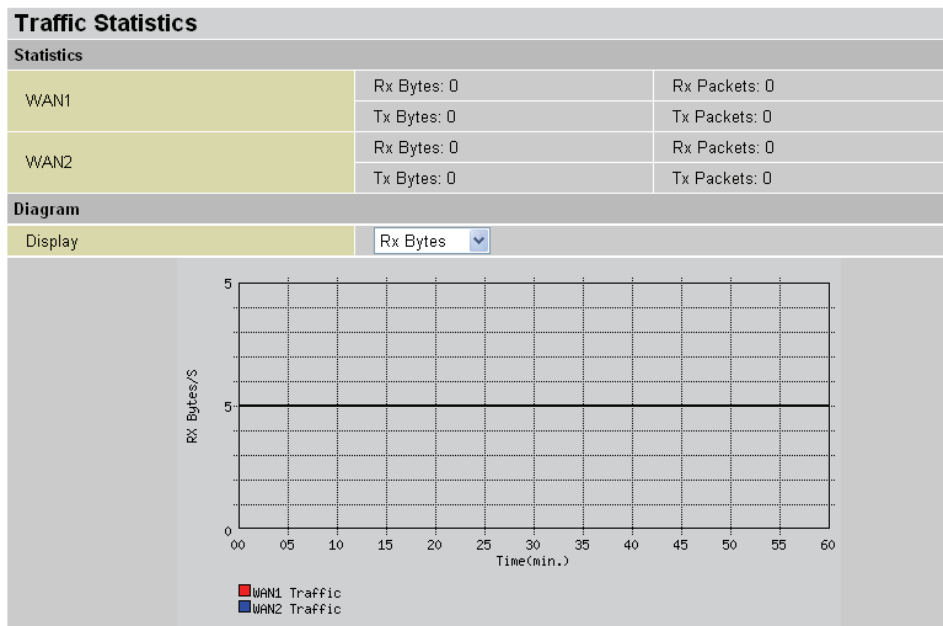


Remote Network	Displays the remote network IP address.
Remote Gateway	Displays the remote gateway IP address.
SA	Shows the connection status of the IPsec tunnel when it is establishing connection.
Action	There are two buttons available; <b>Drop</b> button and the <b>Connect</b> button. Clicking on the <b>Drop</b> button allows the disconnection of the IPsec tunnel. Clicking on the <b>Connect</b> button allows the connection of the IPsec tunnel.

### Traffic Statistics

The Traffic Statistics window displays both sent and received data (in Bytes/sec) over one hour duration. The line in red represents WAN1, whereas the line in blue represents WAN2.

FIGURE 34 TRAFFIC STATISTICS SCREEN



WAN1	Transmitted (Tx) and Received (Rx) bytes and packets for WAN1.
WAN2	Transmitted (Tx) and Received (Rx) bytes and packets for WAN2.
Display	Allows you to change the units of measurement for the traffic graph.

### System Log

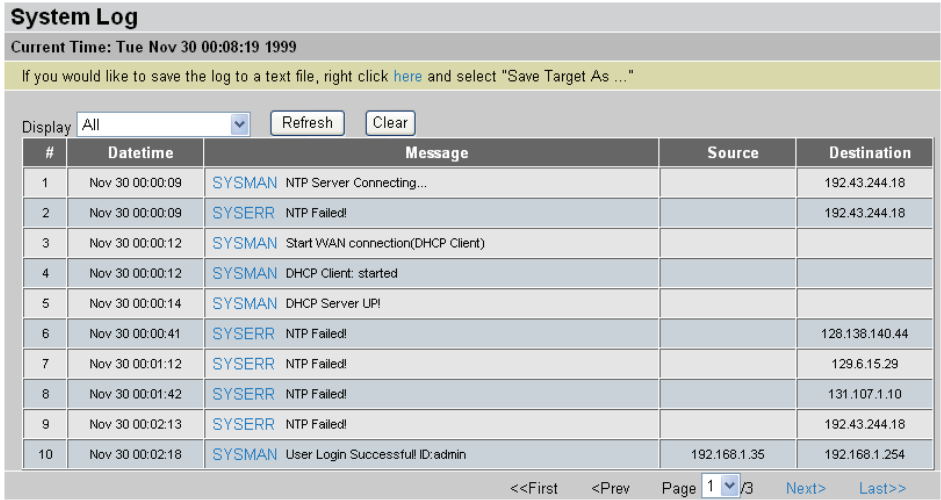
The System Log dialog logs system events for the BiGuard S20.

Click **Status**→ **System Log** in the Menu bar to open system log screen.



**NOTE:** You can modify parameters for the information that is saved to the log. See [Log and E-mail Alerts](#) on page 305.

FIGURE 35 SYSTEM LOG SCREEN



...right click [here](#)... To save the log, right click where indicated, and select “Save Target As...”

- Display

Click to open the drop-down menu. Select a log file to view. Display Options: All, System Maintenance, System Error, Access Control, Packet Filter, MAC Filter, Content Filter, Firewall, Call Data Record, PPP, SSL VPN, and IPsec.
- #

The sequence number for each log entry sorted from oldest dated entry to latest.
- Datetime

Time stamp of log.
- Message

Name of log file. Under the Display category All, an additional link specifying the type of log is listed.
- Source

Lists Incoming IP address.
- Destination

Lists Outgoing IP address
- Refresh

Click to update the system log.
- Clear

Click to clear the current log from the screen.
- First/Prev/Page/  
Next/Last

Click to navigate between screens.

## Configuring the BiGuard S20

This section explains how to configure router settings including the LAN, WAN, DMZ. Also show you how to create network objects such as addresses, services, address and service groups, schedules, bandwidth control items, and content blocking scenarios. You can set up security policies which include 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, static ARP, enabling DDNS and SNMP, configuring the firewall, Proxy and L2TP, 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**, **Alias IP** and **DHCP Server**.

##### CONFIGURING THE ETHERNET

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

FIGURE 36 LAN SCREEN

Ethernet

Parameters

IP Address	192.168.1.254
Subnet Mask	255.255.255.0
RIP	Disabled
LAN IP Subnet Sync	<input checked="" type="checkbox"/> Auto Configure the IP Range of Network Extender

Apply

Cancel

IP Address	Enter the preferred IP address. (default 192.168.1.254)
Subnet Mask	Enter the preferred subnet mask.
RIP	Click the RIP drop-down menu to enable Routing Information Protocol (RIP). The options are: Disabled; RIPv1; RIPv2; RIPv1 + RIPv2; RIPv2 Multicast; and RIPv1 + RIPv2 Multicast.
LAN IP Subnet Sync	Check the check box if you want the device to automatically configure the IP range of the Network Extender configuration according to LAN IP subnet (this saves you the worry of manually changing the IP address of Network Extender, everytime you have a IP change).

**CONFIGURING THE ALIAS IP**

The Alias IP Screen lists any IP alias presently configured.

**FIGURE 37** ALIAS IP SCREEN

Alias IP		
Alias IP List		
Name	IP Address	Subnet Mask
<a href="#">Create</a>		

Click **Create** to display LAN Alias IP Create screen.

---

---

IName	Enter the given Name.
IP Address	Enter the given IP address.
Subnet Mask	Enter the subnet mask.

---

---

**CONFIGURING DHCP SERVER SETTINGS**

The BiGuard S20 enables to act as a DHCP server for your network. Disable this function if the stations that connect to the BiGuard S20 LAN ports use static IP addresses.

**FIGURE 38** DHCP STATUS SCREEN

DHCP Server

Configuration

DHCP Server Mode

☐ Disable

☒ DHCP Server

☐ DHCP Relay Agent

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 <b>Disable</b> if IP addresses are assigned manually to stations on your network. Choose <b>DHCP Server</b> to have the BiGuard S20 assign IP addresses automatically to stations on your network. Choose <b>DHCP Relay Agent</b> 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 displayed only. To change these settings, click **Next**.

**DISABLING DHCP SERVER**

1.

From the DHCP Server Configuration screen, click the **Disable** radio button.
2.

Click **Next** to display the confirmation screen.

**FIGURE 39** DHCP DISABLE SERVER AND RELAY AGENT

DHCP

Disable server and relay agent

The DHCP server and relay agent will be disabled.

Apply

Cancel

3.

Click **Apply** to disable the DHCP server and relay agent. Disable this function if the stations that connect to the BiGuard S20 LAN ports use static IP addresses.

**CONFIGURING DHCP SERVER PARAMETERS**

This section describes how to configure DHCP server parameters. Follow these instructions.

1. Choose **DHCP Server** from DHCP Server Mode and click **Next**.
2. Complete the blanks in the following screen.

**FIGURE 40 DHCP SERVER PARAMETERS SCREEN**

DHCP Server		
Parameters		
Domain Name	SSLVPN.gateway	
Use Router as DNS Server	<input checked="" type="checkbox"/>	
Primary DNS Server Address	192.168.1.254	
Secondary DNS Server Address		
Default Lease Time	43200	seconds
Maximum Lease Time	86400	seconds
Range Start	192.168.1.100	
Range End	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"/>		

Domain Name	Enter a given domain name. If you are using the BiGuard S20 to replace another device and do not want to change the original networking environment, enter original domain name for the previous device.
Use Router as DNS Server	When this checkbox is selected, the DNS address that you type in the <b>Primary DNS Server Address</b> field is assigned to stations on the LAN. This makes the DHCP client on the LAN use our device as DNS proxy.
Primary DNS Server Address	Enter the primary DNS address you would like to assign to the DHCP client on the LAN. This allows user to use external DNS server provided by ISP or on intranet directly.
Secondary DNS Server Address	Enter the secondary DNS address you would like to assign to the DHCP client on the LAN. This allows user to use external DNS server provided by ISP or on intranet directly.
Default Lease Time	Enter 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	Enter 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	Enter the start IP address that the BiGuard S20 assigns to stations on the LAN.
Range End	Enter the end IP address that the BiGuard S20 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 56.

- To add a specific fixed MAC Address Mapping to a fixed Address, click **Add**.

Specify fixed MAC Address Mapping to fixed IP Address (optional)		
Host Name	MAC Address	IP Address
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

The following screen appears.

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

- Fill in the **Host Name**, **MAC Address** and **IP Address** fields.
- In the **MAC Address** field, you can click **Candidates** to add the accounts by checking the selected MAC address. Check the check box you want to select and click **Submit**.

Active PC in LAN	
MAC Address	IP Address
<input type="radio"/> 00:05:5D:04:47:73	192.168.1.35

- The new Entry is listed.

Specify fixed MAC Address Mapping to fixed IP Address (optional)			<input type="button" value="Add"/>
Host Name	MAC Address	IP Address	
HOST A	00:05:5D:04:47:71	192.168.1.33	<input type="button" value="Delete"/>
HOAT B	00:05:5D:04:47:72	192.168.1.34	<input type="button" value="Delete"/>
HOST1	00:05:5D:04:47:73	192.168.1.35	<input type="button" value="Delete"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- To delete the MAC Address from the table, click **Delete** next to the item you want to remove.

Specify fixed MAC Address Mapping to fixed IP Address (optional)			<input type="button" value="Add"/>
Host Name	MAC Address	IP Address	
HOST A	00:05:5D:04:47:71	192.168.1.33	<input type="button" value="Delete"/>
HOAT B	00:05:5D:04:47:72	192.168.1.34	<input type="button" value="Delete"/>
HOST1	00:05:5D:04:47:73	192.168.1.35	<input type="button" value="Delete"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

The Delete screen appears.

Fixed Host Entry	
Host Name	HOST1
MAC Address	00:05:5D:04:47:73
IP Address	192.168.1.35
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Click **Apply** to remove this MAC Address.

Specify fixed MAC Address Mapping to fixed IP Address (optional)			Add ➤
Host Name	MAC Address	IP Address	
HOST A	00:05:5D:04:47:71	192.168.1.33	Delete ➤
HOAT B	00:05:5D:04:47:72	192.168.1.34	Delete ➤
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- Click **Apply** to set the settings and you will be returned to the DHCP Server page.

### **CONFIGURING THE DHCP RELAY AGENT**

Choose **DHCP Relay Agent** if you want to place DHCP servers and clients on different networks.

- From the DHCP Server Configuration screen, click the **DHCP Relay Agent** radio button.
- Click **Next** to display the Parameters screen.

**FIGURE 41** DHCP RELAY PARAMETERS SCREEN

DHCP Relay	
Parameters	
DHCP Relay Agent	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Enter the address of the relay agent in the field above.
- Click **Apply** to save settings.



## Configuring WAN settings

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



WAN refers to your Wide Area Network connection. In most cases, this means the connection of your router is connected on the internet through your ISP.

Click **WAN** in the Interface menu to display the WAN Settings screen. Configure WAN ISP and Bandwidth settings and display any WAN Alias IP addresses using the WAN menu.



**NOTE:** The BiGuard S20 features Dual WAN capability, WAN1 and WAN2. The configuration steps are identical but in the following examples, the WAN1 connection is used.

**FIGURE 42** WAN SETTINGS SCREEN

WAN Settings		
WAN Service Table		
Name	Description	
WAN1	DHCP Client	Edit 
WAN2	DHCP Client	Edit 

### ISP SETTINGS

The WAN Service Table displays the different WAN connections that are configured on BiGuard S20.

Define how your router will connect to the Internet using the **Protocol** drop-down menu. Selections include PPPoE, Static IP, or automatically obtain an IP address by using DHCP (default). If your ISP does not use DHCP, select the correct connection method and configure the connection accordingly. Configurable items will vary depending on the connection method selected.

1. Migrate to the **Configuration** → **Interface** → **WAN** menu.
2. In the WAN Settings screen, click **Edit** in the **WAN1** field.  
The WAN1 Settings screen is displayed.
3. Select and configure the type of ISP setting to use.

DHCP

If your ISP requires IP address for your WAN connection by using DHCP protocol, please select **Obtain an IP address Automatically** from the **Protocol** drop-down menu.

FIGURE 43 WAN SETTINGS DHCP SCREEN

WAN1 Settings

Obtain an IP Address Automatically (DHCP Client)

Protocol

Obtain an IP Address Automatically

Host Name

Mode

☒ NAT

☐ Router

MAC Address

☒ Default MAC Address

☐ Specify a MAC Address (MAC Clone)

00:00:00:00:00:00

Candidates

DNS

☒ Obtain DNS Automatically

Primary DNS

Secondary DNS

RIP

Disable

MTU

1492

Apply

Cancel

Return

Protocol	Displays the current protocol. Click the drop-down arrow to change the protocol.
Mode	<p>There are two modes for the connection: NAT (Network Address Translation) and Router.</p> <p>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 <b>NAT</b> to add an extra layer of security when user on the internal network need to access the Internet. Select <b>Router</b> for an internal network.</p>
MAC Address	If your ISP requires you to input a WAN Ethernet MAC, check the <b>Specify a MAC Address (MAC Clone)</b> radio button and fill in your MAC address in the supplied field. Otherwise, click <b>Default MAC Address</b> .
DNS	If your ISP requires you to manually input DNS settings, uncheck the <b>Obtain DNS Automatically</b> box and enter your primary and secondary DNS.
RIP	To activate RIP, select the required version from the drop-down menu. To disable RIP, select Disable from the drop-down menu.
MTU	Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save the changes or **Cancel** to return to the WAN Settings screen.

## PPPoE

To connect to your ISP by using PPPoE, select **PPPoE** from the **Protocol** drop-down menu and type in the required settings.

**FIGURE 44 WAN SETTINGS PPPoE SCREEN**

WAN1 Settings	
<b>PPPoE</b>	
Protocol	PPPoE
Mode	<input checked="" type="radio"/> NAT <input type="radio"/> Router
User Name	
Password	
Retype Password	
Service Name	
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
	Secondary DNS
RIP	Disable
MTU	1492
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Return"/>	

Protocol	Displays the current protocol. Click the drop-down arrow to change the protocol.
Mode	Select <b>NAT</b> or <b>Router</b> by checking the check box.
Username	Enter your user name.
Password	Enter your password.
Retype Password	Retype your password.
Service Name	TCP/IP service name configuration parameter.
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	<p>Select either Auto, Pap or Chap for the authentication protocol.</p> <p><b>Auto:</b> automatically configures the access protocol. This is the default option.</p> <p><b>CHAP:</b> (Challenge Handshake Authentication Protocol) select this access protocol for dialing into a network that provides a moderate degree of security.</p> <p><b>PAP:</b> (Password Authentication Protocol) select this access protocol for dialing into a network that provides only basic functionality.</p>

---

Connection	<p>Select either the connection should be <b>Always On</b> or <b>Connect on Demand</b>. If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP, select <b>Always On</b>. If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet), select <b>Connect on Demand</b>. When you select <b>Connect on Demand</b>, the following field <b>Idle Timeout</b> is available.</p> <p><b>Note:</b> If your ISP charges a fee for connection time, select <b>Connect on Demand</b>.</p>
Idle Timeout	<p>This field is only available when the <b>Connection</b> field is set to <b>Connect on Demand</b>. Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Input idle time in the supplied field.</p>
DNS	<p>If your ISP requires you to manually setup DNS settings, uncheck the <b>Obtain DNS Automatically</b> check box and enter your primary and secondary DNS.</p>
RIP	<p>To activate RIP, select the required version from the drop-down menu. To disable RIP, select <b>Disable</b> from the drop-down menu.</p> <p><b>Note:</b> If you are not sure which version to choose, select <b>Disable</b>.</p>
MTU	<p>Enter the Maximum Transmission Unit (MTU) for your network. 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.</p>

---

Click **Apply** to save your changes or **Cancel** to return to the WAN Settings screen.

Static IP

To connect to your ISP by using a static IP, firstly, obtain the necessary information and settings from the ISP provider. Then enter the given settings in the fields below.

FIGURE 45 WAN SETTINGS STATIC IP SCREEN

WAN1 Settings

Static IP

Protocol

Static IP

Mode

☒ NAT
 ☐ Router

IP Address

Subnet Mask

Gateway

MAC Address

☒ Default MAC Address
   
☐ Specify a MAC Address (MAC Clone)
 

00:00:00:00:00:00

Candidates

DNS

Primary DNS

Secondary DNS

RIP

Disable

MTU

1492

Apply

Cancel

Return

Protocol	Displays the current protocol. Click the drop-down arrow to change the protocol.
Mode	Select <b>NAT</b> or <b>Router</b> by checking the check box.
IP Address	Enter the static IP assigned by your ISP.
Subnet Mask	Enter the IP subnet mask provided by your ISP.
Gateway	Enter the ISP gateway address provided by your ISP.
MAC Address	If your ISP requires you to input a WAN Ethernet MAC, check the <b>Specify a MAC Address (MAC Clone)</b> radio button and fill in your MAC address in the supplied field. Otherwise, click <b>Default MAC Address</b> .
DNS	Enter the primary and secondary DNS provided by your ISP.
RIP	To activate RIP, select the required version from the drop-down menu. To disable RIP, select <b>Disable</b> from the drop-down menu.
	<b>Note:</b> If you are not sure which version to choose, select <b>Disable</b> .
MTU	Enter the Maximum Transmission Unit (MTU) for your network. 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.

Click **Apply** to save the changes or **Cancel** to return to the WAN Settings screen.

**BANDWIDTH SETTINGS**

Under Bandwidth Settings, you can easily configure both inbound and outbound bandwidth for each WAN port.

**FIGURE 46 BANDWIDTH SETTINGS SCREEN**

Bandwidth Settings		
Max Bandwidth Provided by ISP		
WAN1 Outbound Bandwidth	<input type="text" value="102400"/>	Kbps
WAN1 Inbound Bandwidth	<input type="text" value="102400"/>	Kbps
WAN2 Outbound Bandwidth	<input type="text" value="102400"/>	Kbps
WAN2 Inbound Bandwidth	<input type="text" value="102400"/>	Kbps

---

WAN1 Outbound Bandwidth    Enter your ISP outbound bandwidth for WAN1.

WAN1 Inbound Bandwidth    Enter your ISP inbound bandwidth for WAN1.

WAN2 Outbound Bandwidth    Enter your ISP outbound bandwidth for WAN2.

WAN2 Inbound Bandwidth    Enter your ISP inbound bandwidth for WAN2.

---



**NOTE:** The values entered here are referred by both QoS and Load Balancing functions.

### WAN ALIAS IP

The Alias IP screen lists any IP alias presently configured.

**FIGURE 47** WAN ALIAS IP SCREEN

WAN Alias IP

Alias IP List

Name	IP Address	Interface
------	------------	-----------

Create

Click **Create** to display the WAN Alias IP Create screen.

WAN Alias IP

Create

Name	
IP Address	0.0.0.0
Interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2

Apply

Cancel

Name	Enter alias name.
IP Address	Enter the IP address of the alias.
Interface	Select the required WAN interface.

Click **Apply** to confirm the settings.

### Dual WAN

In this section, you can setup the fail over or load balance function, outbound load balance or inbound load balance function, or setup specific protocol to bind with specific WAN port. In this menu, there are the following sections: General Settings, Outbound Load Balance, and Protocol Binding.

#### GENERAL SETTINGS

Clicking the **General Settings** tab displays the following options.

**FIGURE 48** GENERAL SETTING SCREEN

General Setting

Dual WAN Mode

Mode

☐ Load Balance

☒ Fail Over

WAN Port Service Detection Policy

Service Detection  
(for load balance.)

☐ Enable

☐ Disable

Connectivity Decision

Not in service when probing failed after 

3

 consecutive times.

Probe Cycle

Every 

30

 seconds.

Probe WAN1

☒ Gateway

☐ Host

0.0.0.0

Probe WAN2

☒ Gateway

☐ Host

0.0.0.0

Failback to WAN1 when possible  
(for failover.)

☒ Enable

☐ Disable

Apply

Mode	You can select <b>Load Balance</b> or <b>Fail Over</b> .
Service Detection	Enable as you would like to detect if WAN is alive or dead by probing the gateway address or the specified IP address. For failover mode, this function is always enabled.
Connectivity Decision	Establishes the number of times probing the connection has to fail before the connection is judged as failed.
Probe Cycle	Enter the number of seconds between each probe.
Probe WAN1	Determine whether the target of the probing is the default gateway or the user specified IP address.
Probe WAN2	Determine whether the target of the probing is the default gateway or the user specified IP address.
Fail back to WAN1 when possible	If it is enabled, the device will keep trying to failback to WAN1 whenever WAN2 is active. This will make WAN1 as a preferred link so that it use it whenever possible. This only applies to failover mode.

Click **Apply** to save your changes.





Balance by weight of link capacity	Use an IP hash to balance traffic based on weight of link bandwidth capacity.
Balance by weight	Use an IP hash to balance traffic based on a ratio. Enter the desired ratio into the fields provided.

Click **Apply** to save your changes.

### **PROTOCOL BINDING**

Protocol Binding lets you direct specific traffic to go out from a specific WAN port. Clicking **Protocol Binding** displays the following screen.

**FIGURE 50** PROTOCOL BINDING SCREEN

Protocol Binding							
Protocol Binding Table							
No.	Interface	Src. IP	Src. Netmask	Dest. IP	Dest. Netmask	Protocol	Port Range
Create ➤							

Policies determine how specific types of internet traffic are routed, for example, traffic from a particular IP range granted access to only one WAN port rather than using both of the WAN ports as with load balancing.



**NOTE:** Protocol Binding entries take precedence over the settings already configured in the Load Balance Setting section.

1. Click on the **Create** button to create a new policy entry. The Add Protocol Binding Rules screen is displayed.

Protocol Binding	
Add Protocol Binding Rules	
Interface	WAN1 ▼
Source IP Range	<input checked="" type="radio"/> All Source IP <input type="radio"/> Specified Source IP
Source IP Address	0.0.0.0
Source IP Netmask	0.0.0.0
Destination IP Range	<input checked="" type="radio"/> All Destination IP <input type="radio"/> Specified Destination IP
Destination IP Address	0.0.0.0
Destination IP Netmask	0.0.0.0
Packet Type	Any ▼
Port Range	1 ~ 65535
Apply	

Interface	Select which WAN port to use, WAN1 or WAN2.
Source IP Range	<b>All Source IP:</b> Click to specify all source IPs. <b>Specified Source IP:</b> Click to specify a specific source IP address and source IP netmask.

---

Source IP Address	If Specified Source IP was chosen, enter IP address.
Source IP Netmask	If Specified Source IP was chosen, enter subnet mask.
Destination IP Range	<b>All Destination IP:</b> Click to specify all destination IPs. <b>Specified Destination IP:</b> Click to specify a specific destination IP address and destination IP netmask.
Destination IP Address	If Specified Destination IP was chosen, enter IP address.
Destination IP Netmask	If Specified Destination IP was chosen, enter subnet mask.
Packet Type	The particular protocol of Internet traffic for the specified policy. Choose from TCP, UDP, or Any.
Port Range	The range of ports for the specified policy (if only one port is required, enter the same value in both boxes).

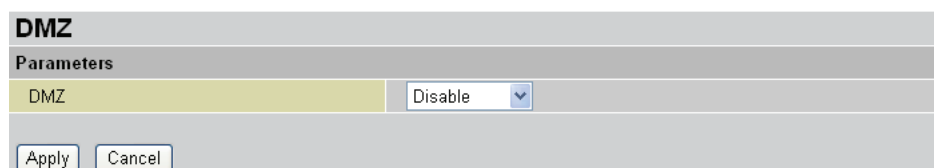
---

2. Click **Apply** to save your changes.

## Configuring the DMZ

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

**FIGURE 51** ENABLING THE DMZ



DMZ	
Parameters	
DMZ	Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

When the DMZ is enabled, the DMZ LED is lit, indicating that the LAN port 8 is set as the DMZ port.

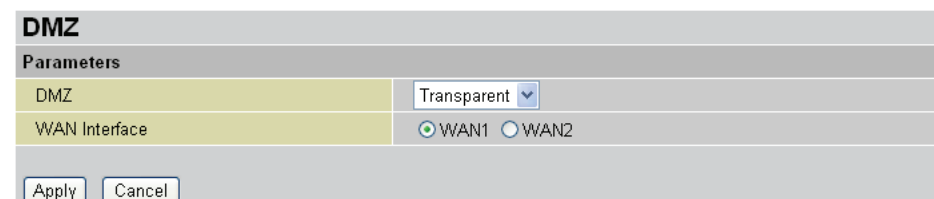
The DMZ is a section of the network that is located between an organization's trusted internal network and an untrusted external network such as the Internet. The DMZ is a subnet that is located between firewalls or off one leg of a firewall.

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

When set to **Transparent** or **NAT** mode, the DMZ LED on the front panel is lit. The DMZ uses LAN Port 8 when enabled.

In **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.

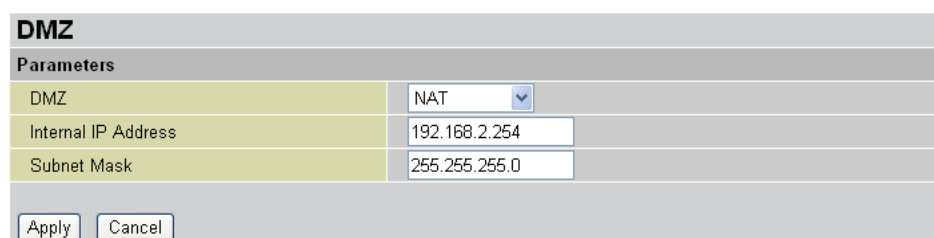
**FIGURE 52** DMZ TRANSPARENT MODE



DMZ	
Parameters	
DMZ	Transparent
WAN Interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

In **NAT** mode, it goes through subnet from virtual server.

**FIGURE 53** DMZ NAT MODE



DMZ	
Parameters	
DMZ	NAT
Internal IP Address	192.168.2.254
Subnet Mask	255.255.255.0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

## Multiple NAT/Subnet

Click the **Multiple NAT/Subnet** menu to display the parameters screen.

**FIGURE 54** MULTIPLE NAT/SUBNET TABLE

Multiple NAT/Subnet			
Parameters			
Name	IP Address	Subnet Mask	WAN IP
Default LAN	192.168.1.254	255.255.255.0	ANY

This table shows the administrator the current multiple NAT or Subnets that exists on the router.

Name	Displays the name of the multiple NAT/Subnet.
IP Address	Displays the IP address.
Subnet Mask	Displays the subnet mask associated with the IP address.
WAN IP	Displays the WAN IP associated with the multiple NAT/Subnet.

## 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 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, 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 table:

**FIGURE 55** CONFIGURING NETWORK OBJECT ADDRESSES

Address		
Address Table		
Name	IP Address	Subnet Mask/Range
**Any	All IP Addresses	
**Default WAN1 IP	WAN1 IP Address	
**Default WAN2 IP	WAN2 IP Address	
Create		

### CREATING IP ADDRESS NETWORK OBJECTS

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

**FIGURE 56** ADDING ADDRESSES TO THE ADDRESS TABLE

Address	
Create	
Name	<input type="text"/>
Type	IP Address
IP Address	<input type="text"/> Candidates
<div>ApplyCancel</div>	

Name	Enter 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"><li>• IP Address</li><li>• IP Address / Subnet Mask</li><li>• IP Address Range</li></ul>
IP Address	Enter the IP address or click <b>Candidates</b> where display a list of active PCs on the LAN select the computer you want.
Subnet Mask	When <b>IP Address / Subnet Mask</b> is selected from the drop-down menu, this field is displayed. Enter the subnet mask associated with the IP address.

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.

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

**FIGURE 57** CONFIRMED ADDRESSES IN THE ADDRESS TABLE

Address				
Address Table				
Name	IP Address	Subnet Mask/Range		
**Any	All IP Addresses			
**Default WAN1 IP	WAN1 IP Address			
**Default WAN2 IP	WAN2 IP Address			
test	123.123.123.123		Edit ▶	Delete ▶
Create ▶				

### EDITING IP ADDRESS NETWORK OBJECTS

Refer to the following to edit an IP address Network Object:

1. In the Address menu, click **Edit** next to the item you want to change.

Address				
Address Table				
Name	IP Address	Subnet Mask/Range		
**Any	All IP Addresses			
**Default WAN1 IP	WAN1 IP Address			
**Default WAN2 IP	WAN2 IP Address			
test	123.123.123.123		Edit ▶	Delete ▶
Create ▶				

The following screen appears showing the item's properties.

Address	
Edit	
Name	test
Type	IP Address ▼
IP Address	123.123.123.123 Candidates ▶
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Select the type from the drop-down menu.

Address	
Edit	
Name	test
Type	IP Address ▼
IP Address	IP Address IP Address / Subnet Mask IP Address Range
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3. Type the IP address and subnet mask.

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

Address	
Edit	
Name	test
Type	IP Address / Subnet Mask
IP Address	123.123.123.123 <a href="#">Candidates</a>
Subnet Mask	255.255.255.0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

### DELETING IP ADDRESS NETWORK OBJECTS

Refer to the following to delete an IP address Network Object:

- In the Address menu, click **Delete** next to the item you want to remove.

Address				
Address Table				
Name	IP Address	Subnet Mask/Range		
**Any	All IP Addresses			
**Default WAN1 IP	WAN1 IP Address			
**Default WAN2 IP	WAN2 IP Address			
test	123.123.123.123	255.255.255.0	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>				

The Delete screen appears.

Address	
Delete	
Name	test
Type	IP Address / Netmask
IP Address	123.123.123.123
Subnet Mask	255.255.255.0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Click **Apply** to remove this IP address from the Address Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.



Creating Address Groups Network Objects

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

FIGURE 58 ADDRESS GROUP LIST

Address Group

Address Group Table

Group Name	Address	
------------	---------	--

Create

CREATING AN ADDRESS GROUP NETWORK OBJECT

Refer to the following to create an Address Group Network Object:

1. Click **Create** to create a new Address Group.

Address Group

Create

Address Group Name

Available Addresses

\*\*Default WAN1 IP

\*\*Default WAN2 IP

Add>>

<<Delete

Selected Addresses

Apply

Cancel

Address Group Name	Enter a given name in <b>Address Group Name</b> field.
Available Addresses	Displays the list of IP addresses which you can add to this group. Select the addresses you want to add and click <b>Add</b> .
Selected Addresses	Displays the list of IP addresses in this group. To delete addresses from this list, select the addresses and click <b>Delete</b> .

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

**Address Group**

Create

Address Group Name S20

Available Addresses

- \*\*Default WAN1 IP
- \*\*Default WAN2 IP

Add>>

<<Delete

Selected Addresses

- \*\*Default WAN1 IP

Apply Cancel

### **EDITING ADDRESS GROUP NETWORK OBJECTS**

Refer to the following to edit an Address Group Network Object:

1. In the Address Group menu, click **Edit** next to the item you want to change.

**Address Group**

Address Group Table

Group Name	Address		
S20	**Default WAN1 IP	Edit ▶	Delete ▶

Create ▶

The following screen appears showing the item's properties.

**Address Group**

Edit

Address Group Name S20

Available Addresses

- \*\*Default WAN1 IP
- \*\*Default WAN2 IP

Add>>

<<Delete

Selected Addresses

- \*\*Default WAN1 IP

Apply Cancel

2. Add or delete addresses from the Available Addresses/Selected Addresses columns.
3. Click **Apply** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

**DELETING ADDRESS GROUP NETWORK OBJECTS**

Refer to the following to delete an Address Group Network Object:

1. In the Address Group menu, click **Delete** next to the item you want to remove.

Address Group			
Address Group Table			
Group Name	Address		
S20	**Default WAN1 IP	Edit ➤	Delete ➤
Create ➤			

The Delete screen appears.

Address Group	
Delete	
Address Group Name	S20
Selected Addresses	
<div>**Default WAN1 IP</div>	
<div>Delete Cancel</div>	

2. Click **Delete** to remove this Address Group from the Address Group Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

Allowing Services

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

FIGURE 59 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.

CREATING USER-DEFINED SERVICES

Refer to the following to add a user-defined service at the Service Table:

1. Click **Create** to add a user-defined service.

FIGURE 60 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"/>
Apply <input type="button" value="Cancel"/>	

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

---

**Service Port End** Enter the port number or protocol ID that defines the end of the port range that this service is allowed to use. This option is available when the Type is TCP or UDP.

---

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

### EDITING USER-DEFINED SERVICES

Refer to the following to edit a User-defined Service Network Object:

1. In the Service menu, click **Edit** next to the item you want to change.

User-defined Service Table				
Name	Type	Port/protocol ID		
test	TCP	80~140	Edit	Delete
Create				

The following screen appears showing the item's properties.

Service	
Edit	
Name	test
Type	TCP
Service Port Start	80
Service Port End	140
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Select the type from the drop-down menu.

Service	
Edit	
Name	test
Type	TCP
Service Port Start	
Service Port End	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3. Type the service port start and end numbers.

Service	
Edit	
Name	test
Type	TCP
Service Port Start	22
Service Port End	23
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

**DELETING USER-DEFINED SERVICES**

Refer to the following to delete a User-defined Service Network Object:

1. In the Service menu, click **Delete** next to the item you want to remove.

User-defined Service Table				
Name	Type	Port/protocol ID		
test	TCP	22~23	Edit ▶	Delete ▶
Create ▶				

The Delete screen appears.

Service	
Delete	
Name	test
Type	TCP
Service Port Start	22
Service Port End	23
Delete Cancel	

2. Click **Delete** to remove this service from the User-defined Service table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

**Creating Service Group Network Objects**

Click **Service Group**, the Service Group screen appears.

**FIGURE 61 THE SERVICE GROUP TABLE**

Service Group

Service Group Table

Group Name	Service	
------------	---------	--

Create

**CREATING SERVICE GROUP NETWORK OBJECTS**

Refer to the following to create a Service Group Network Object:

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

Service Group

Create

Service Group Name

Available Services

\*\*HTTP

\*\*DNS-TCP

\*\*DNS

\*\*FTP

\*\*Telnet

\*\*SMTP

\*\*POP3

\*\*NEWS

\*\*RealAudio

\*\*Ping

\*\*H.323

\*\*T.120

Add>>

<<Delete

Selected Services

Apply

Cancel

Service Group Name	Enter the name that you want this service group to have.
Available Services	Displays the list of available services which you can add to this group. Select the services you want and click <b>Add</b> .
Selected Services	Displays the list of selected services in this group. To delete services from the list, select the service and click <b>Delete</b> .

2. Enter the name of the service.
3. Choose a service from the Available Services list, and click **Add**.
4. Click **Apply** to set the settings.

**EDITING SERVICE GROUP NETWORK OBJECTS**

Refer to the following to edit a Service Group Network Object:

1. In the Service Group menu, click **Edit** next to the item you want to change.

Service Group			
Service Group Table			
Group Name	Service		
Service Group Test	**HTTP	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>			

The following screen appears showing the item's properties.

Service Group		
Edit		
Service Group Name	Service Group Test	
<b>Available Services</b> <div> <div>**HTTP</div> <div>**DNS-TCP</div> <div>**DNS</div> <div>**FTP</div> <div>**Telnet</div> <div>**SMTP</div> <div>**POP3</div> <div>**NEWS</div> <div>**RealAudio</div> <div>**Ping</div> <div>**H.323</div> <div>**T.120</div> </div>	<div>Add&gt;&gt;</div> <div>&lt;&lt;Delete</div>	<b>Selected Services</b> <div>**HTTP</div>
<div> <div>Apply</div> <div>Cancel</div> </div>		

2. Add or delete services from the Available Services and Selected Services columns.

Service Group		
Edit		
Service Group Name	Service Group Test	
<b>Available Services</b> <div> <div>**HTTP</div> <div>**DNS-TCP</div> <div>**DNS</div> <div>**FTP</div> <div>**Telnet</div> <div>**SMTP</div> <div>**POP3</div> <div>**NEWS</div> <div>**RealAudio</div> <div>**Ping</div> <div>**H.323</div> <div>**T.120</div> </div>	<div>Add&gt;&gt;</div> <div>&lt;&lt;Delete</div>	<b>Selected Services</b> <div>**HTTP</div> <div>**Telnet</div>
<div> <div>Apply</div> <div>Cancel</div> </div>		

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



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.



**DELETING SERVICE GROUP NETWORK OBJECTS**

Refer to the following to delete a Service Group Network Object:

1. In the Service Group menu, click **Delete** next to the item you want to remove.

Service Group			
Service Group Table			
Group Name	Service		
Service Group Test	**HTTP , ...	Edit ▶	Delete ▶
Create ▶			

The Delete screen appears.

Service Group	
Delete	
Service Group Name	Service Group Test
Selected Services	
<div> <div>**HTTP</div> <div>**Telnet</div> </div>	
<div> <div>Delete</div> <div>Cancel</div> </div>	

2. Click **Delete** to remove this service group from the Service Group Table.




**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

Scheduling BiGuard S20 operation

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

FIGURE 62 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.

CREATING A SCHEDULE NETWORK OBJECT

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

FIGURE 63 ADDING A SCHEDULE NETWORK OBJECT PROFILE

Schedule

Create

Name

Day

☐ Sun. ☐ Mon. ☐ Tue. ☐ Wed. ☐ Thu. ☐ Fri. ☐ Sat.

Start Time

08 : 00

End Time

18 : 00

Apply

Cancel

Name	Enter the given 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.

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

Schedule

Create

Name

Schedule

Day

☐ Sun. ☒ Mon. ☒ Tue. ☐ Wed. ☐ Thu. ☐ Fri. ☐ Sat.

Start Time

08 : 00

End Time

16 : 00

Apply

Cancel

## EDITING SCHEDULE NETWORK OBJECTS

Refer to the following to edit a Schedule Network Object:

1. In the Schedule menu, click **Edit** next to the item you want to change.

Schedule				
Schedule Table				
Name	Day in a week	Time		
**Always On	Sun. Mon. Tue. Wed. Thu. Fri. Sat.	From 00:00 To 24:00		
Schedule	Mon. Tue.	From 08:00 To 16:00	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>				

The following screen appears showing the item's properties.

Schedule	
Edit	
Name	Schedule
Day	<input type="checkbox"/> Sun. <input checked="" type="checkbox"/> Mon. <input checked="" 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	16 : 00
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Change the schedule as desired.
3. Click **Apply** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

## DELETING SCHEDULE NETWORK OBJECTS

Refer to the following to delete a Schedule Network Object:

1. In the Schedule menu, click **Delete** next to the item you want to remove.

Schedule				
Schedule Table				
Name	Day in a week	Time		
**Always On	Sun. Mon. Tue. Wed. Thu. Fri. Sat.	From 00:00 To 24:00		
Schedule	Mon. Tue.	From 08:00 To 16:00	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>				

The Delete screen appears.

Schedule	
Delete	
Name	Schedule
Day	<input type="checkbox"/> Sun. <input checked="" type="checkbox"/> Mon. <input checked="" 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	16 : 00
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

2. Click **Delete** to remove this schedule from the Schedule Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

## Managing Bandwidth Network Objects

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

**FIGURE 64** BANDWIDTH CONTROL TABLE

Bandwidth Control		
Bandwidth Table		
Name	Downstream	Upstream
<a href="#">Create</a>		

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

### CREATING BANDWIDTH CONTROL NETWORK OBJECTS

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

**FIGURE 65** ADDING A BANDWIDTH CONTROL NETWORK OBJECT

Bandwidth Control			
Create			
Name		<input type="text"/>	
Downstream	Guaranteed	<input type="text"/>	Kbps
	Maximum	<input type="text"/>	Kbps
Upstream	Guaranteed	<input type="text"/>	Kbps
	Maximum	<input type="text"/>	Kbps
<div><a href="#">Apply</a> <a href="#">Cancel</a></div>			

Name	Enter a given name for this bandwidth control Network Object.
Downstream	Enter values for the downstream bandwidth in the text boxes in kilobits per second. <ul style="list-style-type: none"><li>Guaranteed: type a value that defines the lower limit for downstream bandwidth.</li><li>Maximum: type a value that defines the upper limit for downstream bandwidth.</li></ul>
Upstream	Enter values for the upstream bandwidth in the text boxes in kilobits per second. <ul style="list-style-type: none"><li>Guaranteed: type a value that defines the lower limit for upstream bandwidth.</li><li>Maximum: type a value that defines the upper limit for upstream bandwidth.</li></ul>

Click **Apply** to confirm the settings.

## EDITING BANDWIDTH CONTROL NETWORK OBJECTS

Refer to the following to edit a Bandwidth Control Network Object:

1. In the Bandwidth Control menu, click **Edit** next to the item you want to change.

Bandwidth Control

Bandwidth Table

Name	Downstream	Upstream		
test	Guaranteed:12000 Maximum:12000	Guaranteed:12000 Maximum:12000	<div>Edit</div>	<div>Delete</div>
<div>Create</div>				

The following screen appears showing the item's properties.

Bandwidth Control				
Edit				
Name	test			
Downstream	Guaranteed	<input type="text" value="12000"/>	Kbps	
	Maximum	<input type="text" value="12000"/>	Kbps	
Upstream	Guaranteed	<input type="text" value="12000"/>	Kbps	
	Maximum	<input type="text" value="12000"/>	Kbps	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

2. Change the values in the screen as desired.
3. Click **Apply** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

## DELETING BANDWIDTH CONTROL NETWORK OBJECTS

Refer to the following to delete a Bandwidth Control Network Object:

1. In the Bandwidth Control menu, click **Delete** next to the item you want to remove.

Bandwidth Control

Bandwidth Table

Name	Downstream	Upstream		
test	Guaranteed:12000 Maximum:12000	Guaranteed:12000 Maximum:12000	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>				

The Delete screen appears.

Bandwidth Control				
Delete				
Name	test			
Downstream	Guaranteed	12000 Kbps		
	Maximum	12000 Kbps		
Upstream	Guaranteed	12000 Kbps		
	Maximum	12000 Kbps		
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>				

2. Click **Delete** to remove this Bandwidth Control item from the Bandwidth Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

### Setting Content Blocking parameters

Content Blocking enables you to create filters that prohibits users from accessing specified content. You can create keyword and domain filters, and restrict URL features.

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

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

FIGURE 66 KEYWORD FILTER PROFILES

Content Blocking

Keyword Filtering

Profile	Keyword
---------	---------

Create

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

#### CREATING KEYWORD FILTER NETWORK OBJECTS

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

FIGURE 67 ADDING A KEYWORD FILTER NETWORK OBJECT PROFILE

Keyword Filtering

Create

Profile	
Keyword	

Add

Block WEB URLs which contain these keywords

Keyword	
---------	--

ApplyCancel

Profile	Enter a given name of this Network Object profile.
Keyword	Enter the keyword to be filtered.

- Click **Add** to add this to the content filtering keyword list. The word is displayed under **Block WEB URLs which contain these keywords**.

Keyword Filtering

Create

Profile	violence
Keyword	

Add

Block WEB URLs which contain these keywords

Keyword	
murder	Delete

ApplyCancel

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

**EDITING KEYWORD FILTER NETWORK OBJECT**

Refer to the following to edit a Keyword Filter Network Object:

1. In the Content Blocking Keyword Filtering menu, click **Edit** next to the item you want to change.

Content Blocking			
Keyword Filtering			
Profile	Keyword		
violence	murder	Edit ▶	Delete ▶
Create ▶			

The following screen appears showing the item's properties.

Keyword Filtering	
Edit	
Profile	violence
Keyword	<input type="text"/>
Add	
Block WEB URLs which contain these keywords	
Keyword	
murder	Delete
Apply Cancel	

2. Type a keyword into the Edit section and click **Add** to add the keyword to the profile.  
The keyword is listed to the **Block WEB URLs which contain these keywords** section.
3. Click **Delete** to delete a keyword from the list.
4. Click **Apply** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

**DELETING KEYWORD FILTER NETWORK OBJECTS**

Refer to the following to delete a Keyword Filter Network Object:

1. In the Content Blocking Keyword Filtering menu, click **Delete** next to the item you want to remove.

Content Blocking			
Keyword Filtering			
Profile	Keyword		
violence	murder	Edit ▶	Delete ▶
Create ▶			

The Delete screen appears.

Keyword Filtering	
Delete	
Profile	violence
Block WEB URLs which contain these keywords	
Keywords	murder
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

2. Click **Delete** to remove this Keyword Filtering item from the Keyword Filtering Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.



**CREATING DOMAIN FILTER NETWORK OBJECTS**

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

**FIGURE 68 DOMAIN FILTER PROFILES**

Content Blocking			
Domain Filtering			
Profile	Forbidden Domain	Trust Domain	
Create			

Domain filters prohibit users from accessing specific domains (such as .ORG, .COM, or .GOV).

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

**FIGURE 69 ADDING A DOMAIN FILTER NETWORK OBJECT PROFILE**

Domain Filtering	
Create	
Profile	<input type="text"/>
Domain	<input type="text"/>
Type	Forbidden Domain
Add	
Block WEB URLs which contain these domains	
Forbidden Domain	<input type="text"/>
UnBlock WEB URLs which contain these domains	
Trusted Domain	<input type="text"/>
Apply Cancel	

Profile	Enter a given name of this profile.
Domain	Enter 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"> <li>• Forbidden Domain: users will not be allowed access to Web sites in this domain. Select this and click <b>Add</b> to add the domain to the <b>Block WEB URLs which contain these domains</b> list.</li> <li>• Trusted Domain: users will be allowed access to Web sites in this domain. Select this and click <b>Add</b> to add the domain to the <b>UnBlock WEB URLs which contain these domains</b> list.</li> </ul>

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

**EDITING DOMAIN FILTER NETWORK OBJECTS**

Refer to the following to edit a Domain Filter Network Object:

1. In the Content Blocking Domain Filtering menu, click **Edit** next to the item you want to change.

Content Blocking				
Domain Filtering				
Profile	Forbidden Domain	Trust Domain		
sex	www.sex.com	www.sexhealth.com	Edit	Delete
Create				

The following screen appears showing the item's properties.

Domain Filtering	
<b>Edit</b>	
Profile	sex
Domain	<input type="text"/>
Type	Forbidden Domain ▾
<input type="button" value="Add"/>	
<b>Block WEB URLs which contain these domains</b>	
Forbidden Domain	
www.sex.com	<input type="button" value="Delete"/>
<b>UnBlock WEB URLs which contain these domains</b>	
Trusted Domain	
www.sexhealth.com	<input type="button" value="Delete"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Add trusted or forbidden domains to the profile as desired.

The trusted and forbidden domains you add are listed in the Block and Unblock sections at the bottom of the screen.

3. To delete a domain from either list, click **Delete** next to the domain that you want to remove.
4. Click **Apply** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

### DELETING DOMAIN FILTER NETWORK OBJECTS

Refer to the following to delete a Domain Filter Network Object:

1. In the Content Blocking Domain Filtering menu, click **Delete** next to the item you want to remove.

Content Blocking				
<b>Domain Filtering</b>				
Profile	Forbidden Domain	Trust Domain		
sex	www.sex.com	www.sexhealth.com	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="button" value="Create"/>				

The Delete screen appears.

Domain Filtering	
<b>Delete</b>	
Profile	sex
<b>Block WEB URLs which contain these domains</b>	
Forbidden Domains	www.sex.com
<b>UnBlock WEB URLs which contain these domains</b>	
Trusted Domains	www.sexhealth.com
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

2. Click **Delete** to remove this Domain Filtering item from the Domain Filtering Table.



**NOTE:** *Be careful when deleting a Network object. You may change a policy rule associated with it.*

**CREATING RESTRICT URL FEATURES NETWORK OBJECTS**

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

**FIGURE 70    RESTRICT URL FEATURES NETWORK OBJECT LIST**

Content Blocking

Restrict URL Feature

Name	Restrict Feature	
Create ➤		

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.

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

**FIGURE 71    RESTRICTING URL FEATURES**

Restrict Filtering

Create

Name	
Restrict URL Features	<input type="checkbox"/> Block Java Applet
	<input type="checkbox"/> Block ActiveX
	<input type="checkbox"/> Block Cookies
	<input type="checkbox"/> Block Proxy
	<input type="checkbox"/> Block Surfing by IP Address
Apply    Cancel	

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

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

**EDITING RESTRICT URL FEATURE NETWORK OBJECTS**

Refer to the following to edit a Restrict URL Feature Network Object:

1. In the Content Blocking Restrict URL Feature menu, click **Edit** next to the item you want to change.

Content Blocking

Restrict URL Feature

Name	Restrict Feature		
test	Java Applet	Edit ➤	Delete ➤
Create ➤			

The following screen appears showing the item's properties.

Restrict URL Feature	
Edit	
Name	test
Restrict URL Features	<input checked="" type="checkbox"/> Block Java Applet
	<input type="checkbox"/> Block ActiveX
	<input type="checkbox"/> Block Cookies
	<input type="checkbox"/> Block Proxy
	<input type="checkbox"/> Block Surfing by IP Address
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Change the **Restrict URL Feature** parameters as desired.
3. Click **Apply** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

### **DELETING RESTRICT URL FEATURE NETWORK OBJECTS**

Refer to the following to delete a Restrict URL Feature Network Object:

1. In the Content Blocking Restrict URL Feature7 menu, click **Delete** next to the item you want to remove.

Content Blocking			
Restrict URL Feature			
Name	Restrict Feature		
test	Java Applet	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
<a href="#">Create</a> ▶			

The Delete screen appears.

Restrict URL Feature	
Delete	
Name	test
Restrict URL Features	<input checked="" type="checkbox"/> Block Java Applet
	<input type="checkbox"/> Block ActiveX
	<input type="checkbox"/> Block Cookies
	<input type="checkbox"/> Block Proxy
	<input type="checkbox"/> Block Surfing by IP Address
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

2. Click **Delete** to remove this Restrict URL Feature item from the Restrict URL Feature Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

Setting Policy parameters

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

Enabling Packet Filtering

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

FIGURE 72 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.

CREATING PACKET FILTERING PARAMETERS

- 1. Click **Create** to add a new parameter to the list.  
The Packet Filtering screen displays.
- 2. Type in the name of the packet filter, and select your settings.

FIGURE 73 CREATING A PACKET FILTERING PROFILE

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

Name	Type the name for this profile.
Active	Check <b>Enable</b> to make this profile active.
Packet Flow	Select the packet flow direction from the drop-down menu. <ul style="list-style-type: none"><li>• LAN to WAN: filters packets being transmitted to the WAN from the LAN.</li><li>• WAN to LAN: filters packets being transmitted to the LAN from the WAN.</li></ul> Check <b>Reverse Direction</b> to apply the same rule with reverse packet flow. (i.e., both directions)

Action	Select the action to be applied to the packets from the drop-down menu. <ul style="list-style-type: none"><li>• Drop: discards the packets.</li><li>• Forward: sends the packets to a specified address.</li></ul>
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 <b>Enable</b> to have the system create a log file when this filter is run.

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

Once two or more filters have been created, the Move option becomes accessible, see figure below. You can now move the filter, which changes the policy rule priority. The rule priority can be moved higher or lower by selecting the order of the rules. The highest priority is the first (#1).

Packet Filtering											
Parameters											
#	Name	Active	Flow	Action	Service	From	To	Schedule			
1	Test1	Yes	LAN to WAN /reverse	Drop	**Any	**Any	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>
2	Test2	Yes	LAN to WAN /reverse	Drop	**Any	**Any	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>

[Create](#)

**EDITING PACKET FILTERING PARAMETERS**

Refer to the following to edit a Packet Filtering profile:

1. In the Packet Filter Parameters menu, click **Edit** next to the item you want to change.

Packet Filtering										
Parameters										
#	Name	Active	Flow	Action	Service	From	To	Schedule		
1	test	Yes	LAN to WAN /reverse	Drop	**Any	**Any	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>										

The following screen appears showing the item's properties.

Packet Filtering	
Edit	
Name	test
Active	<input checked="" type="checkbox"/> Enable
Packet FlowP	LAN to WAN <input type="checkbox"/> Reverse Direction
Action	Drop
Service	**Any
From Address	**Any
To Address	**Any
Schedule	**Always On
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Change Packet Filtering parameters as desired.
3. Click **Apply** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.



**DELETING PACKET FILTERING PARAMETERS**

Refer to the following to delete a Packet Filtering profile:

1. In the Packet Filter Parameters menu, check **Delete** next to the item you want to remove.

Packet Filtering										
Parameters										
#	Name	Active	Flow	Action	Service	From	To	Schedule		
1	test	Yes	LAN to WAN /reverse	Drop	**Any	**Any	**Any	**Always On	Edit ▶	Delete ▶
Create ▶										

The Delete screen appears.

Packet Filtering	
Delete	
Name	test
Active	Yes
Packet Flow	LAN to WAN <input checked="" type="checkbox"/> Reverse Direction
Action	Drop
Service	**Any
From Address	**Any
To Address	**Any
Schedule	**Always On
Log	<input type="checkbox"/> Enable
<div> <div>Delete</div> <div>Cancel</div> </div>	

2. Click **Delete** to remove this Packet Filtering item from the Packet Filtering Parameters Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

Configuring the Virtual Server

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

FIGURE 74 VIRTUAL SERVER PARAMETERS

Virtual Server							
Parameters							
#	Name	Active	Service	Internal IP	Schedule	WAN IP	External Port(s)
Create							

CREATING VIRTUAL SERVER PARAMETERS

- 1. Click **Create** to add a virtual server profile to the list.
- 2. Enter the information in the Virtual Server Parameters screen.

FIGURE 75 ADDING A VIRTUAL SERVER

Virtual Server	
Create	
Name	<input type="text"/>
Active	<input checked="" type="checkbox"/> Enable
Service	<div>**Any </div> <div><input type="checkbox"/> Exposed Host</div>
Internal IP Address	<div><input type="text"/> <a href="#">Candidates </a></div>
Schedule	<div>**Always On </div>
WAN IP Address	<div>**Any </div>
External Service Port(s)	<div><input type="checkbox"/> Redirect to Service</div> <div><input type="text"/> ~ <input type="text"/></div>
<div>Apply Cancel</div>	

Name	Enter the given name of the virtual server.
Active	Click <b>Enable</b> to activate this virtual server.
Service	Select the service you want to assign to this virtual server. Tick <b>Exposed Host</b> if you want to setup the service outside any kind of router firewall with exceptions to Intrusion Detection, NetBIOS and EPMAP (see <a href="#">Configuring Firewall Parameters</a> on page 149).
Internal IP Address	Type the IP address you want to assign to the virtual server or click <b>Candidates</b> 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 <b>Redirect to Service</b> if you need to use port redirecting instead of port forwarding and typing the range of ports to assign to the virtual server.

- 3. Click **Add** to confirm the settings.

Once two or more rules have been created, the Move option becomes accessible, see figure below. You can now move the filter, which changes the policy rule priority. The rule priority can be moved higher or lower by selecting the order of the rules. The highest priority is the first (#1).

### FIGURE 76 MOVING A VIRTUAL SERVER RULE

Virtual Server

Parameters

#	Name	Active	Service	Internal IP	Schedule	WAN IP	External Port(s)			
1	test1	Yes	**Any	1.1.1.1	**Always On	**Any		<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>
2	test2`	Yes	**Any	1.1.1.1	**Always On	**Any		<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>

Create

**EDITING VIRTUAL SERVER PARAMETERS**

Refer to the following to edit a Virtual Server profile:

1. In the Virtual Server Parameters menu, click **Edit** next to the item you want to change.

Virtual Server									
Parameters									
#	Name	Active	Service	Internal IP	Schedule	WAN IP	External Port(s)		
1	test	Yes	**Any	192.168.1.35	**Always On	**Any		<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>									

The following screen appears showing the item's properties.

Virtual Server	
Edit	
Name	test
Active	<input checked="" type="checkbox"/> Enable
Service	**Any <input type="checkbox"/> Exposed Host
Internal IP Address	192.168.1.35 <a href="#">Candidates</a>
Schedule	**Always On
WAN IP Address	**Any
External Service Port(s)	<input type="checkbox"/> Redirect to Service
	<input type="text"/> ~ <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Change Virtual Server parameters as desired.
3. Click **Apply** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

**DELETING VIRTUAL SERVER PARAMETERS**

Refer to the following to edit a Virtual Server profile:

1. In the Virtual Server Parameters menu, check **Delete** next to the item you want to remove.

Virtual Server									
Parameters									
#	Name	Active	Service	Internal IP	Schedule	WAN IP	External Port(s)		
1	test	Yes	**Any	192.168.1.35	**Always On	**Any		Edit ▶	Delete ▶
Create ▶									

The Delete screen appears.

Virtual Server	
Delete	
Name	test
Active	Yes
Service	**Any
Internal IP Address	192.168.1.35
Schedule	**Always On
WAN IP Address	**Any
External Service Port(s)	
Delete Cancel	

2. Click **Delete** to remove this Virtual Server item from the Virtual Server Parameters Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

Configuring Quality of Service (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. In addition, a priority rule can be assigned to each of the applications. The priority set is applied in the order displayed from one to infinity.

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

FIGURE 77 QoS PARAMETERS

QoS										
Parameters										
#	Name	Active	Service	Location	Interface	From	To	Schedule	Bandwidth	Prio.
Create										

CREATING QoS PARAMETERS

- 1. Click **Create** to add a new QoS profile.
- 2. In the Create screen, type in the profile name to use and select your settings.

FIGURE 78 ADDING A QoS PROFILE

QoS	
Create	
Name	<input type="text"/>
Active	<input checked="" type="checkbox"/> Enable
DSCP Marking	Disabled
Service	**Any
Location	<input checked="" type="radio"/> Internet <input type="radio"/> LAN
Interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> ALL
From Address	**Any
To Address	**Any
Schedule	**Always On
Bandwidth	
Priority	3 (Normal)
<div>Apply Cancel</div>	

Name	Type the name for this QoS item.
Active	Check <b>Enable</b> to activate this QoS profile.
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 <b>Disabled</b> , and various levels of QoS from <b>Bronze</b> to <b>Premium</b> .
Service	Select the service you want to assign to this QoS.

Location	Select the Location you want to assign to QoS. If you select <b>Internet</b> , you will apply QoS to the traffic from internet to LAN. If you select <b>LAN</b> , you will apply QoS to the traffic from LAN to internet.
Interface	Select the interface that QoS will be applied to. If you select “WAN1”, QoS will only activate in WAN1. If you select “WAN2”, QoS will only activate in WAN2. If you select “All”, QoS will activate in both WAN1 and WAN2.
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 <b>Bandwidth</b> drop-down menu. If you have not created bandwidth Network Objects, click <b>Bandwidth</b> to open the Bandwidth Control screen and define bandwidth parameters. (See <a href="#">Managing Bandwidth Network Objects</a> on page 96.)
Priority	Select the priority of this QoS.

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

Once two or more rules have been created, the Move option becomes accessible, see figure below. You can now move the rules set, which changes the policy rule priority. The rule priority can be moved higher or lower by selecting the order of the rules. The highest priority is the first (#1).

### FIGURE 79 MOVING A QoS RULE

QoS													
Parameters													
#	Name	Active	Service	Location	Interface	From	To	Schedule	bandwidth	Prio.			
1	test1	Yes	**Any	Internet	WAN1	**Any	**Any	**Always On	test1	3	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>
2	test2	Yes	**Any	Internet	WAN1	**Any	**Any	**Always On	test1	3	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>

[Create](#)

**EDITING QoS PARAMETERS**

Refer to the following to edit a QoS profile:

1. In the QoS Parameters menu, click **Edit** next to the item you want to change. Be aware that QoS Parameters appear in Priority order i.e. #1 takes precedence over all other rules.

QoS												
Parameters												
#	Name	Active	Service	Location	Interface	From	To	Schedule	Bandwidth	Prio.		
1	test	Yes	**Any	Internet	WAN1	**Any	**Any	**Always On	test	3	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>												

The following screen appears showing the item's properties.

QoS	
Edit	
Name	test
Active	<input checked="" type="checkbox"/> Enable
DSCP Marking	Disabled
Service	**Any
Location	<input checked="" type="radio"/> Internet <input type="radio"/> LAN
Interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> ALL
From Address	**Any
To Address	**Any
Schedule	**Always On
Bandwidth	test
Priority	3 (Normal)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Change QoS parameters as desired.
3. Click **Edit** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.



**DELETING QoS PARAMETERS**

Refer to the following to delete a QoS profile:

1. In the QoS Parameters menu, check **Delete** next to the item you want to remove.

QoS												
Parameters												
#	Name	Active	Service	Location	Interface	From	To	Schedule	Bandwidth	Prio.		
1	test	Yes	**Any	Internet	WAN1	**Any	**Any	**Always On	test	3	Edit ▶	Delete ▶
Create ▶												

The Delete screen appears.

QoS	
Delete	
Name	test
Active	Yes
Service	**Any
Location	Internet
Interface	WAN1
From Address	**Any
To Address	**Any
Schedule	**Always On
Bandwidth	test
Priority	3
Delete Cancel	

2. Click **Delete** to remove this QoS item from the QoS Parameters Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

### CONFIGURING SIP QoS PROFILE

SIP (Session Initiation Protocol) is a signalling protocol developed by the IETF (Internet Engineering Task Force). SIP proposes a technology integrating Internet and PSTN environment. It is similar to HTTP protocol, which based on text encoding to send commands and messages to assure that the protocol is simplified and determined by text rather than signal. SIP, as its name, is an initial protocol for sessions, and works in concert with several other protocols. It acts as a carrier for the SDP (Session Description Protocol, RFC 2327, RFC 2365), which describes the media content of the communication session. SIP “sessions” are simply packet streams of the RTP (Real-time Transport Protocol) which is the carrier for the actual data, voice or video content itself.


There are various functions and elements of SIP. SIP elements includes UA (User Agent, SIP hardphone or SIP softphone), Proxy (Proxy Server), Redirect Server (a user agent server that allows SIP Proxy Servers to direct SIP session invitations to external domains), Registry Server (a server that accepts register requests and places the information it receives in those requests into the location service for the domain it handles), Voice Mail Server (voice mail box) and etc. SIP functions can combine the related services such as PSTN, H323, MGCP, MEGECO, and etc., even the most of 3G services are performed based on SIP currently.

QoS (Quality of Service) is a set of quality assurance mechanisms for data transmission. QoS provides different priority to different users or data flows, or to guarantee a certain level of performance to an application. QoS guarantees are important if the network capacity is insufficient, especially for streaming multimedia applications such as voice over IP and IP-TV, since these often require fixed bit rate and are delay sensitive.

Billion's SSL VPN routers with the Quality of Service (QoS) can manager the traffic of applications such as FTP and SMTP. After traffic control function added to the routers, the QoS feature is allowed to control and manager the traffic flow of SIP service. To configure the application such as SIP service administrator want to manager, select **Network Object** → **Service** first to add the SIP Service and set the SIP port number to 5060. Than go to **Policy** → **QoS**, choose SIP service from the drop-down menu, set schedule and bandwidth configurations and prioritize the traffic of data for SIP service. It provides the administrator with controlling the bandwidth of the access to intranet resources for users outside the company or the access to the internet for users in the company. To configure QoS settings, please see User Manual.

Refer to the following to configure SIP QoS profiles:

1. Select **Configuration** → **Network Object** → **Service** to display the list of allowable pre-defined and user-defined services. SIP Service is not defined at Pre-defined Service Table, so it is not available when the administrator wants to select from the **Service** drop-down menu in Qos Parameters screen. Click **Create** to add the SIP Service and configure the Port/protocol ID that this service is allowed to use.

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 				

2. In the Service Create screen, fill in the Name filed, select Type from the drop-down menu, and enter the port number as 5060 that defines the beginning/end of the port range in the Service Port Start/End fields. Click **Apply** to confirm the settings and you

will be directed to the Service page displaying the new added SIP Service in the User-defined Service Table.

User-defined Service Table				
Name	Type	Port/protocol ID		
SIP	UDP	5060~5060	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>				

- After the setting of SIP Service is completed, select **Configuration** → **Network Object** → **Bandwidth Control** to create and configure a Bandwidth Control Network Object. In the Bandwidth Control Create screen, fill in the Name, Downstream, and Upstream fields. Click **Apply** to confirm the settings and you will be directed to the Bandwidth Control page displaying the new added bandwidth object in the Bandwidth Table.

Bandwidth Control				
Bandwidth Table				
Name	Downstream	Upstream		
sip	Guaranteed:22000 Maximum:22000	Guaranteed:22000 Maximum:22000	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>				

- After the setting of Bandwidth Control Network Object is completed, select **Configuration** → **Policy** → **QoS** to create a QoS profile and configure QoS setting for SIP Service.

Create	
Name	<input type="text" value="SIP Qos"/>
Active	<input checked="" type="checkbox"/> Enable
DSCP Marking	<input type="text" value="Disabled"/>
<a href="#">Service</a>	<input type="text" value="SIP"/>
Location	<input checked="" type="radio"/> Internet <input type="radio"/> LAN
Interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> ALL
<a href="#">From Address</a>	<input type="text" value="**Any"/>
<a href="#">To Address</a>	<input type="text" value="**Any"/>
<a href="#">Schedule</a>	<input type="text" value="**Always On"/>
<a href="#">Bandwidth</a>	<input type="text" value="sip"/>
Priority	<input type="text" value="3 (Normal)"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Note:** Select the packet flow direction in the **Location** field. If you select **Internet**, packets will be transmitted to the WAN from the LAN. If you select **LAN**, packets will be transmitted to the LAN from the WAN.

### Configuring Ethernet MAC Filtering

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

**FIGURE 80** ETHERNET MAC FILTERING PROFILES

Ethernet MAC Filtering

Parameters

#	Name	Active	Flow	Action	MAC Address	Schedule
---	------	--------	------	--------	-------------	----------

Create

Ethernet MAC filtering enables you to prevent Ethernet MAC addresses from being accessed.

**CREATING ETHERNET MAC FILTERS**

To create an Ethernet MAC filter, please follow the steps below:

1. Click **Create** to add a new Ethernet MAC Filter profile.
2. Enter the information in the **Ethernet MAC Filter** screen.

**FIGURE 81** ADDING AN ETHERNET MAC FILTER PROFILE

Ethernet MAC Filtering

Create

Name	<input type="text"/>
Active	<input checked="" type="checkbox"/> Enable
Action	Drop <input type="button" value="v"/>
Mac Address	<input type="text"/> <a>Candidates</a> (00:00:00:00:00:00' means 'All MAC Addresses')
Schedule	<a>Always On</a> <input type="button" value="v"/>
Log	<input type="checkbox"/> Enable

Apply Cancel




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

3. Click **Add** to confirm the settings.





**EDITING ETHERNET MAC FILTERS**

Refer to the following to edit an Ethernet MAC filter:

1. In the Ethernet MAC Filtering Parameters menu, click **Edit** next to the item you want to change. Be aware that Ethernet MAC Filters appear in Priority order i.e. #1 takes precedence over all other filters.

Ethernet MAC Filtering							
Parameters							
#	Name	Active	Flow	Action	MAC Address	Schedule	
1	test	Yes	LAN to WAN	Drop	00:05:5D:04:47:73	**Always On	<a href="#">Edit</a>  <a href="#">Delete</a> 
<a href="#">Create</a> 							

The following screen appears showing the item's properties.

Ethernet MAC Filtering	
Edit	
Name	test
Active	<input checked="" type="checkbox"/> Enable
Action	Drop 
MAC Address	00:05:5D:04:47:73 <a href="#">Candidates</a> 
<a href="#">Schedule</a> 	**Always On 
Log	<input type="checkbox"/> Enable
<a href="#">Apply</a> <a href="#">Cancel</a>	

2. Change Ethernet MAC filter parameters as desired.
3. Click **Apply** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

**DELETING ETHERNET MAC FILTERS**

Refer to the following to delete an Ethernet MAC filter:

- 1. In the Ethernet MAC Filtering Parameters menu, check **Delete** next to the item you want to remove.

Ethernet MAC Filtering								
Parameters								
#	Name	Active	Flow	Action	MAC Address	Schedule		
1	test	Yes	LAN to WAN	Drop	00:05:5D:04:47:73	**Always On	Edit	Delete
Create								

The Delete screen appears.

Ethernet MAC Filtering	
Delete	
Name	test
Active	Yes
Packet Flow	LAN to WAN
Action	Drop
MAC Address	00:05:5D:04:47:73
Schedule	**Always On
Log	<input type="checkbox"/> Enable
Delete Cancel	

- 2. Click **Delete** to remove this Ethernet MAC filter from the Ethernet MAC Filtering Parameters Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

## Configuring Content Filtering policies

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

**FIGURE 82** CONTENT FILTERING POLICIES

Content Filtering							
Parameters							
#	Name	Active	Keyword	Domain	Restrict	From	Schedule
Create ▶							
Exception list							
IP Address							
Create ▶							

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.

Click **Create** in the Parameters table to create a defined parameters list.

Click **Create** in the Exception list to create an IP address exception list, which allows specified IP addresses to be accessed.

### CREATING CONTENT FILTERING PARAMETERS

1. Under **Parameters**, click **Create** to set up a new content filtering profile.
2. Enter the information in Content Filtering Parameters screen.

**FIGURE 83** CREATING A CONTENT FILTERING PROFILE

Content Filtering	
Create	
Name	<input type="text"/>
Active	<input checked="" type="checkbox"/> Enable
Keyword Filtering ▶	<input type="checkbox"/> Enable <input type="text" value="violence"/>
Domain Filtering ▶	<input type="checkbox"/> Enable <input type="text" value="sex"/>
	<input type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict Feature ▶	<input type="checkbox"/> Enable <input type="text" value="test"/>
From Address ▶	<input type="text" value="**Any"/>
Schedule ▶	<input type="text" value="**Always On"/>
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



**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	Enter a given name to this profile.
Active	Check <b>Enable</b> to activate this profile.

---

Keywords Filtering	Check <b>Enable</b> to activate keyword filtering and select a Keyword Filtering Network Object from the drop-down menu. (See <a href="#">Creating Keyword Filter Network Objects</a> on page 98.)
Domains Filtering	Check <b>Enable</b> to activate domain filtering and select a Domain Filtering profile from the drop-down menu. (See <a href="#">Creating Domain Filter Network Objects</a> on page 101.) Check <b>Disable all WEB traffic except for Trusted Domains</b> to only allow those domains that have been designated as trusted to have access.
Restrict Feature	Check <b>Enable</b> to activate the <b>Restrict URL Feature</b> and select a Restrict URL Feature profile from the drop-down menu. (See <a href="#">Creating Restrict URL Features Network Objects</a> on page 104.)
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 <b>Enable</b> if you want a log file to be created when this filter is activated.

---

3. Click **Add** to confirm the settings.



**EDITING CONTENT FILTERING PARAMETERS**

Refer to the following to edit a Content filter:

1. In the Content Filtering Parameters menu, click **Edit** next to the item you want to change.

Content Filtering									
Parameters									
#	Name	Active	Keyword	Domain	Restrict	From	Schedule		
1	test	Yes	violence	Disabled	Disabled	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>									
Exception list									
IP Address									
<a href="#">Create</a>									

The following screen appears showing the item's properties.

Content Filtering	
Edit	
Name	test
Active	<input checked="" type="checkbox"/> Enable
Keyword Filtering	<input checked="" type="checkbox"/> Enable <span>violence</span>
Domain Filtering	<input type="checkbox"/> Enable <span>sex</span>
	<input checked="" type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict Feature	<input type="checkbox"/> Enable <span>test</span>
From Address	<span>**Any</span>
Schedule	<span>**Always On</span>
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Change Content Filtering parameters as desired.
3. Click **Apply** to confirm the settings.



**NOTE:** Be careful when editing a Network object. You may change a policy rule associated with it.

**DELETING CONTENT FILTERING PARAMETERS**

Refer to the following to delete a Content filter:

1. In the Content Filtering Parameters menu, check **Delete** next to the item you want to remove.

Content Filtering									
Parameters									
#	Name	Active	Keyword	Domain	Restrict	From	Schedule		
1	test	Yes	violence	Disabled	Disabled	**Any	**Always On	Edit ▶	Delete ▶
Create ▶									
Exception list									
IP Address									
Create ▶									

The Delete screen appears.

Content Filtering	
Delete	
Name	test
Active	Yes
Packet Flow	LAN to WAN
Keyword Filtering	violence
Domain Filtering	Disabled
	<input checked="" type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict Feature	Disabled
From Address	**Any
Schedule	**Always On
Log	<input type="checkbox"/> Enable
Delete Cancel	

2. Click **Delete** to remove this Content Filtering profile from the Content Filtering Parameters Table.



**NOTE:** Be careful when deleting a Network object. You may change a policy rule associated with it.

**CREATING A CONTENT FILTERING EXCEPTION IP PROFILE**

You can exclude specified IP address from the Content Filtering profiles you have set up.

1. Click **Create** under the **Exception List** to add an IP address exception.

**FIGURE 84** ADDING AN IP EXCEPTION

2. Enter the IP address or click **Candidates** and select available from internal IP addresses.
3. Click **Apply** to add the IP address to the exception list.  
To delete the profile, check the **Delete** check box next to the item you want to remove.

**FIGURE 85** DELETING AN IP EXCEPTION

The **Delete** screen appears.

4. Click **Delete** to remove this IP addresses from the Content Filtering Exception IP Table.

## Configuring IPsec

Click **Configuration** in the Menu bar and then click **IPsec**. The IPsec screen appears.

**FIGURE 86** IPsec Tunnels Screen

IPsec

IPsec Tunnels

Name	Enable	Local Network	Remote Network	Remote Gateway	IPsec Proposal
------	--------	---------------	----------------	----------------	----------------

Create

The IPsec screen shows you a table of your current IPsec Tunnels.

### Creating and Enabling IPsec Tunnels

1. Click **Create** to add a new IPsec tunnel to the list. The Create screen is displayed.

IPsec

Create

Connection Name			
Tunnel	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
Interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> Auto		
Local			
ID	IP Address	Data	
Network	Any Local Address	IP Address	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
		Netmask	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Remote			
Secure Gateway			
ID	IP Address	Data	
Network	Subnet	IP Address	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
		Netmask	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Proposal			
Secure Association	<input checked="" type="radio"/> Main Mode <input type="radio"/> Aggressive Mode <input type="radio"/> Manual Key		
Method	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
Encryption Protocol	3DES		
Authentication Protocol	MD5		
Perfect Forward Secure	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
Key Group	MODP 1024 (GROUP 2)		
PreShared Key			
IKE Life Time	28800	Seconds	
Key Life Time	3600	Seconds	
DPD Setting			
DPD Function	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
Detection Interval	30	seconds	
Idle Timeout	4	consecutive times	

Apply

Connection Name	A user-defined name for the connection
Tunnel	Select <b>Enable</b> to activate this tunnel. Select <b>Disable</b> to deactivate this tunnel.

Interface	<p>Select the interface the IPsec tunnel will apply to:</p> <p><b>WAN1:</b> Select interface WAN1.</p> <p><b>WAN2:</b> Select interface WAN2.</p> <p><b>Auto:</b> The device automatically applies the tunnel to WAN1 or WAN2 depending on which WAN interface is active when the IPsec tunnel is established.</p> <p><b>Note:</b> Auto only applies to Fail Over mode. For Load Balance mode, please do not select "Auto". In Load Balance mode, Auto forces the use of the WAN1 interface if selected.</p>
<b>Local</b>	
ID	<p>This is the identity type of the local router or host. Choose from the following four options:</p> <p><b>WAN IP Address:</b> Automatically use the current WAN Address as ID.</p> <p><b>IP Address:</b> Use an IP address format.</p> <p><b>FQDN DNS (Fully Qualified Domain Name):</b> Consists of a hostname and domain name. For example, WWW.VPN.COM is a FQDN. WWW is the host name, VPN.COM is the domain name. When you enter the FQDN of the local host, the router will automatically seek the IP address of the FQDN.</p> <p><b>FQUN E-Mail (Fully Qualified User Name):</b> Consists of a username and its domain name. For example, user@vpn.com is a FQUN. "user" is the username and "vpn.com" is the domain name.</p>
Data	Enter the ID data using the specific ID type.
Network	<p>Set the IP address, IP range, subnet, or address range of the local network:</p> <p><b>Any Local Address:</b> Will enable any local address on the network.</p> <p><b>Subnet:</b> The subnet of the local network. Selecting this option enables you to enter an IP address and netmask.</p> <p><b>Single Address:</b> The IP address of the local host.</p>
<b>Remote</b>	
Secure Gateway	The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.
ID	<p>The identity type of the local host. Choose from the following four options:</p> <p><b>Remote WAN IP. Address:</b> Automatically use the remote gateway Address as the ID.</p> <p><b>IP Address:</b> Use an IP address format.</p> <p><b>FQDN DNS (Fully Qualified Domain Name):</b> Consists of a hostname and domain name. For example, WWW.VPN.COM is a FQDN. WWW is the host name, VPN.COM is the domain name. When you enter the FQDN of the local host, the router will automatically seek the IP address of the FQDN.</p> <p><b>FQUN E-Mail (Fully Qualified User Name):</b> Consists of a username and its domain name. For example, user@vpn.com is a FQUN. "user" is the username and "vpn.com" is the domain name.</p>
Data	Enter the ID data using the specific ID type.

Network	<p>Set the subnet, IP Range, single address, or gateway address of the remote network.</p> <p><b>Subnet:</b> The subnet of the remote network. Selecting this option allows you to enter an IP address and netmask.</p> <p><b>IP Range:</b> The IP Range of the remote network.</p> <p><b>Single Address:</b> The IP address of the remote host.</p> <p><b>Gateway Address:</b> The gateway address of the remote host.</p>
<b>Proposal</b>	
Secure Association (SA)	<p>SA is a method of establishing a security policy between two points. There are three methods of creating SA, each varying in degrees of security and speed of negotiation:</p> <p><b>Main Mode:</b> Uses the automated Internet Key Exchange (IKE) setup; most secure method with the highest level of security.</p> <p><b>Aggressive Mode:</b> Uses the automated Internet Key Exchange (IKE) setup; mid-level security, speed is faster than Main mode.</p> <p><b>Manual Key:</b> Standard level of security. It is the fastest of the three methods.</p>
Method	<p>There are two methods of checking the authentication information, <b>ESP</b> (Encapsulating Security Payload) and <b>AH</b> (Authentication Header). Use ESP for greater security so that data will be encrypted and authenticated. AH data will be authenticated but not encrypted.</p>
Encryption Protocol	<p>Select the encryption method from the pull-down menu. There are five options: DES, 3DES, and AES (128, 192 and 256).</p> <p><b>DES:</b> Data Encryption Standard. It uses a 56-bit encryption method.</p> <p><b>3DES:</b> Triple Data Encryption Standard. It uses a 168-bit encryption method.</p> <p><b>AES:</b> Advanced Encryption Standard. You can use 128, 192 or 256 bits as encryption method.</p> <p><b>Note:</b> 3DES and AES are more powerful but increase latency.</p>
Authentication Protocol	<p>Authentication establishes data integrity and ensures it is not tampered with while in transit.</p> <p>There are two options: Message Digest 5 (MD5), and Secure Hash Algorithm (SHA1).</p> <p><b>MD5:</b> A one-way hashing algorithm that produces a 128 bit hash.</p> <p><b>SHA1:</b> A one-way hashing algorithm that produces a 160 bit hash. SHA1 is slower but more resistant to bruteforce attacks than MD5.</p>
Perfect Forward Secure	<p>Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish shared security over the internet.</p>
Key Group	<p>Select Key Group from MODP 768 (GROUP 1), MODP 1024 (GROUP2), and MODP 1536 (GROUP 5). The default is MODP 1024 (GROUP 2).</p>

---



---

Preshared Key	Used by the Internet Key Exchange (IKE) protocol. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).
IKE Life Time	Allows you to specify the timer interval for renegotiation of the IKE security association. The value is in seconds, eg. 28800 seconds = 8 hours.
Key Life Time	Allows you to specify the timer interval for renegotiation of another key. The value is in seconds eg. 3600 seconds = 1 hour.
<b>DPD Setting</b>	
DPD Function	Enable/disable DPD (Dead Peer Detection) Function. The following fields are available when you click <b>Enable</b> .
Detection Interval	Set the DPD detection interval in seconds.
Idle Timeout	Set the number of detection attempts before the BiGuard S20 timeout.

---



---

2. Select the settings to change and click **Apply** to enable IPSec.

## Configuring the System

Click **System** to set up time zone, remote access, firmware upgrade, backup/restore, password, license upgrade, and restart.

### Setting the Time Zone

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

**FIGURE 87**    **SETTING THE TIME ZONE**

Time Zone

Parameters

Time Zone

☒ Enable ☐ Disable

Local Time Zone (+ -GMT Time)

(GMT)Greenwich Mean Time

SNTP Server IP Address

1. 192.43.244.18

2. 128.138.140.44

3. 129.6.15.29

4. 131.107.1.10


Daylight Saving

☒ Automatic

Resync Period

1440

minutes



Apply

Cancel

Time Zone	Click <b>Enable</b> to allow the BiGuard S20 to automatically update the time from the network time server. Click <b>Disable</b> 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	Enter the IP address or URL (for example <b>time.windows.com</b> ) of the SNTP (Simple Network Time Protocol) server.
Daylight Saving	Check this box to allow the BiGuard S20 to automatically adjust for day-light saving time.
Resync Period	Enter the number of minutes that will elapse before the BiGuard S20 adjusts the time.

Click **Apply** to confirm the settings.



### Enabling Remote Access

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

**FIGURE 88** ENABLING REMOTE ACCESS

Remote Access

You may permit remote access and administration on this network device (HTTPS).

Remote Access Control

☐ Enable Both Remote SSL VPN Portal and Remote Configuration

☒ Enable Remote SSL VPN Portal, but Disable Remote Configuration

☐ Disable Both Remote SSL VPN Portal and Remote Configuration

Remote Address

\*\*Any

Apply

Cancel

Remote Access Control	Enable Both Remote SSL VPN Portal and Remote Configuration Enable Remote SSL VPN Portal, but disable Remote Configuration Disable both Remote SSL VPN Portal and Remote Configuration
	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.

Click **Apply** to confirm the settings.



**WARNING:** It is 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 199.

### Upgrading the BiGuard S20 Firmware

Periodic firmware updates are available from the BiGuard registration web site: [www.biguard.com](http://www.biguard.com).

1. Download the firmware patch, and save to a specified location.
2. Click **Firmware Upgrade** to upgrade the firmware.

**FIGURE 89**   UPGRADING THE FIRMWARE

**Firmware Upgrade**

You may upgrade the system software on your network device

After upgrading, restart the router with factory default settings or current settings

Restart Router with

☐ Factory Default Settings

☒ Current Settings


New Firmware Image

Browse...

Upgrade

Cancel

3. Click **Factory Default Settings** or **Current Settings** to determine how the router will restart after the upgrade.
4. Click **Browse** to go to the location of the downloaded patch.
5. Click **Upgrade** to apply the firmware patch.
6. 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 S20. Any interruption during the upgrade process (Including power loss) may render the device fail.
7. The BiGuard S20 will automatically log out once the upgrade is complete. To make further configuration changes, please log in again.

## Backing up and restoring configurations

You can back up different configurations and restore them for flexible network management from the Backup/Restore page. Open the Backup/Restore page by clicking on the **Backup/Restore** button.

**FIGURE 90** 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"/> Domain 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	

Backup

#### Restore Configuration

Configuration File

Browse...

*"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.*

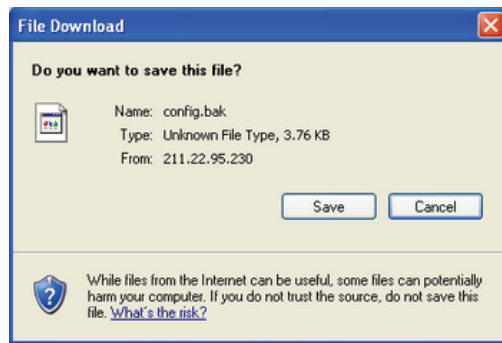
Restore

### **BACKING UP THE CONFIGURATION**

You can choose between two backup scenarios.

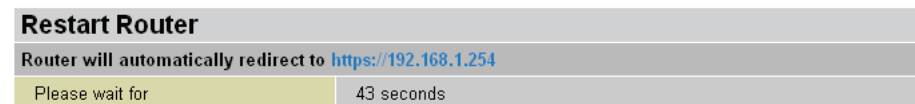
Backup all configuration	Click <b>Backup all configuration to your computer</b> to save all current configuration information to the computer.
Export the checked objects	Click <b>Export the checked objects to your computer</b> and then check which items you want to include in the backup.

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

**FIGURE 91** BACKING UP A CONFIGURATION**RESTORING A SAVED CONFIGURATION**

Refer to the following to restore a saved configuration:

1. Click **Browse** and go to the location of the configuration file.
2. Click on the desired file to enter the file path into the **Configuration File** field.
3. Click **Restore** to begin restoring the configuration.

**FIGURE 92** RESTORING A CONFIGURATION

4. Wait for the router to restart before performing any actions. The BiGuard S20 will automatically log out once the restore is complete. To make further configuration changes, please log in again.



**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 136.

**NOTE:** To restore your configurations, you must have an existing backup file before starting.

## Configuring and changing passwords

Click **Password** to change the password needed to access the BiGuard S20 web configuration interface.

**FIGURE 93** CHANGING PASSWORDS

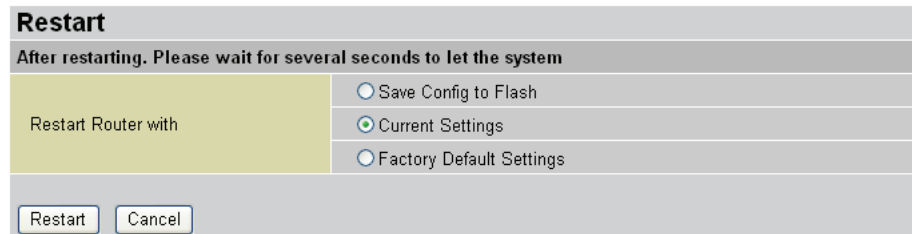
Password	
Parameters	
User Name	admin
Password	••••••
Retype Password	••••••

Enter the new password in the Password text box. Retype the password to confirm and click **Apply** to save the new password. A confirmation message is displayed. Click **OK** in the Administrator's password has Changed dialog box to confirm changes.

## Restarting the system

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

**FIGURE 94** RESTARTING THE SYSTEM



The screenshot shows a web interface titled "Restart". Below the title is a message: "After restarting. Please wait for several seconds to let the system". The main area is divided into two sections. On the left, there is a yellow box with the text "Restart Router with". On the right, there are three radio button options: "Save Config to Flash", "Current Settings" (which is selected), and "Factory Default Settings". At the bottom of the interface, there are two buttons: "Restart" and "Cancel".

2. You can restart the system using the following options:
  - Save Config to Flash: save any recent configuration changes to flash before restarting.
  - Current Settings: restart using the latest saved configuration.
  - Factory Default Settings: restart using factory default settings.
3. Click **Restart** to restart the system with the selected option. A count down is initiated after which the machine will restart.



The following screen appears showing the properties of the item.

Static Route

Edit

Destination	192.168.2.0
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Interface	LAN
Cost	0

Apply

Cancel

2. Change the static route’s parameters as desired.

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

**DELETING STATIC ROUTES**

Refer to the following to delete a static route:

1. In the Static Route Static Routing List menu, click **Delete** next to the item you want to remove.

Static Route

Static Routing List

#	Valid	Destination	Subnet Mask	Gateway/Interface	Cost		
1	True	192.168.2.0	255.255.255.0	192.168.1.254/LAN	0	<div>Edit</div>	<div>Delete</div>

Create

The Delete screen appears.

Static Route

Delete

Destination	192.168.2.0
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Interface	LAN
Cost	0

Delete

Cancel

2. Click **Delete** to remove this static route entry from the Static Routing List.



## Configuring Static ARP

The Static ARP allows you to manually assign an IP address to a MAC Address. A new feature for BiGuard S20 is that it allows **Wake On LAN (WOL)** to be used in co-operation with Static ARP.

**WOL functionality:** Allows the router to turn on computers from a powered-off state.

**Steps:** In the router, set up a new static ARP (static ARP table). A special data packet will be sent from outside which goes through the Router and then sent to the designated computer to be turned on.



**NOTE:** Your network card must be able to support WOL for WOL to work.

**FIGURE 97 THE STATIC ARP TABLE**

ARP Table	
IP <> MAC List	
IP Address	<input type="text"/>
MAC Address	<input type="text"/>
Interface	LAN <input type="button" value="v"/>
<input type="button" value="Add"/> <input type="button" value="Edit/Delete"/> <input type="button" value="Cancel"/>	

IP Address	Enter the IP address for the ARP entry.
MAC Address	Enter the MAC address for the ARP entry.
Interface	Select the interface for the ARP entry.
Add	Click on the <b>Add</b> button to add the new ARP entry.
Edit/Delete	<p>Select the check box on the <b>Edit</b> column and click on the <b>Edit/Delete</b> button to edit the ARP table entry. The ARP entry information will automatically be entered in the space above.</p> <p>Select the check on the <b>Delete</b> column and click on the <b>Edit/Delete</b> button to delete the selected ARP table entry.</p>
Cancel	Click the <b>Cancel</b> button to clean the <b>IP Address</b> and <b>MAC Address</b> field.

### CREATING ARP ENTRY

1. Enter the IP Address and the MAC Address and select the Interface in the **Static ARP** screen.

ARP Table	
IP <> MAC List	
IP Address	192.168.1.20
MAC Address	aa:bb:cc:dd:ee:ff
Interface	LAN <input type="button" value="v"/>
<input type="button" value="Add"/> <input type="button" value="Edit/Delete"/> <input type="button" value="Cancel"/>	

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

### **EDITING ARP ENRTY**

Refer to the following to edit a static ARP entry:

- In the ART Table, check the **Edit** radio button.

ARP Table			
IP <> MAC List			
IP Address		<input type="text"/>	
MAC Address		<input type="text"/>	
Interface		LAN <input type="button" value="v"/>	
<input type="button" value="Add"/>		<input type="button" value="Edit/Delete"/> <input type="button" value="Cancel"/>	
<b>Edit</b>	IP Address	MAC Address	Delete
<input checked="" type="radio"/>	192.168.1.20	aa:bb:cc:dd:ee:ff	<input type="checkbox"/>

The following screen appears showing the item's properties.

ARP Table			
IP <> MAC List			
IP Address		<input type="text" value="192.168.1.20"/>	
MAC Address		<input type="text" value="aa:bb:cc:dd:ee:ff"/>	
Interface		LAN <input type="button" value="v"/>	
<input type="button" value="Add"/>	<input type="button" value="Edit/Delete"/>	<input type="button" value="Cancel"/>	
<b>Edit</b>	IP Address	MAC Address	Delete
<input checked="" type="radio"/>	192.168.1.20	aa:bb:cc:dd:ee:ff	<input type="checkbox"/>

- Change static ARP parameters as desired.
- Click **Edit/Delete** to confirm the settings.

### **DELETING ARP ENRTY**

Refer to the following to delete a static ARP entry:

- In the ART Table, check **Delete** next to the item you want to remove.

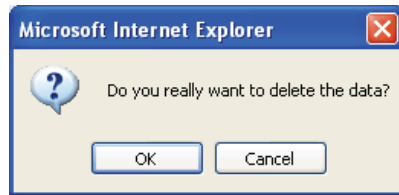
ARP Table			
IP <> MAC List			
IP Address		<input type="text"/>	
MAC Address		<input type="text"/>	
Interface		LAN <input type="button" value="v"/>	
<input type="button" value="Add"/>		<input type="button" value="Edit/Delete"/> <input type="button" value="Cancel"/>	
<b>Edit</b>	IP Address	MAC Address	<b>Delete</b>
<input type="radio"/>	192.168.1.20	aa:bb:cc:dd:ee:ff	<input type="checkbox"/>

The **Delete** screen appears.

ARP Table			
IP <> MAC List			
IP Address		<input type="text" value="192.168.1.20"/>	
MAC Address		<input type="text" value="aa:bb:cc:dd:ee:ff"/>	
Interface		LAN <input type="button" value="v"/>	
<input type="button" value="Add"/>	<input type="button" value="Edit/Delete"/>	<input type="button" value="Cancel"/>	
<b>Edit</b>	IP Address	MAC Address	Delete
<input type="radio"/>	192.168.1.20	aa:bb:cc:dd:ee:ff	<input checked="" type="checkbox"/>

- Click **Edit/Delete** to remove this static ARP item from ARP Table.

3. You will be prompted the following message. Click **OK** to delete the data.




## Enabling Dynamic DNS

Dynamic DNS (DDNS) is a network service that provides the capability for a host assigned a dynamic IP address to alias to a static hostname. If your ISP does not assign you a static IP address, you can still use a domain name (i.e. billion.biguard.com). The domain name and IP address have a one-to-many relationship: each domain name produces many dynamic IP addresses, but each IP is assigned only one static domain name. If the users who use ADSL PPPOE and Cable DHCP set up their own servers, such as Web, Mail, FTP or etc., which the IP addresses can not be fixed, they will need Dynamic DNS to retrieve the IP address used to connect to the web server, even if the IP address is changed.

This dynamic IP address is the WAN IP address. To use DDNS feature in the Billion Router, first you need to register and apply for an account with the Dynamic DNS provider using their web-site, for example <http://www.dyndns.org/>, then enter the related parameters such as the registered domain name and etc., and enter the location of the dynamic DNS server which will be providing the DDNS function. After this have been setup all the other equipment on the Internet can find the assigned WAN IP of the Billion Router (could be WAN1 or WAN2) by just entering the domain name, with resolving a registered domain name into an dynamic IP address. In the Router, the static domain name corresponding to the dynamic IP address could be corresponded to WAN1 or WAN2, which must be configured by the administrator in advance. At the same time, it is allowed a WAN interface to be connected with multiple domain names (For example, billion.dyndns.org and bilion.biguard.com are both corresponded to the WAN 1 port.).

1. Select **Configuration** → **Advanced** → **Dynamic DNS** to view the Dynamic DNS (DDNS) table.

**FIGURE 98** DYNAMIC DNS TABLE

Dynamic DNS							
Dynamic DNS Table							
#	Dynamic DNS Server	Wildcard	Mail Exchange	Domain Name	User Name	Interface	Period
Create 							



**NOTE:** You need to register and establish an account with the Dynamic DNS provider using their Web site before using DDNS. The BiGuard S20 supports several Dynamic DNS providers.

2. Click **Create** to open a screen which allows you to set DDNS parameters. In the Dynamic DNS Create screen, the **Mail Exchange** filed indicates MX Record. It is allowed user to enter MX recode if they have.



**NOTE:** MX Record is a record in DNS. If you have any questions, please look up websites for MX Record function of DNS.

Dynamic DNS	
<b>Create</b>	
Dynamic DNS Server	www.dyndns.org (custom) ▼
Wildcard	<input type="checkbox"/> Enable
Mail Exchange	<input type="text"/>
Domain Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/>
Retype Password	<input type="password"/>
Period	28 Day(s) ▼
Interface	WAN1 ▼
<b>Customization Server Address</b>	
Customization Server Address	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Server Address	<input type="text"/>
Port	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3. Enter the parameters in Create fields.

Dynamic DNS	
<b>Create</b>	
Dynamic DNS Server	www.dyndns.org (dynamic) ▼
Wildcard	<input type="checkbox"/> Enable
Mail Exchange	<input type="text"/>
Domain Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/>
Retype Password	<input type="password"/>
Period	28 Day(s) ▼
Interface	WAN1 ▼
<b>Customization Server Address</b>	
Customization Server Address	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Server Address	<input type="text"/>
Port	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Dynamic DNS Server	Select the corresponding DDNS server you have established an account with from the drop-down menu. In this example, <b>www.dyndns.org (dynamic)</b> is selected.
Wildcard	Click <b>Enable</b> 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.
Mail Exchange	Indicates MX Record which is the host record of the destination mail server. It allows user to enter MX record if they have.

Domain Name	Enter your registered domain name for the DDNS server.
User Name	Enter the user name for accessing the Dynamic DNS server to perform an update between the registered domain name and corresponding IP address.
Password	Enter the password for accessing the Dynamic DNS server to perform an update between the registered domain name and corresponding IP address.
Retype Password	Retype the password.
Period	Set the time period between updates. Enter the period of time and select the units (days or hours) for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.
Interface	If the router is Dual WAN product, select either the IP address <b>WAN1</b> or <b>WAN2</b> from the drop-down menu to apply for DDNS.

4. When the user set up DDNS server to provide static domain name and dynamic IP address translation service, they are required to enter the related parameters in **Customization Server Address** associated fields.

Dynamic DNS

Create

Dynamic DNS Server

www.dyndns.org (custom) ▾

Wildcard

☐ Enable

Mail Exchange

Domain Name

billionrouter.dyndns.org

User Name

billion

Password

...

Retype Password

...

Period

28 ▾ Day(s) ▾

Interface

WAN1 ▾

Customization Server Address

☒ Enable ☐ Disable

Server Address

61.64.xx.xx

Port

8080

Dynamic DNS Server	Select the corresponding DDNS server you have established an account with from the drop-down menu. In this example, <b>www.dyndns.org (custom)</b> is selected.
Domain Name	Enter a domain name as you desired for your own DDNS server.
User Name	Enter the user name for accessing the Dynamic DNS server to perform an update between the registered domain name and corresponding IP address.

---

---

Password	Enter the password for accessing the Dynamic DNS server to perform an update between the registered domain name and corresponding IP address.
Retype Password	Retype the password.
Customization Server Address	Check Enable radio button for Customization Server Address.
Server Address	Enter the IP address for your own DDNS server.
Port	Enter the port value for your own DDNS server.

---

---

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

Configuring SNMP

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

FIGURE 99 ENABLING SNMP

SNMP

Parameters

SNMP

☐ Enable ☒ Disable

Apply

Cancel

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

FIGURE 100 SETTING SNMP PARAMETERS

SNMP

Parameters

SNMP

☒ Enable ☐ Disable

Interface

☒ Access from LAN ☐ Access from WAN & LAN

SNMP V1 and V2

Read Community

public

IP Address

0.0.0.0

Write Community

password

IP Address

0.0.0.0

Trap Community

IP Address

SNMP V3

User Name

Password

Access Right

☒ Read ☐ Read/Write

Apply

Cancel

Parameters	<div><div>This section enables you to set the parameters of SNMP.</div><ul style="list-style-type: none"><li>• <b>SNMP:</b> Enable or Disable the SNMP function.</li><li>• <b>Interface:</b> Allow access from LAN or both WAN and LAN.</li></ul></div>
SNMP V1 and V2	<div><div>This section enables you to set parameters for SNMP versions 1 and 2. The following information is entered:</div><ul style="list-style-type: none"><li>• <b>Read Community:</b> type the name of the read community and the IP address associated with it.</li><li>• <b>Write Community:</b> type the name of the write community and the IP address associated with it.</li><li>• <b>Trap Community:</b> type the name of the trap community and the IP address associated with it.</li></ul></div>
SNMP V3	<div><div>This section enables you to set parameters for SNMP version 3. The following information is entered:</div><ul style="list-style-type: none"><li>• <b>User Name</b> and <b>Password:</b> type the user name and password for accessing SNMP sites.</li><li>• <b>Access Right:</b> Click <b>Read</b> if you only want users to have read access rights. Click <b>Read/Write</b> if you want users to have read and write access rights.</li></ul></div>

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



### Configuring Firewall Parameters

Firewall is an appliance to stop people accessing a computer without permission. Click **Firewall** to set firewall parameters.

FIGURE 101 CONFIGURING THE FIREWALL

Firewall

Block PING Request

Block PING Request

☐ Enable ☒ Disable

Intrusion Detection

Intrusion Detection

☐ Enable ☒ Disable

Exception List

☐ Allow NetBIOS to pass through Intrusion Detection

☐ Allow EPMAP (port:135) to pass through Intrusion Detection

Apply

Cancel

---

#### Block PING Request

Block PING Request	Click <b>Enable</b> to activate the Block PING Request feature.
--------------------	---

#### Intrusion Detection

Intrusion Detection	Click <b>Enable</b> to activate intrusion detection.
---------------------	--

Exception List	Check if <b>Allow NetBIOS to pass through Intrusion Detection</b> . Check if <b>Allow EPMAP (port:135) to pass through Intrusion Detection</b> .
----------------	---

---

Click **Apply** to confirm the settings.

## Configuring Proxy

The network administrator is allowed to enable Transparent Proxy feature at the Router terminal for further controlling the efficiency accessing to internal network in LAN and reducing the bandwidth requesting access to Internet, currently only supporting HTTP protocol. When HTTP Transparent Proxy function is enabled, the administrator must set up a proxy server to work additionally. Once a HTTP request packet sent from user within internal LAN, this packet will be transferred to the Proxy Server through Router. The Proxy Server will require HTTP response web page in cache and will respond or defer the HTTP request packet to the Internet. This would greatly reduce the request of bandwidth accessing to the Internet. In fact, users within internal LAN can access to the Internet via the Proxy Server but not be aware of the existence of this Proxy Server, so this feature called Transparent Proxy.

The administrator is allowed to set the schedule for Proxy to be activated and decide which days and which time during a week he/she wants the schedule to be applicable. Transparent Proxy function will be active only in selected periods. To set up Schedule, you can create schedules through **Configuration → Network Object → Schedule** and select the schedule for when you want Transparent Proxy to be applicable through **Configuration → Advanced → Proxy**.

The administrator can set up exception IP address for flexible network management. The Exception IP packets will not be conducted through the Proxy Server even if Transparent Proxy function activated. To set up Exception IP, you can add IP address through **Configuration → Network Object → Address** and exclude specified IP address from the Exception IP list through **Configuration → Advanced → Proxy**.

1. Select **Configuration → Advanced → Proxy** to enable Transparent Proxy. In the Proxy Parameters screen, check the **Http Transparent Proxy Enable** radio button.

Proxy	
Parameters	
Http Transparent Proxy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Proxy Server IP Address	<input type="text"/> <a href="#">Candidates</a>
Proxy Server Port	<input type="text"/>
<a href="#">Schedule</a>	<b>**Always On</b>
<a href="#">Exception Address</a>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	<b>**Any</b>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. You can either fill in **Proxy Server IP Address** blank, or click **Candidates** link to select the IP address you want to assign, and then input port value in the **Proxy Server Port** field.

Proxy	
Parameters	
Http Transparent Proxy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Proxy Server IP Address	192.168.1.35 <a href="#">Candidates</a>
Proxy Server Port	8080
<a href="#">Schedule</a>	<b>**Always On</b>
<a href="#">Exception Address</a>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	<b>**Any</b>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3. Select the Schedule for this Transparent Proxy to be active from the drop-down menu. Click **Enable** to activate Exception Address and select the exception IP address from the drop-down menu.

Proxy	
Parameters	
Http Transparent Proxy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Proxy Server IP Address	<input type="text" value="192.168.1.35"/> <a href="#">Candidates</a> ▶
Proxy Server Port	<input type="text" value="8080"/>
<a href="#">Schedule</a> ▶	proxy schedule ▼
<a href="#">Exception Address</a> ▶	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	exception ip address ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	


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

Configuring L2TP Parameters

The Layer 2 Tunnel Protocol (L2TP) is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs. L2TP acts like a data link layer (layer 2 of the OSI model) protocol for tunneling network traffic between two peers over an existing network (usually the Internet).

Click **L2TP** to view the L2TP list.

FIGURE 102 L2TP TABLE

L2TP						
L2TP List						
#	Status	Connection Name	Remote IP	Type		
Create 						

#	Displays the number of L2TP connections.
Status	Displays the current status of the L2TP connection (Active or Inactive).
Connection Name	Displays the name of the L2TP connection.
Remote IP	Displays the remote IP of the L2TP connection.
Type	Displays whether the connection is Dialin or Dialout.

Click **Create** to add a new L2TP connection to the list.

FIGURE 103 L2TP CONFIGURATION SCREEN

L2TP Config

Create

L2TP Setup

☒ Enable ☐ Disable

Connection Name

Idle Timeout

seconds

Auth Type

pap

User Name

Password

Type

☒ Dialin ☐ Dialout

Connection Type

☒ Remote Access ☐ LAN to LAN

Peer Network IP

Peer Netmask

Private IP assigned to Dialin User

Remote IP

Apply

Cancel

L2TP Setup	Select whether to <b>Enable</b> or <b>Disable</b> L2TP.
Connection Name	Enter the name of the L2TP connection.

---



---

Idle Timeout	The idle timeout period in seconds. If the connection has been idle for longer than the idle timeout time, then the connection will be disconnected.
Auth Type	There are two authentication types you can choose from the drop-down menu. There two types are <b>pap</b> and <b>chap</b> .
User Name	Enter the user name for the L2TP connection.
Password	Enter the password for the L2TP connection.
Type	Select the type; to dialin (server) or dialout (client).
Connection Type	Select the connection type; Remote Access or LAN to LAN. Remote access allows you to connect to a remote IP, where as LAN to LAN allows you to connect to a remote IP and other IP addresses behind that IP address.
Peer Network IP	Only available when you select Connection Type: LAN to LAN. Please enter the Peer Network IP.
Peer Netmask	Only available when you select Connection Type: LAN to LAN. Please enter the Peer Netmask.
Private IP assigned to Dialin User	Only available when you select Type: Dialin. Please enter the IP address for the Private IP that is assigned to user.
Remote IP	Only available when you select Type: Dialout. Please enter the IP address for the Remote IP that you will be connected to.

---



---

Click **Apply** to confirm the settings.

Managing Device Parameters

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

FIGURE 104 CHANGING PARAMETERS

Device Management		
Device Name		
Name	SSLVPN.gateway	
DNS Backup		
DNS Backup	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
IP Address		
Embedded Web Server		
HTTP Port	80	(80 is default HTTP port)
HTTPS Port	443	(443 is default HTTPS port)
Configuration	<input type="checkbox"/> Same subnet is required to access remote configuration	
SSL Protocol	<input checked="" type="checkbox"/> SSL V2 <input checked="" type="checkbox"/> SSL V3 <input checked="" type="checkbox"/> TLS	
SSL Encryption	<input type="checkbox"/> Key length ≥ 128 bits	
Central Management Server		
CMS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
IP Address/Domain Name		
CMS Server Port	8443	(8443 is default CMS Server Port)
Resync Period	1 minute	
Telnet Setup		
Telnet Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Telnet Port	23	(23 is default Telnet port)
Interface	LAN	
Configurable Address	**Any	
Dial-In Setup		
Dial-In	<input type="radio"/> Enable Dial-In but Disable CLI <input type="radio"/> Enable CLI but Disable Dial-In <input checked="" type="radio"/> Disable CLI and Dial-In	
Baudrate Setting	57600bps(14.4K/28.8K modem)	
Init-String	ATSD=0Q0&D3&C1	
Server IP Address Assign	10.0.0.1	
Client IP Address Assign	10.0.0.2	
CLI Setup		
CLI Account	<input type="radio"/> User Defined <input checked="" type="radio"/> System Default	
User Name	admin	
Password	*****	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Device Name

Name Enter a given name in the Name field to distinguish it from other gateway devices on the network. The value of the field will be shown on the status page so that the administrator can identify the device after login.

DNS Backup

DNS Backup Click **Enable** to use the DNS Backup feature.

---

IP Address	Enter the DNS server's IP Address if you want to use this DNS backup when WAN interface can't connect.
------------	--

<b>Embedded Web Server</b>	
HTTP Port / HTTPS Port	BiGuard S20 allows a user to modify the default port number of HTTP and HTTPS, which are 80 and 443 respectively. Modifying the well-known port numbers can prevent from hacker or internet robot access your site easily.
Configuration	Check the check box if you want to restrict remote configuration access only to people that are within the same subnet as the device.
SSL Protocol	Check the check box to enforce the selection of SSL protocol. Default protocol is auto-negotiation.
SSL Encryption	Check the check box to enforce the higher security of SSL Encryption which key length is more than 128 bits. Default key length is auto-negotiation.

<b>Central Management Server</b>	
CMS	Central Management Server is able to manage several servers which configures S6000 at one time. Click the <b>Enable</b> radio button if you want to enable this function.
IP Address/ Domain Name	Enter the IP Address or Domain Name for the CMS server.
CMS Server Port	Enter the CMS server port, the default is 8443.
Resync Period	Resynchronization period time. The time period that the router and CMS server will communicate with each other (measured in minutes).

<b>Telnet Setup</b>	
Telnet Server	Allow a user to manage the device with telnet if enabled.
Interface	Check the check box to enable telnet access from WAN. For security concern, the default setting only allows access from LAN.
Telnet Port	Enter the Telnet port, the default is 23.

<b>Dial-In Setup</b>	
Dial-In	With <b>Dial-In</b> enabled, administrator can use dial-in modem to perform router configurations through the terminal and web interface.
Baudrate Setting	The <b>Baudrate Setting</b> can be adjusted according to the speed of the modem that will establish a connection with the router.

---

---

Init-String	<b>Init-String</b> are used to configure the modem's options for things like error correction, data compression, flow control and much more. Please look up in your modem manual for the suitable init-string as the incorrect init-string can cause the connection to fail.
Server IP Address Assign	Enter the address in the <b>Server IP Address Assign field</b> that the administrator will access through the modem connection.
Client IP Address Assign	Enter the address in the <b>Client IP Address Assign field</b> that the administrator will be assigned to through the modem connection.

**CLI Setup**

CLI Account	Select either <b>User Defined</b> or <b>System Default</b> user name; and enter password for the CLI login account.
User Name	Enter a given name for the <b>User Defined</b> CLI Account.

---

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



## 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.

**Portal Logo:** 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.

**Product Logo:** This option toggles whether or not the name of the device and the device image will be displayed at the top of the Portal page.

**Default Greeting String:** The default greeting string can also be changed. Just type the desired text string into the Default Greeting String.

**Encoding of Network Place and CIFS application:** This option enables you to set the encoding language character set for Network Place and CIFS applications.

**Login Default Domain:** You can set a new default domain for the login screen from the list in the drop-down menu.

**Login Logo:** You can select the default logo or change to a new login logo by selecting the **Uploaded Logo** option, and click Browse to choose your image or icon.

**Login Greeting String:** The login greeting string displayed at the login screen can be changed here.

**Login Screen:** You can choose between **Default** and **Customization**. The **Default** login screen is the current screen showing BiGuard images for the background of the login screen. The **Customization** login screen has no BiGuard images and it is very plain looking.

**Remember Password:** Select Enable to allow user password to be remembered.

Click the **Apply** button to save your settings for this session.


FIGURE 105 PORTAL LAYOUT

Portal Layout

Portal

Portal Logo

☒ Default Logo



☐ Uploaded Logo

Note!

Uploaded logo with 911 x 72 pixels is better. And its size should smaller than 50 kbytes.

Product Logo

☒ Enable ☐ Disable

Default Greeting String


Encoding of Network Place and CIFS application

Login

Login Default Domain

Login Logo

☒ Default Logo



☐ Uploaded Logo

Note!

Uploaded logo with 170 x 22 pixels is better. And its size should smaller than 5 kbytes.

Login Greeting String

Login Screen

☒ Default ☐ Customization

Remember Password

☒ Enable ☐ Disable

Authentication Domain

The **Authentication Domain** item enables you to add domains to the domain table that will be authenticated by the server. The BiGuard S20 verifies that users who log on to the system are in an authenticated domain.

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

FIGURE 106 AUTHENTICATION DOMAIN TABLE

## Authentication Domain

Domain Table				
Domain Name	Authentication Type	Auth. Server IP Address		
BiGuard	local	Local Machine	Machine's Default Domain	
Create				

CREATING A DOMAIN

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



**NOTE:** To edit or delete a current Domain, you must first create a new domain.

FIGURE 107 DOMAIN AUTHENTICATION TYPES SCREEN

Authentication Domain	
Add Domain	
Domain Name	<input type="text"/>
Authentication Type	Local User Database
Apply	Cancel
	RADIUS - PAP RADIUS - CHAP RADIUS - MSCHAP RADIUS - MSCHAPV2 NT Domain Active Directory LDAP Local User Database

Domain Name	Enter a name for the domain.
<b>Authentication Type</b>	
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. PAP 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. However, 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 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. Since it is built on the Internet's Domain Naming System (DNS), workgroups can be given domain names, as well as 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 S20, 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.

Click **Apply** to confirm the settings.

### **EDITING A DOMAIN**

Refer to the following to edit a domain:

1. In the Authentication Domain menu, click **Edit** next to the item you want to change.

Authentication Domain				
Domain Table				
Domain Name	Authentication Type	Auth. Server IP Address		
BiGuard	local	Local Machine	Machine's Default Domain	
test1	local	Local Machine	<a href="#">Edit</a>	<a href="#">Delete</a>
test2	radius_pap	192.168.1.2	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>				

The Edit screen appears.

- In the Edit Domain screen, change Authentication Domain parameters as desired.

Authentication Domain	
Edit Domain	
Domain Name	test2
Authentication Type	RADIUS - PAP
Server Address	192.168.1.2
Secondary Server Address	
Secret Password	test2
Server Port	1812
Retry Times	2
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



**NOTE:** Once you have created the Domain, the authentication type of this Domain is unable to be changed.

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

### DELETING A DOMAIN

Refer to the following to delete a domain:

- In the Authentication Domain menu, click **Delete** next to the item you want to remove.

Authentication Domain				
Domain Table				
Domain Name	Authentication Type	Auth. Server IP Address		
BiGuard	local	Local Machine	Machine's Default Domain	
test1	local	Local Machine	<a href="#">Edit</a>	<a href="#">Delete</a>
test2	radius_pap	192.168.1.2	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>				

- The Delete screen appears.

Authentication Domain	
Delete Domain	
Domain Name	test2
Authentication Type	RADIUS - PAP
Server Address	192.168.1.2
Secret Password	test2
Server Port	1812
<b>Warning!</b> Deleting this domain will also delete the groups and users under it.	
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

- Click **Delete** to remove the domain.

## 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 authentic domain, and then add only the applications that you want group members to access.

### **GROUP**

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

**FIGURE 108 GROUP/APPLICATION TABLE SCREEN**

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
BiGuard	BiGuard	Yes	Disable	Edit	
Create					

The Group Table 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 108), click **Create**. The Add Group screen appears.

Edit Group						
General Settings						
Group Name	<input type="text"/>					
Domain	BiGuard					
Password Policy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>					
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable					
Inactivity Timeout	<input type="text" value="5"/> Minutes					
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable					
Service						
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>					
Transport Extender Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>					
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>					
Application Table						
<a href="#">Add Application</a>						
Name	Application	IP Address / Path				
<b>Note!</b> To make application changes, press <b>Apply</b> .						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>						

2. Enter a given name in the **Group Name** field.
3. Select a domain where the given group will be from the **Domain** drop-down menu .
4. Choose whether you want to Enable or Disable **Password Policy** by configuring the rules in the **Advanced Setting**.

5. Choose whether you want to Enable or Disable **Force Login** which when enabled allows the username currently logged into the router to be forced to log out by the next person logging in with the same username.
6. Set the time in minutes for **Inactivity Timeout**, so the users will be automatically logged out of the router after a certain time of idleness.
7. Choose whether you want to Enable or Disable **Host Checking**.
8. Enable/Disable **Network Place**.
9. Enable/Disable **Network Extender Services** (Check the check box for a user acquiring **Standalone Application**. The user is able to download a Network Extender program which can be used to connect to Network Extender Service without going through the Web Portal.).
10. Enable/Disable **Transport Extender** (In **Advanced Settings** of Transport Extender, it allows you to set exclusive Transport Extender tunnel for the user.).
11. Enable/Disable **Web Cache Cleaner**.
12. Modify the **Greeting String** field as desired.
13. Check the applications that will be available to the user in the **Applications** field.
14. Click **Apply** to confirm the settings.
15. Click **Add Application** to make applications available to the group.

SSL VPN Application	
<b>Add Application</b>	
Application Name	<input type="text"/>
Application	Terminal Service (RDP) <input type="button" value="v"/>
IP Address/Domain Name	<input type="text"/>
Screen Size	640 x 480 <input type="button" value="v"/>
Local Device	<input type="checkbox"/> Drives
	<input type="checkbox"/> Ports
	<input type="checkbox"/> Printers
	<input type="checkbox"/> Smart Cards
Console Mode	<input type="checkbox"/> Active
Single Sign On Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Application and Path	<input type="text"/>
Terminal Server Port	3389
Log on to	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

16. Enter a name in the **Application Name** field.
17. Select an application from the **Application** drop-down menu.  
See [SSL VPN Applications Overview](#) on page 169.
18. Click **Apply** to confirm the settings.

### Editing Group parameters

Refer to the following to edit the parameters of a group:

1. In the Group/Application Group Table menu, click **Edit** next to the item you want to change.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
Test	BiGuard	No	Disable	<a href="#">Edit</a>	<a href="#">Delete</a>
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

The Edit screen appears.

- In the Edit screen, add an application to associate with the group.

Edit Group		
General Settings		
Group Name	Test	
Domain	BiGuard	
Password Policy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>	
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	<input type="text" value="5"/> Minutes	
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Service		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
	<input type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>	
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>	
Application Table		
<a href="#">Add Application</a>		
Name	Application	IP Address / Path
<b>Note!</b> To make application changes, press <b>Apply</b> .		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

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

## Deleting Groups

Refer to the following to delete a group from the Group Application table.

- In the Group/Application Group Table menu, click **Delete** next to the item you want to remove.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
Test	BiGuard	No	Disable	<a href="#">Edit</a>	<a href="#">Delete</a>
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

The Delete screen appears.



2. In the Delete screen, click **Delete** to remove the group from the Delete Group list.

Delete Group	
<b>Setting Values</b>	
Group Name	Test
Authentication Domain	BiGuard
Inactivity Timeout	5
Host Checking	Disable
<b>Warning!</b> Deleting this group will also delete the users under it.	
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

## APPLICATIONS

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.

In the Group/Application table menu, click **Edit** to add or edit applications for the selected group.

### Creating a Group Application

Refer to the following to create a group's application parameters:

1. In the Edit Group screen, click on **Add Applications** to enter the Add Applications screen (seen below).

Edit Group			
<b>General Settings</b>			
Group Name	Test		
Domain	BiGuard		
Password Policy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>		
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Inactivity Timeout	5	Minutes	
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
<b>Service</b>			
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>		
	<input type="checkbox"/> Standalone Application (Win32 Only)		
Transport Extender Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>		
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>		
<b>Application Table</b>		<input checked="" type="button" value="Add Application"/>	
Name	Application	IP Address / Path	
<b>Note!</b> To make application changes, press <b>Apply</b> .			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- In the Add Applications screen, type in the name in the **Application Name** field, and select an application from the drop-down menu.

SSL VPN Application	
<b>Add Application</b>	
Application Name	<input type="text"/>
Application	Terminal Service (RDP) ▾
IP Address/Domain Name	<input type="text"/>
Screen Size	640 x 480 ▾
Local Device	<input type="checkbox"/> Drives
	<input type="checkbox"/> Ports
	<input type="checkbox"/> Printers
	<input type="checkbox"/> Smart Cards
Console Mode	<input type="checkbox"/> Active
Single Sign On Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Application and Path	<input type="text"/>
Terminal Server Port	3389
Log on to	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- After selecting the application to add, fill in the required information and click **Apply** to save the settings.

### Editing Applications

Refer to the following to edit a group's application parameters:

- In the Edit Group Application Table menu, click **Edit** next to the application you want to change.

Edit Group			
<b>General Settings</b>			
Group Name	Test		
Domain	BiGuard		
Password Policy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<a href="#">Advanced Setting</a>	
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Inactivity Timeout	5	Minutes	
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
<b>Service</b>			
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
<a href="#">Network Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>		
	<input type="checkbox"/> Standalone Application (Win32 Only)		
<a href="#">Transport Extender Service</a>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>		
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>		
<b>Application Table</b> <a href="#">Add Application ▶</a>			
Name	Application	IP Address / Path	
RDP	RDP	1.1.1.1	<input checked="" type="button" value="Edit ▶"/> <input type="button" value="Delete ▶"/>
<b>Note!</b> To make application changes, press <b>Apply</b> .			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

The Edit Application screen appears.

SSL VPN Application	
Edit Application	
Application Name	RDP
Application	Terminal Service (RDP)
IP Address/Domain Name	1.1.1.1
Screen Size	640 x 480
Local Device	<input type="checkbox"/> Drives
	<input type="checkbox"/> Ports
	<input type="checkbox"/> Printers
	<input type="checkbox"/> Smart Cards
Console Mode	<input type="checkbox"/> Active
Single Sign On Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Application and Path	
Terminal Server Port	3389
Log on to	BiGuard
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. In the **Edit** screen, change the settings relating to the application.
3. Click **Apply** to confirm the settings.
4. The Edit Group table displays, click **Apply** to confirm the settings.

### Deleting Group Applications

Refer to the following to delete the application parameters of a group:

1. In the Edit Group/Application Table menu, click **Delete** next to the application you want to delete.

Edit Group				
General Settings				
Group Name	Test			
Domain	BiGuard			
Password Policy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<a href="#">Advanced Setting</a>		
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	5	Minutes		
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<a href="#">Network Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>		
<a href="#">Transport Extender Service</a>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<a href="#">Advanced Setting</a>		
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom	Welcome to SSL/IPSEC \		
Application Table		<a href="#">Add Application</a>		
Name	Application	IP Address / Path		
RDP	RDP	1.1.1.1	<a href="#">Edit</a>	<a href="#">Delete</a>
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

The Delete Application screen appears.

- In the Delete screen, click the **Delete** button to delete the current application.

SSL VPN Application	
Delete Application	
Application Name	RDP
Application	Terminal Service (RDP)
IP Address/Domain Name	1.1.1.1
Screen Size	640 x 480
Local Drives	Not Connect to Remote Host
Local Ports	Not Connect to Remote Host
Local Printers	Not Connect to Remote Host
Local Smart Cards	Not Connect to Remote Host
Mode	Not Console Mode
Singel Sign On	Enable
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

- 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.

Click **SSL VPN** → **User Access** → **Group/Application** → **Edit** → **Add Application**. The SSL VPN Application screen lets you add the following applications:

FIGURE 109 SSL VPN APPLICATION CHOICES

SSL VPN Application

Add Application

Application Name	<input type="text"/>
Application	Terminal Service (RDP) ▼
IP Address/Domain Name	Terminal Service (RDP)
Screen Size	Virtual Network Computing (VNC)
	File Transfer Protocol (FTP)
	Telnet
	Secure Shell (SSH)
	Secure Shell version 2 (SSHv2)
Local Device	Web (HTTP)
	Secure Web (HTTPS)
	Network File Share (CIFS)
	Terminal Service (RDP) - Java
	Citrix(HTTP)
	Wake On LAN(WOL)
Console Mode	
Single Sign On Function	
Application and Path	<input type="text"/>
Terminal Server Port	3389
Log on to	<input type="text"/>

ApplyCancel

Application Name	Enter a given application name.
Terminal Service (RDP)	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. RDP (ActiveX) - RDP is the current version and provides session sound and full-screen mode. RDP 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.
Secure Shell version 2 (SSHv2)	SSHv2 (Secure Shell version 2) is a completely overhauled version of the protocol.
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.).
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.
Network File Share (CIFS)	The Common Network File Share (CIFS) protocol allows a user in a group remote access through the web portal to directed and specific network paths as predefined by the network administrator.
Terminal Service(RDP)-Java	Java version of the Windows Terminal Server, that 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. RDP (ActiveX) - RDP is the current version and provides session sound and full-screen mode. RDP is only available in an ActiveX client.
Citrix(HTTP)	Select this option if you have a Citrix Presentation Server that you wish to connect to. Citrix Presentation Server is a remote access/application publishing product that allows people to connect to applications available from central servers.
Wake On LAN(WOL)	WOL allows the router to set a command to turn on a particular computer that can support this feature.
IP Address/Domain Name	Enter an IP Address or Domain Name.
Screen Size	Select the screen size of Application window from <b>Screen Size</b> drop-down menu. There are 640*480,800*400,1024*768 and full screen.
Local Device	The devices you choose will automatically connected to the remote PC when you log in remote PC.
Console Mode	To start the Console Mode when check <b>Active</b> check box.

Single Sign On Function	<p><b>Enable:</b> When a password and an account are the same in both log in account and remote PC account, it will connect directly on the remote PC. You do not need to retype the account and password.</p> <p><b>Disable:</b> Close Single Sign On Function.</p>
Application and Path	To start a program when a user accesses. For example, Excel or Word.
Terminal Server Port	<p>Enter the port value as a host in this field.</p> <p>On Windows, the Terminal Services client use TCP port 3389 by default.</p>
Log on to	Enter a domain name to log on to the domain from the remote web portal.

### ADDING THE TERMINAL SERVICE (RDP) APPLICATION

Refer to the following to add the application:

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

SSL VPN Application	
<b>Add Application</b>	
Application Name	<input type="text"/>
Application	Terminal Service (RDP) ▼
IP Address/Domain Name	<input type="text"/>
Screen Size	640 x 480 ▼
Local Device	<input type="checkbox"/> Drives
	<input type="checkbox"/> Ports
	<input type="checkbox"/> Printers
	<input type="checkbox"/> Smart Cards
Console Mode	<input type="checkbox"/> Active
Single Sign On Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Application and Path	<input type="text"/>
Terminal Server Port	3389
Log on to	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Select **Terminal Service (RDP)** from the **Application** drop-down menu.
3. Enter 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. Enter a name in the **Application Name** field.

SSL VPN Application	
Add Application	
Application Name	<input type="text"/>
Application	Virtual Network Computing (VNC) ▼
IP Address/Domain Name	<input type="text"/>
TCP Port Number	5900
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. Select an item from the **Application** drop-down menu.
3. Enter 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 S20 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 110 ACCOUNT MANAGEMENT SCREEN**

Account				
Account Table				
Name	Group			
admin	BiGuard	Edit		
Create Move				

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 111 ADMIN ACCOUNT SETTINGS SCREEN**

Edit Account		
General Setting		
Name	admin	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Login Setting		
Password	*****	
Retype Password	*****	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	100	Minutes
Service		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
Application Proxy		
Applications	This group has no application now.	
Apply Cancel		

---

### General Setting

---

---



---

Name	Displays the name of the account. You can not change the name of the admin account.
Active	Check this box to allow the user account to be able to log in to BiGuard SSL VPN. The account is not able to perform if it does not be checked.
Group	Displays the Group the account belongs to.
Group Setting	Inherit Account Setting form Group Setting. <b>Enable</b> if you want to inherit the Account Setting. <b>Disable</b> if you do not want to inherit the Account Setting.

### Login Setting

Password/ Retype Password	Enter and confirm the password. Also can use group default password when set the <b>Password Policy</b> under group.
Host Checking	When Host Checking is checked on Active check box, the user will be checked to see if their account have satisfied the criteria to use services through the Web Portal. The <b>Advanced Setting</b> link leads to the configuration page for the Host Checking criteria. See <a href="#">Configuring Host Checking</a> on page 184.
Force Login	Force Login which when enabled allows the username currently logged into the router to be forced to log out by the next person logging in with the same username
Inactivity Timeout	Displays the amount in minutes of inactivity before a user is automatically logged out. The default setting is 5 minutes.

### Service

Network Place	When enabled, the user can use Network Place to log onto the SSL VPN. See <a href="#">Accessing Network Place</a> on page 229.
Network Extender Service	When enabled, the user can use Network Extender to log onto the SSL VPN. See <a href="#">Installing the Network Extender</a> on page 217.
Transport Extender Service	When enabled, the user can use Transport Extender to log onto the SSL VPN. See <a href="#">Installing the Transport Extender</a> on page 225.
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 <b>Dynamic Assign</b> to assign a new IP address each time the user logs on. Select <b>Fix IP</b> to assign the same IP address each time the user logs on for better monitoring of network activity.
Greeting String	Displays the greeting text when the user log on.

---



---

<b>Application Proxy</b>	
Applications	Lists the applications that are available to the group the user belongs to. See <a href="#">Using Applications</a> on page 230.
Click <b>Apply</b> to confirm the settings.	

### CREATING A NEW USER ACCOUNT

User accounts enable specific users access to services and applications that you define in the **Group/Application** menu item. See [Group/ Application](#) on page 162.

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"/>	<input checked="" type="checkbox"/> Active
Group	BiGuard ▾	
Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Use group default password
Host Checking	<input type="checkbox"/> Active	<a href="#">Advanced Setting</a>

Apply

Cancel

#### Group Setting Details








Force Login	Disable
Inactivity Timeout	5 Minutes
Network Place	Enable
Network Extender Service	Enable
Transport Extender Service	Disable
Web Cache Cleaner	Enable
Greeting String	Use default greeting string
Applications	There had no applications.

3. Enter a user name in the **User Name** field.
4. Select a group of the user will belong to from the **Group** drop-down menu. See [Group/ Application](#) on page 162.
5. Enter a password in the **Password/Retype Password** fields. Also can use group default password when set the **Password Policy** under group.
6. Check/uncheck the **Active** check box to activate/deactivate **Host Checking** on the particular user account.
7. Click **Apply** to confirm the settings.

### EDITING USER ACCOUNT PARAMETERS

Refer to the following to edit user account parameters:

1. In the Account menu, click **Edit** next to the item you want to change.

Account				
Account Table				
Name 	Group			
admin	BiGuard	<a href="#">Edit </a>		
test1	BiGuard	<a href="#">Edit </a>	<a href="#">Delete </a>	<a href="#">Copy </a>
<a href="#">Create </a> <a href="#">Move </a>				

The Edit screen appears.

- In the Edit screen, check enable or disable **Group Setting**. If you choose **Enable**, the Service parameters are inherited automatically to the account, so that the other Service options can not be chosen. If you choose **Disable**, you can change parameters as desired for this user account.

Edit Account		
<b>General Setting</b>		
Name	test1	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>Login Setting</b>		
Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	5	Minutes
<b>Service</b>		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>	
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	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>	
<b>Application Proxy</b>		
Applications	This group has no application now.	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

- Force Login** which when enabled allows the username currently logged into the router to be forced to log out by the next person logging in with the same username.
- Enter a period of time of logging out inactive user in the **Inactivity Timeout** field.
- Enable/disable **Network Place**.
- Enable/disable **Network Extender Services** (Check the check box for a user acquiring **Standalone Application**. The user is able to download a Network Extender program which can be used to connect to Network Extender Service without going through the Web Portal.).
- Enable/disable **Transport Extender** (in **Advanced Settings** of Transport Extender, it allows you to set exclusive Transport Extender tunnel for the user).
- Enable/disable **Web Cache Cleaner**.
- If **Network Extender Service** is enabled, **Dynamic Assign** or **Fix IP** in the **Network Extender IP Assignment** field are available.
- Modify the **Greeting String** field as desired.
- Check the applications that will be available to the user in the **Applications** field.
- Click **Apply** to confirm the settings.



**NOTE:** The Advance Setting for Network Extender Service is almost the same in Group/Application setting. See [Advance Setting for Network Extender Service](#) on page 188.

There is a sort function next to the Name column which will sort the accounts by alphabetical order or reverse order. To save time in creating accounts, there is a **Copy** button where administrators can copy the exact same settings of a previous account onto a new account.

Account				
Account Table				
Name ▲▼	Group			
admin	BiGuard	Edit ▶		
test1	BiGuard	Edit ▶	Delete ▶	Copy ▶
Create ▶ Move ▶				

### DELETING USER ACCOUNTS

Refer to the following to remove a user account:

1. In the Account menu, click **Delete** next to the user account you want to remove.

Account				
Account Table				
Name ▲▼	Group			
admin	BiGuard	Edit ▶		
test1	BiGuard	Edit ▶	Delete ▶	Copy ▶
Create ▶ Move ▶				

The Delete screen appears.

Delete Account	
General Setting	
Name	test1
Group	BiGuard
Inactivity Timeout	5 Minutes
Service	
Network Place	Enable
Network Extender Service	Enable
Transport Extender Service	Disable
Web Cache Cleaner	Enable
Network Extender IP Assignment	Dynamic Assign
Greeting String	Default Greeting String
Delete Cancel	

2. Click **Delete** to remove this account.

## Account Move

Account Move feature enables the administrator to manager user accounts by moving accounts belonging to different groups under different domains that implement different authentication protocols, i.e. accounts which belong to different groups under Local DB Domain, AD Domain, and Radius Domain etc. are allowed to move to each other. Account Move feature is illustrated as follows:

If the company first setup the SSL VPN Router system and then integrate the One Time Password (OTP) system, Account Move function can be used to move accounts that previously belong to AD Group and implement Active Directory (AD) Domain authentication protocol to Radius Group implementing Radius Domain authentication protocol. The administrator is allowed to move all the accounts under the AD Group to Radius Group at one time or select some accounts to Radius Group. This feature makes account management more flexible.

Take the accounts moved from **AD** Group in **AD** domain to **Radius** Group in **Radius** Domain for example to explain the Account Move configuration procedure.

1. Select **SSL VPN** → **User Access** → **Authentication Domain** to create an authentication domain named **Radius**, a Group named **Radius** will be automatically created.

Authentication Domain				
Domain Table				
Domain Name	Authentication Type	Auth. Server IP Address		
BiGuard	local	Local Machine	Machine's Default Domain	
AD	active-directory	192.168.1.115	Edit	Delete
Radius	radius_pap	192.168.1.115	Edit	Delete
Create				

2. After added a Radius domain, go to **SSL VPN** → **User Access** → **Group/Application**. A new Group will be added to the Group Table.

Group/Application				
Group Table				
Name	Authentication Domain	Domain's Default Group	Host Checking	
AD	AD	Yes	Disable	Edit
Radius	Radius	Yes	Disable	Edit
BiGuard	BiGuard	Yes	Disable	Edit
Create				

3. Then select **SSL VPN** → **User Access** → **Account**, click **Move** to move the accounts from **AD** Group to **Radius** Group.

Account				
Account Table				
Name	Group			
John	AD	Edit	Delete	Copy
Mary	AD	Edit	Delete	Copy
George	AD	Edit	Delete	Copy
admin	BiGuard	Edit		
test1	BiGuard	Edit	Delete	Copy
Create Move				

- In Move Account screen, select the domain from the **Domain** drop-down menu, select the group from the **Group** drop-down menu, check the account which you want to move from, and select the group which you want to move to from the **Group** drop-down menu. Click **Apply** to confirm the setting.

Move Account	
<b>Select Domain</b>	
Domain	BiGuard ▼
<b>Move from Group</b>	
Group	BiGuard ▼
<b>Users List</b> <input type="checkbox"/> Select All	
<input type="checkbox"/> admin	<input type="checkbox"/> test1
<b>Move to Group</b>	
Group	AD ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- In this example, administrator select **AD** domain and **AD** group from the **Domain** and **Group** drop-down menu, and check the account **John** to move to **Radius** group from the **Group** drop-down menu. Click **Apply** to confirm the setting.

Move Account	
<b>Select Domain</b>	
Domain	AD ▼
<b>Move from Group</b>	
Group	AD ▼
<b>Users List</b> <input type="checkbox"/> Select All	
<input checked="" type="checkbox"/> John	<input type="checkbox"/> Mary <input type="checkbox"/> George
<b>Move to Group</b>	
Group	Radius ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**NOTE:** If the user account with the password previously verified by the back-end server such as **AD** is moved from an authenticated domain to the other, which the password is not excising and verified by local database of Router such as **Local DB**, the password will be automatically configured to the same with the username of the user account by Router after the account has moved. For example, if an account under **AD** domain with username **John** and password 1234 is moved to **BiGuard** domain, the default password of this user account will be changed to **123**.

**NOTE:** If the user account with the password previously verified by local database of Router such as **Local DB** is moved from an authenticated domain to the other, which the password is verified by the back-end server such as **AD**, the password of the user account will need to be authenticated according to the Authentication Type after the account is moved (the password requires re-verification). For example, create a new account under **BiGuard** Domain, the username and password are **John** and **1234** for it. If this user account is moved to **AD** domain, its password will change automatically as configured with user account under **AD** Domain (it is **a\$12345** in this example). User **John** must input **a\$12345** in the Password field to log on to the web portal. If the account is moved back to **BiGuard** domain, its password will be **1234**.



## Password Policy

Password Policy exists in Group configuration. It allows Administrator to define, how the user can or can not setup their passwords. This allow Administrators to force users to have a password that will not be easily guessed or hacked by malicious attackers.

Refer to the following to turn on and help set the parameters for Password Policy.

1. Select **SSL VPN → User Access → Group/Application** (on the left hand-side menu). **Edit** or **Create** a new group.
2. In the Edit Group or Add Group menu, please enable the **Password Policy** and click on the **Advance Setting**.

Edit Group			
<b>General Settings</b>			
Group Name	BiGuard		
Domain	BiGuard		
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>	
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Inactivity Timeout	5	Minutes	
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
<b>Service</b>			
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>	
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)		
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>	
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom	Welcome to SSL/IPSEC \	
<b>Application Table</b>		<a href="#">Add Application</a>	
Name	Application	IP Address / Path	
<b>Note!</b> To make application changes, press <b>Apply</b> .			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

3. The Password Policy Parameters screen displays. Enter the information in every fields.

Password

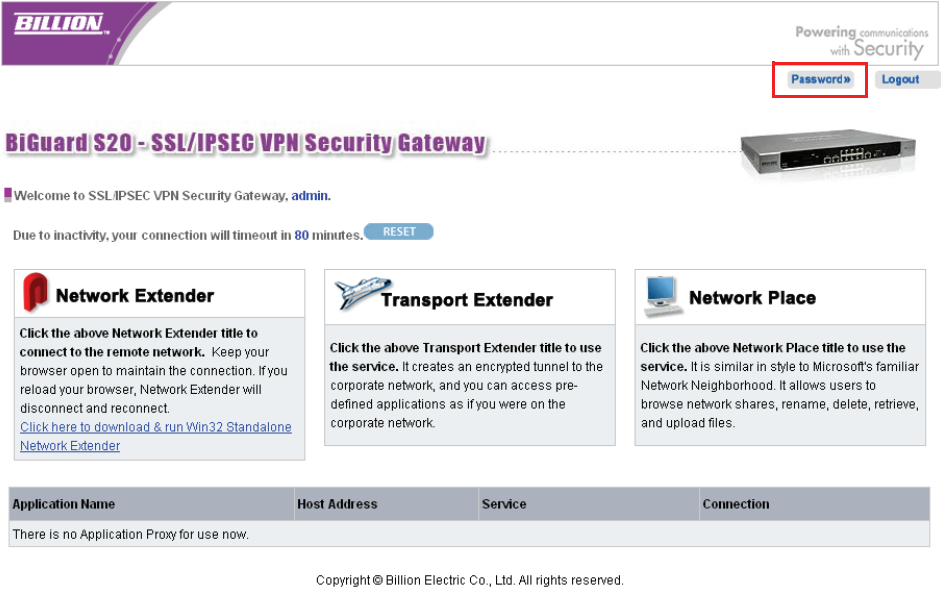
Parameters

Group Name	BiGuard		
Password Rules (Must Contain)	<input type="checkbox"/> Minimum 8 characters	<input type="checkbox"/> Uppercase	
	<input type="checkbox"/> Lowercase	<input type="checkbox"/> Special Symbols	
Default Password	<input type="text"/>		
Retype Default Password	<input type="text"/>		
Retry Password Count	<input type="text" value="0"/>	Times	
Retry Password Timeout	<input type="text" value="0"/>	Minutes	
Allow Password Change	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
<div>ApplyCancel</div>			

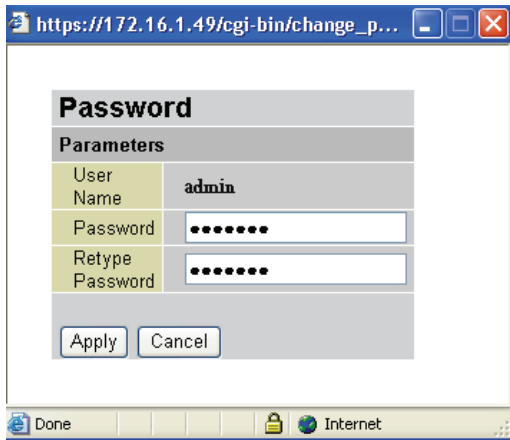
Password Rules (Must Contain)	Check the box for <b>Minimum 8 characters</b> to force user to have 8 or more characters. Check the box for <b>Uppercase</b> to force user to have a password which must contain an uppercase letter. Check the box for <b>Lowercase</b> to force user to have a password which must contain a lowercase letter. Check the box for <b>Special Symbols</b> to force user to have a password which must contain a special character.
Default Password	Enter the default password for the users to login before the users change their own passwords.
Retype Default Password	Enter the default password again.
Retry Password Count	Enter the number of times a user can retry the password during login. When the number of failed tries is exceeded, the user account will be locked for the duration of minutes entered in <b>Retry Password Timeout</b> .
Retry Password Timeout	Enter the number of minutes a user account will be locked.
Allow Password Change	Select Enable to allow the users to change their password after logging in to the Portal web page.

4. Click **Apply** to confirm the settings. In Edit Group screen, click **Apply** again.
5. Select **SSL VPN** → **SSL VPN Portal**, the web portal screen appears.
6. After enabling **Allow Password Change** the user can find a **Password** link at the top right corner of the page which allows them to change their account password.

FIGURE 112 WEB PORTAL SCREEN



7. Click on the Password link will open up a pop-up window which will allow the user to change the account password. Click **Apply** when finished.



## Configuring Host Checking

Host Checking feature allows administrator to assign security checking for client integrity. The function of Host Checking is available for each individual client account to double check account information by three rules as follow:

- Host name: The host name of the user account.
- IP address: The IP address of the user account.
- MAC address: The MAC address of the user account.

When Host Checking is enabled and active, user will be required a security check for authenticity of the account information if his/her password was verified. Succeeding to meet the security checks will result in user able to logon to the Router.

1. Select **SSL VPN** → **User Access** → **Group/Application** (on the left hand-side menu). Click **Edit** or **Create** to either Edit an existing group or Create a new group.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
Test	BiGuard	No	Disable	<a href="#">Edit</a>	<a href="#">Delete</a>
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

2. In the Edit Group or Add Group menu, please **Enable** Host Checking for the entire group.

Edit Group				
General Settings				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	<input type="text" value="5"/> Minutes			
Host Checking	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
	<input type="checkbox"/> Standalone Application (Win32 Only)			
Transport Extender Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>			
Application Table				
<a href="#">Add Application</a>				
Name	Application	IP Address / Path		
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

3. After enabling Host Checking for the Group, please proceed to add a new user account or edit an existing account that is associated with the Group that has Host Checking enabled.

Account				
Account Table				
Name	Group			
admin	BiGuard	<a href="#">Edit</a>		
test1	BiGuard	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Copy</a>
<a href="#">Create</a> <a href="#">Move</a>				

4. Select **SSL VPN** → **User Access** → **Account** (on the left hand-side menu). You can either **Edit** or **Create** an account to locate the link to **Advance Setting** for Host Checking. Please make sure that the **Active** box is checked to turn Host Checking on for this particular user account.

Edit Account		
General Setting		
Name	admin	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Login Setting		
Password	.....	
Retype Password	.....	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	100	Minutes
Service		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
Application Proxy		
Applications	This group has no application now.	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

5. In Host Checking Advanced Setting screen, check the **Host Name** radio button, click **Enable** Check Host Name, and enter the name you want to check in the **Host Name** field. Press **Add** to save the setting and a new rule will be added to the Host Name List.

### Host Checking Advanced Setting

☒ Host Name
 ☐ IP Address
 ☐ MAC Address

#### Host Name Setting

Check Host Name
 ☒ Enable
 ☐ Disable

#### Add Host Name

Host Name

#### Host Name List

Number	Host Name	Edit	Delete
1	hua	<input type="radio"/>	<input type="checkbox"/>



**NOTE:** When more than one items list in the Host Name List, the computer on client side needs to match only one of the rules so that the check can pass.

- In Host Checking Advanced Setting screen, check the **IP Address** radio button, click **Enable** Check IP Address, and select the address you want to check from the **Address** drop-down menu. Press **Add** to save the setting and a new rule will be added to the IP Address List.

### Host Checking Advanced Setting

☐ Host Name
 ☒ IP Address
 ☐ MAC Address

#### IP Address Setting

Check IP Address
 ☒ Enable
 ☐ Disable

#### Add IP Address

Address

#### IP Address List

Name	IP Address	Subnet Mask/Range	Delete
192.168.1.111	192.168.1.111		<input type="checkbox"/>



**NOTE:** When more than one items list in the IP Address List, the computer on client side needs to match only one of the rules so that the check can pass.

**NOTE:** The options in **Address** drop-down menu under **Add IP Address** field are the source IP addresses for users which have to be created previously in Address Create screen through **Network Object** → **Address**.

- In Host Checking Advanced Setting screen, check the **MAC Address** radio button, click **Enable** Check MAC Address, and enter the address you want to check in the **MAC Address** field. Press **Add** to save the setting and a new rule will be added to the MAC Address List. After the settings have been done already, click **Apply** to set the configuration.

### Host Checking Advanced Setting

☐ Host Name
 ☐ IP Address
 ☒ MAC Address

#### MAC Address Setting

Check MAC Address
 ☒ Enable
 ☐ Disable

#### Add MAC Address

MAC Address

#### MAC Address List

Number	MAC Address	Edit	Delete
1	00:12:5E:2F:8D:BE	<input type="radio"/>	<input type="checkbox"/>



**NOTE:** When more than one items list in the MAC Address List, the computer on client side needs to match only one of the rules so that the check can pass.

8. Return to Edit Account or Add Account screen and click **Apply** to confirm the settings.

### Edit Account

#### General Setting

Name: admin ☒ Active

Group: BiGuard

Group Setting: ☐ Enable ☒ Disable

#### Login Setting

Password:

Retype Password:  ☐ Use group default password

Host Checking: ☒ Active [Advanced Setting](#)

Force Login: ☐ Enable ☒ Disable

Inactivity Timeout: 100 Minutes

#### Service

Network Place: ☒ Enable ☐ Disable

Network Extender Service: ☒ Enable ☐ Disable [Advanced Setting](#)  
☒ Standalone Application (Win32 Only)

Transport Extender Service: ☒ Enable ☐ Disable [Advanced Setting](#)

Web Cache Cleaner: ☒ Enable ☐ Disable

Network Extender IP Assignment: ☒ Dynamic Assign ☐ Fix IP 192.168.1.240

Greeting String: ☒ Default ☐ Custom Welcome to SSL/IPSEC

#### Application Proxy

Applications: This group has no application now.



**NOTE:** For Host Checking to work for a particular user account, please make sure that the Account's Host Checking is **checked** Active and its Group's Host Checking is **enabled**.

## Advance Setting for Network Extender Service

The Advance Setting for Network Extender Service is the same in Group/Application setting and in individual Account setting except for some additional options only available for Group/Applications. The document uses the Network Extender advanced setting conducted in Account configuration as the example to explain the Network Extender configuration procedure. This function further enables Network Extender users to set the permission for accessing the LAN services to safeguard the server.

1. Select **SSL VPN → User Access → Group / Application**. Choose a group you desire and press **Edit** to change the Network Extender advanced configuration settings.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
Test	BiGuard	No	Disable	<a href="#">Edit</a>	<a href="#">Delete</a>
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

2. Click **Advanced Setting** option in the Network Extender Service field.

Edit Group	
General Settings	
Group Name	Test
Domain	BiGuard
Password Policy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Inactivity Timeout	5 Minutes
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Service	
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input type="checkbox"/> Standalone Application (Win32 Only)
Transport Extender Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>
Application Table	
<a href="#">Add Application</a>	
Name	Application IP Address / Path
<b>Note!</b> To make application changes, press <b>Apply</b> .	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3. Enter the data required in the fields of the table illustrated below. The contents in the red box only exists through **Group/Application's Network Advance Service's Advance Setting** except **Packet Filter**.



**PACKET FILTER**

### Network Extender Advanced Setting

☒ Packet Filter
☐ Client Address
☐ Client Route
☐ Standalone

**Create Rule**

Name

**Rule Policy**

Active
☒ Enable

Action
Drop ▼

Service ▶
\*\*Any ▼

To Address ▶
\*\*Any ▼

Schedule ▶
\*\*Always On ▼

**Parameters** 

#	Name	Active	Action	Service	To	Schedule	Edit	Delete
1	Default	Yes	Forward	**Any	**Any	**Always On	<input type="radio"/>	<input type="checkbox"/>

Name	Allows you to enter the name of the created rule.
Active	Allows you to enable the rule.
Action	Allows you to select the method used to process the packets.
Service	Select the service for this rule.
To Address	Select an IP address. (You are required to set the IP addresses in Network Object configuration first before you can choose an IP address in this field.)
Schedule	Select a schedule for this rule.

4. After the above configurations are completed, press **Add** to create the rule.
5. The rule created will be displayed in the Parameters table. Press **Apply** to confirm.



**NOTE:** You can also configure the Packet Filter settings through **SSL VPN → User Access → Account → Network Extender Service → Advance Setting**.

**CLIENT ADDRESS**

Use the **Network Extender** menu item to assign client IP addresses to enable client access. 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. See [Modifying the Network Extender IP address range](#) on page 199.

Network Extender Advanced Setting			
<input type="radio"/> Packet Filter		<input checked="" type="radio"/> Client Address	
<input type="radio"/> Client Route		<input type="radio"/> Standalone	
<b>Client IP Address Assignment</b>			
Client Address Range Begin		<input type="text" value="192.168.1.210"/>	
Client Address Range End		<input type="text" value="192.168.1.230"/>	
DNS Server	Primary	<input type="text"/>	
	Secondary	<input type="text"/>	
WINS Server	Primary	<input type="text"/>	
	Secondary	<input type="text"/>	
Tunnel All Mode		<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>	

**CLIENT ROUTE**

Network Extender Advanced Setting			
<input type="radio"/> Packet Filter		<input type="radio"/> Client Address	
<input checked="" type="radio"/> Client Route		<input type="radio"/> Standalone	
<b>Add Client Route</b>			
Destination Address		<input type="text"/>	
Destination Subnet Mask		<input type="text"/>	
<input type="button" value="Add"/>		<input type="button" value="Edit"/>	
<b>Client Route</b>			<input type="button" value="Delete"/>
Destination Address	Destination Subnet Mask	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>	

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 S20 through the SSL VPN tunnel. See [Creating Client Routes](#) on page 200.

**STANDALONE**

Network Extender Advanced Setting	
<input type="radio"/> Packet Filter <input type="radio"/> Client Address <input type="radio"/> Client Route <input checked="" type="radio"/> Standalone	
<b>Portal Setting</b>	
Show Download URL on Portal	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>S.N.E. Win32 Client Side Application Setting</b>	
Save Private Information	<input checked="" type="checkbox"/> Allow Save Username <input checked="" type="checkbox"/> Allow Save Password
Keep Connection Setting	<input type="checkbox"/> Allow Keep Connection <input type="checkbox"/> Allow Re-connect when disconnect
S.N.E. Greeting Setting	<input type="radio"/> Default <input checked="" type="radio"/> User Defined Greeting String: <input type="text" value="Network Extender"/> String Color: <input type="color" value="#0000FF"/> String Shadow: <input type="text" value=""/> Back Ground: <input type="color" value="#A9A9A9"/> String Font: <input type="text" value="Arial"/> Font Style: <input checked="" type="checkbox"/> Bold <input type="checkbox"/> Italic <input type="checkbox"/> Underline Preview: <b>Network Extender</b>
Run AD login script after connected	Delay: <input type="text" value="0"/> Seconds <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Run SSL VPN script after connected	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Run SSL VPN script after disconnected	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Change IE proxy setting after connected or disconnected	<input type="checkbox"/> Enable Proxy Server (IP:Port): <input type="text" value=""/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Standalone allows specific configuration regarding to the Standalone Network Extender. The administrator can manage the advance settings of SNE based on each individual group. The administrator can separately control whether to allow the users to download or run SNE. The administrator can create the name of the company on SNE. Check the **Standalone** radio button to enable further editing of its configuration including the creation of the company's name and the background color.

Show Download URL on Portal	To allow users to be able to download the Standalone Network Extender then this option needs to be <b>Enable</b> .
Save Private Information	Tick to allow users to save username and password.
Keep Connection Setting	Tick to allow Keep Connection which will not let the user's connection go idle. Tick to allow Re-connect when disconnected from the Network Extender Service. SNE re-connect to server when disconnecting abnormally.



**NOTE:** SNE advance setting is for administrator to configure access level for individual user. All functions under Portal Setting will only be available to user when enabled by the administrator.

**SNE SCRIPT AND IE PROXY SETTING**

Script, could be seen as a batch file simply, could also be described as a programming language consisting of a set of instructions to an application or tool program. It allows the user to implement a number of instructions easily by implementing a file without compiling.

A Proxy Server is a server located on a network between client software and another server, which intercepts all requests to the server. It will reply to client's requests by retrieving content saved in its cache to determine whether it can fulfill them itself. If not, it forwards the request to remote www server, and then serves the information to user and keep a local copy in cache.

The administrator can configure in router system that the user is allowed to run some scripts after SNE is implemented. There are two types of script. The first type is script(s) needing to run when user logging into the router interface via AD Domain authentication. The second type is script(s) needing to run when user logging into the router interface over SSL VPN or disconnecting to the router. After the setting of **script** is completed, the script(s) which the administrator configured previously will run automatically with SNE After the users disconnect the SNE, their computer settings will return to the original status.

The administrator can configure in router system that the IE proxy server setting (including IP address and port) is enabled or disabled when SNE implementing. After the setting of script is completed, the script(s) which the administrator configured previously will run automatically with SNE After the users disconnect the SNE, their computer settings will return to the original status.

Refer to the following to set SNE script and IE proxy configuration:

1. In the Network Extender Advanced Setting Standalone screen, there are two types of script: AD login script and SSL VPN script.

Network Extender Advanced Setting	
<input type="radio"/> Packet Filter	<input type="radio"/> Client Address
<input type="radio"/> Client Route	<input checked="" type="radio"/> Standalone
<b>Portal Setting</b>	
Show Download URL on Portal	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>S.N.E. Win32 Client Side Application Setting</b>	
Save Private Information	<input checked="" type="checkbox"/> Allow Save Username <input checked="" type="checkbox"/> Allow Save Password
Keep Connection Setting	<input type="checkbox"/> Allow Keep Connection <input type="checkbox"/> Allow Re-connect when disconnect
S.N.E. Greeting Setting	<input type="radio"/> Default <input checked="" type="radio"/> User Defined
	Greeting String: Network Extender
	String Color: [Blue]
	String Shadow: [White]
	Back Ground: [Grey]
	String Font: Arial
Font Style: <input checked="" type="checkbox"/> Bold <input type="checkbox"/> Italic <input type="checkbox"/> Underline	
Preview	Network Extender
Run AD login script after connected	Dealy 0 Seconds <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Run SSL VPN script after connected	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Run SSL VPN script after disconnected	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Change IE proxy setting after connected or disconnected	<input type="checkbox"/> Enable Proxy Server (IP:Port):
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

2. AD login script setting:  
The administrator can enable or disable **AD login script** by ticking the **Enable** box for **Run AD login script after connected** if he/she wants to allow the user under AD Domain to run the AD login Script program after using SNE to log into the router interface over SSL VPN and enter the number of seconds for the delay time which script runs after this time.

Run AD login script after connected	Dealy 0 Seconds <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Run SSL VPN script after connected	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Run SSL VPN script after disconnected	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Change IE proxy setting after connected or disconnected	<input type="checkbox"/> Enable Proxy Server (IP:Port):

**Note:** When **Run AD login script after connected** is enabled, the Script program runs after user under AD Domain log into the router interface. But the drive or printer mounted this AD Domain cannot be removed when user logout due to no corresponding program. You should configure the **Run SSL VPN script after disconnected** setting to remove them.

3. SSL VPN script setting:  
The default is **Disable**. Check the **Enable** radio button to edit SSL VPN script configura-

tion. For example, to run Script program mounting Z drive when SNE implementing, enter **net use Z:\\server\\share folder name** in the **Run SSL VPN script after connected** field; to run Script program removing Z drive when SNE disconnecting, enter **net use Z:/DELETE** in the **Run SSL VPN script after disconnected** field.

Run AD login script after connected	Delay <input type="text" value="0"/> Seconds <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Run SSL VPN script after connected	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <pre>REM === Map a network drive=== net use z: \\192.168.1.35\\temp</pre>
Run SSL VPN script after disconnected	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <pre>REM === Map a network drive=== net use z: /DELETE</pre>
Change IE proxy setting after connected or disconnected	<input type="checkbox"/> Enable Proxy Server (IP:Port): <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

4. IE proxy setting:  
 The default is left unchecked. Check the **Enable** box to change IE proxy setting. Click **Apply** to confirm the settings.

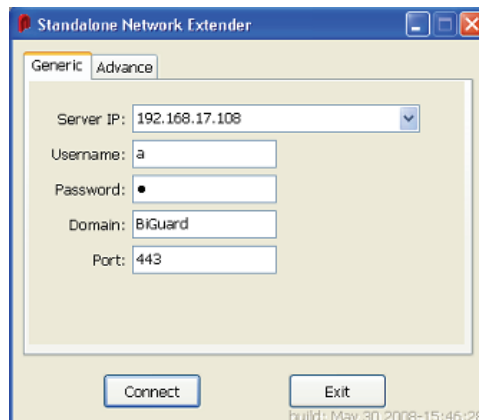
Run AD login script after connected	Delay <input type="text" value="0"/> Seconds <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Run SSL VPN script after connected	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <pre>REM === Map a network drive=== net use z: \\192.168.1.35\\temp</pre>
Run SSL VPN script after disconnected	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <pre>REM === Map a network drive=== net use z: /DELETE</pre>
Change IE proxy setting after connected or disconnected	<input checked="" type="checkbox"/> Enable Proxy Server (IP:Port): <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**SNE SETTING ON CLIENT-SIDE**

1. After the installing is completed, enable Standalone Network Extender and configure the settings. Click Advance to check the advance settings you want to set up.  
**Note:** The advance functions will also be available to user only when enabled by the administrator on the sever-side.
2. If the box for **Remember username** is left unchecked, the box for **Remember password** will not be available for selection.
3. SNE will automatically connect to the server when computer starts only after the **Auto run when windows startup** box is selected, and the administrator has enabled users the access level to save their usernames and passwords.



4. Click **Generic**, enter parameters in every fields. Then press **Connect**.



5. The company's name is shown on the screen when dialing Standalone Network Extender.



## Advance Setting for Transport Extender Service

The Advance Setting for Transport Extender Service allow you to configure applications for use with the Transport Extender. See [Modifying the Transport Extender](#) on page 204.

1. Select **SSLVPN** → **User Access** → **Group / Application**. Choose a group you desire and press **Edit** to change the Transport Extender advanced configuration settings.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
Test	BiGuard	No	Disable	<a href="#">Edit</a>	<a href="#">Delete</a>
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

2. Click **Advanced Setting** option in the Transport Extender Service field.

Edit Group				
General Settings				
Group Name	Test			
Domain	BiGuard			
Password Policy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	<input type="text" value="5"/> Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>			
Application Table				
<a href="#">Add Application</a>				
Name	Application	IP Address / Path		
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

3. Enter the data required in the fields of the table. Press **Add** to save the setting and a new application will be added to the Configured Applications for Transport Extender List.



### Transport Extender

#### Add an Application to be Tunneled by Transport Extender

Local Server IP Address	<input type="radio"/> All IP Addresses <input checked="" type="radio"/> Fixed IP Address 192.168.1.254
Protocol	TCP ▾
Port Number	<input type="radio"/> All Ports <input checked="" type="radio"/> Fixed Port 110 ~ 110

Add Edit

#### Configured Applications for Transport Extender

Edit	Local Server IP Address	Protocol	Port Number	Delete
<input type="radio"/>	192.168.1.254	TCP	110	<input type="checkbox"/>

Apply Cancel

- To edit applications, click **Edit** next to the item you want to change. Change the parameters as desired and click **Edit** to confirm the setting.

### Transport Extender

#### Add an Application to be Tunneled by Transport Extender

Local Server IP Address	<input type="radio"/> All IP Addresses <input checked="" type="radio"/> Fixed IP Address 192.168.1.254
Protocol	TCP ▾
Port Number	<input type="radio"/> All Ports <input checked="" type="radio"/> Fixed Port 110 ~ 110

Add **Edit**

#### Configured Applications for Transport Extender

Edit	Local Server IP Address	Protocol	Port Number	Delete
<input checked="" type="radio"/>	192.168.1.254	TCP	110	<input type="checkbox"/>

Apply Cancel

5. To delete applications, check **Delete** next to the item you want to remove. Click **Delete** to remove this application from the list.

### Transport Extender

Add an Application to be Tunneled by Transport Extender

Local Server IP Address

☐ All IP Addresses

☒ Fixed IP Address 192.168.1.254

Protocol

TCP

Port Number

☐ All Ports

☒ Fixed Port 110 ~ 110

Add

Delete

Configured Applications for Transport Extender

Edit	Local Server IP Address	Protocol	Port Number	Delete
<input type="radio"/>	192.168.1.254	TCP	110	<input checked="" type="checkbox"/>

Apply

Cancel

6. 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 113** 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
DNS Server	Primary	
	Secondary	
WINS Server	Primary	
	Secondary	
NetBIOS Broadcast		<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tunnel All Mode		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<div>ApplyCancel</div>		

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

Modifying the Network Extender client routes

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 S20 through the SSL VPN tunnel.

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

FIGURE 114 NETWORK EXTENDER CLIENT ROUTING TABLE

Network Extender

Client Routing Table

Destination	Subnet Mask		

Create

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

FIGURE 115 ADDING NETWORK EXTENDER CLIENT ROUTES

Network Extender

Add Client Route

Destination Address	
Destination Subnet Mask	

Apply

Cancel

- 3. Type the destination address and destination subnet mask in the **Destination Address** and **Destination Subnet Mask** fields.
- 4. Click **Apply** to confirm the settings.

EDITING NETWORK EXTENDER CLIENT ROUTES

Refer to the following to edit Network Extender client routes:

- 1. In the Network Extender Client Routing Table menu, click **Edit** next to the item you want to change.

Network Extender

Client Routing Table

Destination	Subnet Mask		
192.168.2.0	255.255.255.254	Edit	Delete

Create

The Edit screen appears.

- 2. In the Edit screen, change parameters as desired for this client route.

Network Extender

Add Client Route

Destination Address	192.168.2.0
Destination Subnet Mask	255.255.255.254

Apply

Cancel

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

**DELETING NETWORK EXTENDER CLIENT ROUTES**

Refer to the following to delete Network Extender client routes:

1. In the Network Extender Client Routing Table menu, click **Delete** next to the client route you want to remove.

Network Extender			
Client Routing Table			
Destination	Subnet Mask		
192.168.2.0	255.255.255.254	Edit ▶	Delete ▶
Create ▶			

The Delete screen appears.

Network Extender	
Delete Client Route	
Destination Address	192.168.2.0
Destination Netmask	255.255.255.254
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

2. Click **Delete** to remove this client route.

Configuring Network Extender Host Name Resolution

This function allows the administrator to define the hostname corresponds to IP Address. When the user connects on the device through Network Extender, the predefined host name will be allocated to the given IP.

FIGURE 116 NETWORK EXTENDER HOST NAME RESOLUTION SCREEN

Network Extender

Add a Host Name Resolution to Network Extender

Local Server IP Address

Full Qualified Domain Name

Add

Edit

Host Name Resolution for Network Extender

Edit

Local Server IP Address

Fully Qualified Domain Name

Delete

Apply

Cancel

Local Server IP Address      Enter Local Server IP Address.

Full Qualified Domain Name      Enter Full Qualified Domain Name.

CREATING NETWORK EXTENDER HOST NAME RESOLUTIONS

- 1. Enter the Local Server IP Address and the Full Qualified Domain Name in the **Local Server IP Address** and **Full Qualified Domain Name** fields.

FIGURE 117 ADDING A HOST RESOLUTION TO NETWORK EXTENDER

Network Extender

Add a Host Name Resolution to Network Extender

Local Server IP Address

192.168.1.254

Full Qualified Domain Name

aa:bb:cc:dd:ee:ff

Add

Edit

Host Name Resolution for Network Extender

Edit

Local Server IP Address

Fully Qualified Domain Name

Delete

Apply

Cancel

- 2. Click **Add** to add the host name resolution. The resolution is displayed under **Host Name Resolution for Network Extender**.

EDITING NETWORK EXTENDER HOST NAME RESOLUTIONS

Refer to the following to edit Network Extender host name resolutions:

- 1. In the Network Extender Host Name Resolution Table, click **Edit** next to the item you want to change.

**Network Extender**

Add a Host Name Resolution to Network Extender

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

**Host Name Resolution for Network Extender**

Edit	Local Server IP Address	Fully Qualified Domain Name	Delete
<input type="radio"/>	192.168.1.254	aa:bb:cc:dd:ee:ff	<input type="button" value="Delete"/>

The following screen appears showing the item's properties.

**Network Extender**

Add a Host Name Resolution to Network Extender

Local Server IP Address	192.168.1.254
Full Qualified Domain Name	aa:bb:cc:dd:ee:ff

**Host Name Resolution for Network Extender**

Edit	Local Server IP Address	Fully Qualified Domain Name	Delete
<input checked="" type="radio"/>	192.168.1.254	aa:bb:cc:dd:ee:ff	<input type="button" value="Delete"/>

2. Change host name resolution parameters as desired.
3. Click **Edit** to confirm the settings.

### **DELETING NETWORK EXTENDER HOST NAME RESOLUTIONS**

Refer to the following to delete Network Extender host name resolutions:

1. In the Network Extender Host Name Resolution Table, click **Delete** next to the item you want to remove.

**Network Extender**

Add a Host Name Resolution to Network Extender

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

**Host Name Resolution for Network Extender**

Edit	Local Server IP Address	Fully Qualified Domain Name	Delete
<input type="radio"/>	192.168.1.254	aa:bb:cc:dd:ee:ff	<input type="button" value="Delete"/>

2. This host name resolution will be remove from the Table.

## Managing Transport 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.

### Modifying the Transport Extender

#### **CREATING A TUNNELED TRANSPORT EXTENDER APPLICATION**

Refer to the following to create a secure access application tunnel:

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

**FIGURE 118** TRANSPORT EXTENDER CONFIGURED APPLICATIONS SCREEN

Transport Extender			
Configured Applications for Transport Extender			
Local Server IP Address	Protocol	Port Number	

Create ➡

2. Click **Create**.

The Transport Extender Configured Applications screen lists the local server IP address and the TCP, UDP or both port number for applications that are configured for tunneling via Transport Extender.

**FIGURE 119** ADDING TUNNELED APPLICATIONS TO TRANSPORT EXTENDER

Transport Extender	
Add an Application to be Tunneled by Transport Extender	
Local Server IP Address	<input type="radio"/> All IP Addresses <input checked="" type="radio"/> Fixed IP Address 192.168.1.254
Protocol	TCP
Port Number	TCP UDP Both Port 110 ~ 110
Apply Cancel	

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

#### **EDITING TRANSPORT EXTENDER APPLICATIONS**

Refer to the following to edit Transport Extender applications:

1. In the Transport Extender Configured Applications menu, click **Edit** next to the item you want to change.

Transport Extender			
Configured Applications for Transport Extender			
Local Server IP Address	Protocol	Port Number	
192.168.1.254	TCP	110	Edit ➡ Delete ➡

Create ➡

The Edit screen appears.



2. In the Edit screen, change parameters as desired for this application.

Transport Extender

Edit an Configured Application

Local Server IP Address	<div><div>All IP Addresses</div><div><div>Fixed IP Address</div><div>192.168.1.254</div></div></div>
Protocol	<div>TCP</div>
Port Number	<div><div>All Ports</div><div><div>Fixed Port</div><div>110 ~ 110</div></div></div>

Apply

Cancel

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

**DELETING TRANSPORT EXTENDER APPLICATIONS**

Refer to the following to delete Transport Extender applications:

1. In the Transport Extender Configured Applications menu, click **Delete** next to the item you want to remove.

Transport Extender

Configured Applications for Transport Extender

Local Server IP Address	Protocol	Port Number		
192.168.1.254	TCP	110	<div>Edit</div>	<div>Delete</div>

Create

The Delete screen appears.

Transport Extender

Delete an Configured Application

Local Server IP Address	192.168.1.254
Protocol	TCP
TCP Port Number	110 ~ 110

Delete

Cancel

2. Click **Delete** to remove this application.

## Configuring host names for Transport Extender

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

**FIGURE 120** TRANSPORT EXTENDER CONFIGURED HOST NAME RESOLUTION SCREEN

Transport Extender			
Configured Host Name Resolution for Transport Extender			
Local Server IP Address	Fully Qualified Domain Name		
<a href="#">Create</a>			

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

### **CREATING TRANSPORT EXTENDER HOST NAME RESOLUTIONS**

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

**FIGURE 121** TRANSPORT EXTENDER ADD AN 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"/>
<a href="#">Apply</a> <a href="#">Cancel</a>	

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

### **EDITING TRANSPORT EXTENDER HOST NAME RESOLUTIONS**

Refer to the following to edit Transport Extender host name resolutions:

1. In the Transport Extender Configured Host Name Resolution menu, click **Edit** next to the item you want to change.

Transport Extender			
Configured Host Name Resolution for Transport Extender			
Local Server IP Address	Fully Qualified Domain Name		
192.168.1.254	110	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>			

The Edit screen appears.

2. In the Edit screen, change parameters as desired for this application.

Transport Extender	
Edit an Configured Host Name Resolution	
Local Server IP Address	<input type="text" value="192.168.1.254"/>
Full Qualified Domain Name	<input type="text" value="110"/>
<a href="#">Apply</a> <a href="#">Cancel</a>	

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

**DELETING TRANSPORT EXTENDER HOST NAME RESOLUTIONS**

Refer to the following to delete Transport Extender host name resolutions:

1. In the Transport Extender Configured Host Name Resolution menu, click **Delete** next to the item you want to remove.

Transport Extender			
Configured Host Name Resolution for Transport Extender			
Local Server IP Address	Fully Qualified Domain Name		
192.168.1.254	110	Edit ▶	Delete ▶
Create ▶			

The Delete screen appears.

Transport Extender	
Delete an Configured Host Name Resolution	
Local Server IP Address	192.168.1.254
Full Qualified Domain Name	110
Delete Cancel	

2. Click **Delete** to remove this host name resolution entry.

## 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. Select **SSL VPN** → **SSL Certificate** and click **Generate CSR**.

**FIGURE 122** SSL CERTIFICATE CURRENT CERTIFICATE SCREEN

SSL Certificate

Current Certificates

Enable	Description	Status	Expiration	Password
<input checked="" type="radio"/>	sha1WithRSAEncryption	Active	Jan 14 02:12:30 2018 GMT	

Apply

Import Certificate

Generate CSR/CRT

2. The Generate Certificate Signing Request (CSR) or Generate a New Self-signed Certificate (CRT) screen appears.

You are prompted to fill out a CSR (Certificate Signing Request) form.

**FIGURE 123** GENERATE CSR/CRT SCREEN

SSL Certificate

Generate Certificate Signing Request (CSR) or Generate a New Self-signed Certificate (CRT)

Name	<input type="text"/>
Organization	<input type="text"/>
Unit/Department	<input type="text"/>
City/Locality	<input type="text"/>
State (Full Name)	<input type="text"/>
Country	<input type="text"/>
FQDN (Domain Name)	<input type="text"/>
Email	<input type="text"/>
Password	<input type="password"/>
Retype Password	<input type="password"/>
New Key Pair Length	1024 <input type="button" value="v"/>
Generate a Self-signed Certificate	<input type="checkbox"/>

Apply

Cancel

Name	Enter a given name.
Organization	Enter your organization.
Unit/Department	Enter the department you belong to.
City/Locality	Enter your city.
State (Full Name)	If in the US, type the name of your State.
Country	Enter your two letter country code

FQDN (Domain Name)	Enter 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	Enter your email address.
Password/Retype Password	These fields are for typing and confirming the password.
New Key Pair Length	This item refers to the strength of the key encryption for the private key (extracted from the zip file).
Generate a Self- signed Certificate	If you do not check the check box, it will generate two files, server.csr and server.key, which you can sign a certificate by well-known certification orgaizaitions. If you check the check box, the certification is verified by yourself.

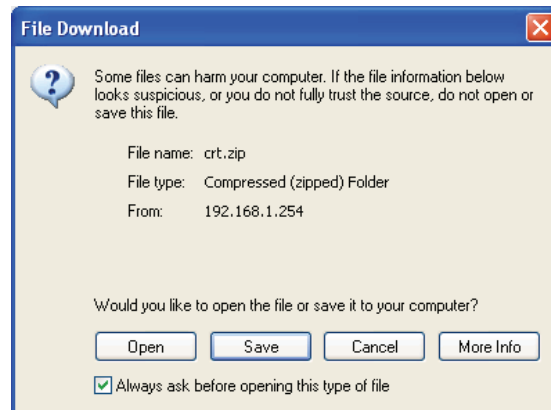


**NOTE:** The country code is two English characters.

**NOTE:** Be sure to write the password down and put it in a safe place.

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

**FIGURE 124** DOWNLOADING THE CSR

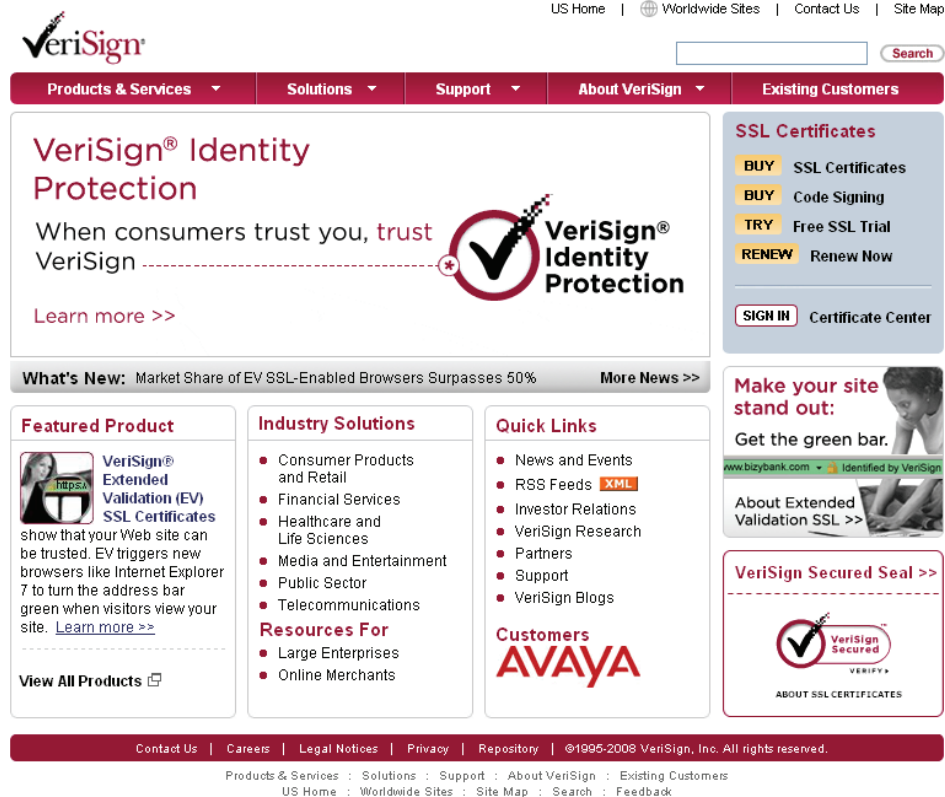


- Click **Save**. You are prompted for a download location. Save the files below to your computer and extract the files to a folder.

**FIGURE 125** CSR FILES



5. Once extracted, you can sign a certificate (for example, Verisign - [www.verisign.com](http://www.verisign.com)).



6. Follow the instructions from the web. You will be prompted to input your CSR.
7. Open `server.csr` with a text editor such as Windows Notepad.

### FIGURE 126 OPENING THE CSR



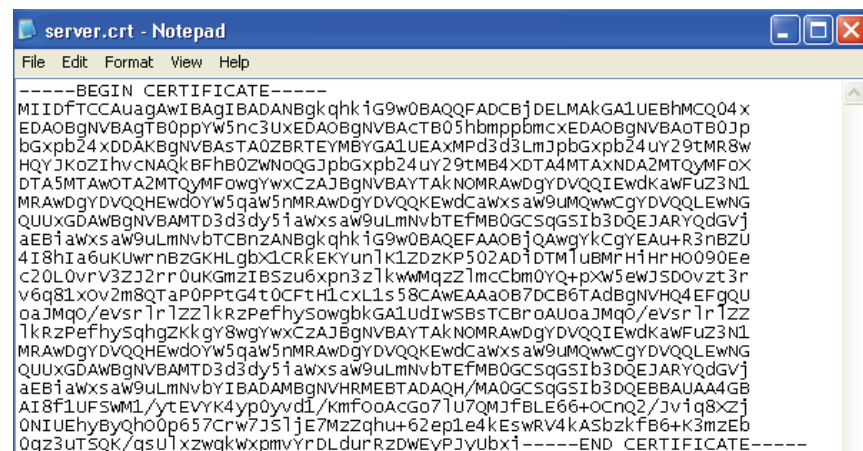
- Copy the CSR text and paste it in the appropriate field on the certificate provider's website and finish following the certificate provider's instructions for getting a certificate. The certificate provider will send you the certificate by email.

### FIGURE 127 CERTIFICATE SIGNING REQUEST

[illegible]

9. Copy the certificate text and paste into a text editor. Save the file as “server.crt”.

### FIGURE 128 CERTIFICATE TEXT



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**.

**SSL Certificate**

**Current Certificates**

Enable	Description	Status	Expiration	Password
<input checked="" type="radio"/>	sha1WithRSAEncryption	Active	Jan 14 02:12:30 2018 GMT	

Apply Import Certificate Generate CSR/CRT

12. The screen below appears, then click **Browse** and go to the location of the zipped file. When the file is listed in the Certificate File text box, click **Upload**.

**SSL Certificate**

**Import Digital Certificate**

Certificate File  Browse...

Upload a zip file containing "server.key" and "server.crt" files.

Upload Cancel

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

**SSL Certificate**

**Current Certificates**

Enable	Description	Status	Expiration	Password
<input type="radio"/>	md5WithRSAEncryption	Non-Active	Oct 9 06:14:20 2009 GMT	Input  Delete
<input checked="" type="radio"/>	sha1WithRSAEncryption	Active	Jan 14 02:12:30 2018 GMT	

Apply Import Certificate Generate CSR/CRT

13. Now you must activate the imported certificate. Click **Input** to type in the password.

**FIGURE 129 INPUTTING THE CSR PASSWORD**

**SSL Certificate**

**Input Password**

Certificate Description: www.billion.com

Issuer: C=CN, ST=Jiangsu, L=Nanjing, O=Billion, OU=FAE, CN=www.billion.com/emailAddress=tech@billion.com

Subject: C=CN, ST=Jiangsu, L=Nanjing, O=Billion, OU=FAE, CN=www.billion.com/emailAddress=tech@billion.com

Serial Number: 0 (0x0)

Expiration Date: Oct 9 06:14:20 2009 GMT

Password:

Apply Cancel

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



FIGURE 130 NEW CERTIFICATE

SSL Certificate

Current Certificates

Enable	Description	Status	Expiration	Password	
<input checked="" type="radio"/>	md5WithRSAEncryption	Active	Oct 9 06:14:20 2009 GMT	<a href="#">Input</a>	<a href="#">Delete</a>
<input type="radio"/>	sha1WithRSAEncryption	Active	Jan 14 02:12:30 2018 GMT		

Apply

Import Certificate

Generate CSR/CRT

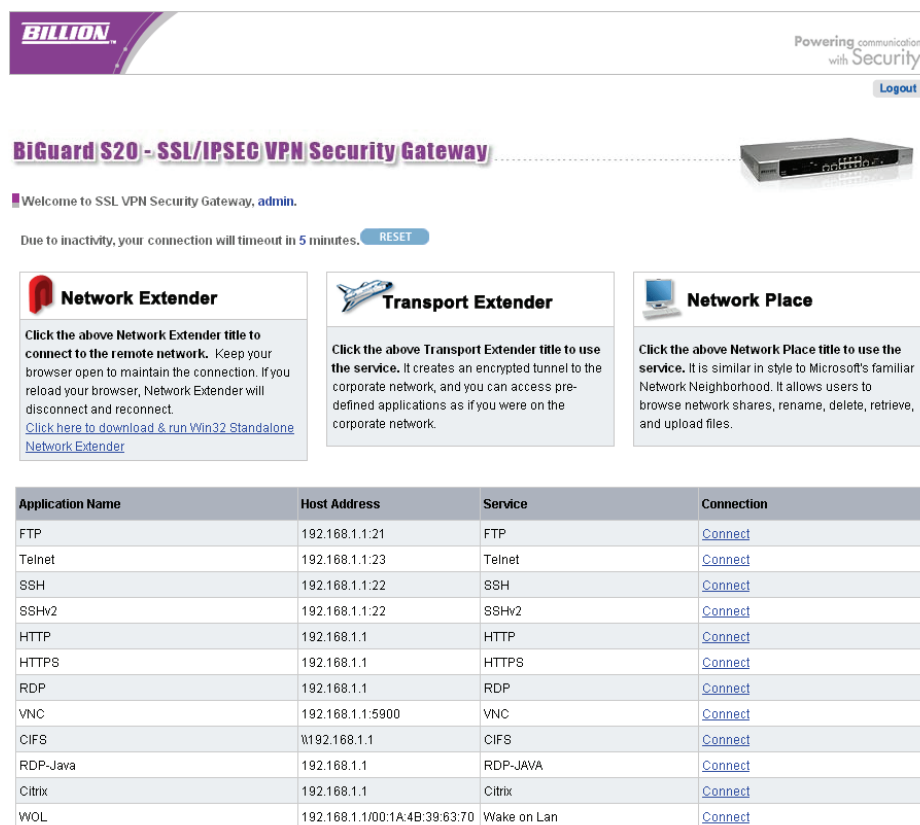
16. Click **Enable** to enable the certificate.
17. Click **Apply** and the certificate is imported.

## SSL VPN Portal

The BiGuard S20 provides a secure and flexible enterprise-wide solution for data and application access anytime and anywhere. By using the BiGuard S20 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 S20 the ideal, secure gateway solution for the novice and the veteran. 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 Name	Host Address	Service	Connection
FTP	192.168.1.1:21	FTP	<a href="#">Connect</a>
Telnet	192.168.1.1:23	Telnet	<a href="#">Connect</a>
SSH	192.168.1.1:22	SSH	<a href="#">Connect</a>
SSHv2	192.168.1.1:22	SSHv2	<a href="#">Connect</a>
HTTP	192.168.1.1	HTTP	<a href="#">Connect</a>
HTTPS	192.168.1.1	HTTPS	<a href="#">Connect</a>
RDP	192.168.1.1	RDP	<a href="#">Connect</a>
VNC	192.168.1.1:5900	VNC	<a href="#">Connect</a>
CIFS	\\192.168.1.1	CIFS	<a href="#">Connect</a>
RDP-Java	192.168.1.1	RDP-JAVA	<a href="#">Connect</a>
Citrix	192.168.1.1	Citrix	<a href="#">Connect</a>
WOL	192.168.1.1/00:1A:4B:39:63:70	Wake on Lan	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

Network Extender	Browser based plug-in that simplifies clientless remote access deployments, while delivering full network connectivity for any IP-based application. See <a href="#">Installing the Network Extender</a> on page 217. 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.

File Transfer Protocol (FTP)	<p>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.</p> <p>Click <b>Connect</b> to easily access the files on the FTP server.</p>
Telnet	<p>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.</p> <p>Click <b>Connect</b> and follow the on-screen instructions to complete the connection.</p>
Secure Shell (SSH)	<p>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.</p> <p>Click <b>Connect</b> and follow the on-screen instructions.</p>
Secure Shell version 2 (SSHv2)	<p>SSHv2 (Secure SHell version 2) is a completely overhauled version of the protocol.</p> <p>Click <b>Connect</b> and follow the on-screen instructions.</p>
HTTP	<p>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.).</p> <p>Click <b>Connect</b> to connect to the HTTP server in the office.</p>
HTTPS	<p>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.</p> <p>Click <b>Connect</b> to connect to the HTTPS server in the office.</p>
Terminal Service (RDP)	<p>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.</p> <p>RDP (ActiveX) - RDP is the current version and provides session sound and full-screen mode. RDP is only available in an ActiveX client.</p> <p>Click <b>Connect</b> and follow the on-screen instructions.</p>
Virtual Network Computing (VNC)	<p>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.</p> <p>Click <b>Connect</b> and follow the on-screen instructions.</p>
Network File Share (CIFS)	<p>The Common Network File Share (CIFS) protocol allows a user in a group remote access through the web portal to directed and specific network paths as predefined by the network administrator.</p> <p>Click <b>Connect</b> to connect to the CIFS service.</p>

Terminal Service (RDP)-Java	<p>Java version of the Windows Terminal Server, that 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.</p> <p>RDP (ActiveX)-RDP is the current version and provides session sound and full-screen mode. RDP is only available in an ActiveX client. Click <b>Connect</b> and follow the on-screen instructions.</p>
Citrix (HTTP)	<p>Select this option if you have a Citrix Presentation Server that you wish to connect to. Citrix Presentation Server is a remote access/application publishing product that allows people to connect to applications available from central servers.</p> <p>Click <b>Connect</b> to connect to the Citrix service.</p>
Wake On LAN (WOL)	<p>WOL allows the router to set a command to turn on a particular computer that can support this feature.</p>

---



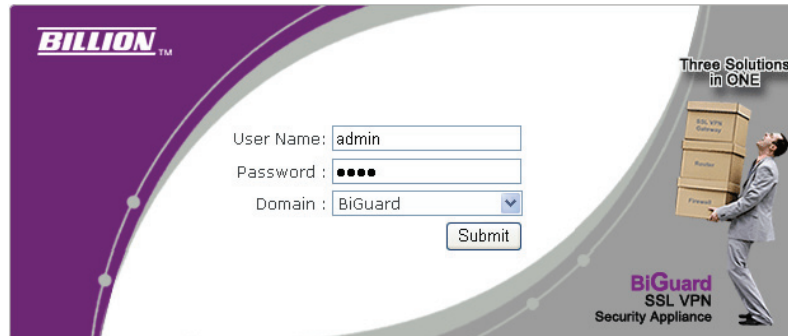
**NOTE:** Portal access authorization is only required if the user name and password do not match the network settings.

## Installing the Network Extender

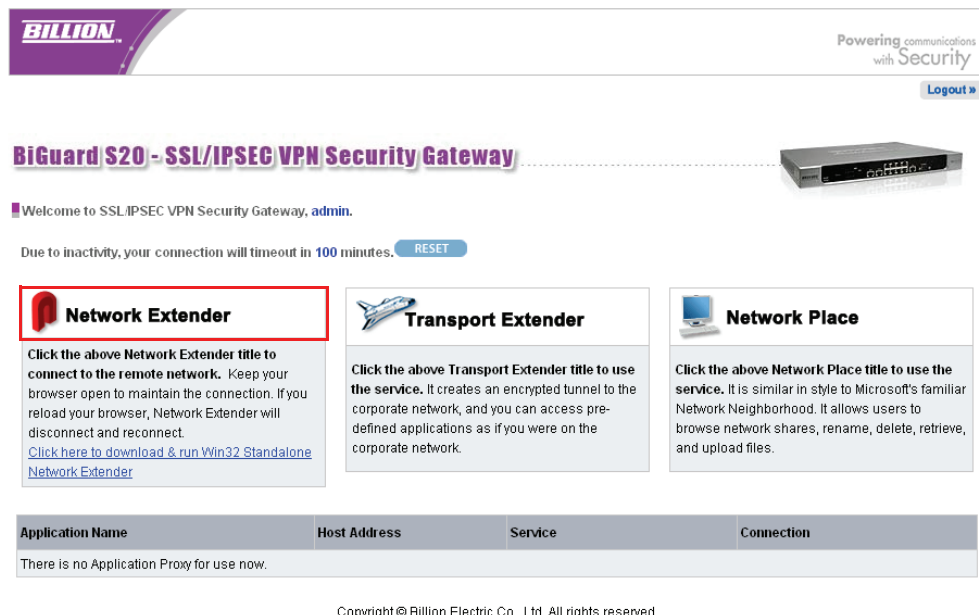
The Network Extender is a web based plug-in that simplifies clientless remote access while delivering full network connectivity for IP-based applications. The Network Extender enables combined IPsec and SSL VPN in one solution, simplifying remote access deployments while providing maximum flexibility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

To use Web Portal Network Extender, first connect to the device by typing `https://wanipaddress` (where *wanipaddress* is the WAN IP address of the BiGuard SSL VPN appliance). After successfully connection and login to the device, the web portal screen appears.

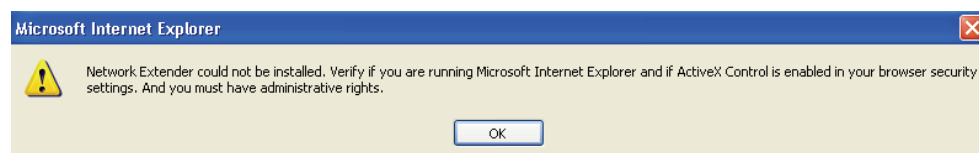
1. Type the WAN IP Address or Domain Name in the Address bar of the browser and log into the BiGuard SSL VPN remote portal as previously configured.



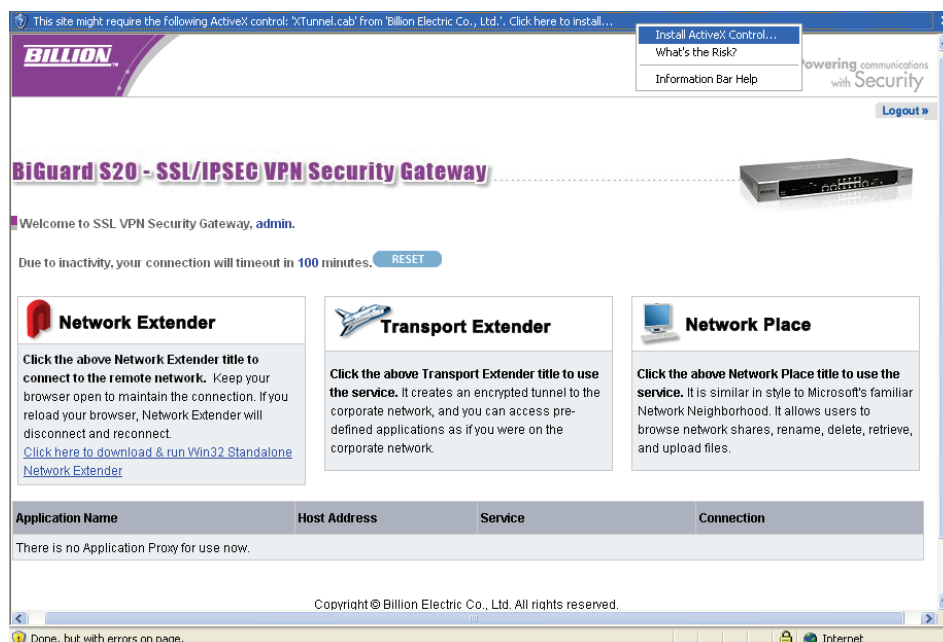
2. Click **Network Extender** in the remote portal window.



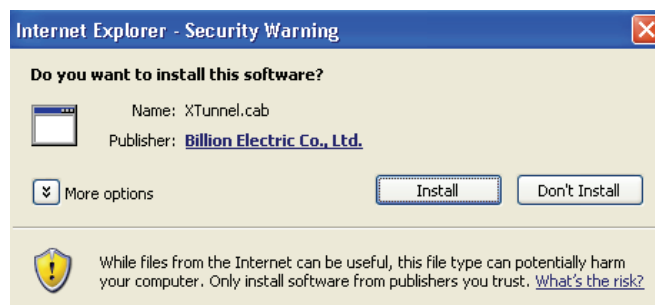
3. If the browser does not launch ActiveX automatically, a warning message appears. Click **OK** to continue. If the browser automatically installs ActiveX, the warning message does not display, then go to **Step 7**.



- Click the **Information** bar on the top of the page and click **Install ActiveX Control**.

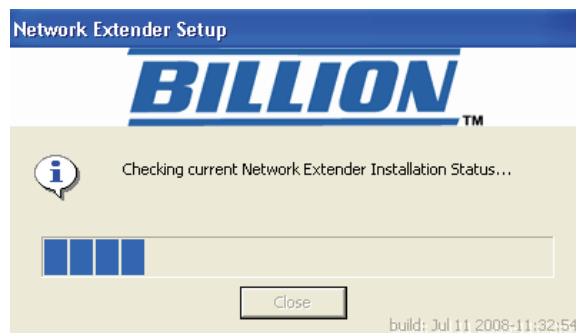


- After the screen refreshes, click **Network Extender** again.
- You are required to install the **XTunnel.cab**. Click **Install** to install the software.



Network Extender setup proceeds.

**FIGURE 131** INSTALLATION PROCEEDING



- You are prompted to install the **SSLDrv Adapter**.

8. Click **Continue Anyway** when prompted to accept the SSLDrv Adapter. Installation proceeds.

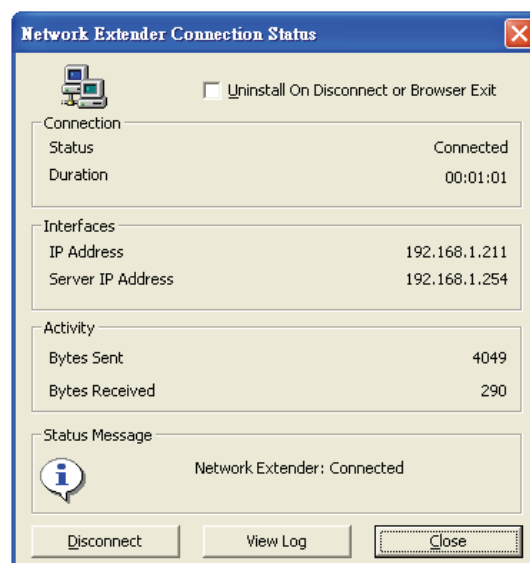


Network Extender setup proceeds.




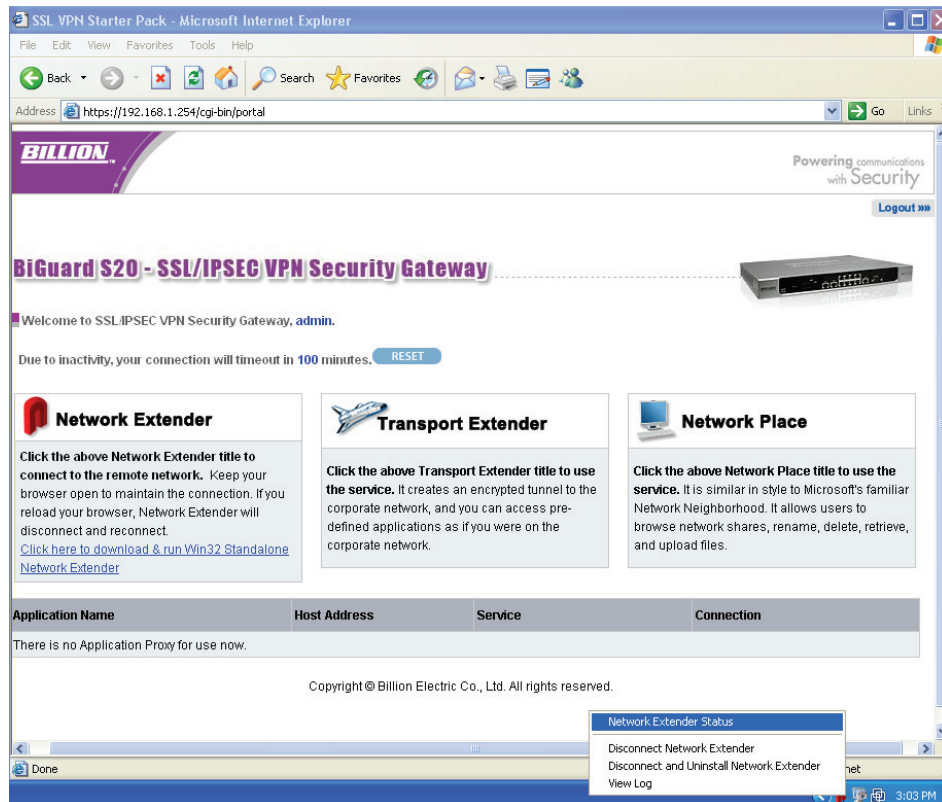
After installation is complete, the **Network Extender Connection Status** window displays.

**FIGURE 132** INSTALLATION COMPLETE



- 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 remains active in the status bar.

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





## Installing the Standalone Network Extender

Installing the Standalone Network Extender works the same way as the normal Network Extender. Except that after the first initial download and installation of the Standalone Network Extender, users will not need to connect to the Portal to access Network Extender, instead they can run the Standalone Network Extender software straight from their PC.

1. To allow Standalone Network Extender to be accessed and downloaded, the Administrator must enable this feature. Click on the Menu, **SSL VPN → User Access → Group/Applications** and either **Edit** or **Create** a Group.

Group/Application				
Group Table				
Name	Authentication Domain	Domain's Default Group	Host Checking	
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>
<a href="#">Create</a>				


2. Tick the **Standalone Application (Win32 Only)** box to allow this group of users to access the Standalone Network Extender link that appears in Network Extender section of the Portal web page. Then click on the **Advanced Setting** to toggle with more configurations.

Edit Group				
General Settings				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	<input type="text" value="5"/> Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)			
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>			
Application Table				
<a href="#">Add Application</a>				
Name	Application	IP Address / Path		
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

3. Select **Standalone** from the top of the Network Extender Advanced Setting page to access the Standalone page. You must then **Enable** the **Show Download URL on Portal** for users to be able to download the Standalone Network Extender. And press **Apply**.

Network Extender Advanced Setting	
<input type="radio"/> Packet Filter	<input type="radio"/> Client Address
<input type="radio"/> Client Route	<input checked="" type="radio"/> Standalone
Portal Setting	
Show Download URL on Portal	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
S.N.E. Win32 Client Side Application Setting	
Save Private Information	<input checked="" type="checkbox"/> Allow Save Username <input checked="" type="checkbox"/> Allow Save Password
Keep Connection Setting	<input type="checkbox"/> Allow Keep Connection <input type="checkbox"/> Allow Re-connect when disconnect
S.N.E. Greeting Setting	<input checked="" type="radio"/> Default <input type="radio"/> User Defined
Run AD login script after connected	Dealy <input type="text" value="0"/> Seconds <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Run SSL VPN script after connected	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Run SSL VPN script after disconnected	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Change IE proxy setting after connected or disconnected	<input type="checkbox"/> Enable Proxy Server (IP:Port): <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	




4. After enabling **Standalone Network Extender** and **Show Download URL on Portal**, log into Web Portal and a link will appear underneath Network Extender section, which can allow users to execute Standalone Network Extender (only if they have installed it already) or download and install Standalone Network Extender for the first time.



**BiGuard S20 - SSL/IPSEC VPN Security Gateway**

Welcome to SSL/IPSEC VPN Security Gateway, admin.

Due to inactivity, your connection will timeout in 100 minutes. [RESET](#)

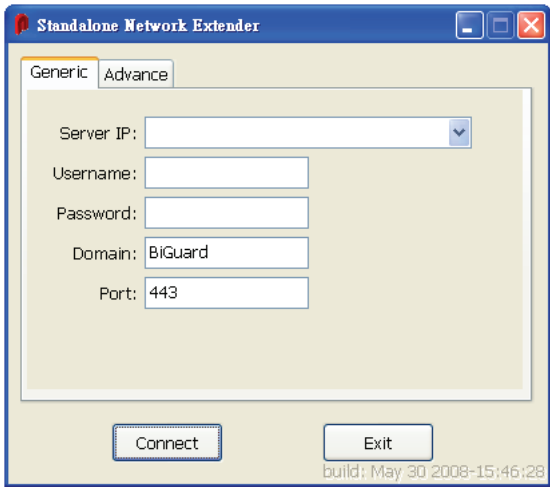
 <b>Network Extender</b> Click the above Network Extender title to connect to the remote network. Keep your browser open to maintain the connection. If you reload your browser, Network Extender will disconnect and reconnect. <a href="#">Click here to download &amp; run Win32 Standalone Network Extender</a>	 <b>Transport Extender</b> Click the above Transport Extender title 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.	 <b>Network PI</b> Click the above Network PI service. It is similar in style Network Neighborhood. It allows you to browse network shares, rer and upload files.
--	---	---

Application Name	Host Address	Service	Connection
------------------	--------------	---------	------------

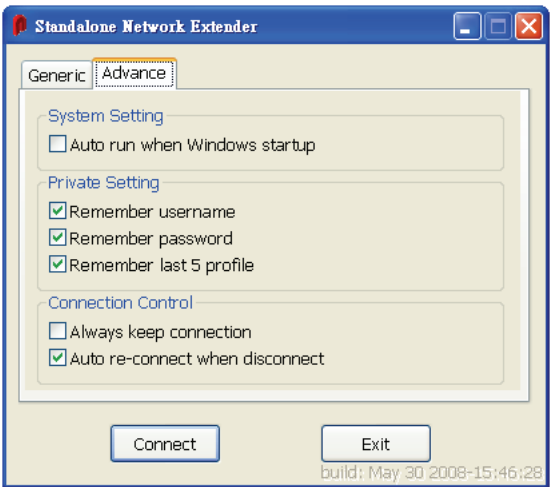
**NOTE:** Standalone Network Extender can be executed from the PC or accessed through the Web Portal by clicking on the **Click here to download and run Win32 Standalone Network Extender** when it is available. The difference between the two methods of running Standalone Network Extender is that when running from the PC, Standalone Network Extender will require the user to input the Server IP, username and etc. But accessing through the Web Portal you have already bypassed those required information and can connect straight away through the click of the link.

**STANDALONE NETWORK EXTENDER FEATURES**

After installing and running the Standalone Network Extender, click on the Standalone Network Extender file from **Start** → **Programs** → **Standalone Network Extender** and click on the Standalone Network Extender file. The standalone Network Extender program will start.



There are two tabs to the Standalone Network Extender software, one is **Generic** will allow users to enter the **Server IP**, **Username**, **Password**, **Domain** and **Port number** to access the server through the Network Extender service without going through to the Portal web page. Once the settings are all configured, click on **Connect** to connect to the Network Extender service.



In the **Advance** tab, there are several configuration boxes for users to set.

Auto run when Windows startup	Tick to allow Standalone Network Extender to be loaded at Windows startup.
Remember username	Tick to allow users to save username.
Remember password	Tick to allow users to save password.

---

Remember last 5 profile	Tick to allow users to remember the last 5 profiles that was accessed through the Standalone Network Extender.
Always keep connection	Tick to allow Keep Connection which will not let the user's connection go idle. SNE send packets to the server every one minute to keep constant connection.
Auto re-connect when disconnect	Tick to allow Re-connect when disconnected from the Network Extender Service. SNE re-connect to server after sixty seconds when disconnecting abnormally.

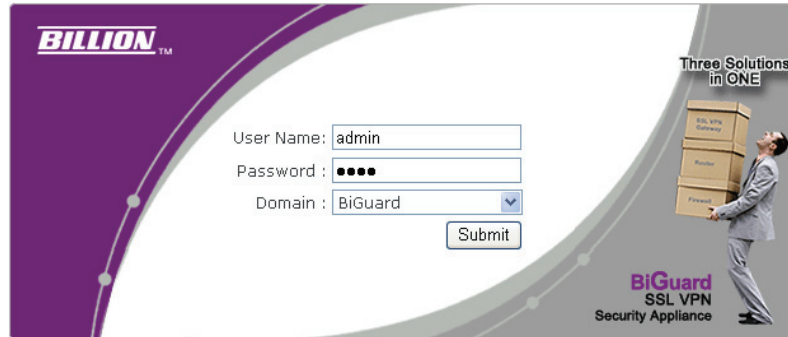
---

## 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.

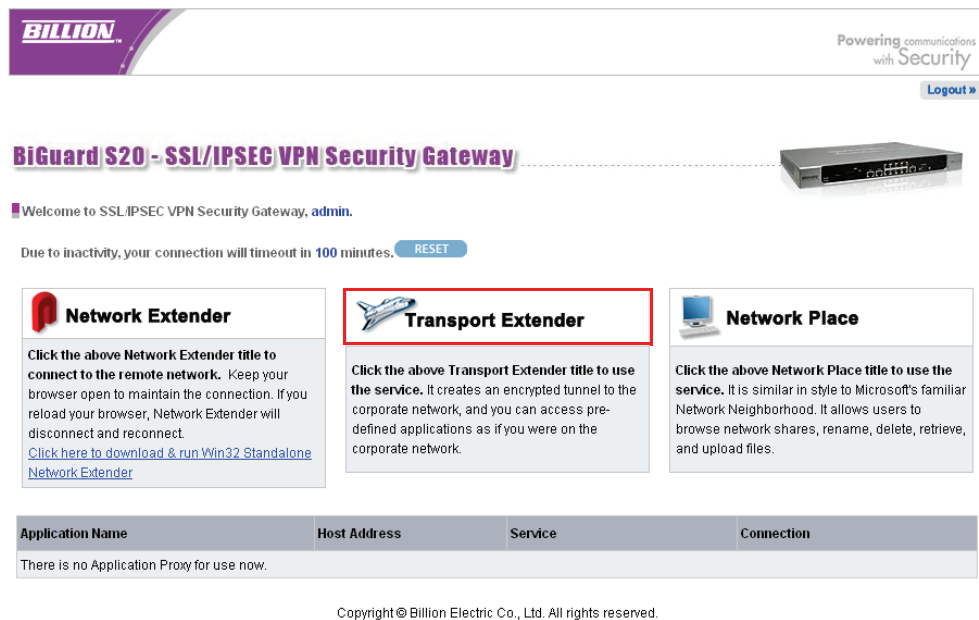
To use Transport Extender, connect to the web portal by first typing in the browser address bar `https://wanipaddress` (where wanipaddress is the WAN IP address of the BiGuard SSL VPN appliance). After you successfully connect to the device and successfully log in to the device, the web portal screen appears. Please click **Transport Extender** in order to connect to the office network. Follow the procedures below to use the Remote Portal.

1. Type the WAN IP Address or Domain Name in the Address bar of the browser and log into the BiGuard SSL VPN remote portal as previously configured.



The login screen for the BiGuard SSL VPN Security Appliance. It features a purple header with the 'BILLION' logo. The main area has a white background with a login form. The form includes fields for 'User Name' (containing 'admin'), 'Password' (masked with dots), and 'Domain' (a dropdown menu showing 'BiGuard'). A 'Submit' button is located below the password field. To the right of the login form, there is an illustration of a man carrying boxes, with the text 'Three Solutions in ONE' above it. The bottom right corner of the screen displays the 'BiGuard SSL VPN Security Appliance' logo.

2. Click **Transport Extender**.

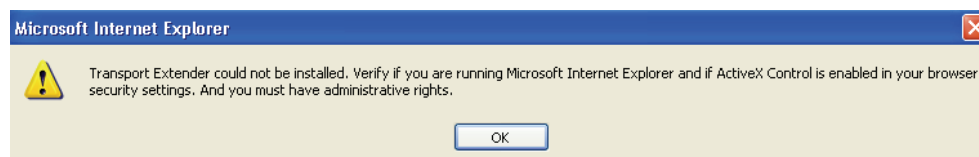


The web portal for the BiGuard S20 - SSL/IPSEC VPN Security Gateway. The header includes the 'BILLION' logo and the text 'Powering communications with Security'. Below the header, there is a 'Logout' button. The main content area features a banner for 'BiGuard S20 - SSL/IPSEC VPN Security Gateway' with an image of the device. Below the banner, a welcome message reads 'Welcome to SSL/IPSEC VPN Security Gateway, admin.' and a timeout notice states 'Due to inactivity, your connection will timeout in 100 minutes.' with a 'RESET' button. The portal is divided into three main sections: 'Network Extender', 'Transport Extender' (highlighted with a red border), and 'Network Place'. Each section contains instructions on how to use the service. At the bottom, there is a table with columns for 'Application Name', 'Host Address', 'Service', and 'Connection'. The table currently shows 'There is no Application Proxy for use now.' and a copyright notice for Billion Electric Co., Ltd.

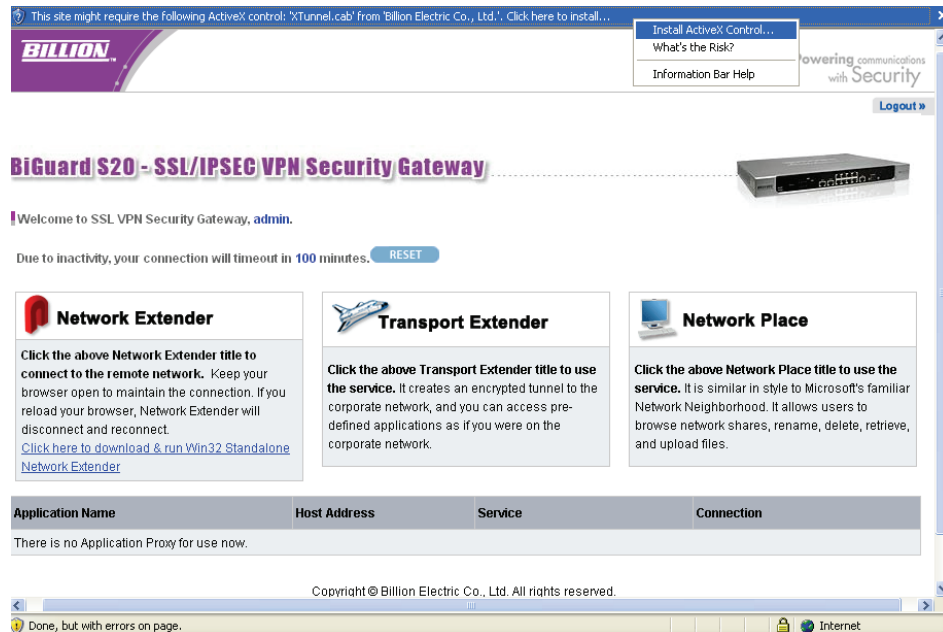
Application Name	Host Address	Service	Connection
There is no Application Proxy for use now.			

Copyright © Billion Electric Co., Ltd. All rights reserved.

3. If the browser does not launch ActiveX automatically, a warning message appears. Click **OK** to continue. If the browser automatically installs ActiveX (the warning message does not display), then go to **Step 7**.



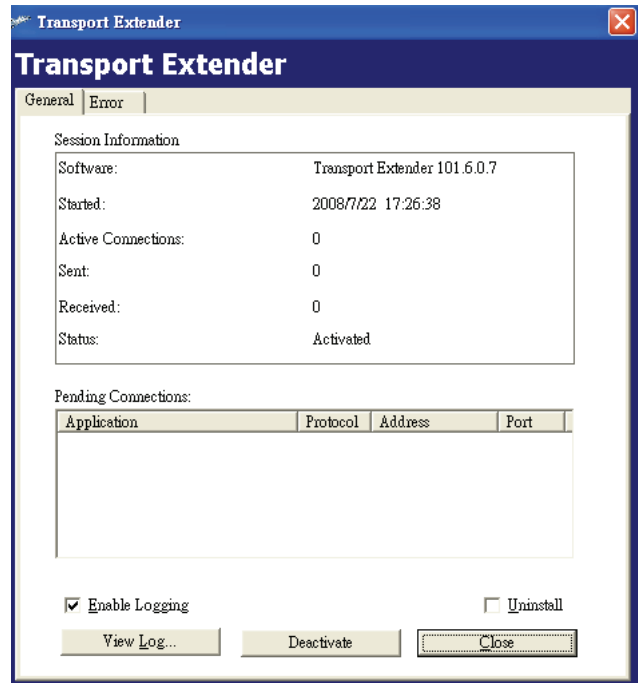
- Click the **Information** bar on the top of the page and click **Install ActiveX Control**.



- After the screen refreshing, click **Transport Extender** again.
- You are required to install the **MenloLSP.cab**. Click **Install** to install the software.



- The Transport Extender Setup proceeds. After the installation is complete, the Transport Extender window displays.



- 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 is left unchecked, ActiveX Control will not to be installed when you log on again. If the box is checked, ActiveX will uninstall when you log off to prevent unauthorized access, such as in the event that 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.

SSL VPN Starter Pack - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back

Forward

Stop

Home

Search

Favorites

Feeds

Print

Tools

Windows

Address 

https://192.168.1.254/cgi-bin/portal

Go


Links

**BILLION**

Powering communications  
with Security

Logout


**BiGuard S20 - SSL/IPSEC VPN Security Gateway**




Welcome to SSLIPSEC VPN Security Gateway, **admin**.

Due to inactivity, your connection will timeout in 100 minutes. 


RESET

**Network Extender**

Click the above Network Extender title 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.  
[Click here to download & run Win32 Standalone Network Extender](#)

**Transport Extender**

Click the above Transport Extender title 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 above Network Place title 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
There is no Application Proxy for use now.			

Copyright © Billion Electric Co., Ltd. All rights reserved.

Open Transport Extender

Deactivate

rnet

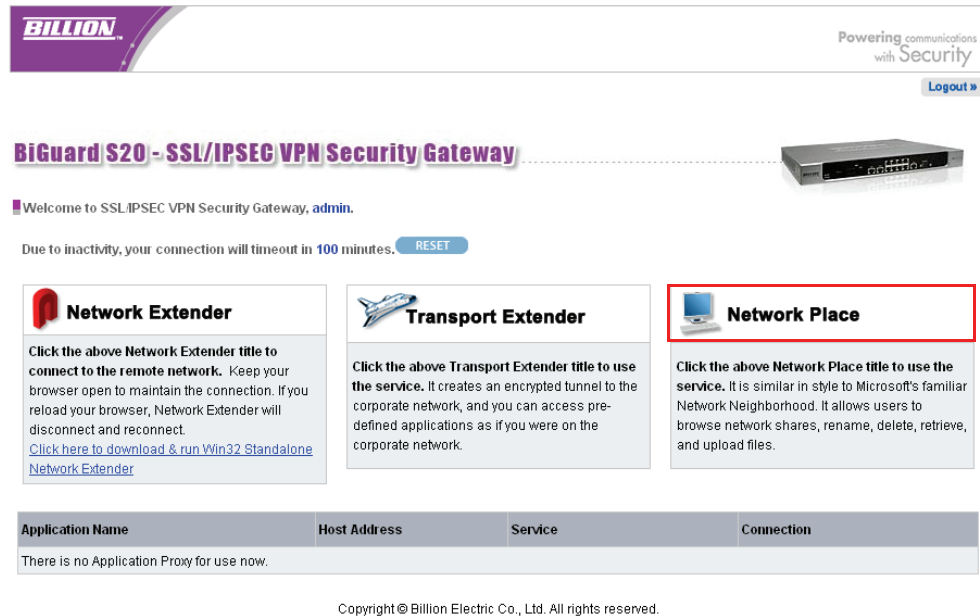
EN 3:30 PM



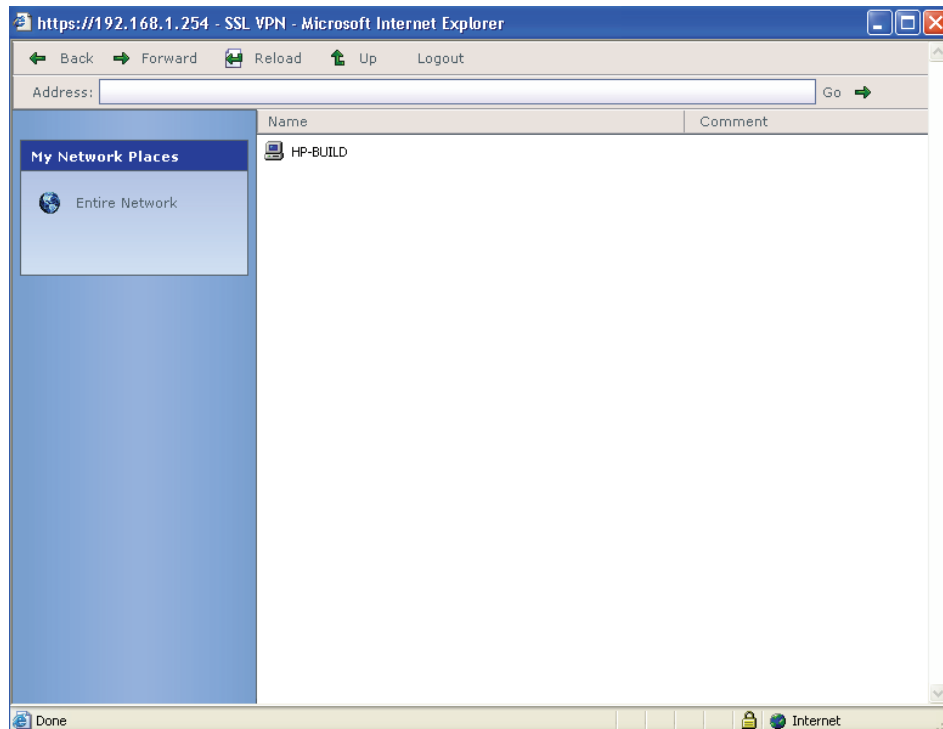
## Accessing Network Place

Network Place 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.

1. Click the **Network Place** icon.



2. 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	192.168.1.100:21	FTP	<a href="#">Connect</a>
Telnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
SSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
SSHv2	192.168.1.100:22	SSHv2	<a href="#">Connect</a>
HTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
HTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
RDP	192.168.1.100	RDP	<a href="#">Connect</a>
VNC	192.168.1.100:5900	VNC	<a href="#">Connect</a>
CIFS	\\192.168.1.100	CIFS	<a href="#">Connect</a>
RDP-Java	192.168.1.100	RDP-JAVA	<a href="#">Connect</a>
Citrix	192.168.1.100	Citrix	<a href="#">Connect</a>
WOL	192.168.1.100 00:1A:4B:39:63:70	Wake on Lan	<a href="#">Connect</a>

The following sections explain how to access each application.

## Using FTP



This tutorial contains two sections, one dealing with the Administrator FTP configuration and the other with the Remote User to demonstrate how a user will log in to the FTP server after it is created.

### **ADMINISTRATOR FTP CONFIGURATION**

Before you start to configure FTP proxy settings for the BiGuard SSL VPN appliance, you have to first create an account on the FTP server.

The following are the steps to configure FTP proxy settings in the BiGuard SSL VPN appliance for the *FTP user*. (In the example **BiGuard** Group/Application is the default Group profile.)

1. Select the following **SSL VPN** → **User Access** → **Group/Application**.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a> 	
<a href="#">Create</a> 					

2. To edit **BiGuard** group, click the **Edit** link on the right hand side of the group profile Name.

The Edit Group screen displays and you can add applications under your chosen Group profile to allow the users within that Group access to the applications.

### Edit Group

General Settings	
Group Name	BiGuard
Domain	BiGuard
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Inactivity Timeout	5 Minutes
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Service	
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>
<a href="#">Add Application</a>	
Application Table	
Name	Application IP Address / Path
<b>Note!</b> To make application changes, press <b>Apply</b> .	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Click **Add Application** to display the SSL VPN Application screen.

From the SSL VPN Applications screen, add an application to this Group (Multiple applications under each Group are also available).

### SSL VPN Application

Add Application	
Application Name	<input type="text" value="TestFTP"/>
Application	File Transfer Protocol (FTP) ▼
IP Address/Domain Name	Terminal Service (RDP)
TCP Port Number	Virtual Network Computing (VNC)
	File Transfer Protocol (FTP)
	Telnet
	Secure Shell (SSH)
	Secure Shell version 2 (SSHv2)
	Web (HTTP)
	Secure Web (HTTPS)
	Network File Share (CIFS)
	Terminal Service (RDP) - Java
	Citrix(HTTP)
	Wake On LAN(WOL)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Application Name: **TestFTP** was inputted as an example for the application name.

Application: Select **File Transfer Protocol (FTP)** from the drop-down menu.

In this example, the IP address for the FTP server is set as 192.168.1.100.

### SSL VPN Application

Add Application	
Application Name	<input type="text" value="TestFTP"/>
Application	File Transfer Protocol (FTP) ▼
IP Address/Domain Name	<input type="text" value="192.168.1.100"/>
TCP Port Number	<input type="text" value="21"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

4. Click **Apply** to set the configuration and return to Group/Application.

Edit Group				
<b>General Settings</b>				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	5 Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
<b>Service</b>				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>			
<b>Application Table</b> <a href="#">Add Application</a>				
Name	Application	IP Address / Path		
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

After creating a group profile, you will need to create user accounts to use the applications assigned to that group profile.

5. Select **SSL VPN → User Access → Account**.

Account				
<b>Account Table</b>				
Name <a href="#">▲▼</a>	Group			
admin	BiGuard	<a href="#">Edit</a>		
<a href="#">Create</a> <a href="#">Move</a>				

6. To create an Account, click **Create**.

The Add Account screen displays, you can create a user account and edit this account to use the FTP application that was created in the previous steps.



**NOTE:** It is suggested you create the same User Name and Password as the one for your FTP server's account. So that you will not have to input user name and password again when accessing the FTP server.

Add Account

General Setting

User Name

user

☒ Active

Group

BiGuard

Password

••••

Retype Password

••••

☐ Use group default password

Host Checking

☒ Active

[Advanced Setting](#)

Apply

Cancel

Group Setting Details

Force Login

Disable

Inactivity Timeout

5 Minutes

Network Place

Enable

Network Extender Service

Enable

Transport Extender Service

Standalone Application (Win32 Only) Enable

Web Cache Cleaner

Enable

Greeting String

Use default greeting string

Applications

There had no applications.

User Name	<b>User</b> was inputted as an example for the user name.
Group	<b>BiGuard</b> group was chosen from the drop-down menu.
Password	A password was inputted.
Retype Password	Type the password again to confirm the password.
Host Checking	Check or uncheck the box to activate or deactivate Host Checking on this account.

7. Or you can edit existing accounts to use the applications assigned to that group profile.

Edit Account

General Setting

Name

admin

☒ Active

Group

BiGuard

Group Setting

☐ Enable ☒ Disable

Login Setting

Password

••••••

Retype Password

••••••

☐ Use group default password

Host Checking

☒ Active

[Advanced Setting](#)

Force Login

☐ Enable ☒ Disable

Inactivity Timeout

100

Minutes

Service

Network Place

☒ Enable ☐ Disable

Network Extender Service

☒ Enable ☐ Disable

[Advanced Setting](#)

☒ Standalone Application (Win32 Only)

Transport Extender Service

☒ Enable ☐ Disable

[Advanced Setting](#)

Web Cache Cleaner

☒ Enable ☐ Disable

Network Extender IP Assignment

☒ Dynamic Assign ☐ Fix IP

192.168.1.240

Greeting String

☒ Default ☐ Custom

Welcome to SSL/IPSEC \

Application Proxy

Applications

☒ TestFTP

Apply

Cancel

Please check the application **TestFTP** (FTP application) to enable the application for the user.

8. Click **Apply** to set the configurations and return to Account Table.

Account

Account Table

Name	Group			
user	BiGuard	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Copy</a>
admin	BiGuard	<a href="#">Edit</a>		

[Create](#) [Move](#)

9. In the Account screen, click **Save Config to Flash** to permanently save the settings.

Save Config to Flash

Write settings to flash

Apply

**REMOTE USER**

The following steps demonstrate how a user will log in to the FTP server from the remote web portal.

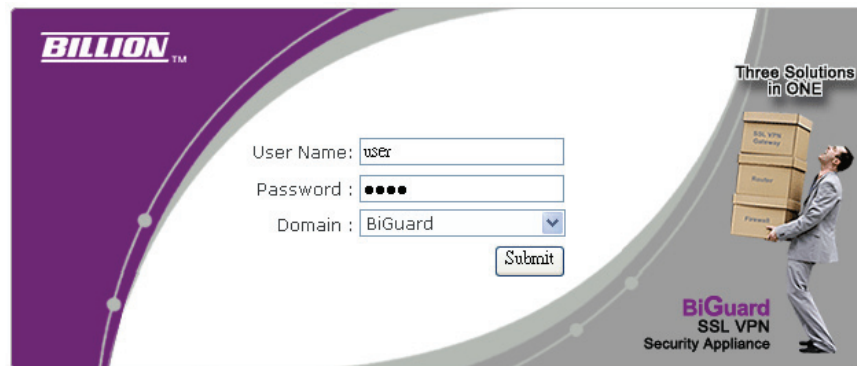
To access the remote web portal, please connect to the https://wanipaddress (where wanipaddress is the WAN IP address of the BiGuard SSL VPN appliance).

A Security Alert message appears.

1. Click **Yes** to proceed (to accept the certificate sent by the BiGuard system).



The log in screen appears.

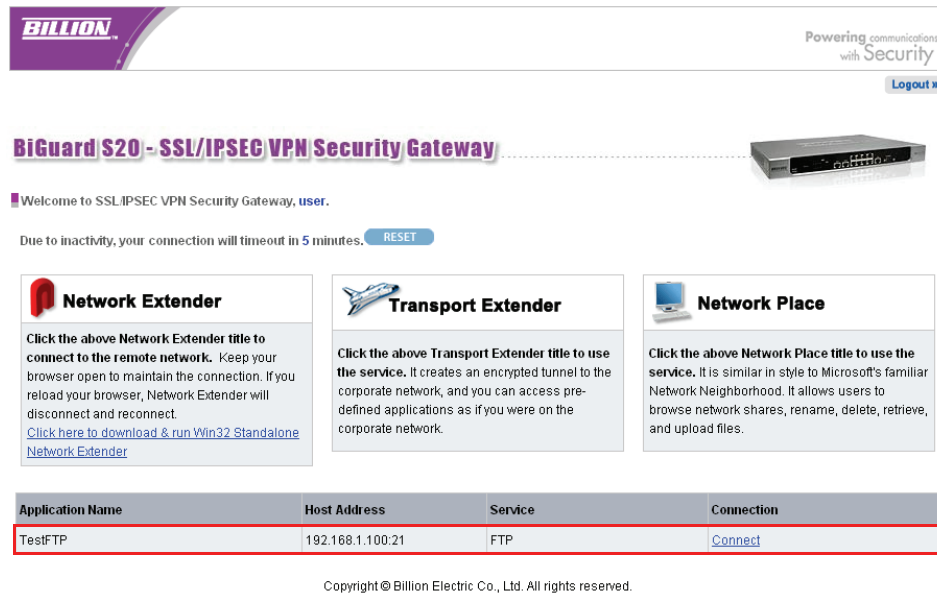


User Name: **user** (As previously added in Administrator FTP Configuration section).  
Domain: Select **BiGuard** from the drop-down menu.



**NOTE:** User Name and Password are case sensitive.

2. Click **Submit** to enter into the Remote Web Portal page.

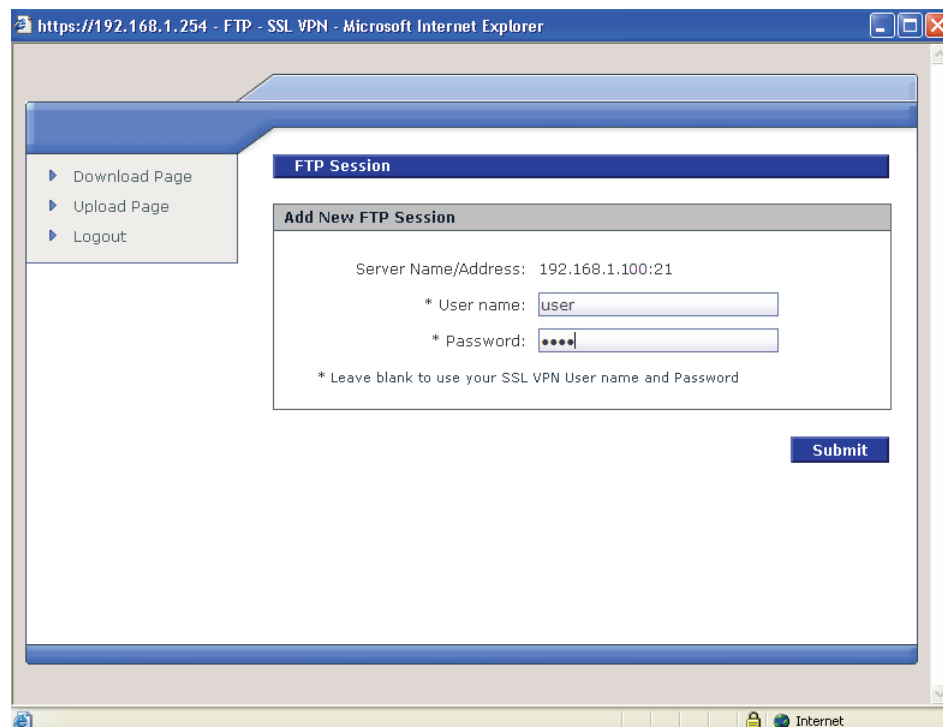


- Click **Connect** to connect to the TestFTP service.

If the user account is the same as the FTP server's account, you will not be asked to input the user name and password, and the FTP session screen appears.

If your user name differs from the FTP server's account, the following message appears.

**FIGURE 133 FTP LOGIN**



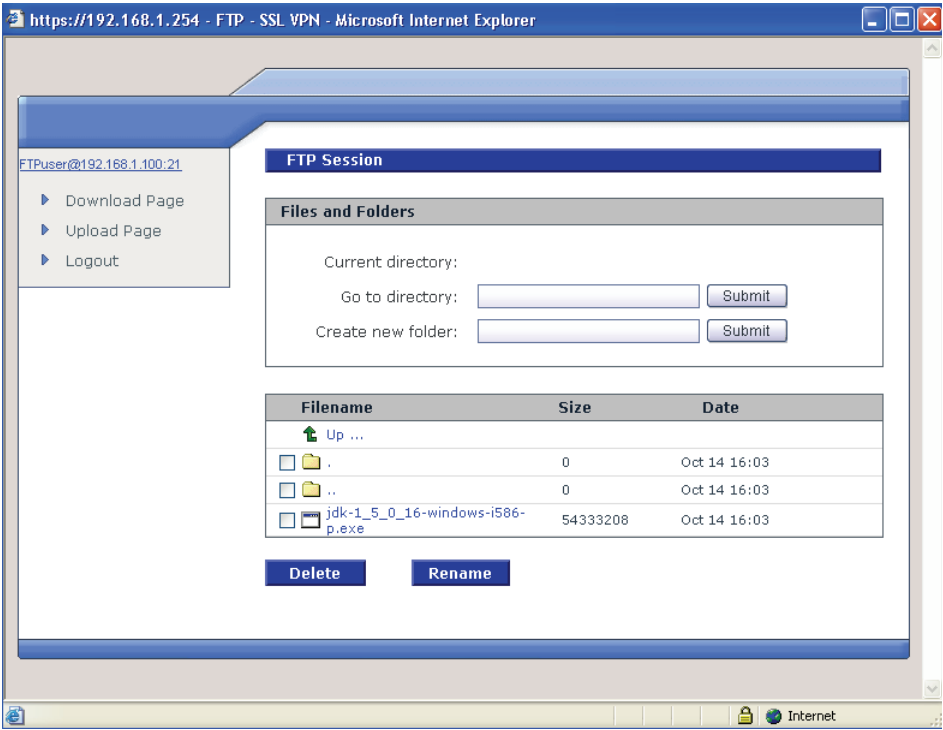
User name: Type in the username.

Password: Type in the password.

(In this example, both user name and password are **user**.)



FIGURE 134 FTP SESSION



You are logged in to your account in the designated FTP server.

## Using Telnet/SSH

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

In the tutorial that follows, you will be instructed how to administer a Telnet configuration and how a Remote User can log on the Telnet server after it is created.

### **ADMINISTRATOR TELNET CONFIGURATION**

The following procedures will allow you to configure the Telnet proxy settings in the BiGuard SSL VPN appliance for the Telnet user. Before you start to configure the Telnet proxy settings, create an account on Telnet server.

In the following example, **BiGuard** Group/Application is the default Group profile and it will be used for the tutorial.

1. Select the following link: **SSL VPN → User Access → Group/Application**.
2. To edit the BiGuard group, click **Edit** on the group profile Name.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

The Edit Group screen appears. You can add applications under your chosen Group profile to allow the users within that Group to use the applications.

Edit Group				
General Settings				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	5 Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<a href="#">Network Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)			
<a href="#">Transport Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>			
Application Table				
<a href="#">Add Application</a>				
Name	Application	IP Address / Path		
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

3. Click **Add Application** to add an application to this Group.  
You are allowed to add multiple applications under each Group.

4. Type in the application name and select the application to add to the group.  
In the following illustration, the application Name is **TestTelnet** and **Telnet** is selected from the drop-down menu as the application.

SSL VPN Application	
Add Application	
Application Name	TestTelnet
Application	File Transfer Protocol (FTP) ▼
IP Address/Domain Name	Terminal Service (RDP)
TCP Port Number	Virtual Network Computing (VNC)
	File Transfer Protocol (FTP)
	Telnet
	Secure Shell (SSH)
	Secure Shell version 2 (SSHv2)
	Web (HTTP)
	Secure Web (HTTPS)
	Network File Share (CIFS)
	Terminal Service (RDP) - Java
	Citrix(HTTP)
	Wake On LAN(WOL)
Apply	Cancel

5. Type the IP Address and the port value.  
In the illustration that follows, the IP address is 192.168.1.100 and the Telnet port is 23.

SSL VPN Application	
Add Application	
Application Name	TestTelnet
Application	Telnet ▼
IP Address/Domain Name	192.168.1.100
TCP Port Number	23
Server Mode	ASCII Mode ▼
Apply	Cancel

6. Click **Apply** to set the configuration and return to the Edit Group.
7. In the Edit Group screen, click **Apply** to set the configuration and return to Group/Application.

### Edit Group

General Settings				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	5 Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)			
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom Welcome to SSL/IPSEC \			
Application Table				
<a href="#">Add Application</a>				
Name	Application	IP Address / Path	Edit	Delete
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>
TestTelnet	Telnet	192.168.1.100:23	<a href="#">Edit</a>	<a href="#">Delete</a>
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

After creating a group profile, create (a) user account(s) and grant the user access to the applications assigned to that group profile.

8. Select the following link: **SSL VPN → User Access → Account**.

### Account

Account Table				
Name	Group			
user	BiGuard	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Copy</a>
admin	BiGuard	<a href="#">Edit</a>		
<a href="#">Create</a> <a href="#">Move</a>				

9. To create an Account, click the **Create** link at the bottom left of the Account Table. The Add Account screen appears, and you can create a user account to use the Telnet application that was created in the previous steps.



**NOTE:** This account is used for remote the web portal and different to the Telnet server account. In this example the Telnet server account is identified as user/user.

In the Add Account screen, type in the user name, the group, password and confirmation password.

10. Or you can edit existing accounts to use the applications assigned to that group profile. In the illustration that follows, the User Name is **user**, and the Group is **BiGuard**.
11. Click on **TestTelnet (Applications Proxy → Applications)** to enable access for the user.

Edit Account		
<b>General Setting</b>		
Name	user	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>Login Setting</b>		
Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	5	Minutes
<b>Service</b>		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
<b>Application Proxy</b>		
Applications	<input checked="" type="checkbox"/> TestFTP	<input checked="" type="checkbox"/> TestTelnet
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

12. Click **Apply** to set the configurations and return to the Account screen.



**NOTE:** Remember to save the settings permanently to the system by clicking on **Save Config to FLASH** on the left hand side main menu.

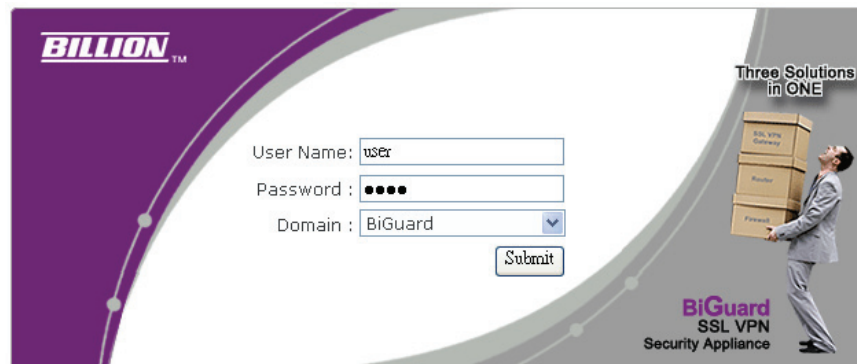
**REMOTE USER**

The following steps demonstrate how a user can log on the Telnet server from the remote web portal.


1. To access the remote web portal, please connect to the `https://wanipaddress` (where `wanipaddress` is the WAN IP address of the BiGuard SSL VPN appliance).
2. When prompted, click **Yes** on the security alert message that appears to accept the certificate and proceed with the process.



The log in screen appears.




3. Type the user name and password (Added in the Administrator Telnet Configuration section).  
In the illustration above, the User Name is **user** (The User Name and Password are case sensitive).
4. Select **BiGuard** from the drop-down **Domain** menu.
5. Click **Submit** to enter the Remote Web Portal page.
6. In the remote portal page, click **Connect** in the Connect in the applications frame to connect to the **TestTelnet** service.



Powering communications  
with Security


Logout

## BiGuard S20 - SSL/IPSEC VPN Security Gateway



Welcome to SSL/IPSEC VPN Security Gateway, user.


Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)



### Network Extender


Click the above Network Extender title 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.

[Click here to download & run Win32 Standalone Network Extender](#)



### Transport Extender

Click the above Transport Extender title 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 above Network Place title 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
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

If a certificate has expired or is invalid, a warning message displays. If the “Always trust content from this publisher” is not selected, the warning message is not disabled.

Warning - Security

The web site's certificate is invalid. Do you want to continue?

**Name:** Billion Electric Co., Ltd.

**Publisher:** Billion Electric Co., Ltd.

☐ Always trust content from this publisher.

[Yes](#) [No](#)

 The certificate cannot be verified by a trusted source. Only continue if you trust the origin of the application. [More Information...](#)

- Click **Yes** to accept the certificate.
- If the name of the site does not match the name of the certificate, the following warning message displays. Click **Run** to continue and enter the service.

Warning - Hostname Mismatch

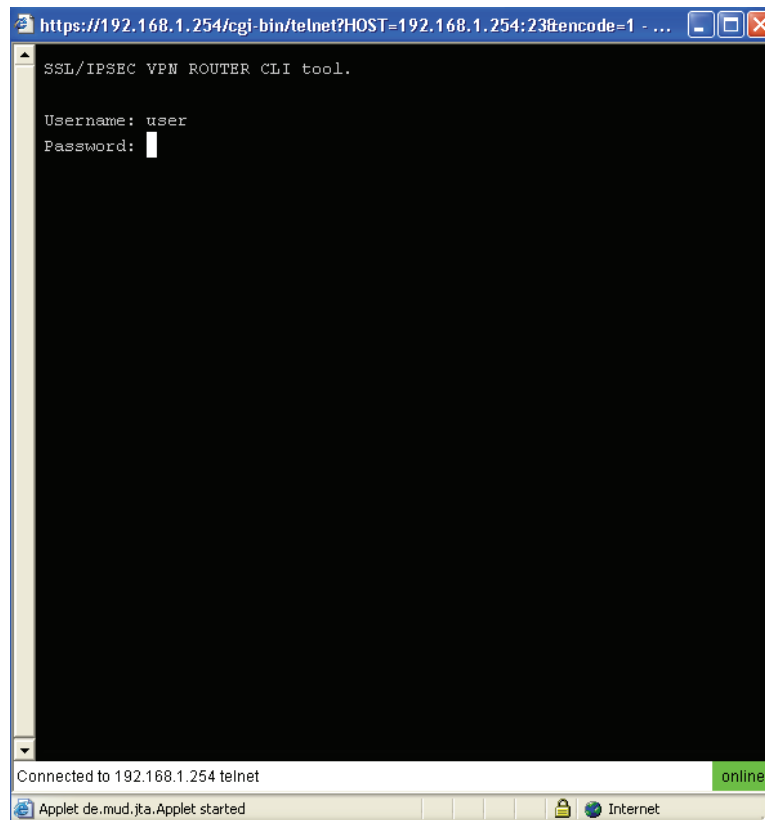
The name of the site does not match the name on the certificate. Do you want to run the application?

**Name:** 192.168.1.254

**Publisher:** "Billion Electric Co., Ltd."

[Run](#) [Cancel](#)

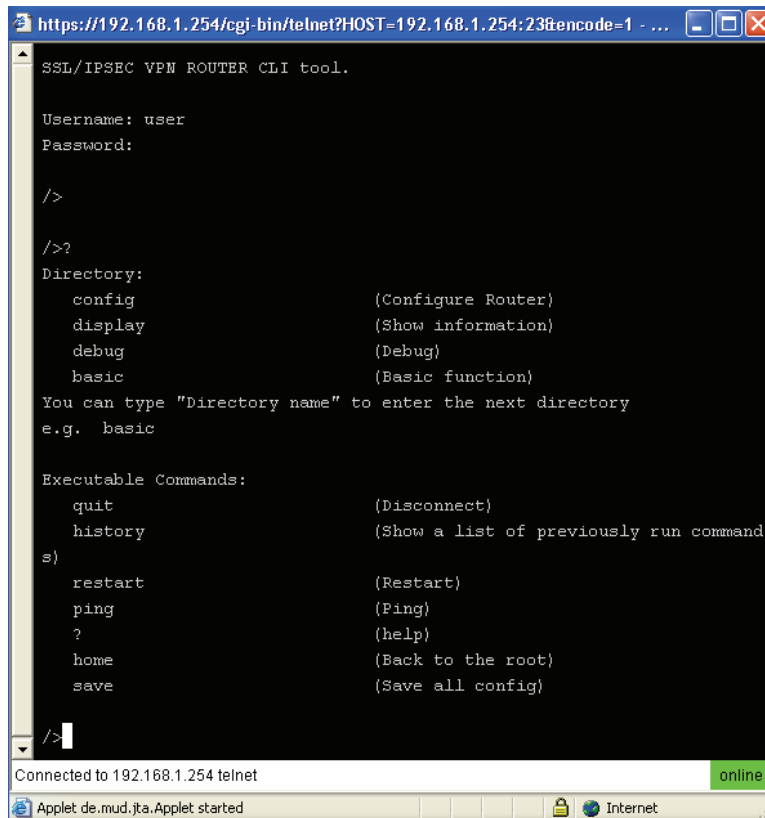
The Telnet screen appears.



9. Type the user name and password in the login screen.  
In the illustration above, the user name and password are designated as **user**.



The Welcome screen appears.



```

https://192.168.1.254/cgi-bin/telnet?HOST=192.168.1.254:23&encode=1 - ...
SSL/IPSEC VPN ROUTER CLI tool.

Username: user
Password:

/>

/>?
Directory:
  config                (Configure Router)
  display               (Show information)
  debug                 (Debug)
  basic                 (Basic function)
You can type "Directory name" to enter the next directory
e.g.  basic

Executable Commands:
  quit                  (Disconnect)
  history               (Show a list of previously run commands)
  restart               (Restart)
  ping                  (Ping)
  ?                     (help)
  home                  (Back to the root)
  save                  (Save all config)

/>
Connected to 192.168.1.254 telnet
Applet de.mud.ita.Applet started
Internet

```

The above screen shows a successful log on a Telnet server. You are prompted for a username and password to connect to the remote SSH server in the same way.

## Using HTTP(S)

This tutorial contains two sections, one dealing with Administrator HTTP(S) Configuration and the other with Remote User accessing through the HTTP(S) server after access has been created.

### **ADMINISTRATOR HTTP(S) CONFIGURATION**

Before you start to configure HTTP(S) proxy settings for BiGuard SSL VPN appliance, prepare the HTTP(S) server.

The following are the steps to configure HTTP(S) proxy settings in the BiGuard SSL VPN appliance for the HTTP(S) user: In the following example, the BiGuard Group/Application is the default Group profile and it will be used for the tutorial.

1. Select the following link **SSL VPN → User Access → Group/Application**.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

2. To edit **BiGuard** group, click the **Edit** link on the right hand side of the group profile Name.  
Edit Group screen displays, you can add applications under the chosen Group profile to allow the user(s) within that Group access to the applications.
3. Click **Add Application** to display the SSL VPN Application screen, and add an application to this Group.  
You are allowed to add multiple applications under each Group.

### Edit Group

#### General Settings

Group Name	BiGuard		
Domain	BiGuard		
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>	
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Inactivity Timeout	5	Minutes	
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		

#### Service

Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>	
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)		
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>	
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom	Welcome to SSL/IPSEC \	

#### Application Table

[Add Application](#)

Name	Application	IP Address / Path		
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>
TestTelnet	Telnet	192.168.1.100:23	<a href="#">Edit</a>	<a href="#">Delete</a>
TestSSH	SSH	192.168.1.100:22	<a href="#">Edit</a>	<a href="#">Delete</a>

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

[Apply](#) [Cancel](#)

4. Type in the application name and select the application from the drop-down menu. In the illustration that follows, the Application Name is TestHTTP(S) and the selected application is **Web(HTTP)** from the drop-down menu.

### SSL VPN Application

#### Add Application

Application Name	TestHTTP
Application	Web (HTTP) ▼
HTTP://	

[Apply](#) [Cancel](#)

- Terminal Service (RDP)
- Virtual Network Computing (VNC)
- File Transfer Protocol (FTP)
- Telnet
- Secure Shell (SSH)
- Secure Shell version 2 (SSHv2)
- Web (HTTP)**
- Secure Web (HTTPS)
- Network File Share (CIFS)
- Terminal Service (RDP) - Java
- Citrix(HTTP)
- Wake On LAN(WOL)

- Fill in the HTTP(S) with the IP address. In the following illustration, the IP address is 192.168.1.100.

SSL VPN Application	
<b>Add Application</b>	
Application Name	TestHTTP
Application	Web (HTTP) ▼
HTTP://	192.168.1.100
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Click **Apply** to set the configuration and return to the Group/Application screen.

Edit Group				
<b>General Settings</b>				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	5 Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
<b>Service</b>				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<a href="#">Network Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)			
<a href="#">Transport Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom Welcome to SSL/IPSEC \			
<b>Application Table</b>	<a href="#">Add Application</a> ▶			
Name	Application	IP Address / Path		
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
TestTelnet	Telnet	192.168.1.100:23	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
TestSSH	SSH	192.168.1.100:22	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
TestHTTP	HTTP	192.168.1.100	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

- After creating a group profile, you will need to create user accounts to use the applications assigned to that group profile.
- Select the following links **SSL VPN** → **User Access** → **Account**.

Account				
<b>Account Table</b>				
Name ▲▼	Group			
user	BiGuard	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶	<a href="#">Copy</a> ▶
admin	BiGuard	<a href="#">Edit</a> ▶		
<a href="#">Create</a> ▶ <a href="#">Move</a> ▶				

- To create an account, click the **Create** link at the bottom left of the Account Table. The Add Account screen appears, you can create a user account to use the HTTP(S)

application that was created in the previous steps.

In the Add Account screen, type in the user name, the group, password and confirmation password.

10. Or you can edit existing accounts to use the applications assigned to that group profile. In the illustration that follows, the User Name is **user**, and the Group is **BiGuard**.

Edit Account		
<b>General Setting</b>		
Name	user	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>Login Setting</b>		
Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	5	Minutes
<b>Service</b>		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
<b>Application Proxy</b>		
Applications	<input checked="" type="checkbox"/> TestFTP	<input checked="" type="checkbox"/> TestTelnet
	<input checked="" type="checkbox"/> TestSSH	<input checked="" type="checkbox"/> TestHTTP
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

11. Click the application **TestHTTP (HTTP application)** to enable the application for the user.
12. Click **Apply** to set the configurations and return to Account screen.

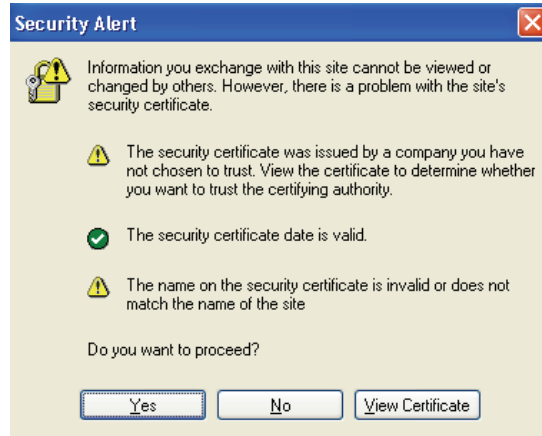


**NOTE:** Remember to save the settings permanently to the system by clicking on **Save Config to FLASH** on the left hand side main menu.

**REMOTE USER**

The following steps demonstrate how a user will log on to the HTTP(S) server from the remote web portal.


1. To access the remote web portal, please connect to the `https://wanipaddress` (where wanipaddress is the WAN IP address of the BiGuard SSL VPN appliance).



2. A Security Alert message appears, when prompted click **Yes** to proceed (to accept the certificate sent by the BiGuard system).
3. The log on screen appears.



4. Type the user name and password that were set under the Administrator HTTP Configuration section, then select the domain.  
In the following illustration, the user name is **user** and the selected domain from the drop-down menu is **BiGuard**.
5. Click **Submit** to enter into the Remote Web Portal page.
6. Click **Connect** to connect to the TestHTTP service.




Powering communications  
with Security  
[Logout »](#)

## BiGuard S20 - SSL/IPSEC VPN Security Gateway

Welcome to SSL/IPSEC VPN Security Gateway, **user**.

Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)



### Network Extender

Click the above Network Extender title 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.  
[Click here to download & run Win32 Standalone Network Extender](#)

### Transport Extender

Click the above Transport Extender title 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.

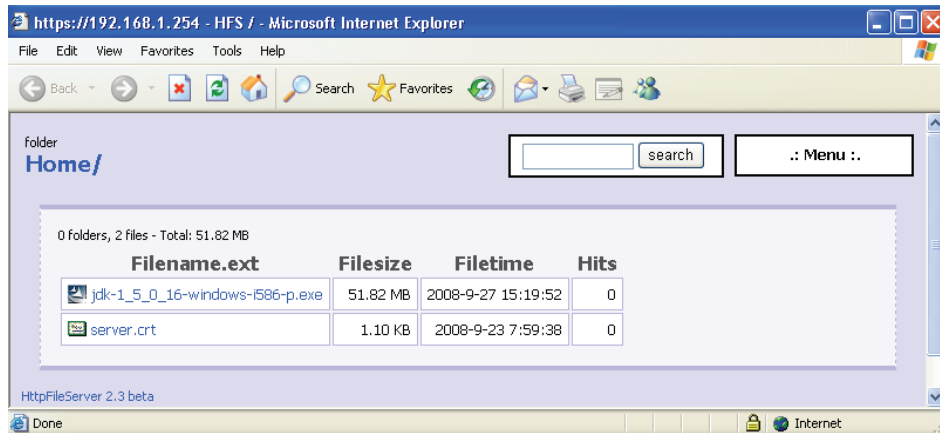
### Network Place

Click the above Network Place title 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
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

The screen below shows a successful access to the remote HTTP(S) server.



## Using RDP

This tutorial contains two sections that deal with the configuration for the Administrator Terminal Service (RDP) and the Remote User access after the configuration is created.

### **ADMINISTRATOR TERMINAL SERVICE (RDP) CONFIGURATION**

Before you start to configure the Terminal Service (RDP) proxy settings for the BiGuard SSL VPN appliance, set up the Terminal Service (RDP) settings for the computer that will access the remote site. The User Name and Password used are both user/user for this example.

1. Select the following link **SSL VPN → User Access → Group/Application**.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

2. To edit the BiGuard group, click the **Edit** link on the right hand side of the group profile Name.  
The Edit Group screen appears, and you can add applications under your chosen Group profile to allow the users within that Group to use them.
3. Click **Add Application** in the SSL VPN Application screen to add an application (Multiple applications under each Group is also allowed).

Edit Group				
General Settings				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	<input type="text" value="5"/> Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<a href="#">Network Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
<a href="#">Transport Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>			
Application Table		<a href="#">Add Application</a>		
Name	Application	IP Address / Path		
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>
TestTelnet	Telnet	192.168.1.100:23	<a href="#">Edit</a>	<a href="#">Delete</a>
TestSSH	SSH	192.168.1.100:22	<a href="#">Edit</a>	<a href="#">Delete</a>
TestHTTP	HTTP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestHTTPS	HTTPS	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				



- Enter the application name, and select the application to add from the drop-down menu. In the illustration that follows, the application name is **TestRDP** and the application is **Terminal Service (RDP)**.

SSL VPN Application	
Add Application	
Application Name	TestRDP
Application	Terminal Service (RDP) ▼
IP Address/Domain Name	Terminal Service (RDP)
Screen Size	Virtual Network Computing (VNC)
Local Device	File Transfer Protocol (FTP)
	Telnet
	Secure Shell (SSH)
	Secure Shell version 2 (SSHv2)
	Web (HTTP)
	Secure Web (HTTPS)
	Network File Share (CIFS)
	Terminal Service (RDP) - Java
Single Sign On Function	Citrix(HTTP)
Application and Path	Wake On LAN(WOL)
Terminal Server Port	
Log on to	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Enter the IP address and select the screen size. In the following illustration, the IP address is 192.168.1.100.

SSL VPN Application	
Add Application	
Application Name	TestRDP
Application	Terminal Service (RDP) ▼
IP Address/Domain Name	192.168.1.100
Screen Size	640 x 480 ▼
Local Device	<input type="checkbox"/> Drives
	<input type="checkbox"/> Ports
	<input type="checkbox"/> Printers
	<input type="checkbox"/> Smart Cards
Console Mode	<input type="checkbox"/> Active
Single Sign On Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Application and Path	
Terminal Server Port	3389
Log on to	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Click **Apply** to set the configuration and return to the Edit Group screen.

### Edit Group

General Settings				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	<input type="text" value="5"/> Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)			
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>			
Application Table				
<a href="#">Add Application</a>				
Name	Application	IP Address / Path	Edit	Delete
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>
TestTelnet	Telnet	192.168.1.100:23	<a href="#">Edit</a>	<a href="#">Delete</a>
TestSSH	SSH	192.168.1.100:22	<a href="#">Edit</a>	<a href="#">Delete</a>
TestHTTP	HTTP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestHTTPS	HTTPS	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestRDP	RDP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

- Click **Apply** again to set the configuration and return to Group/Application screen.

After creating a group profile, you will need to create user accounts to use the applications assigned to that group profile.

- Select the following link **SSL VPN** → **User Access** → **Account**.

### Account

Account Table				
Name	Group			
user	BiGuard	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Copy</a>
admin	BiGuard	<a href="#">Edit</a>		
<a href="#">Create</a> <a href="#">Move</a>				

- To create an Account, click the **Create** link at the bottom left of the Account Table. The Add Account screen appears, you can create a user account for the Terminal Service (RDP) application that was created in the previous steps.



**NOTE:** We suggest you create the same User Name and Password as your Terminal Service's account. In so doing, you will not need to type in your user name and password when accessing the Terminal Service (RDP5).

In the Add Account screen, type in the user name, the group, password and confirmation password.

10. Or you can edit existing accounts to use the applications assigned to that group profile. In the illustration that follows, the User Name is **user**, and the Group is **BiGuard**.

Edit Account		
<b>General Setting</b>		
Name	user	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>Login Setting</b>		
Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	5	Minutes
<b>Service</b>		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
<b>Application Proxy</b>		
Applications	<input checked="" type="checkbox"/> TestFTP	<input checked="" type="checkbox"/> TestTelnet
	<input checked="" type="checkbox"/> TestRDP	<input checked="" type="checkbox"/> TestSSH
	<input checked="" type="checkbox"/> TestHTTP	<input checked="" type="checkbox"/> TestHTTPS
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

11. Click **Apply** to set the configurations and return to Account Table screen.



**NOTE:** Remember to save the settings permanently to the system by clicking on **Save Config to FLASH** on the left hand side main menu.

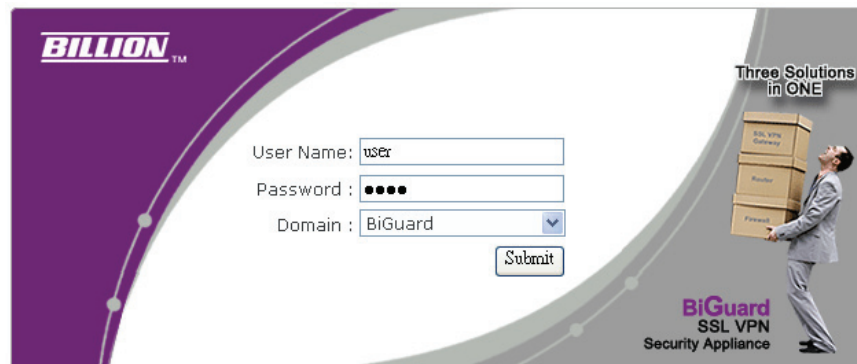
**REMOTE USER**

The following steps demonstrate how a user will log on the Terminal Service (RDP) server from the remote web portal.


1. To access the remote web portal, please connect to the <https://wanipaddress> (where wanipaddress is the WAN IP address of the BiGuard SSL VPN appliance).
2. A security alert message appears, click **Yes** when prompted to proceed (accepts the certificate sent by the BiGuard system).



The log on screen appears.




3. Enter the user name and password as it was added in the steps under the Administrator RDP Configuration section (The User Name and Password are case sensitive.).
4. Select the **BiGuard** domain from the drop-down menu.
5. Click **Submit** to enter the Remote Web Portal page.



Powering communications with Security


[Logout »](#)

## BiGuard S20 - SSL/IPSEC VPN Security Gateway



Welcome to SSL/IPSEC VPN Security Gateway, user.


Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)



### Network Extender


Click the above Network Extender title 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.

[Click here to download & run Win32 Standalone Network Extender](#)



### Transport Extender

Click the above Transport Extender title 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 above Network Place title 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
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
TestHTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
TestRDP	192.168.1.100	RDP	<a href="#">Connect</a>

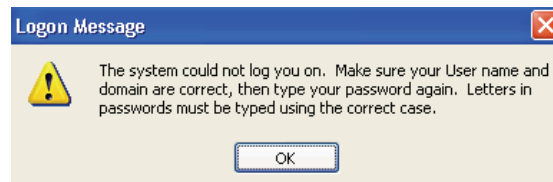
Copyright © Billion Electric Co., Ltd. All rights reserved.

6. Click **Connect** to connect to the TestRDP service.

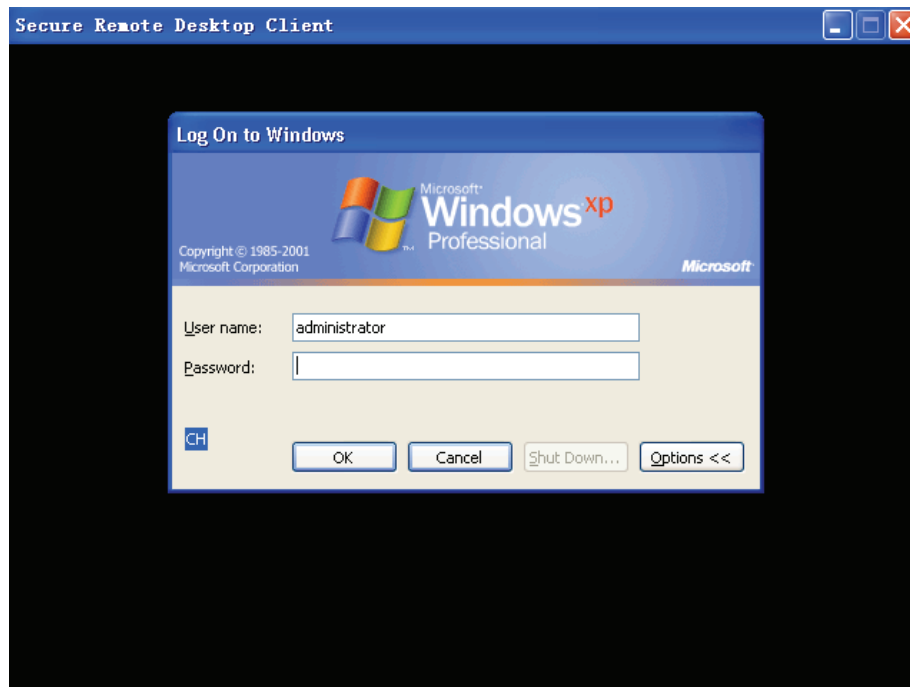
If the user account is the same as the Terminal Service's account, you will not be asked to input user name and password again. Proceed to **Step 5**.

If your user name is different from the Terminal Service's account, the following message appears.

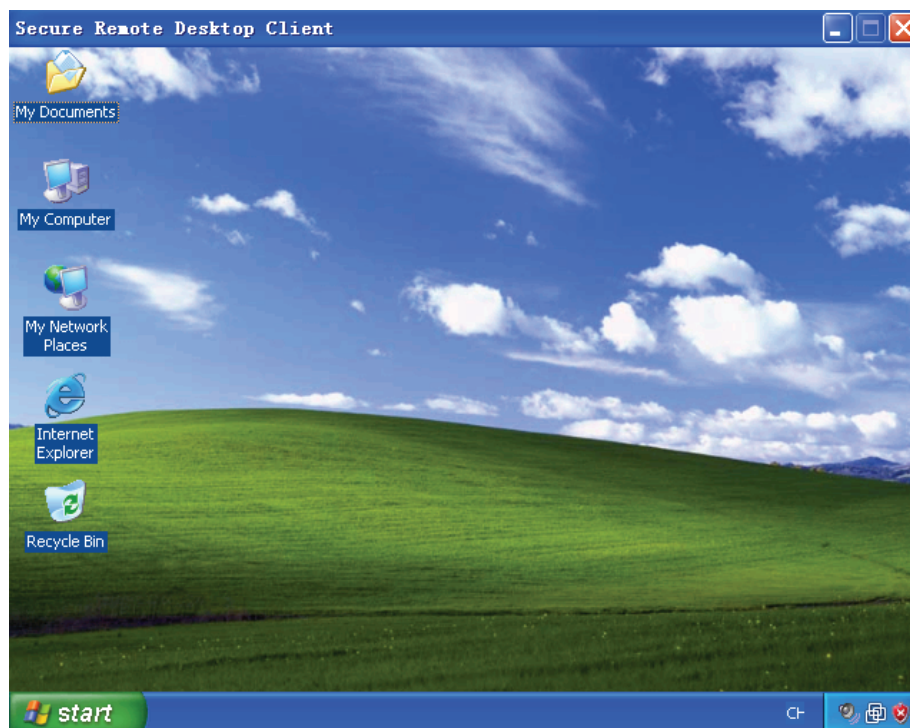
**FIGURE 135** LOGON MESSAGE



7. Click **OK** and the Window's log on screen appears.
8. Type in the user name and password of the Terminal Service's account, and click **OK** to continue.



After establishing connection, the remote computer's screen (see the following) is displayed through the Terminal Service (RDP). You successfully configured the Terminal Service (RDP).



## 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.

In this tutorial it will contain two sections, one dealing with the Administrator VNC Configuration and the other the Remote User showing how a user can log in to the VNC server after it is created.

### **ADMINISTRATOR VNC CONFIGURATION**

Before you start to configure VNC proxy settings for BiGuard SSL VPN appliance, you have to install a VNC server to be accessed from the remote site.

1. Select the following **SSL VPN → User Access → Group/Application**.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

2. Click **Edit** on the right hand side of the group profile Name to edit the Group.

The Edit Group screen displays. You can add applications under your chosen Group profile to allow the users within that Group access to the applications.

Edit Group									
General Settings									
Group Name	BiGuard								
Domain	BiGuard								
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>								
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable								
Inactivity Timeout	5	Minutes							
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable								
Service									
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable								
<a href="#">Network Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>								
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)								
<a href="#">Transport Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>								
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable								
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>								
Application Table		<a href="#">Add Application</a>							
Name	Application	IP Address / Path							
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>					
TestTelnet	Telnet	192.168.1.100:23	<a href="#">Edit</a>	<a href="#">Delete</a>					
TestSSH	SSH	192.168.1.100:22	<a href="#">Edit</a>	<a href="#">Delete</a>					
TestHTTP	HTTP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>					
TestHTTPS	HTTPS	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>					
TestRDP	RDP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>					
<b>Note!</b> To make application changes, press <b>Apply</b> .									
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>									

3. Click **Add Application**.

The SSL VPN Application screen displays. You can add an application to this Group. You are allowed to add multiple applications under each Group.

SSL VPN Application	
Add Application	
Application Name	TestVNC
Application	Virtual Network Computing (VNC) ▼
IP Address/Domain Name	Terminal Service (RDP)
TCP Port Number	Virtual Network Computing (VNC)
	File Transfer Protocol (FTP)
	Telnet
	Secure Shell (SSH)
	Secure Shell version 2 (SSHv2)
	Web (HTTP)
	Secure Web (HTTPS)
	Network File Share (CIFS)
	Terminal Service (RDP) - Java
	Citrix(HTTP)
	Wake On LAN(WOL)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Enter the IP address and TCP Port number.

IP Address: As an example, the IP address 192.168.1.100 is used for the VNC server IP Address.

TCP Port number: The default value of the VNC port is 5900.

SSL VPN Application	
Add Application	
Application Name	TestVNC
Application	Virtual Network Computing (VNC) ▼
IP Address/Domain Name	192.168.1.100
TCP Port Number	5900
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

4. Click **Apply** to set the configuration and return to the Edit Group.



### Edit Group

General Settings				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	5 Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)			
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom Welcome to SSL/IPSEC \			
Application Table				
<a href="#">Add Application</a>				
Name	Application	IP Address / Path		
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>
TestTelnet	Telnet	192.168.1.100:23	<a href="#">Edit</a>	<a href="#">Delete</a>
TestRDP	RDP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestSSH	SSH	192.168.1.100:22	<a href="#">Edit</a>	<a href="#">Delete</a>
TestHTTP	HTTP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestHTTPS	HTTPS	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestVNC	VNC	192.168.1.100:5900	<a href="#">Edit</a>	<a href="#">Delete</a>

- Click **Apply** to set the configuration.

After creating a group profile, you will need to create user accounts to use the applications assigned to that group profile.

- Select the following **SSL VPN** → **User Access** → **Account**.

### Account

Account Table				
Name	Group			
user	BiGuard	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Copy</a>
admin	BiGuard	<a href="#">Edit</a>		

[Create](#) [Move](#)

- Click the **Create** link at the bottom left of the Account Table to create an account.

The Add Account screen displays. You can create a user account to use the VNC application that created in the previous steps.



**NOTE:** This account is used in the remote web portal.

In the Add Account screen, type in the user name, the group, password and confirmation password.

8. Or you can edit existing accounts to use the applications assigned to that group profile. In the illustration that follows, the User Name is **user**, and the Group is **BiGuard**.

Edit Account		
<b>General Setting</b>		
Name	user	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>Login Setting</b>		
Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	5	Minutes
<b>Service</b>		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>
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	<input checked="" type="radio"/> Default <input type="radio"/> Custom	<input type="text" value="Welcome to SSL/IPSEC \"/>
<b>Application Proxy</b>		
Applications	<input checked="" type="checkbox"/> TestFTP	<input checked="" type="checkbox"/> TestTelnet
	<input checked="" type="checkbox"/> TestRDP	<input checked="" type="checkbox"/> TestVNC
	<input checked="" type="checkbox"/> TestSSH	<input checked="" type="checkbox"/> TestHTTP
	<input checked="" type="checkbox"/> TestHTTPS	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

9. Click the application **TestVNC** (VNC application) to enable the application for the user.
10. Click **Apply** to set the configurations and return to Account Table.

Account				
Account Table				
Name ▲▼	Group			
user	BiGuard	<a href="#">Edit ▶</a>	<a href="#">Delete ▶</a>	<a href="#">Copy ▶</a>
admin	BiGuard	<a href="#">Edit ▶</a>		
<a href="#">Create ▶</a> <a href="#">Move ▶</a>				



**NOTE:** Remember to save the settings permanently to the system by clicking on **Save Config to FLASH** on the left hand side main menu.

## REMOTE USER

The following steps demonstrate how a user will log in to the VNC server from the remote web portal.

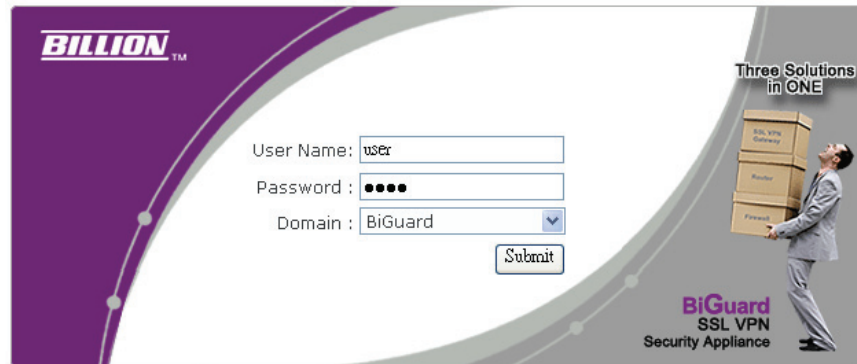
To access the remote web portal, please connect to the <https://wanipaddress> (where wanipaddress is the WAN IP address of the BiGuard SSL VPN appliance).

A Security Alert message appears.

1. Click **Yes** to proceed (to accept the certificate sent by the BiGuard system).



After **Yes** is clicked, the log on screen will appear.




User Name: **user** (As previously added in Administrator VNC Configuration section.)  
 Domain: Select **BiGuard** from the drop-down menu.



**NOTE:** User Name and Password are case sensitive.


2. Click **Submit** to enter into the Remote Web Portal page.



Powering communications  
with Security

Logout


BiGuard S20 - SSL/IPSEC VPN Security Gateway



Welcome to SSLIPSEC VPN Security Gateway, user.


Due to inactivity, your connection will timeout in 5 minutes. 

RESET




Network Extender

Click the above Network Extender title 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.  
[Click here to download & run Win32 Standalone Network Extender](#)



Transport Extender

Click the above Transport Extender title 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 above Network Place title 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.

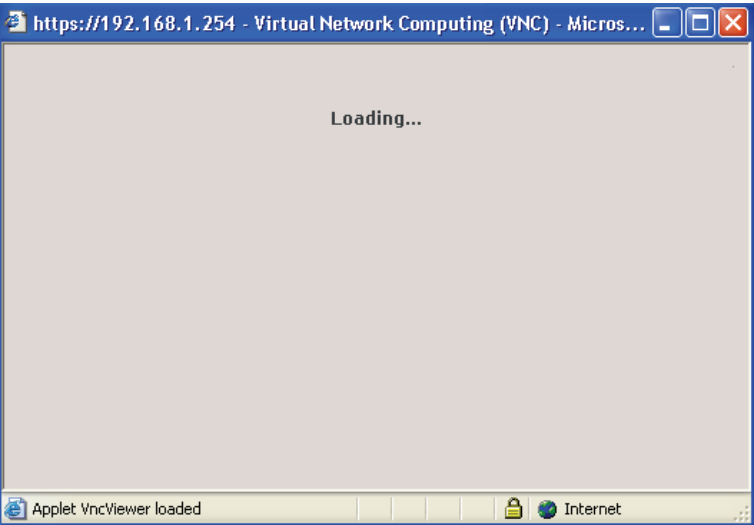
Application Name	Host Address	Service	Connection
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
TestHTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
TestRDP	192.168.1.100	RDP	<a href="#">Connect</a>
TestVNC	192.168.1.100:5900	VNC	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

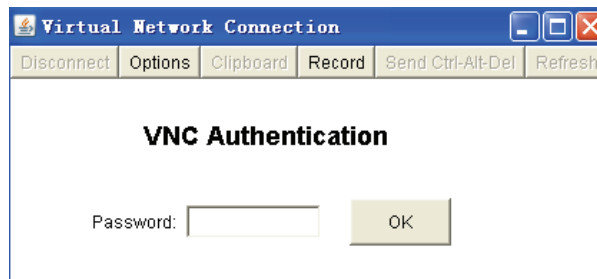
3. Click **Connect** to connect to the TestVNC service.

The following page appears when loading the VNC client program into your computer.

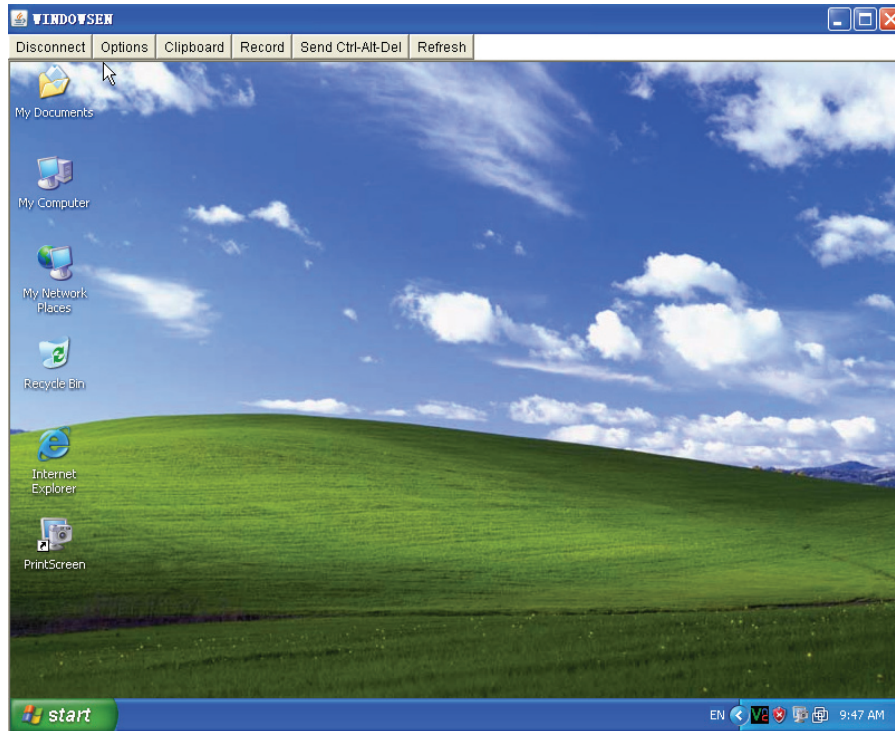
FIGURE 136 VNC LOADING



Next, the VNC Authentication log on screen appears.



4. Input the VNC server password, and click **OK**.



The above screen shot represents the remote computer as accessed through the VNC server.

## Using CIFS

The Common Internet File System (CIFS) is an application protocol designed to allow remote users direct access to specific network resources.

### **ADMINISTRATOR CIFS CONFIGURATION**

In the following tutorial you will be guided on administrator CIFS configuration and remote user access to the CIFS application after it has been created. Administrator CIFS Configuration:

1. Select the following links: **SSL VPN** → **User Access** → **Group/Application**.
2. In the Group/Applications menu, click the **Edit** link on the right hand side of the group profile name.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

The Edit Group screen displays.


3. In the Edit Group screen, click **Add Application** to add applications to the selected group. You can add multiple applications.

Edit Group				
General Settings				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	<input type="text" value="5"/> Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<a href="#">Network Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
<a href="#">Transport Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>			
Application Table		<a href="#">Add Application</a>		
Name	Application	IP Address / Path		
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>
TestTelnet	Telnet	192.168.1.100:23	<a href="#">Edit</a>	<a href="#">Delete</a>
TestRDP	RDP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestSSH	SSH	192.168.1.100:22	<a href="#">Edit</a>	<a href="#">Delete</a>
TestHTTP	HTTP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestHTTPS	HTTPS	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestVNC	VNC	192.168.1.100:5900	<a href="#">Edit</a>	<a href="#">Delete</a>
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

4. Type in the application name, and select the application to add from the drop-down menu.  
In the illustration that follows, **Network File Share (CIFS)** is selected as the application to be added.

SSL VPN Application

Add Application


Application Name	TestCIFS
Application	Network File Share (CIFS) 
Network Path	<div>Terminal Service (RDP) Virtual Network Computing (VNC) File Transfer Protocol (FTP) Telnet Secure Shell (SSH) Secure Shell version 2 (SSHv2) Web (HTTP) Secure Web (HTTPS) <b>Network File Share (CIFS)</b> Terminal Service (RDP) - Java Citrix(HTTP) Wake On LAN(WOL)</div>

Apply Cancel

5. Type the application name adn network path in the **Application Name** and **Network Path** fields.  
In the following illustration, the application name is *TestCIFS* and the network path is *\192.168.1.100\folder*.

SSL VPN Application

Add Application

Application Name	TestCIFS
Application	Network File Share (CIFS) 
Network Path	\192.168.1.100\folder (ex: \\Computer Name\Folder)

Apply Cancel

6. Click **Apply** to set the configuration and return to the Group/Application menu.

### Edit Group

#### General Settings

Group Name	BiGuard		
Domain	BiGuard		
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>	
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Inactivity Timeout	5	Minutes	
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		

#### Service

Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>	
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)		
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>	
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom	Welcome to SSL/IPSEC \	

#### Application Table

[Add Application](#)

Name	Application	IP Address / Path		
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>
TestTelnet	Telnet	192.168.1.100:23	<a href="#">Edit</a>	<a href="#">Delete</a>
TestRDP	RDP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestVNC	VNC	192.168.1.100:5900	<a href="#">Edit</a>	<a href="#">Delete</a>
TestSSH	SSH	192.168.1.100:22	<a href="#">Edit</a>	<a href="#">Delete</a>
TestHTTP	HTTP	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestHTTPS	HTTPS	192.168.1.100	<a href="#">Edit</a>	<a href="#">Delete</a>
TestCIFS	CIFS	\\192.168.1.100\Folder	<a href="#">Edit</a>	<a href="#">Delete</a>

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

[Apply](#) [Cancel](#)

- After creating a group profile, you will need to create user accounts to use the applications assigned to that group profile.
- Select the following link **SSL VPN** → **User Access** → **Account**.

### Account

#### Account Table

Name	Group			
user	BiGuard	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Copy</a>
admin	BiGuard	<a href="#">Edit</a>		

[Create](#) [Move](#)

- To create an Account, click the **Create** link at the bottom left of the Account Table. The Add Account screen appears, and you can create a user account to use the CIFS application that was created in the previous steps.



**NOTE:** We suggest you create the same User Name and Password as your CIFS server's account. In this way, the CIFS application can be accessed without having to type in a user name and password again.



In the Add Account screen, type in the user name, the group, password and confirmation password.

10. Or you can edit existing accounts to use the applications assigned to that group profile. In the illustration that follows, the User Name is **user**, and the Group is **BiGuard**.

Edit Account		
<b>General Setting</b>		
Name	user	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>Login Setting</b>		
Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	5	Minutes
<b>Service</b>		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
<b>Application Proxy</b>		
Applications	<input checked="" type="checkbox"/> TestFTP	<input checked="" type="checkbox"/> TestTelnet
	<input checked="" type="checkbox"/> TestRDP	<input checked="" type="checkbox"/> TestVNC
	<input checked="" type="checkbox"/> TestSSH	<input checked="" type="checkbox"/> TestHTTP
	<input checked="" type="checkbox"/> TestHTTPS	<input checked="" type="checkbox"/> TestCIFS
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

11. Select **TestCIFS** (CIFS application) to enable the application for the user.
12. Click **Apply** to set the configurations and return to the Account screen.

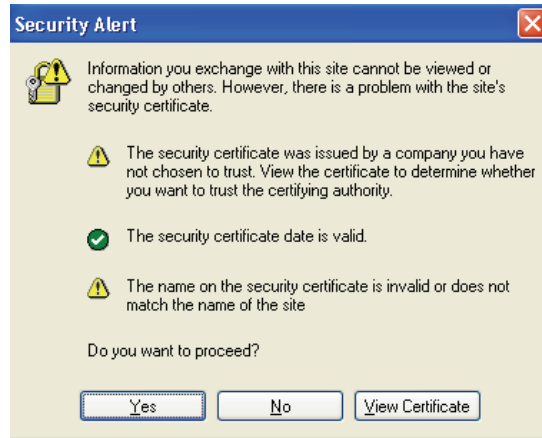


**NOTE:** Remember to save the settings permanently to the system by click on **Save Config to FLASH** on the left hand side of the main menu.

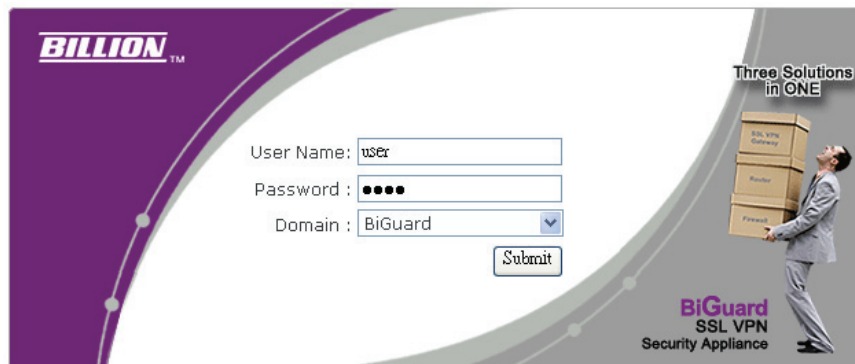
**REMOTE USER**

The following steps demonstrate how a user will log on the CIFS server from the remote web portal.

1. To access the remote web portal, please connect to the `https://wanipaddress` (where `wanipaddress` is the WAN IP address of the BiGuard SSL VPN appliance).



2. A Security Alert message appears, click **Yes** when you are prompted to proceed (to accept the certificate sent by the BiGuard system).  
The log in screen appears.
3. Type in the user name and password as created in the previous steps under the Administrator CIFS Configuration section and select the **BiGuard** domain from the drop-down menu.



4. Click **Submit** to enter into the Remote Web Portal page.
5. In the Remote Web Portal, click **Connect** on the TestCIFS application to connect to the service.



## Additional Applications

Additional applications, such as the Mail server, are available and can be configured for user requirements. Access to the Mail server can be obtained through either the Network Extender or Transport Extender applications.

In this tutorial you will be introduced to two areas of the Mail Server Application, they include Configuring the Administrator Mail server and Remote User access after configuring the Mail Server Application.

### Mail server (Network Extender)

Before you start to configure Mail server proxy settings for BiGuard SSL VPN appliance, you have to make sure the Mail server is ready, and you can arrange the user to access the Mail server by Network Extender.

In the example that follows, the mail server's IP address is set to 192.168.1.254.

#### **ADMINISTRATOR MAIL SERVER CONFIGURATION**

To configure Mail server settings on the BiGuard SSL VPN appliance for the Mail server user, see the following steps:

1. Choose **SSL VPN → User Access → Account**.

Account				
Account Table				
Name ▲▼	Group			
user	BiGuard	Edit ▶	Delete ▶	Copy ▶
admin	BiGuard	Edit ▶		
Create ▶ Move ▶				

2. To create an Account, click the **Create** link at the bottom left of the Account Table. The Add Account screen appears, and you can create a user account with access to the Mail server.
3. In the Add Account screen, type the user name, select the group from the drop-down menu, and type the password for the account.

In the illustration below: the user name is **NetworkUser** and the **BiGuard** is the group selection.

4. Check whether or not you will like the **Host Checking** to be Active.

Add Account

General Setting

User Name

NetworkUser

☒ Active

Group

BiGuard

Password

\*\*\*\*\*

Retype Password

\*\*\*\*\*

☐ Use group default password

Host Checking

☒ Active

[Advanced Setting](#)

Apply

Cancel

Group Setting Details

Force Login

Disable

Inactivity Timeout

5 Minutes

Network Place

Enable

Network Extender Service

Enable

Transport Extender Service

Standalone Application (Win32 Only) Enable

Web Cache Cleaner

Enable

Greeting String

Use default greeting string

Applications

TestFTP , TestTelnet , TestRDP , TestVNC , TestSSH , TestHTTP , TestHTTPS , TestCIFS

5. Click **Apply** to set the configurations and return to the Account screen. Then click **Edit** to change the setting of **NetworkUser** account.

Account				
Account Table				
Name	Group			
user	BiGuard	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Copy</a>
admin	BiGuard	<a href="#">Edit</a>		
NetworkUser	BiGuard	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Copy</a>
<a href="#">Create</a> <a href="#">Move</a>				

6. Select the Network Extender Service to enable the application for the user.

Edit Account		
<b>General Setting</b>		
Name	NetworkUser	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>Login Setting</b>		
Password	••••••	
Retype Password	••••••	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	5	Minutes
<b>Service</b>		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
<b>Application Proxy</b>		
Applications	<input checked="" type="checkbox"/> TestFTP	<input checked="" type="checkbox"/> TestTelnet
	<input checked="" type="checkbox"/> TestRDP	<input checked="" type="checkbox"/> TestVNC
	<input checked="" type="checkbox"/> TestSSH	<input checked="" type="checkbox"/> TestHTTP
	<input checked="" type="checkbox"/> TestHTTPS	<input checked="" type="checkbox"/> TestCIFS
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

When you choose to assign the IP address dynamically, you have to setup the client IP address assignment by inputting the beginning and ending Client Address Range. If you choose **Fix IP**, proceed to **Step 9** and skip the steps that follow.

7. Select **SSL VPN** → **Network Extender** → **Client Address**.

Network Extender		
<b>Client IP Address Assignment</b>		
Client Address Range Begin	192.168.1.210	
Client Address Range End	192.168.1.230	
DNS Server	Primary	
	Secondary	
WINS Server	Primary	
	Secondary	
NetBIOS Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Tunnel All Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

8. Type in the client address range for the remote user.
9. Select whether to enable or disable **NetBIOS Broadcast**. When enabled, **NetBIOS Broadcast** performs a communication from the computer to all other computers on the network for the purpose of trying to resolve NetBIOS names.

10. Select ☐ to enable or disable **Tunnel All Mode**. When it is enabled, **Tunnel All Mode** sends all data traffic from the computer through Network Extender to the remote network.

11. Click **Apply** to set the configurations.

When the client IP address and the office network address are in the different subnet, you have to add a client route to the office network so that the IP packets to the office network will be routed to the SSL connection. If the client IP address and the office network address are in the same subnet, proceed to the Remote User section.

12. Select **SSL VPN** → **Network Extender** → **Client Route**.

Network Extender			
Client Routing Table			
Destination	Subnet Mask		
<a href="#">Create</a>			

13. Click **Create** to create a Client Route profile.

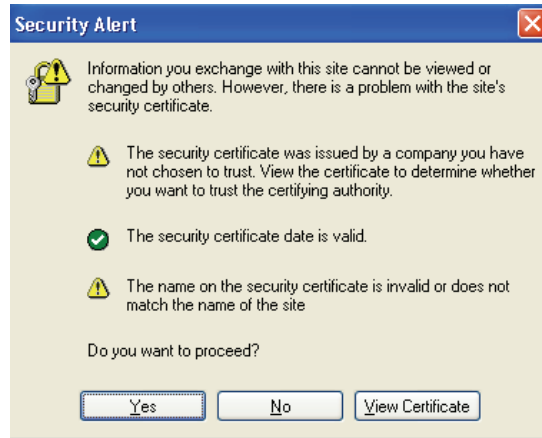
Network Extender	
Add Client Route	
Destination Address	<input type="text"/>
Destination Subnet Mask	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

14. Type the Destination Address and Destination Subnet Mask from the client route to add.
15. Click **Apply** to set the configuration.

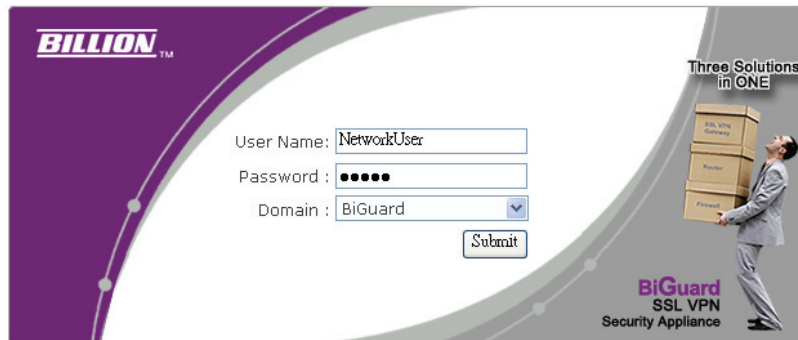
**REMOTE USER**

The following steps demonstrate how a user log on the Mail server from the remote web portal.

1. To access the remote web portal, please connect to the <https://wanipaddress> (where wanipaddress is the WAN IP address of the BiGuard SSL VPN appliance).  
A Security Alert message appears.




2. Click **Yes** when prompted to proceed (to accept the certificate sent by the BiGuard system).  
The log on screen appears.
3. Type in the user name and password as created in the previous steps under Administrator Mail server Configuration section and select the **BiGuard** domain from the drop-down menu.



4. Click **Submit** to enter into the Remote Web Portal page.






Powering communications  
with Security  
[Logout](#)


---

## BiGuard S20 - SSL/IPSEC VPN Security Gateway



Welcome to SSL/IPSEC VPN Security Gateway, **NetworkUser**.


Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)



### Network Extender


Click the above Network Extender title 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.

[Click here to download & run Win32 Standalone Network Extender](#)



### Transport Extender

Click the above Transport Extender title 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 above Network Place title 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
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
TestHTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
TestRDP	192.168.1.100	RDP	<a href="#">Connect</a>
TestVNC	192.168.1.100:5900	VNC	<a href="#">Connect</a>
TestCIFS	192.168.1.100/folder	CIFS	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

### 5. Click **Network Extender**.


This website wants to install the following add-on: 'XTunnel.cab' from 'Billion Electric Co., Ltd.'. If you trust the website and the add-on and want to install it, click here...



Powering communications  
with Security  
[Logout](#)


---

## BiGuard S20 - SSL/IPSEC VPN Security Gateway



Welcome to SSL/IPSEC VPN Security Gateway, **NetworkUser**.


Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)



### Network Extender


Click the above Network Extender title 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.

[Click here to download & run Win32 Standalone Network Extender](#)



### Transport Extender

Click the above Transport Extender title 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 above Network Place title 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
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
TestHTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
TestRDP	192.168.1.100	RDP	<a href="#">Connect</a>
TestVNC	192.168.1.100:5900	VNC	<a href="#">Connect</a>
TestCIFS	192.168.1.100/folder	CIFS	<a href="#">Connect</a>

If the browser is not allowed to launch the ActiveX automatically, the following warning message displays, then click **OK** to continue. If the browser is allowed to install the ActiveX automatically, the message will not display. Please go to **Step 8** directly.

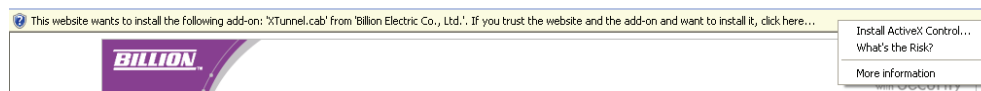
Microsoft Internet Explorer



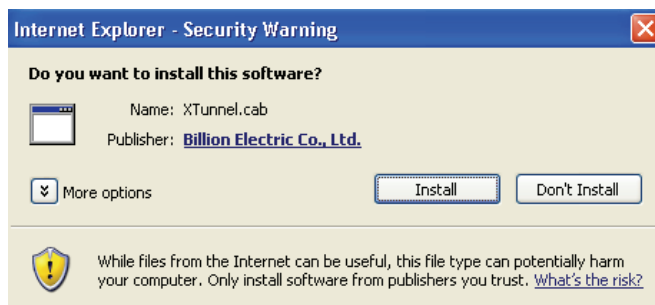
Network Extender could not be installed. Verify if you are running Microsoft Internet Explorer and if ActiveX Control is enabled in your browser security settings. And you must have administrative rights.

OK

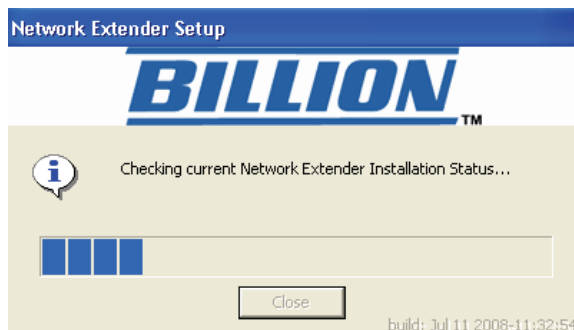
6. On the information bar, click **Install ActiveX Control**.



7. After the screen refreshes, click **Network Extender** once again.
8. You are required to install the **XTunnel.cab**. Click **Install** to install the software.



The Network Extender Setup proceeds.



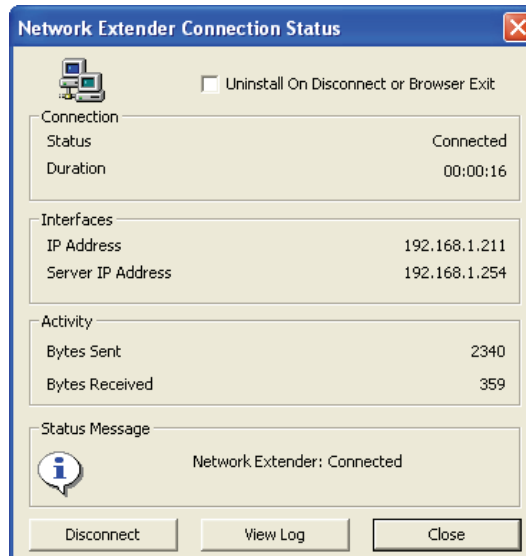
9. You are prompted to install the **SSLDrv Adapter**.




10. Click **Continue Anyway** when prompted to accept the SSLDrv Adapter. The procedure continues.

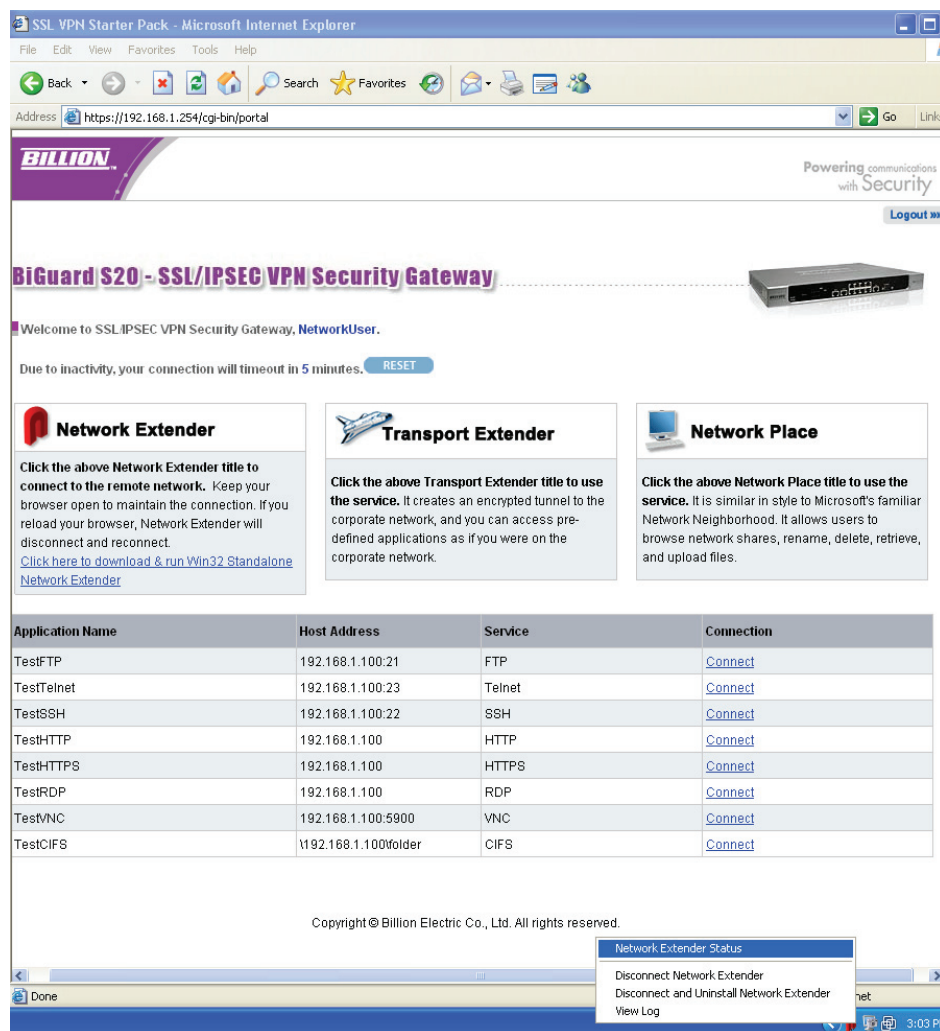


11. After the installation is complete, the Network Extender Connection Status window displays.



- 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 Network Extender Status, right-click the Network Extender icon  on the tool bar, and select an option from the menu in order to view the status screen again, or perform one of the actions above.



Now the client users can access the Mail server through their mail software as if they were in the office.

## Mail server (Transport Extender)

Before you start to configure Mail server proxy settings for BiGuard SSL VPN appliance, you have to make sure the Mail server is read, and you can arrange the user to access the Mail server by Transport Extender.

In the example below, the mail server's IP address is set to 192.168.1.254.

### **ADMINISTRATOR MAIL SERVER CONFIGURATION**

To configure Mail server settings on the BiGuard SSL VPN appliance for the Mail server user, follow the steps below:

1. Select the following link **SSL VPN → User Access → Account**.

Account				
Account Table				
Name ▲▼	Group			
user	BiGuard	Edit ►	Delete ►	Copy ►
admin	BiGuard	Edit ►		
Create ► Move ►				

2. To create an Account, click the **Create** link at the left bottom of the Account Table. The Add Account screen appears, and you can create a user account with access to the Mail server.
3. In the Add Account screen, type the user name, select the group from the drop-down menu, and type the password for the account.

In the illustration below: the user name is **NetworkUser** and the **BiGuard** is the group selection.

4. Type in the minutes for inactivity timeout and check whether or not you will like the **Host Checking** to be Active.

Add Account		
General Setting		
User Name	NetworkUser	<input checked="" type="checkbox"/> Active
Group	BiGuard ▼	
Password	*****	
Retype Password	*****	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Group Setting Details	
Force Login	Disable
Inactivity Timeout	5 Minutes
Network Place	Enable
Network Extender Service	Enable
Transport Extender Service	Standalone Application (Win32 Only) Enable
Web Cache Cleaner	Enable
Greeting String	Use default greeting string
Applications	TestFTP , TestTelnet , TestRDP , TestVNC , TestSSH , TestHTTP , TestHTTPS , TestCIFS

- Click **Apply** to set the configurations and return to the Account screen. Then click **Edit** to change the setting of **NetworkUser** account.

Account				
Account Table				
Name ▲▼	Group			
user	BiGuard	<a href="#">Edit ▶</a>	<a href="#">Delete ▶</a>	<a href="#">Copy ▶</a>
admin	BiGuard	<a href="#">Edit ▶</a>		
NetworkUser	BiGuard	<a href="#">Edit ▶</a>	<a href="#">Delete ▶</a>	<a href="#">Copy ▶</a>
<a href="#">Create ▶</a> <a href="#">Move ▶</a>				

- Select the Transport Extender Service to enable the application for the user.

Edit Account		
General Setting		
Name	NetworkUser	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Login Setting		
Password	••••••	
Retype Password	••••••	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	5	Minutes
Service		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
Application Proxy		
Applications	<input checked="" type="checkbox"/> TestFTP	<input checked="" type="checkbox"/> TestTelnet
	<input checked="" type="checkbox"/> TestRDP	<input checked="" type="checkbox"/> TestVNC
	<input checked="" type="checkbox"/> TestSSH	<input checked="" type="checkbox"/> TestHTTP
	<input checked="" type="checkbox"/> TestHTTPS	<input checked="" type="checkbox"/> TestCIFS
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

- After the user account is created with the Transport Extender service enabled, setup the designated service port and the server's IP address.
- Select **SSL VPN** → **Transport Extender** → **Application**.

Transport Extender				
Configured Applications for Transport Extender				
Local Server IP Address	Protocol	Port Number		
<a href="#">Create ▶</a>				

- Click **Create** to create a POP3 application profile.

Transport Extender	
Add an Application to be Tunneled by Transport Extender	
Local Server IP Address	<input type="radio"/> All IP Addresses <input checked="" type="radio"/> Fixed IP Address 192.168.1.254
Protocol	TCP
Port Number	<input type="radio"/> All Ports <input checked="" type="radio"/> Fixed Port 110 ~ 110
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

10. In Local Server IP Address, choose the Fixed IP address to the office network through the secure SSL VPN connection (the mail server's IP address is 192.168.1.254 in this example).
11. In TCP Port Number, choose the Fixed TCP Port of the specified IP Addresses to the mail server and input 110 to the fields. (In the above example, the POP3 port is 110.)
12. Click **Apply** to save configurations.
13. Click **Create** to create an SMTP application profile.
14. In the **Local Server IP Address** field, select **Fixed IP Address** and enter the office networks, SSL VPN, secured IP address (the mail server's IP address is 192.168.1.254 in this example.)
15. In the **TCP Port Number** field, select **Fixed TCP Port** and enter the corresponding port in the fields. (In the example, the SMTP port is 25.)
16. Click **Apply** to set the configuration.

### **HOST NAME RESOLUTION**

In the Transport Extender, you can setup the domain name for an IP address. This will allow you to access the server's IP address by typing the domain name.

1. Select **SSL VPN → Transport Extender → Host Name Resolution**.

Transport Extender	
Configured Host Name Resolution for Transport Extender	
Local Server IP Address	Fully Qualified Domain Name
<input type="button" value="Create"/>	

2. Click **Create** to create a Host Name Resolution profile.

Transport Extender	
Add a Host Name Resolution to Transport Extender	
Local Server IP Address	192.168.1.254
Full Qualified Domain Name	mail.billion.com
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

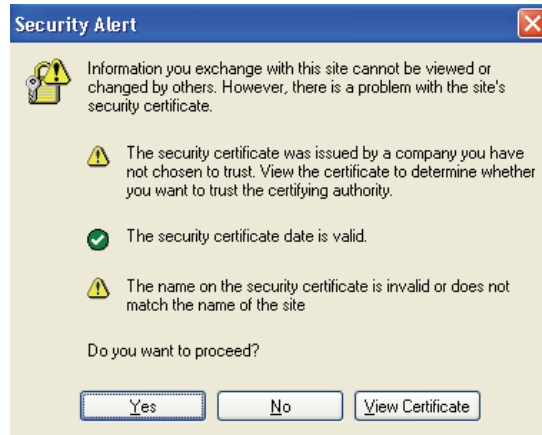
3. In the **Local Server IP Address** field, type in the mail server's IP address (192.168.1.254 in this example).
4. In the **Full Qualified Domain Name** field, type in the domain name for the mail server's IP address (mail.test.com in this example).
5. Click **Apply** to set the configurations.

**REMOTE USER**

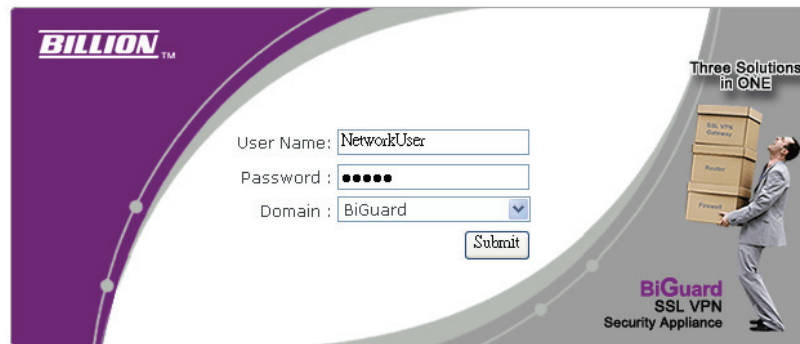
The following steps demonstrate how a user will log in to the Mail server from the remote web portal.

1. To access the remote web portal, please connect to the `https://wanipaddress` (where `wanipaddress` is the WAN IP address of the BiGuard SSL VPN appliance).

A Security Alert message appears.




2. Click **Yes** when prompted to proceed (to accept the certificate sent by the BiGuard system).  
The log in screen appears.
3. Type in the user name and password as created in the previous steps under **Administrator Mail Server Configuration** section and select the BiGuard domain from the drop-down menu.



4. Click **Submit** to enter into the Remote Web Portal page.






Powering communications  
with Security  
[Logout](#)


---

## BiGuard S20 - SSL/IPSEC VPN Security Gateway




Welcome to SSL/IPSEC VPN Security Gateway, **NetworkUser**.

Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)




### Network Extender

Click the above Network Extender title 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.  
[Click here to download & run Win32 Standalone Network Extender](#)



### Transport Extender

Click the above Transport Extender title 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 above Network Place title 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
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
TestHTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
TestRDP	192.168.1.100	RDP	<a href="#">Connect</a>
TestVNC	192.168.1.100:5900	VNC	<a href="#">Connect</a>
TestCIFS	192.168.1.100/folder	CIFS	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

### 5. Click Transport Extender.


This website wants to install the following add-on: 'MLWebCacheCleaner.cab' from 'Billion Electric Co., Ltd.'. If you trust the website and the add-on and want to install it, click here... ✕



Powering communications  
with Security  
[Logout](#)


---

## BiGuard S20 - SSL/IPSEC VPN Security Gateway




Welcome to SSL/IPSEC VPN Security Gateway, **NetworkUser**.

Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)




### Network Extender

Click the above Network Extender title 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.  
[Click here to download & run Win32 Standalone Network Extender](#)



### Transport Extender

Click the above Transport Extender title 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 above Network Place title 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
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>

If the browser is not allowed to launch the ActiveX automatically, the warning message below appears, click **OK** to continue. If the browser is allowed to install the ActiveX automatically, the message will not display. Please go to **Step 8** directly.

Microsoft Internet Explorer
✕



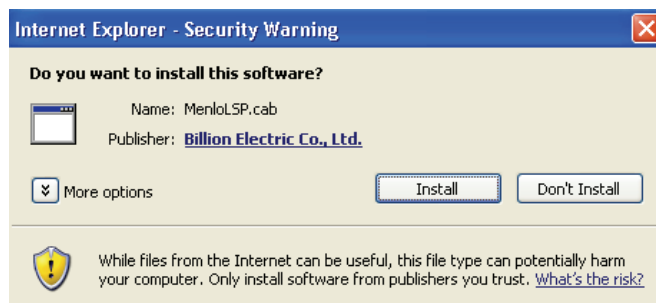
Transport Extender could not be installed. Verify if you are running Microsoft Internet Explorer and if ActiveX Control is enabled in your browser security settings. And you must have administrative rights.

OK

- On the information bar, click **Install ActiveX Control**.

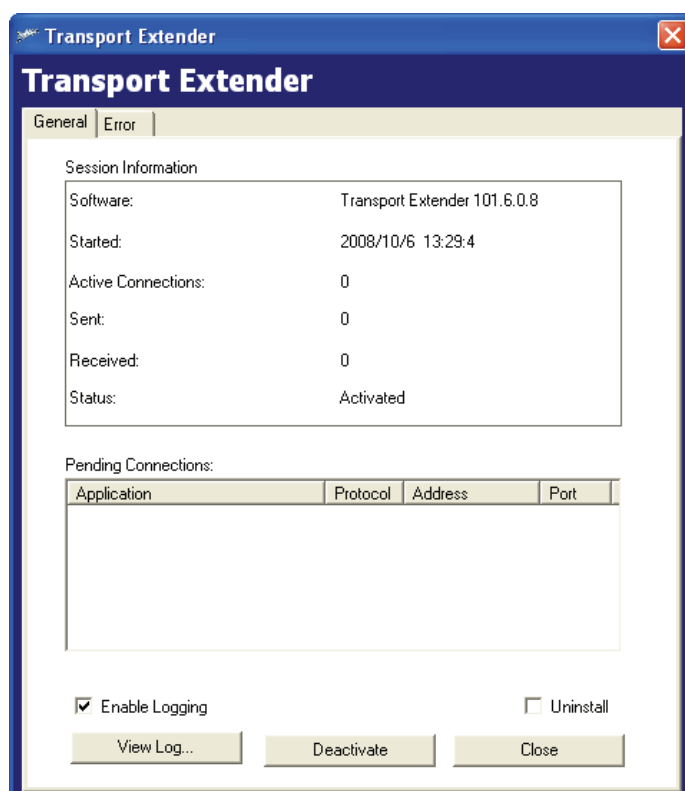


- After the screen refreshes, click **Transport Extender** once again.
- Please click **Install** to install the **MenloLSP.cab** software.




The Transport Extender Setup proceeds.

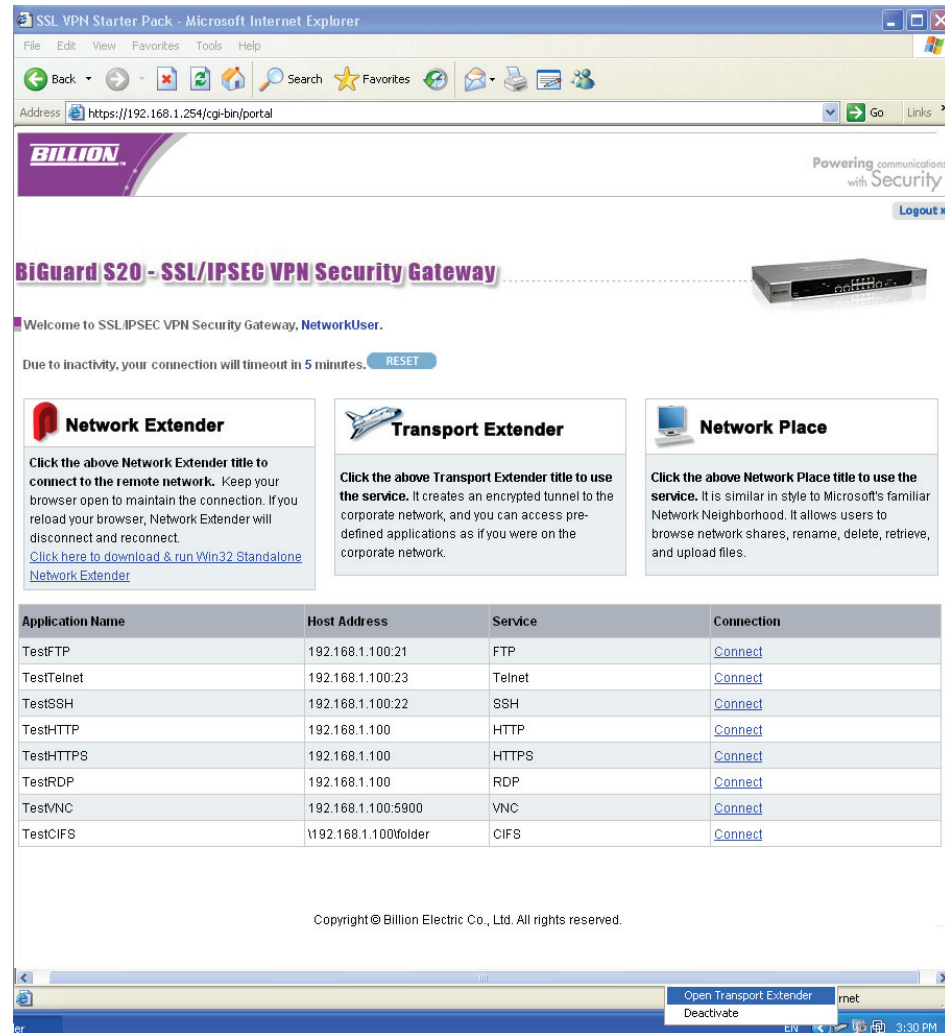
- After the installation is complete, the Transport Extender Connection Status window displays.



- 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 is left unchecked, ActiveX Control will not to be installed when you log on again. If the box is checked, ActiveX will uninstall 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 Transport Extender Status, right-click the Transport Extender icon  on the tool bar, and select an option from the menu in order to view the status screen again, or perform one of the actions above.



Application Name	Host Address	Service	Connection
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
TestHTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
TestRDP	192.168.1.100	RDP	<a href="#">Connect</a>
TestVNC	192.168.1.100:5900	VNC	<a href="#">Connect</a>
TestCIFS	192.168.1.100\folder	CIFS	<a href="#">Connect</a>

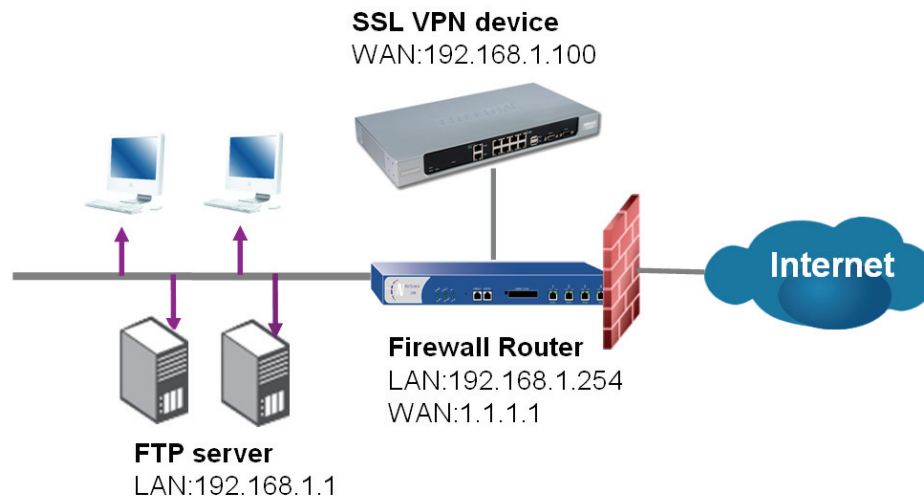
Now the client users can access the Mail server through their mail software as if they were in the office.

## SSL VPN Concentrator

In the company scenario, SSL VPN can help users protect business information from hackers easily and usefully. SSL VPN device can be configured as a gateway on the network border of intranet, called SSL VPN gateway. You also can locate the SSL VPN device behind gateway providing SSL VPN service to remote users, just like a server, and commonly referred to as SSL VPN concentrator. You can only connect the WAN interface or LAN interface of SSL VPN device when you configure SSL VPN concentrator.

### Only connect WAN interface of SSL VPN device

To configure the SSL VPN device as SSL VPN concentrator, you must enable the virtual server function in Firewall Router and enable the SSL VPN service in SSL VPN device.



Firewall Router	Model: BiGuard S series WAN: 1.1.1.1 LAN: 192.168.1.254
FTP Server	LAN: 192.168.1.1
SSL VPN device	Model: BiGuard S series WAN: 192.168.1.100

1. Login to the **Firewall Router** with **admin** account and select **Configuration** → **Policy** → **Virtual Server**.

Virtual Server							
Parameters							
#	Name	Active	Service	Internal IP	Schedule	WAN IP	External Port(s)
Create							

2. Click **Create**. You are prompted to configure some parameters. Type **SSL VPN concentrator** as Name, check **Enable** check box, select **HTTPS** service and type **192.168.1.100** as Internal IP Address.

Virtual Server	
<b>Create</b>	
Name	SSL VPN concentrator
Active	<input checked="" type="checkbox"/> Enable
Service	**HTTPS <input type="checkbox"/> Exposed Host
Internal IP Address	192.168.1.100 <a href="#">Candidates</a>
Schedule	**Always On
WAN IP Address	**Any
External Service Port(s)	<input type="checkbox"/> Redirect to Service
	<input type="text"/> ~ <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Click **Apply** to confirm the settings.
- Click **SAVE CONFIG** to write the new settings to the router's configuration file.
- Login to **SSL VPN device** with **admin** account and select **SSL VPN → User Access Group/Application**.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

- To edit **BiGuard** group, click the **Edit** link on the right hand side of the group profile Name.

The Edit Group screen displays and you can add applications under your chosen Group profile to allow the users within that Group access to the applications.

Edit Group	
<b>General Settings</b>	
Group Name	BiGuard
Domain	BiGuard
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Inactivity Timeout	5 Minutes
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Service</b>	
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<a href="#">Network Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)
<a href="#">Transport Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom Welcome to SSL/IPSEC \
<b>Application Table</b> <a href="#">Add Application</a>	
Name	Application IP Address / Path
<b>Note!</b> To make application changes, press <b>Apply</b> .	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

7. Click **Add Application** to display the SSL VPN Application screen.

SSL VPN Application	
Add Application	
Application Name	<input type="text"/>
Application	Terminal Service (RDP) ▼
IP Address/Domain Name	Terminal Service (RDP) Virtual Network Computing (VNC) File Transfer Protocol (FTP)
Screen Size	File Transfer Protocol (FTP)
Local Device	Telnet Secure Shell (SSH) Secure Shell version 2 (SSHv2) Web (HTTP) Secure Web (HTTPS) Network File Share (CIFS) Terminal Service (RDP) - Java Citrix(HTTP) Wake On LAN(WOL)
Console Mode	
Single Sign On Function	
Application and Path	<input type="text"/>
Terminal Server Port	3389
Log on to	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

---

Application Name **TestFTP** was inputted as an example for the application name.

Application Select **File Transfer Protocol (FTP)** from the drop-down menu.

IP address/  
Domain Name Type **192.168.1.1** as IP address of FTP server.

TCP Port Number **21** is default port number. You can change the port number if needed.

---

SSL VPN Application	
Add Application	
Application Name	TestFTP
Application	File Transfer Protocol (FTP) ▼
IP Address/Domain Name	192.168.1.1
TCP Port Number	21
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

8. Click **Apply** to save the settings.

Edit Group				
<b>General Settings</b>				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>		
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	5	Minutes		
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
<b>Service</b>				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<a href="#">Network Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>		
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)			
<a href="#">Transport Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>		
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom	Welcome to SSL/IPSEC \		
<b>Application Table</b>		<a href="#">Add Application</a>		
Name	Application	IP Address / Path		
TestFTP	FTP	192.168.1:21	<a href="#">Edit</a>	<a href="#">Delete</a>
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

9. Click **Apply** to set the configuration and return to **Group/Application** Screen.
10. Select **SSL VPN** → **User Access** → **Account**.

Account				
Account Table				
Name ▲▼	Group			
admin	BiGuard	<a href="#">Edit</a>		
<a href="#">Create</a> <a href="#">Move</a>				

11. To create an Account, click **Create** at the bottom left of the Account Table.

### Add Account

#### General Setting

User Name	<input type="text" value="Test1"/>	<input checked="" type="checkbox"/> Active
Group	<input type="text" value="BiGuard"/>	
Password	<input type="password" value="*****"/>	
Retype Password	<input type="password" value="*****"/>	<input type="checkbox"/> Use group default password
Host Checking	<input type="checkbox"/> Active	<a href="#">Advanced Setting</a>

#### Group Setting Details

Force Login	Disable
Inactivity Timeout	5 Minutes
Network Place	Enable
Network Extender Service	Enable
Transport Extender Service	Standalone Application (Win32 Only) Enable
Web Cache Cleaner	Enable
Greeting String	Use default greeting string
Applications	TestFTP

---

User Name      **Test1** was inputted as an example for the user name.









Group            **BiGuard** group was chosen from the drop-down menu.

Password        A password was inputted.

Retype Password   Type the password again to confirm the password.

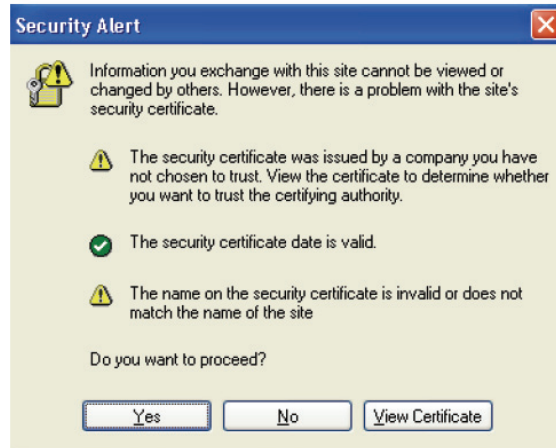
---

12. Click **Apply** to set the configurations and return to Account Table.

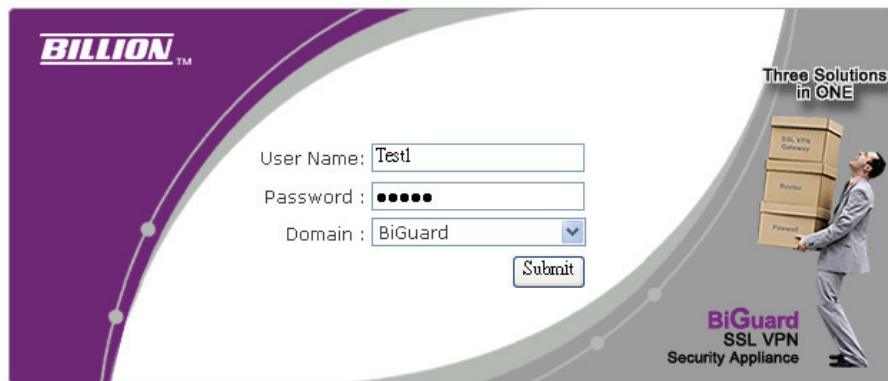
Account				
Account Table				
Name  	Group			
Test1	BiGuard	<a href="#">Edit</a> 	<a href="#">Delete</a> 	<a href="#">Copy</a> 
admin	BiGuard	<a href="#">Edit</a> 		
<a href="#">Create</a>  <a href="#">Move</a> 				

13. Click **SAVE CONFIG** to write the new settings to the router's configuration file.
14. To access the remote SSL VPN portal, please connect to the https://1.1.1.1.
15. When prompted, click **Yes** on the security alert message that appears to accept the certificate and proceed with the process.





The login screen appears.



User Name: **Test1** (As previously added in Administrator FTP Configuration section)  
Domain: Select **BiGuard** from the drop-down menu.

16. Click **Submit** to enter into the Remote Web Portal page.

**BILLION™**

Powering communications with Security

Logout

**BiGuard S20 - SSL/IPSEC VPN Security Gateway**

Welcome to SSLIPSEC VPN Security Gateway, Test1.

Due to inactivity, your connection will timeout in 5 minutes. RESET

**Network Extender**

Click the above Network Extender title 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.

[Click here to download & run Win32 Standalone Network Extender](#)

**Transport Extender**

Click the above Transport Extender title 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 above Network Place title 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
TestFTP	192.168.1.1:21	FTP	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

17. Click **Connect** to connect to the TestFTP service.

If the user account is the same as the FTP server's account, you will not be asked to input the user name and password, and the FTP session screen appears. If your user name differs from the FTP server's account, the following message appears.

User name: **FTPuser**

Password: Type in the password.

Then click **Submit** to login.

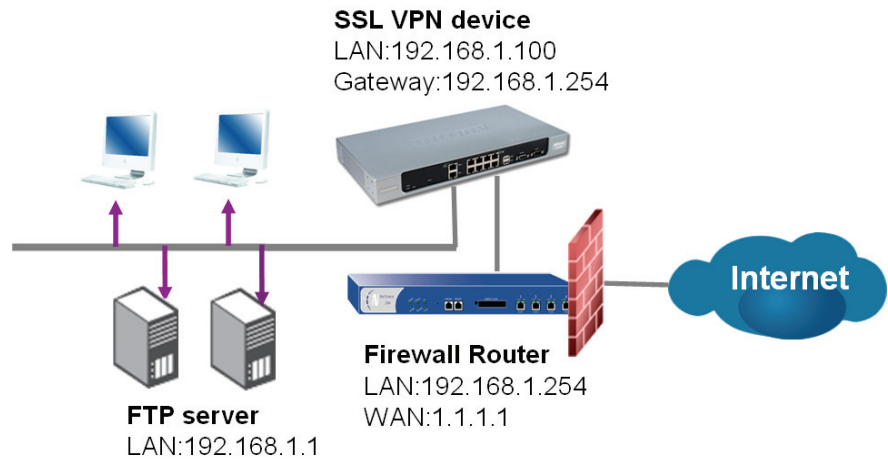
Filename	Size	Date
Up ...		
.	0	Oct 14 16:03
..	0	Oct 14 16:03
jdk-1_5_0_16-windows-i586-p.exe	54333208	Oct 14 16:03

At the bottom of the file list are two buttons: 'Delete' and 'Rename'.

You are logged in to your account in the designated FTP server.

Only connect LAN interface of SSL VPN device

In the example, the FTP server connects to the LAN interface of SSL VPN device, and the SSL VPN device connect to gateway with its own LAN interface. You should configure virtual server in Firewall Router, set default route and enable SSL VPN service in SSL VPN device.



Firewall Router	Model: BiGuard S series WAN: 1.1.1.1 LAN: 192.168.1.254
FTP Server	LAN: 192.168.1.1
SSL VPN device	Model: BiGuard S series LAN: 192.168.1.100 Gateway: 192.168.1.254

1. Login to the **Firewall Router** with **admin** account and select **Configuration** → **Policy** → **Virtual Server**.

Virtual Server							
Parameters							
#	Name	Active	Service	Internal IP	Schedule	WAN IP	External Port(s)
<a href="#">Create</a>							

2. Click **Create**. You are prompted to configure some parameters. Type **SSL VPN concentrator** as Name, check **Enable** check box, select **HTTPS** service and type as Name, check **Enable** check box, select **HTTPS** service and type **192.168.1.100** as Internal IP Address.

Virtual Server

Create

Name	SSL VPN concentrator		
Active	<input checked="" type="checkbox"/> Enable		
Service	**HTTPS	<input type="checkbox"/> Exposed Host	
Internal IP Address	192.168.1.100	<a href="#">Candidates</a>	
Schedule	**Always On		
WAN IP Address	**Any		
External Service Port(s)	<input type="checkbox"/> Redirect to Service		
		~	
<div>ApplyCancel</div>			

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

4. Click **SAVE CONFIG** to write the new settings to the router’s configuration file.

5. Login to **SSL VPN device** with **admin** account and select **Configuration** → **Advanced** → **Static Route**.

Static Route

Static Routing List

#	Valid	Destination	Subnet Mask	Gateway/Interface	Cost		
<a href="#">Create</a>							

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

Static Route

Create

Destination	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	192.168.1.254
Interface	LAN
Cost	0
<div>ApplyCancel</div>	

Destination	Type <b>0.0.0.0</b> as the destination IP address for the static route.
Netmask	Type <b>0.0.0.0</b> as the netmask associated with the destination IP address.
Gateway	Type <b>192.168.1.254</b> as the IP address of gateway.
Interface	Select the <b>LAN</b> interface from the drop-down menu.
Cost	Select the number of hops counted as the cost of route.

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

8. Select **SSL VPN** → **User Access** → **Group/Application**.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

9. To edit BiGuard group, click the **Edit** link on the right hand side of the group profile Name. To create an Account, click **Create** at the bottom left of the Account Table.

The Edit Group screen displays and you can add applications under your chosen Group profile to allow the users within that Group access to the applications.

Edit Group				
General Settings				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	<input type="text" value="5"/> Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)			
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>			
Application Table				
<a href="#">Add Application</a>				
Name	Application	IP Address / Path		
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

10. Click **Add Application** to display the SSL VPN Application screen.

SSL VPN Application	
Add Application	
Application Name	<input type="text"/>
Application	Terminal Service (RDP) ▼
IP Address/Domain Name	Terminal Service (RDP)
Screen Size	Virtual Network Computing (VNC)
Local Device	File Transfer Protocol (FTP)
	Telnet
	Secure Shell (SSH)
	Secure Shell version 2 (SSHv2)
	Web (HTTP)
	Secure Web (HTTPS)
	Network File Share (CIFS)
	Terminal Service (RDP) - Java
	Citrix(HTTP)
	Wake On LAN(WOL)
Console Mode	
Single Sign On Function	
Application and Path	<input type="text"/>
Terminal Server Port	3389
Log on to	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

---

Application Name **TestFTP** was inputted as an example for the application name.

Application Select **File Transfer Protocol (FTP)** from the drop-down menu.

IP address/  
Domain Name Type **192.168.1.1** as IP address of FTP server

TCP Port Number **21** is default port number. You can change the port number if needed.

---

SSL VPN Application	
Add Application	
Application Name	TestFTP
Application	File Transfer Protocol (FTP) ▼
IP Address/Domain Name	192.168.1.1
TCP Port Number	21
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

11. Click **Apply** to save the settings.

Edit Group				
<b>General Settings</b>				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>		
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	5	Minutes		
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
<b>Service</b>				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<a href="#">Network Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>		
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)			
<a href="#">Transport Extender Service</a>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<a href="#">Advanced Setting</a>		
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom	Welcome to SSL/IPSEC \		
<b>Application Table</b>		<a href="#">Add Application</a>		
Name	Application	IP Address / Path		
TestFTP	FTP	192.168.1:21	<a href="#">Edit</a>	<a href="#">Delete</a>
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

12. Click **Apply** to set the configuration and return to **Group/Application** Screen.
13. Select **SSL VPN** → **User Access** → **Account**.

Account				
Account Table				
Name ▲▼	Group			
admin	BiGuard	<a href="#">Edit</a>		
<a href="#">Create</a> <a href="#">Move</a>				

14. To create an Account, click **Create** at the bottom left of the Account Table.

Add Account	
<b>General Setting</b>	
User Name	Test1 <input checked="" type="checkbox"/> Active
Group	BiGuard ▼
Password	•••••
Retype Password	••••• <input type="checkbox"/> Use group default password
Host Checking	<input type="checkbox"/> Active <a href="#">Advanced Setting</a>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Group Setting Details	
Force Login	Disable
Inactivity Timeout	5 Minutes
Network Place	Enable
Network Extender Service	Enable
Transport Extender Service	Standalone Application (Win32 Only) Enable
Web Cache Cleaner	Enable
Greeting String	Use default greeting string
Applications	TestFTP

---

User Name      **Test1** was inputted as an example for the user name.

Group            **BiGuard** group was chosen from the drop-down menu.

Password        A password was inputted.

Retype Password   Type the password again to confirm the password.

---

15. Click **Apply** to set the configurations and return to Account Table.

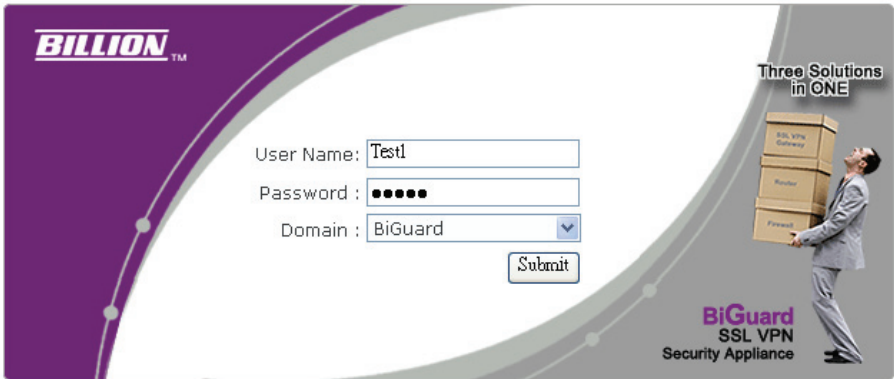
Account				
Account Table				
Name ▲▼	Group			
Test1	BiGuard	<a href="#">Edit ▶</a>	<a href="#">Delete ▶</a>	<a href="#">Copy ▶</a>
admin	BiGuard	<a href="#">Edit ▶</a>		
<a href="#">Create ▶</a> <a href="#">Move ▶</a>				

16. Click **SAVE CONFIG** to write the new settings to the router's configuration file.
17. To access the remote SSL VPN portal, please connect to the https://1.1.1.1.
18. When prompted, click **Yes** on the security alert message that appears to accept the certificate and proceed with the process.



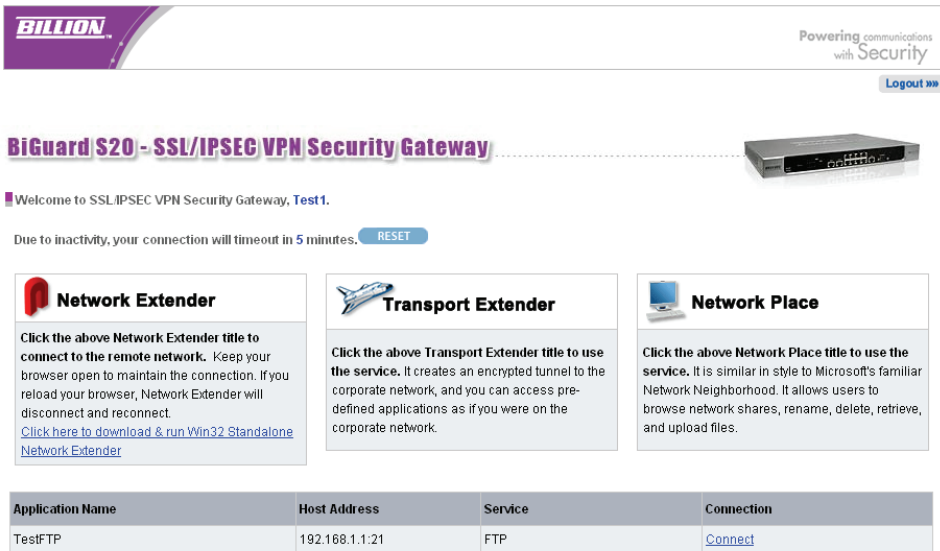


The login screen appears.



User Name: **Test1** (As previously added in Administrator FTP Configuration section)  
Domain: Select **BiGuard** from the drop-down menu.

19. Click **Submit** to enter into the Remote Web Portal page.



20. Click **Connect** to connect to the TestFTP service.

If the user account is the same as the FTP server's account, you will not be asked to input the user name and password, and the FTP session screen appears.  
If your user name differs from the FTP server's account, the following message appears.

User name: **FTPuser**

Password: Type in the password.

Then click **Submit** to login.

Filename	Size	Date
Up ...		
.	0	Oct 14 16:03
..	0	Oct 14 16:03
jdk-1_5_0_16-windows-i586-p.exe	54333208	Oct 14 16:03

Buttons: Delete, Rename

You are logged in to your account in the designated FTP server.

## SSL VPN Connection Verification

Whenever a connection is being established, BiGuard S Series Client performs verification of the VPN server's SSL certificate (the same verification is performed by web browsers when it is attempting to use the HTTPS protocol). If any certificate-related problems are detected, a warning appears inquiring when the user finds the VPN server trustworthy or the connection to the server should be allowed.

**FIGURE 138 SSL CERTIFICATE SCREEN**

SSL Certificate					
Current Certificates					
Enable	Description	Status	Expiration	Password	
<input checked="" type="radio"/>	sha1WithRSAEncryption	Active	Jan 14 02:12:30 2018 GMT		

Click **View Certificate** to view detailed information about the VPN server's certificate (issuer, server for which it was issued, expiration date, etc.). According to the information provided, the user can decide whether to handle the server as trustworthy and allow the connection or to reject it.

If **Yes** is clicked, the BiGuard S Series Client considers the VPN server as trustworthy. The certificate is saved and no warning is displayed upon next connections to the server.

### Common certificate-related problems and their solutions

Certificate-related problems are often caused by one of the following issues:

#### **THE CERTIFICATE WAS ISSUED BY AN UNTRUSTWORTHY AUTHORITY**

The BiGuard S Series verifies whether a certificate was issued by an authority included in the list of trustworthy certificate publishers stored in the operating system (the Certificates section of the Content tab under Control Panel / Internet Options). Since a certificate is imported, any certificates issued by the same authority will be accepted automatically (unless any problem is detected).



**NOTE:** When the Generate Certificate option is used, a self-signed certificate is created - the publisher of the certificate is identical with its subject. This type of certificate does not guarantee the highest security and it cannot be accepted automatically at the client's side. To provide the full security, it is necessary to use a certificate issued by a trustworthy certification authority. See [Importing a certificate](#) on page 208.

#### **THE NAME REFERRED IN THE CERTIFICATE DOES NOT MATCH WITH THE SERVER'S NAME**

Name of the server specified in the certificate does not correspond with the server name which the BiGuard S Series is connecting to. This problem might occur when the server uses an invalid certificate or when the server name has changed. However, it may also point at an intrusion attempt (a false DNS record with an invalid IP address is used). We recommend to discuss this issue with the administrator of the corresponding VPN server.

Note: Certificates can be issued only for servers' DNS names, not for IP addresses.

#### **DATE OF THE CERTIFICATE IS NOT VALID**

For secure reasons, validity of SSL certificates is limited by time. If an invalid date is reported, it means that the certificate's validity has already expired and it is necessary to update it. Contact the VPN server's administrator.

**THE SECURITY CERTIFICATE HAS CHANGED SINCE THE LAST CHECK**

When a user accepts connection to a VPN server, the BiGuard S Series Client saves the certificate of the server as trustworthy. For any later connections, the BiGuard S Series Client checks certificates with the saved one. If these certificates do not correspond, it might be caused by the fact that the certificate has been changed at the server (e.g. for expiration of the original certificate). However, this might also point at an intrusion attempt (another server using a different certificate). Contact the VPN server's administrator.

## Log and E-mail Alerts

The BiGuard S20 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

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

**FIGURE 139** LOG CONFIGURATION SCREEN

Log Configuration

Parameters

Categories	System/SSL VPN Log	Syslog Server	E-mail Alert
System Maintenance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Error	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Packet Filter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MAC Filter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Content Filter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firewall	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Call Data Record	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PPP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SSL VPN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPSEC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

Cancel

Categories	Select <b>System/SSL VPN Log</b> to capture to a log. Select <b>Syslog Server</b> to capture and send to a specified external server. Select <b>Email Alert</b> to send information log to a pre-specified E-mail account.
System Maintenance	Enable reporting of system maintenance information.
System Error	Enable reporting of system or hardware error messages.
Access Control	Enable access control.
Packet Filter	Enable packet filtering. <b>Note:</b> Packet filtering does not 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 S20 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.
Firewall	Enable security alerts for network traffic or program blocking.

---

---

Call Data Record	Check this item to enable call data record.
PPP	Check this item to enable PPP logs.
SSL VPN	Check this item to enable SSL activity logs.
IPSec	Check this item to enable IPSec activity logs.

---

---

2. 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 140 SYSLOG SERVER SCREEN

Syslog Server

Parameters

Syslog Server

☒ Enable ☐ Disable

Server IP Address

Apply

Cancel

Syslog Server	Enables system logs to be sent to an external syslog server. When it is 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 141** E-MAIL ALERT SCREEN

E-mail Alert

Parameters

E-mail Alert	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Recipient's E-mail Address	<input type="text"/>
Sender's E-mail Address	<input type="text"/>
SMTP Mail Server	<input type="text"/>
Mail Server Login	<input type="checkbox"/>
User Name	<input type="text"/>
Password	<input type="password"/>
Period of Send E-mail Alert	<input type="text" value="1"/> minutes

Apply

Cancel

E-mail Alert	Enables a log of security-related events to be sent to a specified e-mail address. When it is enabled, the following fields are available.
Recipient's E-mail Address	Enter the e-mail account to receive the log alerts.
Sender's E-mail Address	Enter a sender e-mail name if this is required by the SMTP provider.
SMTP Mail Server	Enter the SMTP mail server name.
Mail Server Login	Check this box if login is required.
User Name	Enter the user name for the login account.
Password	Enter 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 142** SAVE CONFIG TO FLASH SCREEN



Click **Apply** to save the configuration.

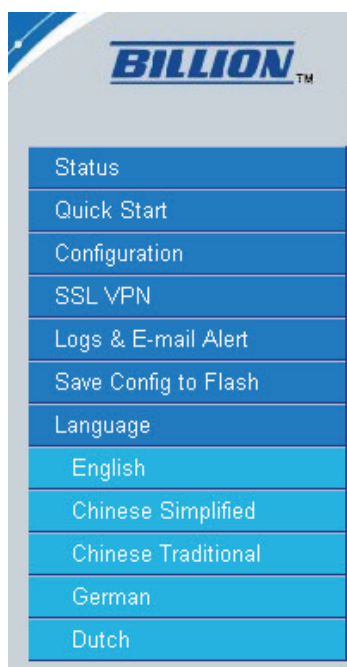
## Language

Language provides 5 different type of languages to be displayed on the interface (currently supporting English, Simplified Chinese, Traditional Chinese, German and Dutch).



**NOTE:** If you accidentally mistakenly clicked on one of the foreign language that you do not understand, don't be panic. Just locate where **language** link should be and click on the 1st item under Language which will always be in **English**.

**FIGURE 143** LANGUAGE MENU



Click on the language name and your interface language will switch to the language that you have just clicked.

## Product Registration

Product registration is now possible through the Status page or by going directly to the BiGuard registration site, <http://www.biguard.com>. Registered users can get access to the latest product information, priority BiGuard product users' support and service, customized personal service portal, and regular news and information sharing and update notification.

### VPN Status Page Registration

1. Log on to the BiGuard S20.  
The default account and password is **admin/admin**.

The image shows the login screen of a BiGuard S20 device. It features a purple header with the 'BILLION' logo. The login form includes fields for 'User Name' (pre-filled with 'admin'), 'Password' (masked with dots), and 'Domain' (a dropdown menu showing 'BiGuard'). A 'Submit' button is located below the password field. To the right, there is a graphic of a person carrying boxes, with text 'Three Solutions in ONE' and 'BiGuard SSL VPN Security Appliance'.

2. If the appliance has not been registered, the Registration field of the Status page shows **Not Registered**.

Status

Device Information

Registration	Not Registered	Register
Model Name	BiGuard S20	
Device Name	SSLVPN.gateway	
System Up-Time	6 minutes, 43 seconds	
Current Time	Tue Nov 30 00:06:43 1999	Sync Now
Software Version	3.17	
Bootrom Version	1.13_dbg	
LAN MAC Address	00:04:ED:46:23:7C	
WAN1 MAC Address	00:04:ED:46:23:7D	
WAN2 MAC Address	00:04:ED:46:23:7E	
Home URL	Billion Electric Co.,Ltd.	

VPN

SSL	Active Users: 1, Maximum: 20
IPSec	Established: 0, Configured: 0, Maximum: 30

LAN

IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server	DHCP Server Running

WAN1

Link Status	Link Down
Connection Method	DHCP Client
Connection	
IP Address	
Subnet Mask	
Gateway	

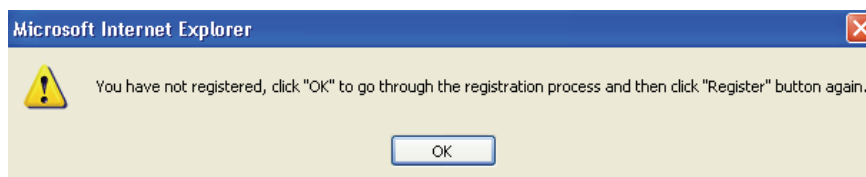
WAN2

Link Status	Link Down
Connection Method	DHCP Client
Connection	
IP Address	
Subnet Mask	
Gateway	


3. Click **Register**. (Also can register from [Http://www.biguard.com](http://www.biguard.com).)

Status	
<b>Device Information</b>	
Registration	Not Registered <span>Register</span>
Model Name	BiGuard S20
Device Name ▶	SSLVPN.gateway
System Up-Time	6 minutes, 43 seconds
Current Time ▶	Tue Nov 30 00:06:43 1999 <span>Sync Now</span>
Software Version	3.17
Bootrom Version	1.13_dbg
LAN MAC Address	00:04:ED:46:23:7C
WAN1 MAC Address	00:04:ED:46:23:7D
WAN2 MAC Address	00:04:ED:46:23:7E
Home URL	<a href="#">Billion Electric Co.,Ltd.</a>
<b>VPN</b>	
SSL	Active Users: 1, Maximum: 20
IPSec	Established: 0, Configured: 0, Maximum: 30
<b>LAN</b>	
IP Address ▶	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server ▶	DHCP Server Running
<b>WAN1</b>	
Link Status	Link Down
Connection Method ▶	DHCP Client
Connection	
IP Address	
Subnet Mask	
Gateway	
<b>WAN2</b>	
Link Status	Link Down
Connection Method ▶	DHCP Client
Connection	
IP Address	
Subnet Mask	
Gateway	

4. Click **OK**.



5. Click **Yes**.



Powering communications with Security

Home | Product Registration | Member Profile | Education | Support | Download | Contact Us

About this Site | Help | Sitemap

Home > Member Registration

## BiGuard User Club

Are you a registered member of BiGuard website?

### New Firmware Upgrades

- BiGuard S6000
- BiGuard S5/S10/S20
- BiGuard 210/30/50G

### BiGuard CMS series

Central Management System

6. Click **Join Now**.

## BiGuard User Club

### ■ BiGuard end-user registration portal

Billion is committed to customer service before and after sales. This site is our commitment to customers who purchase our BiGuard line of products. By registering your products through this site, you get access to a wealth of information, FAQs, white papers, demos, customized support and updates, and more. Registration is quick and simple.

<h4>BiGuard User Login</h4> <p>Account: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="GO"/></p> <p><a href="#">Forgot password?</a></p>	<h4>BiGuard Partner Center Login</h4> <p>Authorized partners in selling BiGuard series of products are given access to BiGuard Partner Center, which contains plenty of resources and materials for promoting BiGuard products.</p> <p><input type="button" value="Click here to login"/></p>
<h4>Member Application</h4> <p><b>Not yet a Member? Become one!</b></p> <p>Registration is EASY and FREE, and you get special benefits. Find out more below.</p> <p><input type="button" value="Join Now!"/></p>	<h4>Partner Application</h4> <p><b>To become a Partner?</b></p> <p>No matter you are to register as a partner, or just consider to initiate business engagement with Billion, you are welcome to fill out <a href="#">Application Form</a>. Applications are subject to review and approval.</p>

7. Click **Member**.

## BiGuard User Club

Member Registration → Email Verification → Registration Complete

To access certain features of this site, you must register first. Please select a membership type to continue.

**Member**

Members have full access to the site, including all its content.

8. You will prompted to fill in the form.

## BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

[Next](#) [Clear](#)

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

9. Select **BiGuard S Series** from the **Product Category** drop-down menu.

## BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

[Next](#) [Clear](#)

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

10. Select **BiGuard S20** from the **Product Model** drop-down menu.

### BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

11. If you register by using the BiGuard S20 web portal, the **MAC Address** will be entered in automatically by the appliance. Then type in the **Product Serial Number**. Only users that register by going directly to the BiGuard registration site (<http://www.biguard.com>) need to type in both the **MAC Address** and **Product Serial Number**.
12. Fill in the **Purchase Date** and **Purchase Location** and click **Next**.

### BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

13. Fill in the fields and click **Register**.

## BiGuard User Club

Member Registration → Email Verification → Registration Complete

Please complete this form to take full advantage BiGuard product supports from Billion. Please read our [Privacy Policy](#) [here](#)

(\*) Required fields

• Account Information

Username*:	<input type="text" value="username"/>	1. Please create your user account and password with 6 to 20 characters, numbers, letters and the underscore character. The characters: !#\$%^&*~.-;,:=>?@[~^`{} '" are not allowed.
Password*:	<input type="password" value="*****"/>	
Confirm Password*:	<input type="password" value="*****"/>	2. A valid e-mail address is required. It is used to activate your account.
E-mail*:	<input type="text" value="mail@bgs.com.tw"/>	
Confirm E-mail*:	<input type="text" value="mail@bgs.com.tw"/>	

• General Information

First Name*:	<input type="text" value="First Name"/>	Last Name*:	<input type="text" value="Last Name"/>
Company Name*:	<input type="text" value="Billion"/>	Job Title*:	<input type="text" value="Job"/>
Company Address:	<input type="text" value="7F., No. 192, Sec. 2, Chung Hsing Rpad, Hsin Tein City, Taipei Hsien, Taiwan"/>		
City:	<input type="text" value="Taipei"/>		
Province / State:	<input type="text" value="Hsin Tein"/>		
Zip/Postal Code:	<input type="text" value="23146"/>		
Country*:	<input type="text" value="Taiwan"/>		
Phone Number:	<input type="text" value="02-29145665"/> (country code + area code + phone number)		
Fax Number:	<input type="text"/> (country code + area code + fax number)		
Company Website URL:	<input type="text" value="http://www.billion.com"/>		
User Organization Type*:	<input checked="" type="radio"/> Head Office <input type="radio"/> Branch Office <input type="radio"/> SOHO Office <input type="radio"/> Others <input type="text"/>		
No. of Company Employees*:	<input type="text" value="0 ~ 10"/>		
No. of MIS Personnel*:	<input type="text" value="2"/>		
Company's primary business activity*:	<input type="text" value="Technology"/>		

• Questionnaire

1. Why did you choose Billion BiGuard products?\*

- ☒ Billion brand name and good reputation  
☒ Price  
☒ Product feature and specification  
☒ Recommended by friend  
☐ Recommended by local retailer   
☐ Other reason

2. Where do you know about Billion?\*

- ☒ Local retailer  
☒ Billion website  
☐ Advertisement, please indicate the media name   
☐ Press release, please indicate the media name   
☒ Friends  
☐ Others, please indicate the details

3. Why did you need this product?\*

- ☒ Internet access  
☒ Remote access  
☒ File and printer sharing  
☒ VPN security connection  
☒ Traffic Prioritization and Bandwidth Management  
☒ Load Balancing and Auto Failover  
☒ Firewall Security  
☒ LAN extension  
☐ Other reason

• Preferences

- ☒ Yes, I would like to be a Beta Tester  
☒ I would like to receive e-mailers regarding Billion's latest information

[Register](#)



14. The system will send a mail to the mail address you registered. Then the page will appear and request you to fill in the **Verification Code**.

## BiGuard User Club

Member Registration → **Email Verification** → Registration Complete

You are almost there. An email confirmation has been sent to the email address you entered in the previous step. In order to complete your registration, please copy and paste the verification code from your email into the input box below and click submit.

E-mail: mail@bgs.com.tw

Verification Code:

**Submit**

NOTE: the email notification may take some time before reaching your mail box depending on network traffic and your mail server. You may have to wait 5-10 minutes. If you do not receive any email confirmation within 24 hours, please contact our customer service.

15. Receive the mail and copy the **Verification Code**.

**BILLION**
Powering communications  
with Security

Dear Username:

Thank you for registering on our website. You may edit your personal information at any time on our website. Here are your user name and password. Please keep them in a safe place for future reference.

Name: Username  
Registration date: 2006-10-17

username: First Name Last Name  
password: username

*note: password is CaSe SenSiTive*

Your registration is not complete yet. We need to verify that your email is valid. You may complete the verification process by clicking on the link below or copying it and pasting on our browser:

**Verification Code: 18796**  
[http://www.biguard.com/reg\\_emailverify.php?sn=1&e=BGS10@mail.biguard.com&c=18796](http://www.biguard.com/reg_emailverify.php?sn=1&e=BGS10@mail.biguard.com&c=18796)

Thank you for choosing Billion products!

Biguard support team  
[www.biguard.com](http://www.biguard.com)

16. Fill in the **Verification Code** and click **Submit**.

## BiGuard User Club

Member Registration → **Email Verification** → Registration Complete

You are almost there. An email confirmation has been sent to the email address you entered in the previous step. In order to complete your registration, please copy and paste the verification code from your email into the input box below and click submit.

E-mail: mail@bgs.com.tw  
Verification Code:

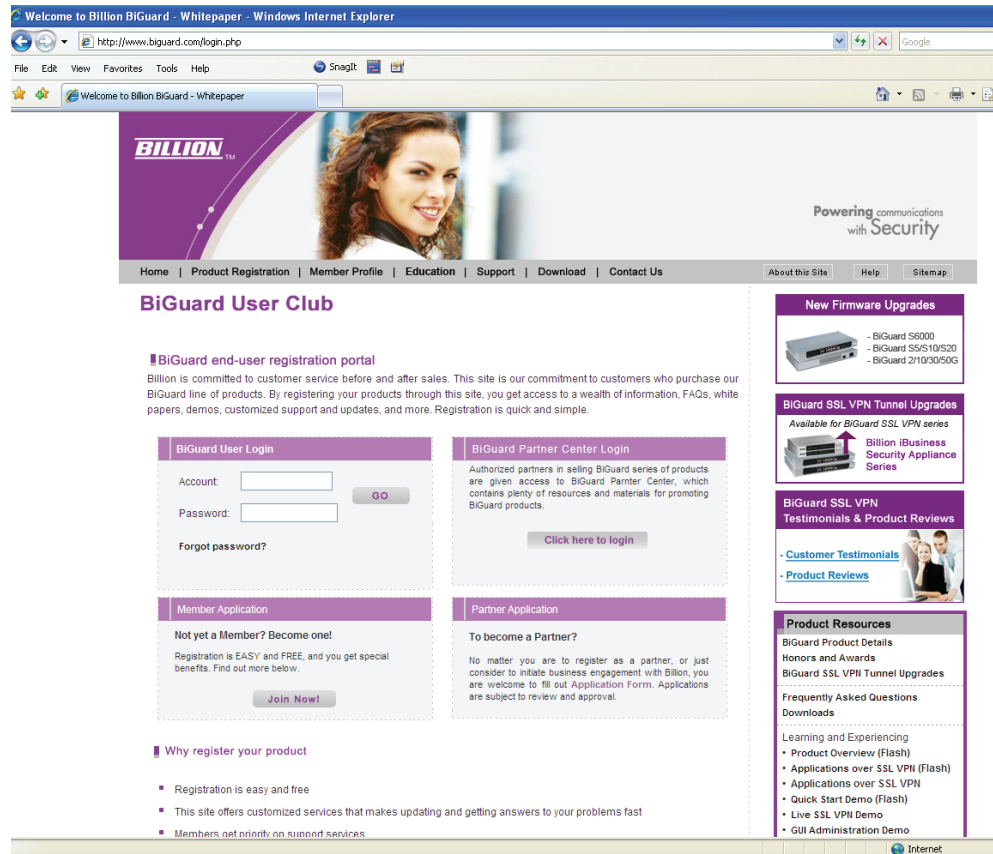
**Submit**

NOTE: the email notification may take some time before reaching your mail box depending on network traffic and your mail server. You may have to wait 5-10 minutes. If you do not receive any email confirmation within 24 hours, please contact our customer service.

## Web Site Registration

Follow these instructions to register directly from the **BiGuard** web site.

1. Type the address in the IP Address field to get into the Web site and click **Join Now**.  
The Web site address is <http://www.biguard.com>



2. Click **Member**.

## BiGuard User Club

Member Registration → Email Verification → Registration Complete

To access certain features of this site, you must register first. Please select a membership type to continue.

**Member**

Members have full access to the site, including all its content.

3. You will be prompted to fill in the form.

## BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

4. Select **BiGuard S Series** from the **Product Category** drop-down menu.

## BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

5. Select **BiGuard S20** from the **Product Model** drop-down menu.

### BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

6. If you manually register online, you must also input the **Product Serial** and **MAC Address**.
7. Fill in the **Purchase Date** and **Purchase Location** and click **Next**.

### BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

8. Fill in the fields and click **Register**.

## BiGuard User Club

Member Registration → Email Verification → Registration Complete

Please complete this form to take full advantage BiGuard product supports from Billion. Please read our [Privacy Policy](#) [here](#)

(\*) Required fields

• Account Information

Username*:	<input type="text" value="username"/>	1. Please create your user account and password with 6 to 20 characters, numbers, letters and the underscore character. The characters: !#\$%^&*~.;,:<=>?@[\`~^{} '" are not allowed.
Password*:	<input type="password" value="••••••"/>	
Confirm Password*:	<input type="password" value="••••••"/>	
E-mail*:	<input type="text" value="mail@bgs.com.tw"/>	2. A valid e-mail address is required. It is used to activate your account.
Confirm E-mail*:	<input type="text" value="mail@bgs.com.tw"/>	

• General Information

First Name*:	<input type="text" value="First Name"/>	Last Name*:	<input type="text" value="Last Name"/>
Company Name*:	<input type="text" value="Billion"/>	Job Title*:	<input type="text" value="Job"/>
Company Address:	<input type="text" value="7F., No. 192, Sec. 2, Chung Hsing Rpad, Hsin Tein City, Taipei Hsien, Taiwan"/>		
City:	<input type="text" value="Taipei"/>		
Province / State:	<input type="text" value="Hsin Tein"/>		
Zip/Postal Code:	<input type="text" value="23146"/>		
Country*:	<input type="text" value="Taiwan"/>		
Phone Number:	<input type="text" value="02-29145665"/> (country code + area code + phone number)		
Fax Number:	<input type="text"/> (country code + area code + fax number)		
Company Website URL:	<input type="text" value="http://www.billion.com"/>		
User Organization Type*:	<input checked="" type="radio"/> Head Office <input type="radio"/> Branch Office <input type="radio"/> SOHO Office <input type="radio"/> Others <input type="text"/>		
No. of Company Employees*:	<input type="text" value="0 ~ 10"/>		
No. of MIS Personnel*:	<input type="text" value="2"/>		
Company's primary business activity*:	<input type="text" value="Technology"/>		

• Questionnaire

1. Why did you choose Billion BiGuard products?\*

- ☒ Billion brand name and good reputation  
☒ Price  
☒ Product feature and specification  
☒ Recommended by friend  
☐ Recommended by local retailer   
☐ Other reason

2. Where do you know about Billion?\*

- ☒ Local retailer  
☒ Billion website  
☐ Advertisement, please indicate the media name   
☐ Press release, please indicate the media name   
☒ Friends  
☐ Others, please indicate the details

3. Why did you need this product?\*

- ☒ Internet access  
☒ Remote access  
☒ File and printer sharing  
☒ VPN security connection  
☒ Traffic Prioritization and Bandwidth Management  
☒ Load Balancing and Auto Failover  
☒ Firewall Security  
☒ LAN extension  
☐ Other reason

• Preferences

- ☒ Yes, I would like to be a Beta Tester  
☒ I would like to receive e-mailers regarding Billion's latest information

[Register](#)

9. The system will send a mail to the mail address you registered. Then the page will appear and request you to fill in the **Verification Code**.

## BiGuard User Club

Member Registration → **Email Verification** → Registration Complete

You are almost there. An email confirmation has been sent to the email address you entered in the previous step. In order to complete your registration, please copy and paste the verification code from your email into the input box below and click submit.

E-mail: mail@bgs.com.tw

Verification Code:

**Submit**

NOTE: the email notification may take some time before reaching your mail box depending on network traffic and your mail server. You may have to wait 5-10 minutes. If you do not receive any email confirmation within 24 hours, please contact our customer service.

10. Receive the mail and copy the **Verification Code**.

**BILLION**
Powering communications  
with Security

Dear Username:

Thank you for registering on our website. You may edit your personal information at any time on our website. Here are your user name and password. Please keep them in a safe place for future reference.

Name: Username  
Registration date: 2006-10-17

username: First Name Last Name  
password: username

*note: password is CaSe SenSiTive*

Your registration is not complete yet. We need to verify that your email is valid. You may complete the verification process by clicking on the link below or copying it and pasting on our browser:

**Verification Code: 18796**  
[http://www.biguard.com/reg\\_emailverify.php?sn=1&e=BGS10@mail.biguard.com&c=18796](http://www.biguard.com/reg_emailverify.php?sn=1&e=BGS10@mail.biguard.com&c=18796)

Thank you for choosing Billion products!

Biguard support team  
[www.biguard.com](http://www.biguard.com)

11. Fill in the **Verification Code** and click **Submit**.

## BiGuard User Club

Member Registration → **Email Verification** → Registration Complete

You are almost there. An email confirmation has been sent to the email address you entered in the previous step. In order to complete your registration, please copy and paste the verification code from your email into the input box below and click submit.

E-mail: mail@bgs.com.tw

Verification Code:



**Submit**

NOTE: the email notification may take some time before reaching your mail box depending on network traffic and your mail server. You may have to wait 5-10 minutes. If you do not receive any email confirmation within 24 hours, please contact our customer service.

You will be returned to the main page as shown.

## BiGuard User Club **Welcome back Username!**

### Newest downloads

Download name	Type Version	Description	Version	Download
BiGuard S20 Firmware (v3.17)	Firmware	BiGuard S20 firmware and release note	v3.17	
BiGuard S5 Firmware (v3.17)	Firmware	BiGuard S5 firmware and release note	v3.17	
BiGuard S10 Firmware (v3.17)	Firmware	BiGuard S10 firmware and release note	v3.17	

### Member news/announcements

- ▶ [2008-01-18 - BiGuard SSL VPN Tunnel Upgrades are available for BiGuard S5 and BiGuard S10](#)
- ▶ [2007-10-25 - BILLION expands its range of BiGuard IPSec VPN Security Appliances High-grade 802.11g Dual-WAN Security Gateway for SMBs - BiGuard 50G](#)
- ▶ [2007-10-08 - Billion launches Two-Factor Authentication with One-Time Password - BiGuard OTP for higher security level of remote access](#)
- ▶ [2007-05-31 - Billion to highlight SMB and Digital Home networking devices at Computex 2007](#)
- ▶ [2007-05-03 - Billion Reasons to Visit PC Range at CeBIT 2007](#)

### Newest FAQ

- ▶ [Are there any restrictions when using BiGuard SSL Certificate?](#)
- ▶ [Changing the ASAS Server/Database IP ADDRESS](#)
- ▶ [Migrating ASAS to another server](#)
- ▶ [Restoring Deleted Users](#)

You have successfully registered the product.



# Troubleshooting

## Before you begin

This appendix covers possible problems you may have with the hardware setup and configuration of your BiGuard S Series. Before continuing, ensure that you have correctly installed the hardware.

If you can not 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.

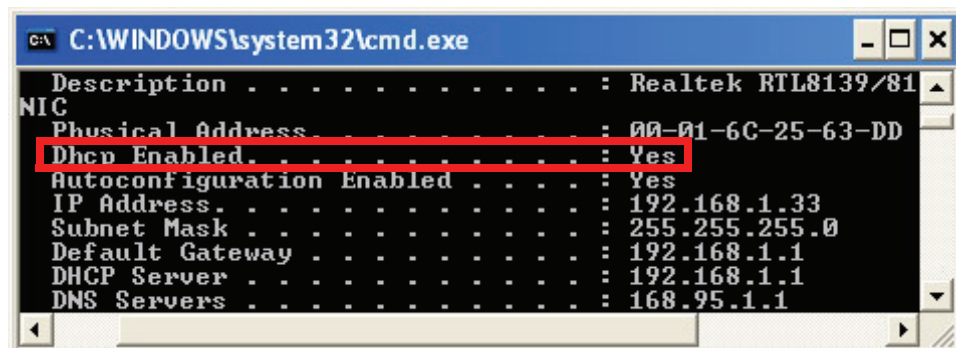
All computers (or any device such as a printer) that are on a network, must have a network IP address. The IP address is either assigned manually (a static IP address), or it is assigned automatically (dynamic IP address) by a DHCP router or server. This is the same for both wired and wireless connections.

### 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 RTL8139/8101
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 S Series. See [Configuring the WAN for DHCP](#) on page 41.

## Hardware problems

This section deals with issues regarding the BiGuard S Series hardware.

### My BiGuard S Series will not turn on

If the power, status, WAN, LAN, and DMZ LEDs fail to light up when you turn on the BiGuard S Series, 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 S Series LEDs do not turn off after powering on

When your BiGuard S Series 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 S Series 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:** Both the User Name and Password are case sensitive.

If this fails, restore your BiGuard S Series 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 S Series LAN Interface.

### I can not access the BiGuard S Series from the LAN

There is no response from my BiGuard S Series 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 not ping any PC on the LAN

- Check the 10/100M LAN LEDs on the BiGuard S Series front panel. One of these LEDs should be on. If they are both off, check the cable connections between the BiGuard S Series 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 S Series 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 S Series 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** on the right side of the table.

### I can not access the BiGuard S Series Web Configuration Interface

I have trouble accessing the BiGuard S Series' 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 S Series' IP address has changed and you do not 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** check box is checked, and click **OK**.
4. Click **OK** under **Internet Options** to close the dialog.
  - 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 S Series 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 dialog.

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

### **ENABLING POP-UP BLOCKERS WITH EXCEPTIONS**

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

1. In Internet Explorer, select **Tools** → **Internet Options**.
2. Under the **Privacy** tab, click **Settings** to open the Pop-up Blocker Settings dialog.
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 dialog.
6. Click **Apply** to save your changes.

## Java scripts

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** and click **OK**.

## 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 dialog.



**NOTE:** *If Java from Sun Microsystems is installed, scroll down to Java (Sun) and ensure that the check box is filled.*

## WAN interface problems

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

### I can not get a WAN IP address from the ISP

My WAN IP address can not 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:** 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 S Series' WAN MAC address. Click **Specify a MAC Address (MAC Clone)** and type the MAC address in the WAN Settings dialog.

WAN1 Settings	
Static IP	
Protocol	Static IP
Mode	<input checked="" type="radio"/> NAT <input type="radio"/> Router
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Gateway	<input type="text"/>
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"/> <a href="#">Candidates</a>
DNS	Primary DNS <input type="text"/> Secondary DNS <input type="text"/>
RIP	Disable
MTU	1492
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Return"/>	

- If your ISP requires host name authentication, configure your computer's name as BiGuard S Series system name.

## Internet service provider problems

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

### I can not access the Internet when connected to the BiGuard S Series

If your BiGuard S Series 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.

WAN1	
Link Status	Link Down
Connection Method ▶	DHCP Client
Connection	<input type="text"/>
IP Address	
Subnet Mask	
Gateway	
WAN2	
Link Status	Link Up (1000 Mbps Full Duplex)
Connection Method ▶	DHCP Client
Connection	Disconnected <input type="button" value="Renew"/> <input type="button" value="Release"/>
IP Address	
Subnet Mask	
Gateway	

### I can not get an IP address from my ISP

If an IP address can not be obtained:

1. Turn off the power to your cable or DSL modem.
2. Turn off the power to your BiGuard S Series.
3. Wait 5 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 not 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 you to log in, 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 can not 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.

## Troubleshooting Q&A

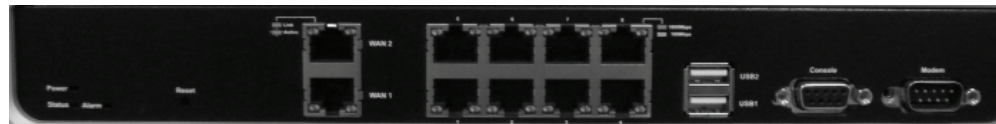
This section answers some common questions about the BiGuard S Series operation and provides some troubleshooting tips.

**QUESTION:** What is the LED sequence of the BiGuard S Series when powering on?

---

**ANSWER:** The LED sequence for powering on the BiGuard S Series is as follows:

- ALL LEDs flash in sequence three times.
- Power, status and connected port LEDs light.
- The status LED turns off to indicate the system is operational.



Power and  
status LEDs

WAN LEDs

**QUESTION:** What is the default username and password of the BiGuard S Series?

---

**ANSWER:** The default username and password for the BiGuard S Series is as follows:

- **Username:** admin
- **Password:** admin

**QUESTION:** What is the factory default LAN IP address for the BiGuard S Series?

---

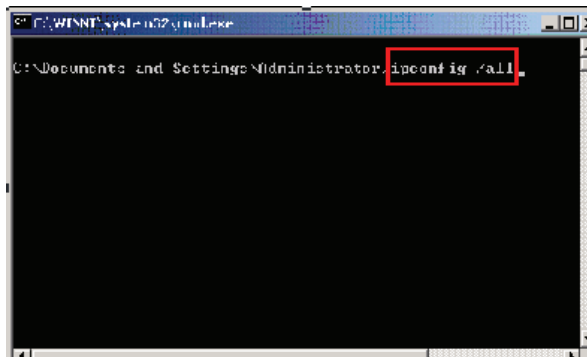
**ANSWER:** The factory default LAN IP address for the BiGuard S Series is as follows:

- **IP address:** 192.168.1.254
- **Subnet Mask:** 255.255.255.0

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

**ANSWER:** Follow these 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 **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 do not work, power off the router, wait a few moments and power on the router and perform steps 1 ~ 3 again.
5. If you are still unable to login, do a hardware reset which will restore factory default settings. Refer to the next question.



**QUESTION:** How do I reset the BiGuard S Series?

**ANSWER:** There are two ways to reset factory default: Hardware Reset and Software Reset.

### Performing a hardware reset

You can restore your BiGuard S Series to its factory settings by performing a hardware reset of the router.



**WARNING:** Performing a hardware reset of the router will erase all settings and return the router to the configuration it was in when you first installed it. To reset the router without erasing all your settings, perform a software reset. See [Restarting the system on page 138](#).

To perform a hardware reset, press and hold down the reset button for 6 seconds, and wait for the status LED to blink. Then release the reset button.



When the hardware load default procedure is complete, the status LED turns off.

## Performing a software reset

To initiate a software reset, follow the steps below.

1. Click the **Configuration** → **System** → **Restart**.

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"/>	

2. Select **Factory Default Settings**.

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

3. Click **Restart**.

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

After a minute, the status LED will begin to blink. The LED will turn off after the default settings are reset.



**NOTE:** If all of the above procedures still do not work, contact your dealer for further instructions.

**QUESTION:** I have just upgraded the router firmware to the latest version, but I found some of the buttons or pages do not display or work properly.

---

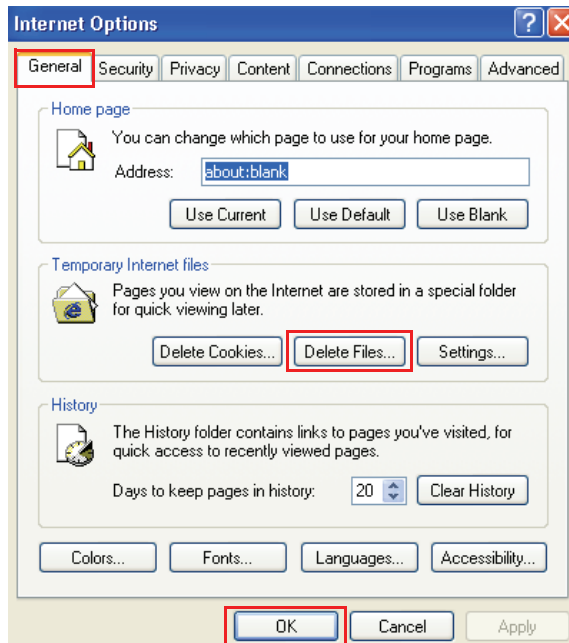
**ANSWER:** It is possible that the browser is referencing data stored in the cache. Clear the offline browser data in the cache, restart the browser, and try again.

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 not I ping the WAN IP address of the BiGuard S Series from the Internet?

---

**ANSWER:** Make sure the Block WAN Request is disabled.

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

Firewall	
Block PING Request	
Block PING Request	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Intrusion Detection	
Intrusion Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Exception List	<input type="checkbox"/> Allow NetBIOS to pass through Intrusion Detection
	<input type="checkbox"/> Allow EPMAP (port:135) to pass through Intrusion Detection
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Firewall	
Block PING Request	
Block PING Request	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Intrusion Detection	
Intrusion Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Exception List	<input type="checkbox"/> Allow NetBIOS to pass through Intrusion Detection
	<input type="checkbox"/> Allow EPMAP (port:135) to pass through Intrusion Detection
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3. Click **Apply**.

You can now ping the BiGuard S Series WAN IP address.

# BiGuard S Series FAQ

## DMZ

**QUESTION:** What is 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 S Series supports hardware DMZ. To set up a DMZ for the BiGuard S Series, follow these instructions.

1. From the **Configuration** menu, select **Interface** → **DMZ**. The DMZ Parameters screen appears.

2. From the drop down menu, select **Transparent** and click **Apply**.

When the DMZ is enabled, the DMZ LED is lit, indicating that the LAN port 4 is set as the DMZ port.

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 a 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 192.168.1.100 to the Address table. Follow these instructions.

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

Address				
Address Table				
Name	IP Address	Subnet Mask/Range		
**Any	All IP Addresses			
**Default WAN1 IP	WAN1 IP Address			
**Default WAN2 IP	WAN2 IP Address			
Create ➤				

2. Click **Create**.

Address	
Create	
Name	IP 192.168.1.100
Type	IP Address
IP Address	192.168.1.100 <a href="#">Candidates</a>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3. Type a name for this address in the **Name** field.
4. Select IP Address from the drop-down menu, and type the address (ex. 192.168.1.100) in the **IP Address** text box.
5. Click **Apply** to save the new item.
6. Click **Configuration** → **Policy** → **Packet Filtering**. Click **Create** to add a Packet Filtering Profile.

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

7. Type a descriptive name for this filter, select **LAN** to **WAN** from the **Packet Flow** drop-down menu and check the **Reverse Direction** box.
8. Select the **HTTP** option from the Service drop-down menu, and select the newly created address (IP 192.168.1.100) from the **From Address** drop-down menu.

Packet Filtering	
Create	
Name	Packet Filtering
Active	<input checked="" type="checkbox"/> Enable
Packet Flow	LAN to WAN <input checked="" type="checkbox"/> Reverse Direction
Action	Drop
Service	**Any
From Address	IP 192.168.1.100
To Address	**Any
Schedule	**Always On
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



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

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

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

**QUESTION:** What does the Rule Number (#) mean in Packet Filtering? Is it related to the priority?

**ANSWER:** Rule Number (#) is the packet filtering identification. It is related to the policy priority.

Packet Filtering											
Parameters											
#	Name	Active	Flow	Action	Service	From	To	Schedule			
1	Packet Filtering	Yes	LAN to WAN /reverse	Drop	**Any	IP 192.168.1.100	**Any	**Always On	Edit	Delete	Move
2	Packet Filtering1	Yes	LAN to WAN /reverse	Drop	**Any	**Any	**Any	**Always On	Edit	Delete	Move
Create											

To determine the priority for Packet Filtering rules, you can click **Move** and the rule priority can be moved higher or lower by selecting before or after a specified rule number.

https://192.168.1.254/cgi-bin/policy\_pf\_move?policy\_pf\_id=0 - Microsoft Internet Expl...

Packet Filtering			
Move Policy			
Rule Name	Packet Filtering	Rule No	1
Move	<input checked="" type="radio"/> Before <input type="radio"/> After	Rule No	1
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

**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 related web sites. First, the user must set up a keyword filtering profile.

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

Content Blocking			
Keyword Filtering			
Profile	Keyword		
Create			

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 **Keyword** field.
4. Click **Add**. The keyword is added to the Block WEB URLs list.
5. Add more keywords to this filter by typing the keywords into the **Keyword** field and click **Add**.

Keyword Filtering	
Create	
Profile	Sex-Websites
Keyword	
Add	
Block WEB URLs which contain these keywords	
Keyword	
sex	Delete
porn	Delete
sexy	Delete
Apply Cancel	

6. 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.

Now that you have created a Keyword Filtering Profile, you can activate the filter.

7. Click **Configuration** → **Policy** → **Content Filtering**. Click **Create** to add a Keyword Filtering Profile.

Content Filtering	
Create	
Name	<input type="text" value="Pomography"/>
Active	<input checked="" type="checkbox"/> Enable
Keyword Filtering ▶	<input checked="" type="checkbox"/> Enable <span>Sex-Websites ▼</span>
Domain Filtering ▶	<input type="checkbox"/> Enable
	<input type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict Feature ▶	<input type="checkbox"/> Enable
From Address ▶	<span>**Any ▼</span>
Schedule ▶	<span>**Always On ▼</span>
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

8. Type a descriptive name for this content filtering profile and check **Active** to enable content filtering.
9. In **Keywords Filtering**, check **Enable** and select your new **Keywords Filtering** profile from the drop-down menu.
10. Click **Apply**. The new content filter is listed.

Content Filtering									
Parameters									
#	Name	Active	Keyword	Domain	Restrict	From	Schedule		
1	Pomography	Yes	Sex-Websites	Disabled	Disabled	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>									
Exception list									
IP Address									
<a href="#">Create</a>									

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.

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 field or click **Candidates** to select an IP address from the list.

**Content Filtering Exception IP**

Create

IP Address  Candidates

Apply Cancel

**Active PC in LAN**

IP Address	MAC
<input type="radio"/> 192.168.1.35	00:05:5D:04:47:73

**QUESTION: What is Domain 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**.

**Content Blocking**

**Domain Filtering**

Profile	Forbidden Domain	Trust Domain

Create

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

**Domain Filtering**

Create

Profile

Domain

Type

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 (ex. *www.sexpicture.com*) in the text boxes.
4. Select **Forbidden Domain** (block URL) from the drop-down menu.

- Click **Add**. The keyword is added to the Block WEB URLs list.

Domain Filtering	
<b>Create</b>	
Profile	Sex Sites
Domain	<input type="text"/>
Type	Forbidden Domain ▼
<input type="button" value="Add"/>	
<b>Block WEB URLs which contain these domains</b>	
Forbidden Domain	
www.sexpicture.com	<input type="button" value="Delete"/>
<b>UnBlock WEB URLs which contain these domains</b>	
Trusted Domain	
<input type="button" value="Apply"/> <input type="button" value="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 allow in the Domain text box and select **Trusted Domain** (unblock URL) from the Type drop-down menu.

Domain Filtering	
<b>Create</b>	
Profile	Sex Sites
Domain	<input type="text" value="www.sexhealth.com"/>
Type	Forbidden Domain ▼
<input type="button" value="Add"/> <div> Forbidden Domain  Trusted Domain </div>	
<b>Block WEB URLs which contain these domains</b>	
Forbidden Domain	
www.sexpicture.com	<input type="button" value="Delete"/>
<b>UnBlock WEB URLs which contain these domains</b>	
Trusted Domain	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Domain Filtering	
<b>Create</b>	
Profile	Sex Sites
Domain	<input type="text"/>
Type	Forbidden Domain ▾
<input type="button" value="Add"/>	
<b>Block WEB URLs which contain these domains</b>	
Forbidden Domain	
www.sexpicture.com	<input type="button" value="Delete"/>
<b>UnBlock WEB URLs which contain these domains</b>	
Trusted Domain	
www.sexhealth.com	<input type="button" value="Delete"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

8. Click **Apply**. The new domain filter is listed.

Content Blocking				
Domain Filtering				
Profile	Forbidden Domain	Trust Domain		
Sex Sites	www.sexpicture.com	www.sexhealth.com	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>				

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

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

## Content Filtering

Parameters

#	Name	Active	Keyword	Domain	Restrict	From	Schedule		
1	Pornography	Yes	Sex-Websites	Disabled	Disabled	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>

Create

Exception list

IP Address	
------------	--

Create

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

Content Filtering	
<b>Create</b>	
Name	Sex Sites
Active	<input checked="" type="checkbox"/> Enable
Keyword Filtering	<input type="checkbox"/> Enable Sex-Websites
Domain Filtering	<input checked="" type="checkbox"/> Enable Sex Sites <input type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict Feature	<input type="checkbox"/> Enable
From Address	**Any
Schedule	**Always On
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

11. Type a descriptive name for this content filtering profile and check **Active** to enable content filtering.
12. In **Domains Filtering**, check **Enable** and select your new Domain Filtering profile from the drop-down menu.
13. Click **Apply**. The new content filter is listed.

Content Filtering									
Parameters									
#	Name	Active	Keyword	Domain	Restrict	From	Schedule		
1	Pomography	Yes	Sex-Websites	Disabled	Disabled	**Any	**Always On	Edit	Delete
2	Sex Sites	Yes	Disabled	Sex Sites	Disabled	**Any	**Always On	Edit	Delete
<a href="#">Create</a>									
Exception list									
IP Address									
<a href="#">Create</a>									

**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 that is listed under Trusted Domains list.

### Example:

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

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

Content Blocking			
Restrict URL Feature			
Name	Restrict Feature		
Block Java and ActiveX	Java Applet, ActiveX	<a href="#">Edit</a>	<a href="#">Delete</a>
Block Web Proxy	Proxy	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>			

- Click **Configuration** → **Policy** → **Content Filtering** and select both **Domain Filtering** and **Disable all WEB traffic except for Trusted Domains** options. This will block all URLs except for www.billion.com.

Content Filtering	
Create	
Name	<input type="text" value="Content"/>
Active	<input checked="" type="checkbox"/> Enable
Keyword Filtering	<input type="checkbox"/> Enable <input type="text" value="Sex-Websites"/>
Domain Filtering	<input checked="" type="checkbox"/> Enable <input type="text" value="Sex Sites"/>
	<input checked="" type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict Feature	<input type="checkbox"/> Enable <input type="text" value="Block Java and ActiveX"/>
From Address	<input type="text" value="**Any"/>
Schedule	<input type="text" value="**Always On"/>
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**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 can breach an user’s system. In addition, “buggy” applets hampers performance and can waste network bandwidth. Once this function is enabled, malicious code can not 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.

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

Content Blocking			
Restrict URL Feature			
Name	Restrict Feature		
<a href="#">Create</a>			

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



### Restrict Filtering

**Create**

Name	Block Java and ActiveX
Restrict URL Features	<input checked="" type="checkbox"/> Block Java Applet
	<input checked="" type="checkbox"/> Block ActiveX
	<input type="checkbox"/> Block Cookies
	<input type="checkbox"/> Block Proxy
	<input type="checkbox"/> Block Surfing by IP Address

Apply Cancel

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

### Content Blocking

Restrict URL Feature			
Name	Restrict Feature		
Block Java and ActiveX	Java Applet, ActiveX	Edit ▶	Delete ▶

Create ▶

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 add a new content filter.

### Content Filtering

**Create**

Name	Java and ActiveX
Active	<input checked="" type="checkbox"/> Enable
Keyword Filtering ▶	<input type="checkbox"/> Enable Sex-Websites ▼
Domain Filtering ▶	<input type="checkbox"/> Enable Sex Sites ▼
	<input type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict Feature ▶	<input checked="" type="checkbox"/> Enable Block Java and ActiveX ▼
From Address ▶	**Any ▼
Schedule ▶	**Always On ▼
Log	<input type="checkbox"/> Enable

Apply Cancel

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

Content Filtering										
Parameters										
#	Name	Active	Keyword	Domain	Restrict	From	Schedule			
1	Pornography	Yes	Sex-Websites	Disabled	Disabled	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>
2	Java and ActiveX	Yes	Disabled	Disabled	Block Java and ActiveX	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>
<a href="#">Create</a>										
Exception list										
IP Address										
<a href="#">Create</a>										

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, which changes the order of the rules.

#### 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**.

Content Blocking			
Restrict URL Feature			
Name	Restrict Feature		
Block Java and ActiveX	Java Applet, ActiveX	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>			

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

Restrict Filtering	
Create	
Name	<input type="text" value="Block Web Proxy"/>
Restrict URL Features	<input type="checkbox"/> Block Java Applet
	<input type="checkbox"/> Block ActiveX
	<input type="checkbox"/> Block Cookies
	<input checked="" type="checkbox"/> Block Proxy
	<input type="checkbox"/> Block Surfing by IP Address
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Content Blocking			
Restrict URL Feature			
Name	Restrict Feature		
Block Java and ActiveX	Java Applet, ActiveX	<a href="#">Edit</a>	<a href="#">Delete</a>
Block Web Proxy	Proxy	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>			

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 add a new content filter.

Content Filtering	
Create	
Name	<input type="text" value="Block Web Proxy"/>
Active	<input checked="" type="checkbox"/> Enable
Keyword Filtering	<input type="checkbox"/> Enable <input type="text" value="Sex-Websites"/>
Domain Filtering	<input type="checkbox"/> Enable <input type="text" value="Sex Sites"/>
	<input checked="" type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict Feature	<input checked="" type="checkbox"/> Enable <input type="text" value="Block Web Proxy"/>
From Address	<input type="text" value="**Any"/>
Schedule	<input type="text" value="**Always On"/>
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Content Filtering										
Parameters										
#	Name	Active	Keyword	Domain	Restrict	From	Schedule			
1	Pornography	Yes	Sex-Websites	Disabled	Disabled	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>
2	Java and ActiveX	Yes	Disabled	Disabled	Block Java and ActiveX	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>
3	Block Web Proxy	Yes	Disabled	Disabled	Block Web Proxy	**Any	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Move</a>
<a href="#">Create</a>										
Exception list										
IP Address										
<a href="#">Create</a>										

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.

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

**ANSWER:** This policy blocks the saving and reading of cookies. Both secure and insecure websites are blocked from using cookies by this function.

To block cookies, follow these instructions.

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

Content Blocking			
Restrict URL Feature			
Name	Restrict Feature		
Block Java and ActiveX	Java Applet, ActiveX	<a href="#">Edit</a>	<a href="#">Delete</a>
Block Web Proxy	Proxy	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>			

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

Restrict Filtering	
Create	
Name	<input type="text" value="Block Cookies"/>
Restrict URL Features	<input type="checkbox"/> Block Java Applet
	<input type="checkbox"/> Block ActiveX
	<input checked="" type="checkbox"/> Block Cookies
	<input type="checkbox"/> Block Proxy
	<input type="checkbox"/> Block Surfing by IP Address
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Content Blocking			
Restrict URL Feature			
Name	Restrict Feature		
Block Java and ActiveX	Java Applet, ActiveX	<a href="#">Edit</a>	<a href="#">Delete</a>
Block Web Proxy	Proxy	<a href="#">Edit</a>	<a href="#">Delete</a>
Block Cookies	Cookies	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>			

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 add a new content filter.

Content Filtering	
<b>Create</b>	
Name	Block Cookies
Active	<input checked="" type="checkbox"/> Enable
Keyword Filtering	<input type="checkbox"/> Enable Sex-Websites
Domain Filtering	<input type="checkbox"/> Enable Sex Sites
	<input type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict Feature	<input checked="" type="checkbox"/> Enable Block Cookies
From Address	**Any
Schedule	**Always On
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Content Filtering										
Parameters										
#	Name	Active	Keyword	Domain	Restrict	From	Schedule			
1	Pornography	Yes	Sex-Websites	Disabled	Disabled	**Any	**Always On	Edit	Delete	Move
2	Java and ActiveX	Yes	Disabled	Disabled	Block Java and ActiveX	**Any	**Always On	Edit	Delete	Move
3	Block Web Proxy	Yes	Disabled	Disabled	Block Web Proxy	**Any	**Always On	Edit	Delete	Move
4	Block Cookies	Yes	Disabled	Disabled	Block Cookies	**Any	**Always On	Edit	Delete	Move
<a href="#">Create</a>										
Exception list										
IP Address										
<a href="#">Create</a>										

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.

#### 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**.

Content Blocking			
Restrict URL Feature			
Name	Restrict Feature		
Block Java and ActiveX	Java Applet, ActiveX	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
Block Web Proxy	Proxy	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
Block Cookies	Cookies	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
<a href="#">Create</a> ▶			

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

Restrict Filtering	
Create	
Name	<input type="text" value="http://123.123.123.123"/>
Restrict URL Features	<input type="checkbox"/> Block Java Applet
	<input type="checkbox"/> Block ActiveX
	<input type="checkbox"/> Block Cookies
	<input type="checkbox"/> Block Proxy
	<input checked="" type="checkbox"/> Block Surfing by IP Address
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Content Blocking			
Restrict URL Feature			
Name	Restrict Feature		
Block Java and ActiveX	Java Applet, ActiveX	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
Block Web Proxy	Proxy	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
Block Cookies	Cookies	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
<a href="http://123.123.123.123">http://123.123.123.123</a>	Surfing by IP	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
<a href="#">Create</a> ▶			

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.

Content Filtering	
<b>Create</b>	
Name	Block IP
Active	<input checked="" type="checkbox"/> Enable
Keyword Filtering ▶	<input type="checkbox"/> Enable Sex-Websites ▼
Domain Filtering ▶	<input type="checkbox"/> Enable Sex Sites ▼ <input type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict Feature ▶	<input checked="" type="checkbox"/> Enable http://123.123.123.123 ▼
From Address ▶	**Any ▼
Schedule ▶	**Always On ▼
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Content Filtering										
Parameters										
#	Name	Active	Keyword	Domain	Restrict	From	Schedule			
1	Pornography	Yes	Sex-Websites	Disabled	Disabled	**Any	**Always On	Edit ▶	Delete ▶	Move ▶
2	Java and ActiveX	Yes	Disabled	Disabled	Block Java and ActiveX	**Any	**Always On	Edit ▶	Delete ▶	Move ▶
3	Block Web Proxy	Yes	Disabled	Disabled	Block Web Proxy	**Any	**Always On	Edit ▶	Delete ▶	Move ▶
4	Block Cookies	Yes	Disabled	Disabled	Block Cookies	**Any	**Always On	Edit ▶	Delete ▶	Move ▶
5	Block IP	Yes	Disabled	Disabled	http://123.123.123.123	**Any	**Always On	Edit ▶	Delete ▶	Move ▶
<a href="#">Create ▶</a>										
Exception list										
IP Address										
<a href="#">Create ▶</a>										

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.

### 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.

- Click **Configuration** → **Policy** → **Content Filtering**. And under the Exception List, click **Create**.

Content Filtering								
Parameters								
#	Name	Active	Keyword	Domain	Restrict	From	Schedule	
Create								
Exception list								
IP Address								
Create								

2. Type the IP address you want excluded from the **Content Filtering** (ex. 192.168.1.100), or click **Candidates** and select an available IP address from the list.

Content Filtering Exception IP	
Create	
IP Address	192.168.1.100 <a href="#">Candidates </a>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3. Click **Apply**. The IP address is added to the Exception List.

Content Filtering								
Parameters								
#	Name	Active	Keyword	Domain	Restrict	From	Schedule	
Create								
Exception list								
IP Address								
192.168.1.100				<a href="#">Delete </a>				
Create								

4. 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 S Series checks MAC addresses against a list of allowed or denied addresses before allowing or denying the 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**.

Ethernet MAC Filtering						
Parameters						
#	Name	Active	Flow	Action	MAC Address	Schedule
Create						



- Click **Create** to add a Ethernet MAC Filtering profile.

Ethernet MAC Filtering	
<b>Create</b>	
Name	MAC Filter1
Active	<input checked="" type="checkbox"/> Enable
Action	Drop
Mac Address	00:11:11:11:11:11 <a href="#">Candidates</a> (00:00:00:00:00:00 means 'All MAC Addresses')
<a href="#">Schedule</a>	**Always On
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Ethernet MAC Filtering								
Parameters								
#	Name	Active	Flow	Action	MAC Address	Schedule		
1	MAC Filter1	Yes	LAN to WAN	Drop	00:11:11:11:11:11	**Always On	<a href="#">Edit</a>	<a href="#">Delete</a>
<a href="#">Create</a>								

## 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.

- Click **Configuration** → **Policy** → **Ethernet MAC Filtering**. And click **Create** to add an Ethernet MAC filter.

Ethernet MAC Filtering								
Parameters								
#	Name	Active	Flow	Action	MAC Address	Schedule		
<a href="#">Create</a>								

- Type a descriptive name for this filter and check **Enable** in the Active row to activate the filter.
- From the **Action** drop-down menu, select **Forward**.

4. Type the MAC address in the text box or click **Candidates** and select an available MAC address from the list.
5. Click **Add**. The new filter is added to the list.

Ethernet MAC Filtering								
Parameters								
#	Name	Active	Flow	Action	MAC Address	Schedule		
1	Sole Access	Yes	LAN to WAN	Drop	00:11:11:11:11:11	**Always On	Edit ▶	Delete ▶
Create ▶								

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.

Ethernet MAC Filtering	
Create	
Name	<input type="text" value="No Access"/>
Active	<input checked="" type="checkbox"/> Enable
Action	<input type="text" value="Drop"/>
Mac Address	<input type="text" value="00:00:00:00:00:00"/> Candidates ▶ (00:00:00:00:00:00' means 'All MAC Addresses')
Schedule ▶	<input type="text" value="**Always On"/>
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

6. Type a descriptive name for this filter and check **Enable** in the Active row to activate the filter.
7. From the **Action** drop-down menu, 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 S services.

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

Ethernet MAC Filtering								
Parameters								
#	Name	Active	Flow	Action	MAC Address	Schedule		
1	Sole Access	Yes	LAN to WAN	Forward	00:11:11:11:11:11	**Always On	Edit ▶	Delete ▶
2	No Access	Yes	LAN to WAN	Drop	00:00:00:00:00:00	**Always On	Edit ▶	Delete ▶
Create ▶								



**WARNING:** Priority is defined by order. In the above example, if the current Rule #2 is created first, it would be prioritized before any other rule. Consequently, all MAC address packets will be dropped before the Forward 00:11:11:11:11:11 rule is applied.

**QUESTION:** Why can not I ping the WAN IP address of the BiGuard S Series from the Internet?

**ANSWER:** Make sure the Block WAN Request is disabled.

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

Firewall	
Block PING Request	
Block PING Request	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Intrusion Detection	
Intrusion Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Exception List	<input type="checkbox"/> Allow NetBIOS to pass through Intrusion Detection
	<input type="checkbox"/> Allow EPMAP (port:135) to pass through Intrusion Detection
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

Firewall	
Block PING Request	
Block PING Request	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Intrusion Detection	
Intrusion Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Exception List	<input type="checkbox"/> Allow NetBIOS to pass through Intrusion Detection
	<input type="checkbox"/> Allow EPMAP (port:135) to pass through Intrusion Detection
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3. Click **Apply**.

You can now ping the BiGuard S Series WAN IP address.

## Remote Access

**QUESTION:** How do I configure the remote access setting of BiGuard S Series?

**ANSWER:** The Remote Access function is configured through the **Configuration → System → Remote Access** menu. There are three options available: **Enable Both Remote SSL VPN Portal and Remote Configuration**, **Enable Remote SSL VPN Portal, but Disable Remote Configuration** (Default), and **Disable Both Remote SSL VPN Portal and Remote Configuration**.

Remote Access	
You may permit remote access and administration on this network device (HTTPS).	
Remote Access Control	<input type="radio"/> Enable Both Remote SSL VPN Portal and Remote Configuration <input checked="" type="radio"/> Enable Remote SSL VPN Portal, but Disable Remote Configuration <input type="radio"/> Disable Both Remote SSL VPN Portal and Remote Configuration
Remote Address	**Any
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

1. Select the desired setting.
2. Click **Apply** to save the settings.

**QUESTION:** What is the Auto log-out timer?

**ANSWER:** There is an inactivity timeout period 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 S Series.

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

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

Account				
Account Table				
Name	Group			
admin	BiGuard	<a href="#">Edit </a>		
<a href="#">Create </a> <a href="#">Move </a>				

2. Click **Edit** next to the account you would like to modify (ex. *admin*).

Edit Account		
<b>General Setting</b>		
Name	admin	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>Login Setting</b>		
Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	100	Minutes
<b>Service</b>		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
<b>Application Proxy</b>		
Applications	This group has no application now.	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

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

---

**QUESTION:** Can I upgrade firmware remotely from the WAN port?

**ANSWER:** Yes. However, Billion does not recommend doing so as Internet service reliability varies in different areas. The connection can be easily disrupted, causing a firm-ware upgrade failure.

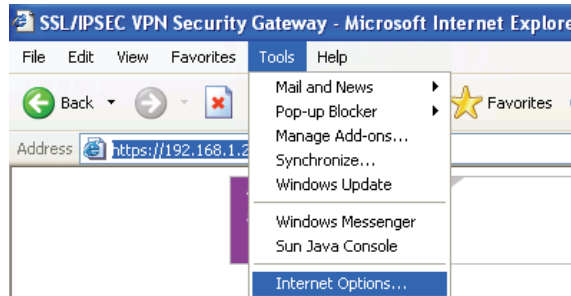
---

**QUESTION:** I have just upgraded the router firmware to the latest version, but I found some of the buttons or pages do not display or work properly.

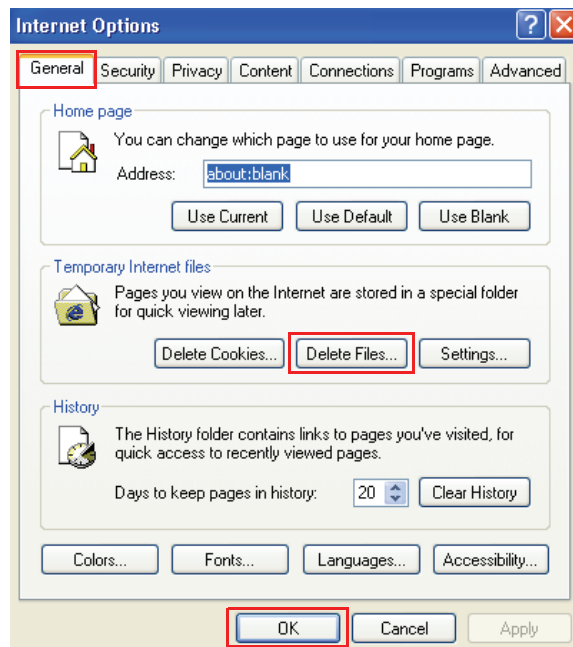
**ANSWER:** It is possible that the browser is referencing data stored in the cache. Clear the offline browser data in the cache, restart the browser, and try again.

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

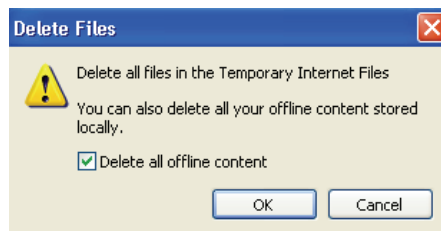
1. Open the Internet Explorer browser, select **Tools** → **Internet Options**.



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



3. Select **Delete all offline content** when prompted.



4. Click **OK** to exit, and then click **Apply**.

## SNMP

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

---

**ANSWER:** The following MIBs are supported by the BiGuard S 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 S 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 S 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 S 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 S Series provide? What do they do?

---

**ANSWER:** The Billion BiGuard S Series provides clientless, identity-based, secure remote access to your protected internal network. Using the 'SSL VPN Portal' environment, the Billion BiGuard S 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** provides a transparent IP tunnel for trusted users to access full network resources. BiGuard SSL VPN appliances support Network Extender technology to virtually extend your connection to the central office network and allow you to access your office resources seamlessly from anywhere, as if you had never left the office. You can remotely access office files and applications through your computer, desktop or PDA, as if you were using a computer in your corporate network. A sales person on a business trip, who needs to know the product inventory can use the Network Extender technology in BiGuard SSL VPN appliances to connect to the corporate network and access the stock database to check instead of phoning back to the office to request the information.
- **Transport Extender** provides a transparent service tunnel for users to access client server applications. BiGuard SSL VPN appliances support Transport Extender technology to enable specific remote users or specific remote groups of users to use the SSL VPN connection to connect to the corporate network to access the services as configured by IT administrators. Therefore the remote user does not have to change any specific settings in the web portal to make the service work. For instance, when a user remotely accesses MS Outlook e-mail, the Transport Extender technology will transport the e-mail service through the SSL VPN tunnel to the e-mail server in the corporate network, as configured by the IT administrator. Since the remote user doesn't have to modify any settings in the web portal, the remote user will feel as if they are using MS Outlook in the office when in fact they are really somewhere else.
- **Network Places** provides network places function for users to access company network resources. Just like the Windows Network Neighborhood, My Network Places allows users to browse network files in the office network. From home computer, users can connect directly to My Network Places and access information inside the office from now on and there is no need to go back to the office if users forget an important document.
- **FTP Client** provides client function to remote access company files. BiGuard SSL VPN appliances support File Transfer Protocol (FTP) client function to access FTP server on the internal network, or any other network segments that can be reached by the SSL VPN appliances, including the Internet. The remote user communicates with the BiGuard SSL VPN appliances via SSL VPN connections and is granted with appropriate permissions of the logon user to upload, download or create folders just like a FTP client software.
- **HTTP/HTTPS** provides HTTP/HTTPS proxy function to access company resources through the web interface. BiGuard SSL VPN appliances support HTTP/HTTPS proxy function to access HTTP/HTTPS server on the internal network, or any other network segment that can be reached by the BiGuard

SSL VPN appliances, including the Internet. The remote user communicates with the BiGuard SSL VPN appliances by HTTP/HTTPS protocol using a URL which is defined by administrator. The BiGuard SSL VPN appliances will then redirect the HTTP/HTTPS session data to the configured HTTP/HTTPS server.

- **Terminal Service and VNC** provides Terminal Service and VNC functions to access remote computers. BiGuard SSL VPN appliances support both Terminal Service (RDP5) and VNC functions to allow users to access to the remote computers. Terminal Server is built in to all Windows 2003 servers and Windows XP Professional desktop systems. It allows users to log in remotely from BiGuard SSL VPN appliances. By logging in users create client sessions to the server. Terminal Server works by knowing how to respond to a client process of BiGuard SSL appliances. This "terminal client" will present you with a window that simulates a local monitor. The Terminal Server manages all computing resources for you and provides you with your own environment. The server receives and processes all key strokes and mouse clicks sent by each client and directs display output (audio and video) to the client as appropriate. You have access to all of your authorized network resources and can run any applications made available to you on the server. All the applications supported by Windows 2003 Server can be run via the Terminal Server.

VNC, or Virtual Network Computing, is software that makes it possible to view and interact with a computer from any other computer or device connected to the internet. VNC client is built into BiGuard SSL VPN appliances, so a person can connect to and interact with an Unix system at home with VNC server software installed without any problems.

- **Telnet, SSH** provide Telnet, SSH services for administrators to remote manage network resources. Telnet is a protocol that allows you to connect to remote computers over a TCP/IP network. BiGuard SSL VPN appliances contain a built-in Java based telnet client to make a connection to a telnet server. To protect your account from interception in the Internet, we suggest you to use SSH instead of telnet. Since SSH encrypts all traffic with a public-private key scheme, only the SSH server can decrypt it and anyone who intercepts the data in transit will have only garbage data. BiGuard SSL VPN appliances contain a built-in Java based SSH client to make the connection.

## 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.

Administrator FTP Configuration:

Before you start to configure FTP proxy settings for the BiGuard SSL VPN appliance, you have to create an account on FTP server first.

### Example:

**Username:** user

**Password:** user

**FTP server's IP address:** 192.168.1.100

The following are the steps to configure FTP proxy settings in the BiGuard SSL VPN appliance for the FTP user: In the example below the BiGuard Group/Application is the default group profile and it will be used for the tutorial.

1. Click the following links: **SSL VPN Application** → **Group/Application**.

Group/Application					
Group Table					
Name	Authentication Domain	Domain's Default Group	Host Checking		
BiGuard	BiGuard	Yes	Disable	<a href="#">Edit</a>	
<a href="#">Create</a>					

2. To edit the **BiGuard** group, click the **Edit** link on the right hand side of the group profile **Name**.

The **Edit** link opens the Edit Group screen to add applications under your chosen group profile. This allows the users within that group to use the applications.

Edit Group			
<b>General Settings</b>			
Group Name	BiGuard		
Domain	BiGuard		
Password Policy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <a href="#">Advanced Setting</a>		
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Inactivity Timeout	5	Minutes	
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
<b>Service</b>			
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>		
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>		
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom Welcome to SSL/IPSEC \		
<b>Application Table</b>		<a href="#">Add Application</a>	
Name	Application	IP Address / Path	
<b>Note!</b> To make application changes, press <b>Apply</b> .			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- Click **Add Application** to open the SSL VPN Application screen to add an application to this group.

**Note:** You are allowed to add multiple applications under each group.

SSL VPN Application	
<b>Add Application</b>	
Application Name	<input type="text"/>
Application	File Transfer Protocol (FTP) <input type="button" value="v"/>
IP Address/Domain Name	<input type="text"/>
TCP Port Number	21
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- In the **Application Name** field, type **TestFTP** as an example for the application name.  
In the **Application** field, select **File Transfer Protocol (FTP)** from the drop-down menu.  
In the **IP Address** field, type the IP address for the server (ex. 192.168.1.100).

SSL VPN Application	
<b>Add Application</b>	
Application Name	TestFTP
Application	File Transfer Protocol (FTP) <input type="button" value="v"/>
IP Address/Domain Name	192.168.1.100
TCP Port Number	21
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

5. Click **Apply** to set the configuration settings, and return to **Group/Application**.

### Edit Group

General Settings				
Group Name	BiGuard			
Domain	BiGuard			
Password Policy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Inactivity Timeout	5 Minutes			
Host Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Service				
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)			
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>			
Web Cache Cleaner	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Greeting String	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/>			
Application Table				
<a href="#">Add Application</a>				
Name	Application	IP Address / Path	Edit	Delete
TestFTP	FTP	192.168.1.100:21	<a href="#">Edit</a>	<a href="#">Delete</a>
<b>Note!</b> To make application changes, press <b>Apply</b> .				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

6. After creating a group profile, you will need to create user accounts to use the applications assigned to that group profile.
7. Click the following links: **SSL VPN** → **User Access** → **Account**.

### Account

Account Table				
Name	Group			
admin	BiGuard	<a href="#">Edit</a>		
<a href="#">Create</a> <a href="#">Move</a>				

8. To create an account, click the **Create**.
9. The Add Account screen opens. You can create a user account to use the **FTP** application that was created in the previous steps.



**NOTE:** We suggest you create the same **User Name** and **Password** as your **FTP** server's account. In this way, you need not input the user name and password again when accessing the **FTP** server.

Add Account

General Setting

User Name

user

☒ Active

Group

BiGuard

Password

••••

Retype Password

••••

☐ Use group default password

Host Checking

☒ Active

Advanced Setting

Apply

Cancel

Group Setting Details

Force Login

Disable

Inactivity Timeout

5 Minutes

Network Place

Enable

Network Extender Service

Enable

Transport Extender Service

Enable

Web Cache Cleaner

Enable

Greeting String

Use default greeting string

Applications

There had no applications.

User Name	<b>User</b> was inputted as an example for the user name.
Group	<b>BiGuard</b> group was chosen from the drop-down menu.
Password	A password was inputted.
Retype Password	Type the password again to confirm the password.
Host Checking	Check or uncheck the box to activate or deactivate Host Checking on this account.

10. Click **Apply** to set the configurations and return to Account Table.


Account

Account Table

Name	Group			
user	BiGuard	Edit	Delete	Copy
admin	BiGuard	Edit		

Create

Move



**NOTE:** To permanently save the settings to the system, click **Save Config to FLASH** on the left hand side of the main menu.

## Remote user access

The following steps demonstrate how a user will log in to the FTP server from the remote web portal.

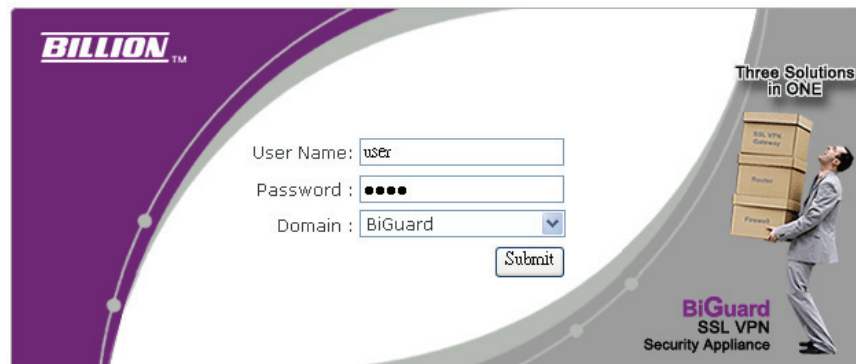
To access the remote web portal, please connect to the `https://wanipaddress` (where wanipaddress is the WAN IP address of the BiGuard SSL VPN appliance).

A Security Alert message appears.

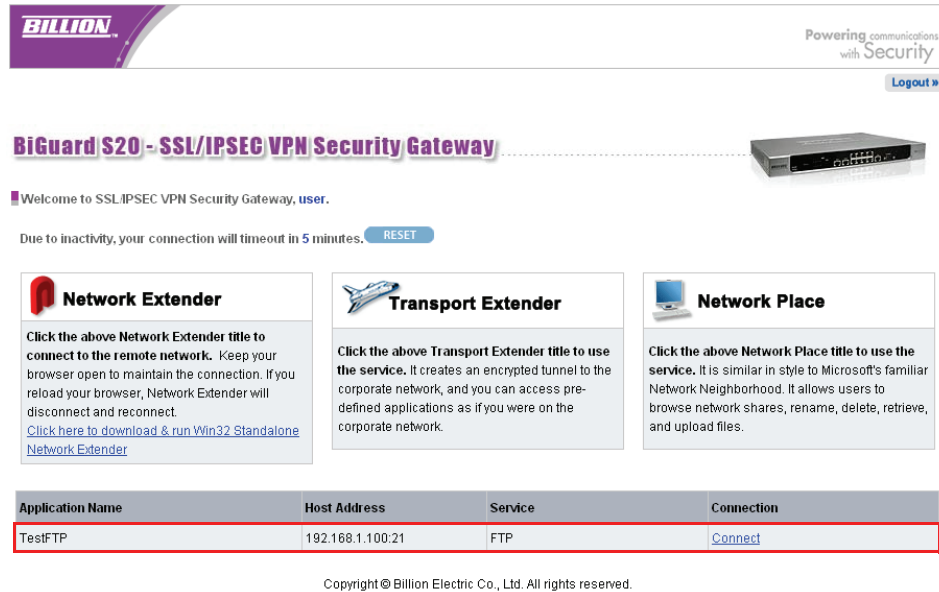
1. Click **Yes** to proceed (to accept the certificate sent by the BiGuard system).



The log in screen appears.




- Type in the user name (**User** as typed in the steps under the Administrator FTP Configuration section. User name and password are case sensitive.
  - Select a domain (ex. *BiGuard*) from the drop-down menu.
2. Click **Submit** to enter into the Remote Web Portal page.




**BiGuard S20 - SSL/IPSEC VPN Security Gateway**

Welcome to SSL/IPSEC VPN Security Gateway, **user**.


Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)


**Network Extender**

Click the above Network Extender title 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.  
[Click here to download & run Win32 Standalone Network Extender](#)


**Transport Extender**

Click the above Transport Extender title 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**

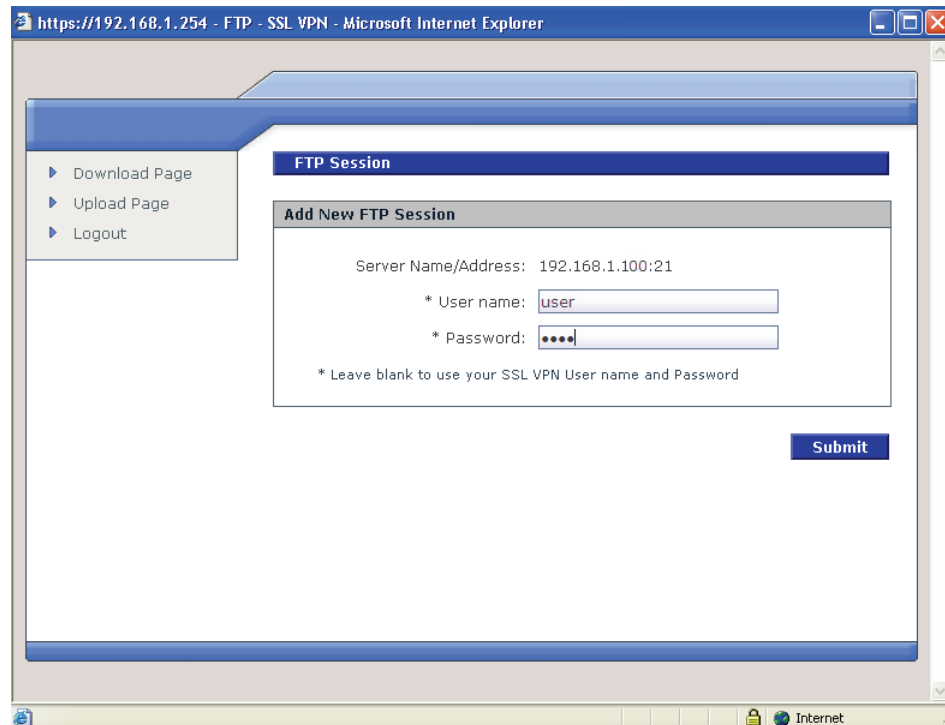
Click the above Network Place title to use the service. It is similar in style to Microsoft's familiar Network Neighborhood. It allows users to browse network shares, rename, delete, retrieve, and upload files.

Application Name	Host Address	Service	Connection
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

3. Click **Connect** to connect to the TestFTP service.

If the user account is the same as the FTP server's account, you will not be asked to input the user name and password, and the FTP session screen appears.  
If your user name differs from the FTP server's account, the following message appears.



https://192.168.1.254 - FTP - SSL VPN - Microsoft Internet Explorer

Download Page  
Upload Page  
Logout

**FTP Session**

**Add New FTP Session**

Server Name/Address: 192.168.1.100:21

\* User name:

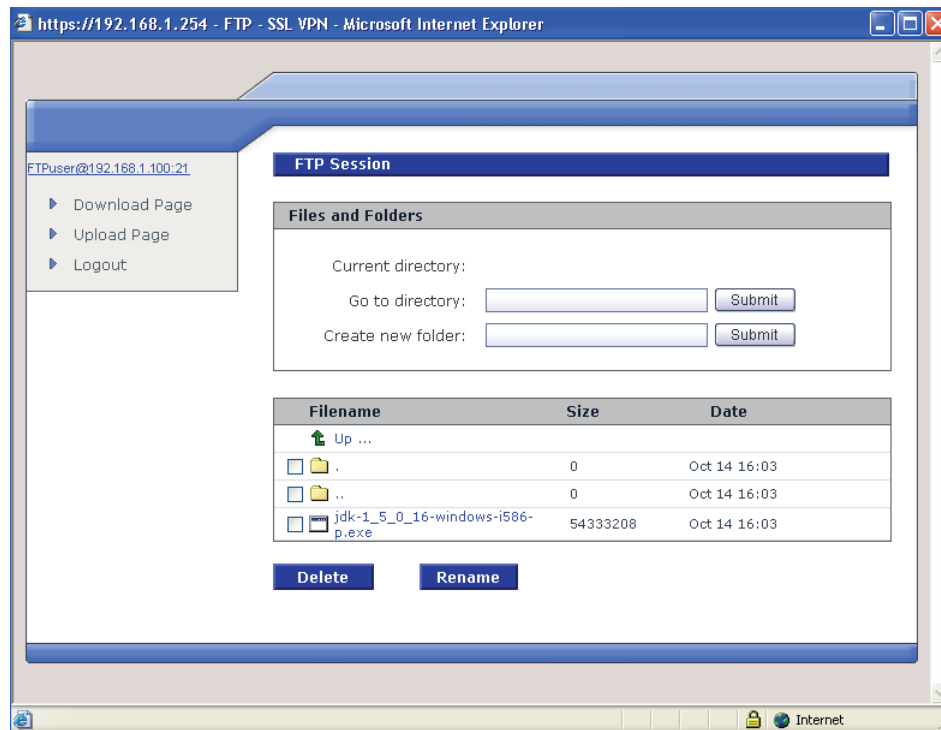
\* Password:

\* Leave blank to use your SSL VPN User name and Password

**Submit**

- Type in the user name (ex. *user*).
- Type in the password (ex. *user*).





You are logged in to your account in the designated FTP server.



**NOTE:** The single sign on (SSO) feature can only be used if the user has the same user name and password on both the remote sign on server and the FTP server.

## Using Network Extender

**QUESTION:** How do I set up Network Extender?

**ANSWER:** Using the guide to set up Network Extender.

## How to configure Network Extender?

1. Create an account with Network Extender Service enabled.

Select **SSL VPN** → **User Access** → **Account**. Click **Create** at the bottom left of the Account Table.

The Add Account screen displays.

### Add Account

**General Setting**

User Name	<input type="text" value="NetworkUser"/>	<input checked="" type="checkbox"/> Active
Group	<input type="text" value="BiGuard"/>	
Password	<input type="password" value="•••••"/>	
Retype Password	<input type="password" value="•••••"/>	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>

Group Setting Details	
Force Login	Disable
Inactivity Timeout	5 Minutes
Network Place	Enable
Network Extender Service	Enable Standalone Application (Win32 Only) Enable
Transport Extender Service	Enable
Web Cache Cleaner	Enable
Greeting String	Use default greeting string
Applications	TestFTP , TestTelnet , TestRDP , TestVNC , TestSSH , TestHTTP , TestHTTPS , TestCIFS

Click **Apply** to set the configurations and return to Account Table. Then click **Edit** to edit this Account.

When configuring a user account, enable the Network Extender service for the user. Assign the IP address dynamically or assign a fix IP for the user.

Edit Account		
<b>General Setting</b>		
Name	NetworkUser	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>Login Setting</b>		
Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	5	Minutes
<b>Service</b>		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
	<input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
<b>Application Proxy</b>		
Applications	<input checked="" type="checkbox"/> TestFTP	<input checked="" type="checkbox"/> TestTelnet
	<input checked="" type="checkbox"/> TestRDP	<input checked="" type="checkbox"/> TestVNC
	<input checked="" type="checkbox"/> TestSSH	<input checked="" type="checkbox"/> TestHTTP
	<input checked="" type="checkbox"/> TestHTTPS	<input checked="" type="checkbox"/> TestCIFS
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

2. Set up Network Extender Client IP Address Range.

Network Extender		
<b>Client IP Address Assignment</b>		
Client Address Range Begin	192.168.1.210	
Client Address Range End	192.168.1.230	
DNS Server	Primary	<input type="text"/>
	Secondary	<input type="text"/>
WINS Server	Primary	<input type="text"/>
	Secondary	<input type="text"/>
NetBIOS Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Tunnel All Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

When you choose to assign the IP address dynamically, you have to setup the client IP address assignment by inputting the beginning and ending Client Address Range.

3. Setup Network Extender Client Route.

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"/>	

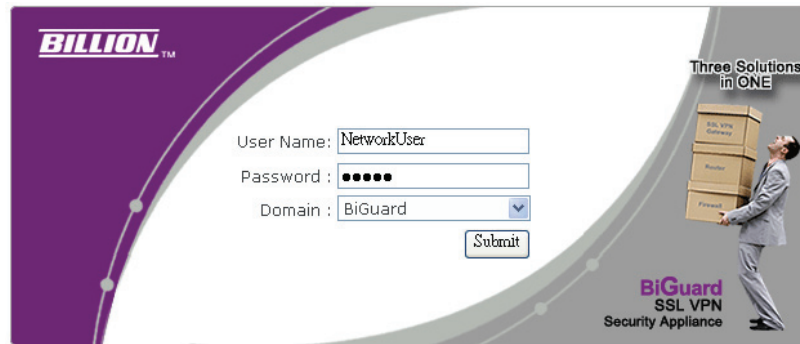
4. Click **Apply** to set the configuration.

## Remote SSL VPN Portal

When the client IP address and the office network address are in a different subnet, add a client route to the office network to route to the SSL connection.

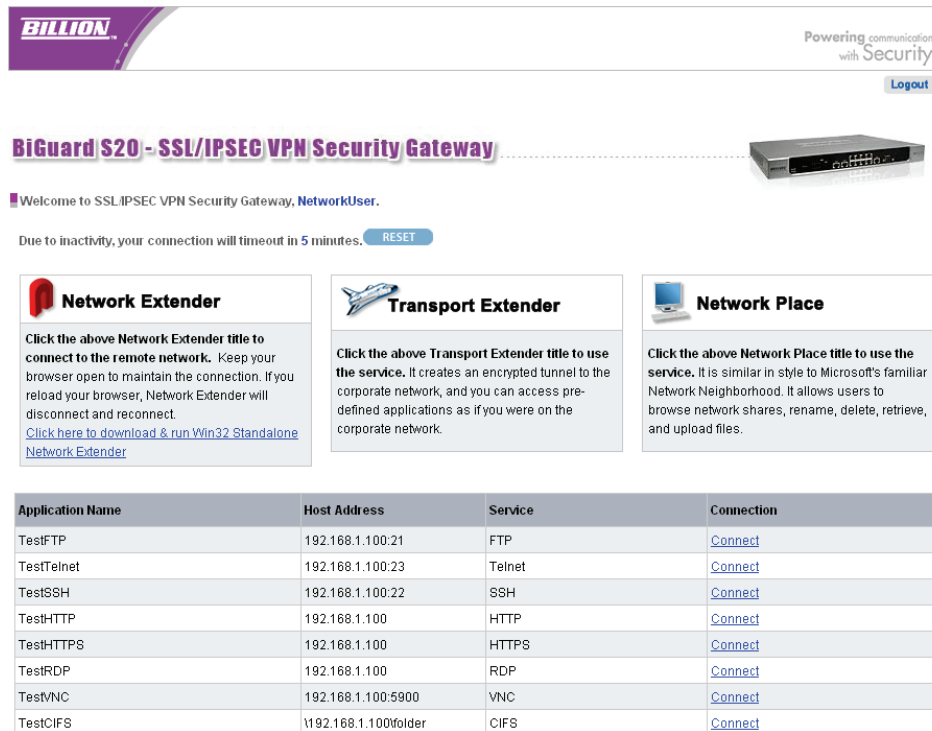
To use Web Portal Network Extender, first connect to the device by typing `https://wanipaddress` (where *wanipaddress* is the WAN IP address of the BiGuard SSL VPN appliance. After successfully connection and login to the device, the web portal screen appears.

1. Type the WAN IP Address or Domain Name in the Address bar of the browser and log into the BiGuard SSL VPN remote portal as previously configured.



The login screen for the BiGuard SSL VPN Security Appliance. It features the BILLION logo in the top left. The main area contains a login form with fields for 'User Name' (containing 'NetworkUser'), 'Password' (masked with dots), and 'Domain' (a dropdown menu showing 'BiGuard'). A 'Submit' button is located below the password field. On the right side, there is a graphic of a person carrying boxes with the text 'Three Solutions in ONE' and 'BiGuard SSL VPN Security Appliance' at the bottom right.

2. Click **Network Extender** in the remote portal window.

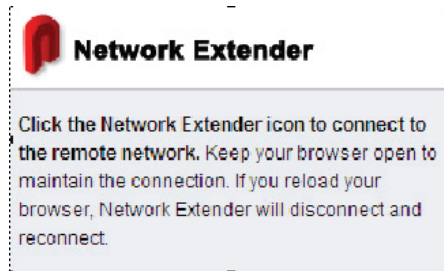


The web portal for the BiGuard S20 - SSL/IPSEC VPN Security Gateway. It features the BILLION logo and the tagline 'Powering communications with Security'. A 'Logout' button is in the top right. The main heading is 'BiGuard S20 - SSL/IPSEC VPN Security Gateway'. Below it, a welcome message says 'Welcome to SSLIPSEC VPN Security Gateway, NetworkUser.' and a timeout notice states 'Due to inactivity, your connection will timeout in 5 minutes.' with a 'RESET' button. There are three main sections: 'Network Extender' (with a red icon), 'Transport Extender' (with a blue icon), and 'Network Place' (with a blue icon). Each section has a brief description and a 'Click here to download & run Win32 Standalone' link. At the bottom, there is a table listing various services and their connection status.

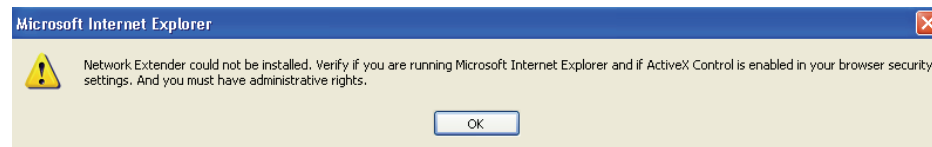
Application Name	Host Address	Service	Connection
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
TestHTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
TestRDP	192.168.1.100	RDP	<a href="#">Connect</a>
TestVNC	192.168.1.100:5900	VNC	<a href="#">Connect</a>
TestCIFS	192.168.1.100\Folder	CIFS	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

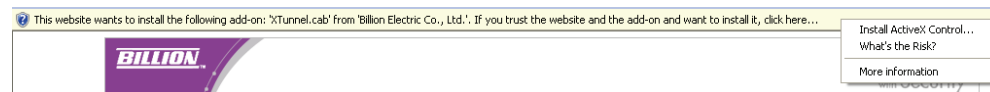
3. Click **Network Extender**.



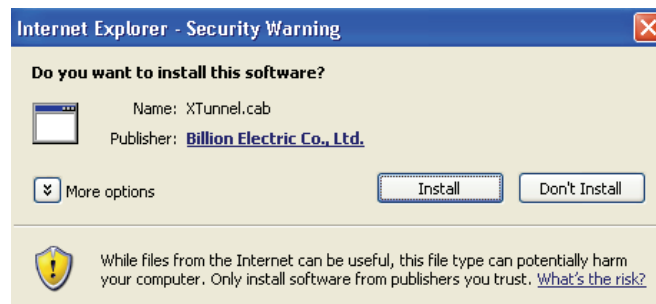
4. If the browser does not launch ActiveX automatically, a warning message appears. Click **OK** to continue. If the browser automatically installs ActiveX (the warning message does not display), then go to **Step 8**.



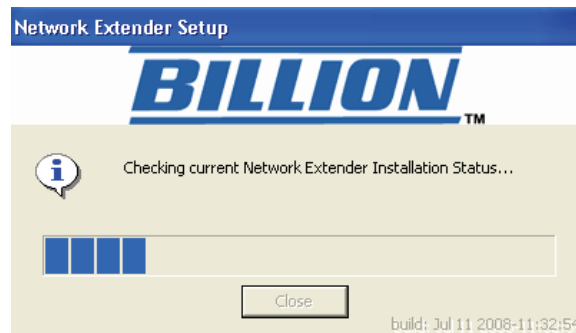
5. Click the **Information** bar on the top of the page and click **Install ActiveX Control**.



6. After the screen refreshes, click **Network Extender** again.
7. You are required to install the **XTunnel.cab**. Click **Install** to install the software.



Network Extender setup proceeds.



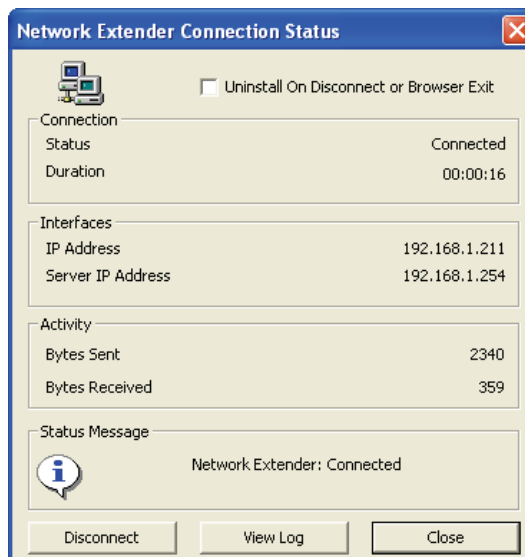
8. You are prompted to install the **SSLDrv Adapter**.



9. Click **Continue Anyway** when prompted to accept the SSLDrv Adapter. The procedure continues.




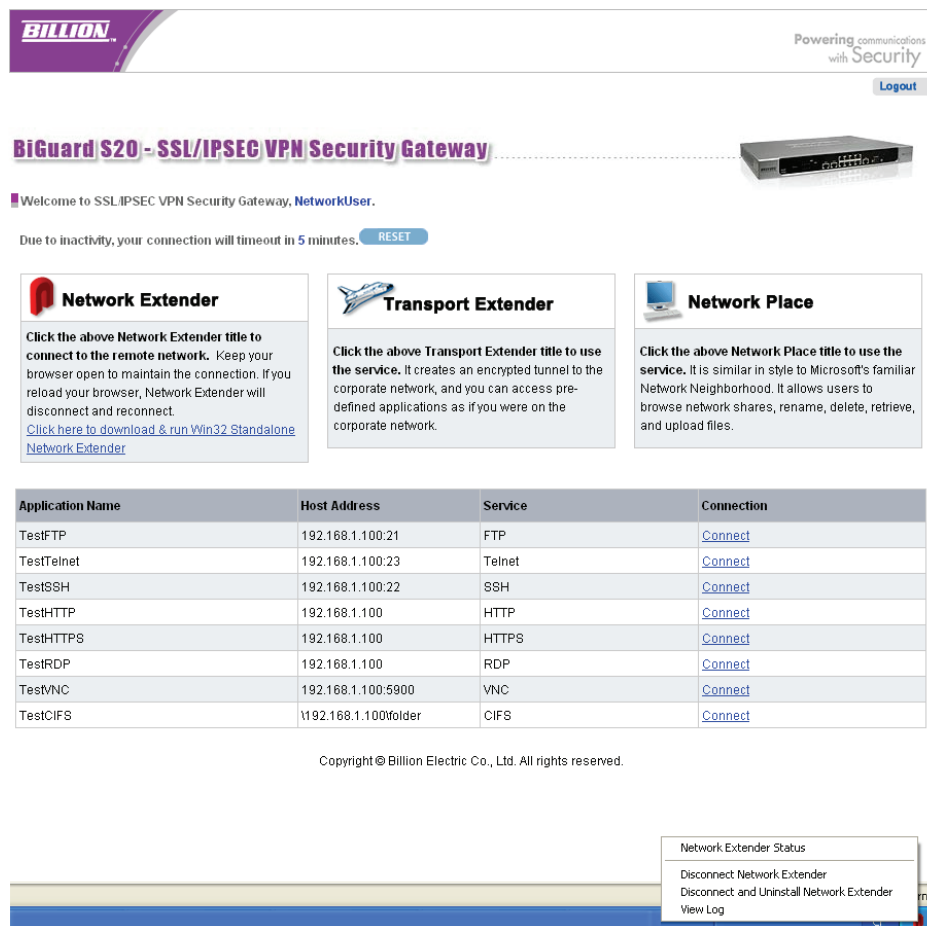
After installation is complete, the Network Extender Connection Status window displays.



- 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 remains active in the status bar.


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




**BiGuard S20 - SSL/IPSEC VPN Security Gateway**

Welcome to SSL/IPSEC VPN Security Gateway, **NetworkUser**.


Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)


**Network Extender**

Click the above Network Extender title 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.  
[Click here to download & run Win32 Standalone Network Extender](#)


**Transport Extender**

Click the above Transport Extender title 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 above Network Place title 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
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
TestHTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
TestRDP	192.168.1.100	RDP	<a href="#">Connect</a>
TestVNC	192.168.1.100:5900	VNC	<a href="#">Connect</a>
TestCIFS	\\192.168.1.100\\folder	CIFS	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

Network Extender Status

Disconnect Network Extender  
Disconnect and Uninstall Network Extender  
View Log

#### 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 remote 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 remote computers to route the IP packets to the corporate office network. For example, if the remote computer's IP packets' destination address is specified in Client Route, the IP packets will be forwarded to the PPP connection which will then pass through the BiGuard S Series via the SSL VPN tunnel to the corporate office network.



**QUESTION:** I have successfully created a Network Extender connection, but I can not 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 S Series LAN network address (192.168.1.254 by default). Alternatively, if your client address is not in the same subnet as your BiGuard S Series LAN network addresses then you have to add the LAN network address to your client route.

## 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 through SSL connection. 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 which will allow secure connections for users from home for example to securely connect into the corporate office network to access the email service.

### QUESTION: How do I setup Transport Extender?

**ANSWER:** Use the following guide to set up Transport Extender.

### How to configure Transport Extender?

1. Click **SSL VPN** → **User Access** → **Account**.
2. To create an Account, click the **Create** link at the left bottom of the Account Table. The Add Account screen appears, and you can create a user account with access to the Mail server.

**Add Account**

General Setting

User Name	NetworkUser	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Password	•••••	
Retype Password	•••••	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>

Group Setting Details

Force Login	Disable
Inactivity Timeout	5 Minutes
Network Place	Enable
Network Extender Service	Enable
Transport Extender Service	Standalone Application (Win32 Only) Enable
Web Cache Cleaner	Enable
Greeting String	Use default greeting string
Applications	TestFTP , TestTelnet , TestRDP , TestVNC , TestSSH , TestHTTP , TestHTTPS , TestCIFS

Click **Apply** to set the configurations and return to Account Table. Then click **Edit** to edit this Account.


When configuring a user account, first enable the Transport Extender service for the user.

Edit Account		
<b>General Setting</b>		
Name	NetworkUser	<input checked="" type="checkbox"/> Active
Group	BiGuard	
Group Setting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>Login Setting</b>		
Password	<input type="password"/>	
Retype Password	<input type="password"/>	<input type="checkbox"/> Use group default password
Host Checking	<input checked="" type="checkbox"/> Active	<a href="#">Advanced Setting</a>
Force Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Inactivity Timeout	5	Minutes
<b>Service</b>		
Network Place	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Network Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a> <input checked="" type="checkbox"/> Standalone Application (Win32 Only)	
Transport Extender Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Advanced Setting</a>	
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 SSL/IPSEC \	
<b>Application Proxy</b>		
Applications	<input checked="" type="checkbox"/> TestFTP	<input checked="" type="checkbox"/> TestTelnet
	<input checked="" type="checkbox"/> TestRDP	<input checked="" type="checkbox"/> TestVNC
	<input checked="" type="checkbox"/> TestSSH	<input checked="" type="checkbox"/> TestHTTP
	<input checked="" type="checkbox"/> TestHTTPS	<input checked="" type="checkbox"/> TestCIFS
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

- Click **Apply** to set the configurations and return to Account Table.

After the user account is created with the Transport Extender service enabled, setup the designated service port and the server's IP address.

- Click **Transport Extender** → **Application**.

Transport Extender				
<b>Configured Applications for Transport Extender</b>				
Local Server IP Address	Protocol	Port Number		
<a href="#">Create</a> 				

- Click **Create** to create an application profile.

Transport Extender	
Add an Application to be Tunneled by Transport Extender	
Local Server IP Address	<input type="radio"/> All IP Addresses <input checked="" type="radio"/> Fixed IP Address 192.168.1.254
Protocol	TCP ▾
Port Number	<input type="radio"/> All Ports <input checked="" type="radio"/> Fixed Port 110 ~ 110
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

---

**Local Server IP Address** Redirect All IP Addresses or the Fixed IP address only to the office network through the secure SSL VPN connection. (Default is Fixed IP Address 192.168.1.254).

**TCP Port Number** Redirect All TCP Ports or Fixed TCP Port of the specified IP Addresses to the office network through the secure SSL VPN connection. If you select the Fixed TCP Port enabled, please input the port numbers you want to redirect. (Default is Fixed TCP Port 110 ~ 110).

---

6. Click **Apply** to set the configurations.

In the Transport Extender, setup the domain name for an IP address. This allows for the access of the server's IP address by typing the domain name.

7. Click **SSL VPN → Transport Extender → Host Name Resolution**.

Transport Extender	
Configured Host Name Resolution for Transport Extender	
Local Server IP Address	Fully Qualified Domain Name
<input type="button" value="Create"/>	

8. Click **Create** to create a Host Name Resolution profile.

Transport Extender	
Add a Host Name Resolution to Transport Extender	
Local Server IP Address	<input type="text"/>
Full Qualified Domain Name	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

---

**Local Server IP Address** Input the IP address of the server.

**Full Qualified Domain Name** Input the domain name for the server's IP address.

---

9. Click **Apply** to set the configurations.

## Remote SSL VPN Portal

To use Transport Extender, connect to the web portal by first typing in the browser address bar <https://wanipaddress> (where wanipaddress is the WAN IP address of the BiGuard SSL VPN appliance). After you successfully connect to the device and successfully log in to the device, the web portal screen appears. Please click Transport Extender in order to connect to the office network. Follow the procedures below to use the Remote Portal.

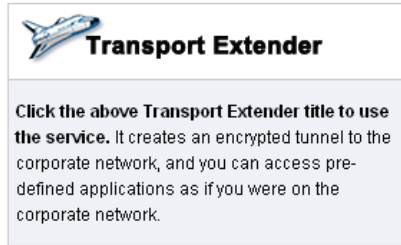
1. Type the WAN IP Address or Domain Name in the Address bar of the browser and log into the BiGuard SSL VPN remote portal as previously configured.

2. Click **Submit** to enter into the Remote Web Portal page.

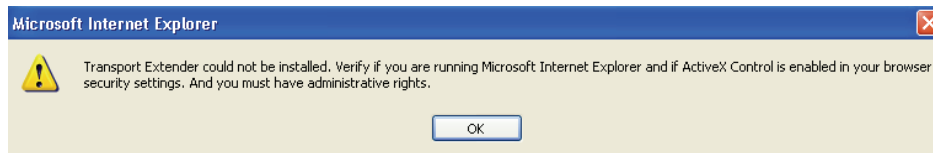
Application Name	Host Address	Service	Connection
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
TestHTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
TestRDP	192.168.1.100	RDP	<a href="#">Connect</a>
TestVNC	192.168.1.100:5900	VNC	<a href="#">Connect</a>
TestCIFS	192.168.1.100:folder	CIFS	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.

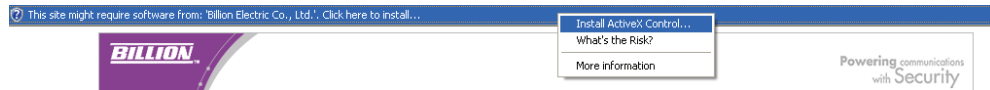
- Click **Transport Extender**



3. If the browser does not launch ActiveX automatically, a warning message appears. Click **OK** to continue. If the browser automatically installs ActiveX (the warning message does not display), then go to **Step 8**.



4. Click the **Information** bar on the top of the page and click **Install ActiveX Control**.

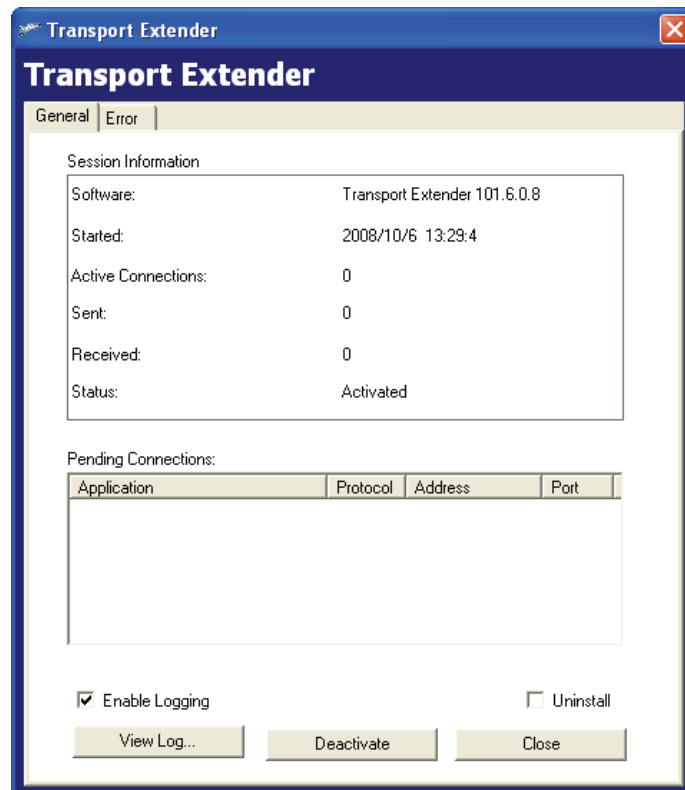


5. After the screen refreshes, click **Transport Extender** again.
6. You are required to install the **MenloLSP.cab**. Click **Install** to install the software.




7. The Transport Extender Setup proceeds.

After the installation is complete, the Transport Extender window displays.



- 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 is left un-checked, ActiveX Control will not be installed when you log on again. If the box is checked, ActiveX will uninstall when you log off to prevent unauthorized access, such as in the event that 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.



Powering communications  
with Security


Logout

BiGuard S20 - SSL/IPSEC VPN Security Gateway




Welcome to SSL/IPSEC VPN Security Gateway, **NetworkUser**.


Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)

**Network Extender**

Click the above **Network Extender** title 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.  
[Click here to download & run Win32 Standalone Network Extender](#)

**Transport Extender**

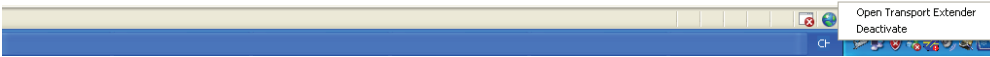
Click the above **Transport Extender** title to use the service. It creates an encrypted tunnel to the corporate network, and you can access pre-defined applications as if you were on the corporate network.

**Network Place**

Click the above **Network Place** title 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
TestFTP	192.168.1.100:21	FTP	<a href="#">Connect</a>
TestTelnet	192.168.1.100:23	Telnet	<a href="#">Connect</a>
TestSSH	192.168.1.100:22	SSH	<a href="#">Connect</a>
TestHTTP	192.168.1.100	HTTP	<a href="#">Connect</a>
TestHTTPS	192.168.1.100	HTTPS	<a href="#">Connect</a>
TestRDP	192.168.1.100	RDP	<a href="#">Connect</a>
TestVNC	192.168.1.100:5900	VNC	<a href="#">Connect</a>
TestCIFS	192.168.1.100\folder	CIFS	<a href="#">Connect</a>

Copyright © Billion Electric Co., Ltd. All rights reserved.





## Importing a certificate

Follow these instructions to import an SSL certificate.

1. Select **SSL VPN/ESSL Certificate** and click **Generate CSR**.

SSL Certificate					
Current Certificates					
Enable	Description	Status	Expiration	Password	
<input checked="" type="radio"/>	sha1WithRSAEncryption	Active	Jan 14 02:12:30 2018 GMT		

The Generate Certificate Signing Request (CSR) or Generate a New Self-signed Certificate (CRT) screen appears.

You are prompted to fill out a CSR (Certificate Signing Request) form.

SSL Certificate	
Generate Certificate Signing Request (CSR) or Generate a New Self-signed Certificate (CRT)	
Name	<input type="text"/>
Organization	<input type="text"/>
Unit/Department	<input type="text"/>
City/Locality	<input type="text"/>
State (Full Name)	<input type="text"/>
Country	<input type="text"/>
FQDN (Domain Name)	<input type="text"/>
Email	<input type="text"/>
Password	<input type="password"/>
Retype Password	<input type="password"/>
New Key Pair Length	1024 <input type="button" value="v"/>
Generate a Self-signed Certificate	<input type="checkbox"/>

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, <i>www.billion.com</i> ).
Email	Type your email address.
Password/Retype Password	Type and confirm a password.

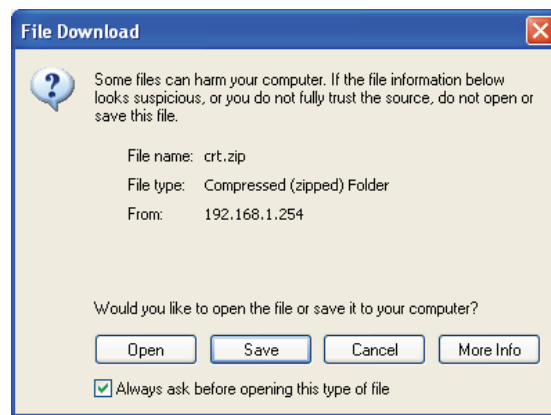
New Key Pair Length	This item refers to the strength of the key encryption for the private key (extracted from the zip file).
Generate a Selfsigned Certificate	If you do not check the check box, it will generate two files, server.csr and server.key, which you can sign a certificate by well-known certification organizations. If you check the check box, the certification is verified by yourself.



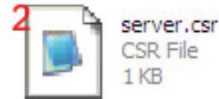
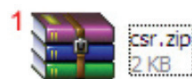
**NOTE:** The country code is a two letter International Organization for Standardization (ISO) designation.

**NOTE:** Store the password in a safe place.

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



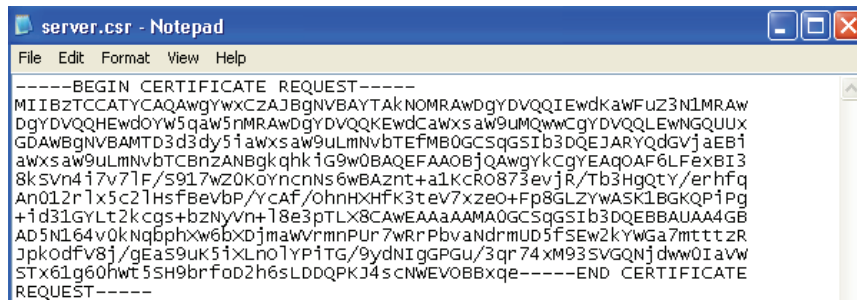
- Click **Save**. You are prompted for a download location. Save the file to your computer and extract the files to a folder.



- Downloaded csr.zip file
- Extracted server.csr file
- Extracted server.key file

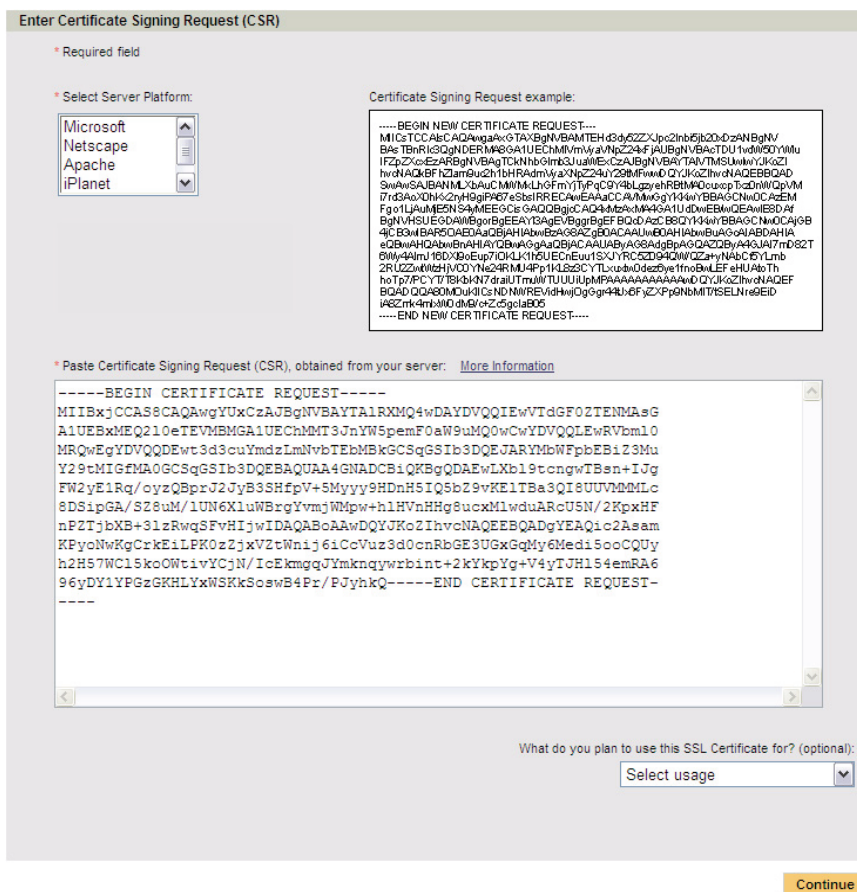
- Once extracted, you can sign a certificate (for example, Verisign - [www.verisign.com](http://www.verisign.com)).
- Follow the instructions from the web. You are prompted to input your CSR.

- Open **server.csr** with a text editor such as Windows Notepad.



```
-----BEGIN CERTIFICATE REQUEST-----
MIIBZTCCATYCAQAwgYwxCzAJBgNVBAYTAkNOMRAwDgYDVQQLIEwkaWZ3N1MRAw
DgYDVQQHEwd0Yw5qaw5nMRAwDgYDVQQKEwdCawxsaw9uMQwwCgYDVQQLLEwNGQUUx
GDAwBgNVBAMTD3d3dy51awxsaw9uLmNvbTEFMBOGCSqGSIb3DQEJARYQdGVjaEB1
awxsaw9uLmNvbTECBnZANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAQAF6LFexBI3
8kSvn4i7v7lF/S9l7wZ0K0ynchnS6wBAZnt+a1KcR0873evjR/Tb3HgQtY/erhfq
An012r1x5c21HsFBevBP/YcaF/ohnHXHFk3teV7xzeO+FP8GLZYwASK1BGKQP1Pg
+1d31GYLT2kcg+bzNyvn+18e3pTLX8CAwEAaAAMA0GCSqGSIb3DQEBAUAA4GB
AD5N164v0kNg6phxw6bxDjmaWvrnnpUR7wRrPbvAndrmUD5fSEw2kYwGa7mttZr
Jpkodfv8j/gEa59uK51XLn01YP1TG/9ydNIgPGu/3qr74xM93SVGQNJdww0IaVw
STx61g60hwt5SH9brf0d2h6sLDDQPKJ4scNWEVOBBxqe-----END CERTIFICATE
REQUEST-----
```

- Copy the CSR text and paste it in the appropriate field on the certificate provider's web-site and finish following the certificate provider's instructions for getting a certificate. The certificate provider will send you the certificate by email.



Enter Certificate Signing Request (CSR)

\* Required field

\* Select Server Platform:

Microsoft  
Netscape  
Apache  
iPlanet

Certificate Signing Request example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICsTCCATYCAQAwgYwxCzAJBgNVBAYTAkNOMRAwDgYDVQQLIEwkaWZ3N1MRAw
DgYDVQQHEwd0Yw5qaw5nMRAwDgYDVQQKEwdCawxsaw9uMQwwCgYDVQQLLEwNGQUUx
GDAwBgNVBAMTD3d3dy51awxsaw9uLmNvbTEFMBOGCSqGSIb3DQEJARYQdGVjaEB1
awxsaw9uLmNvbTECBnZANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAQAF6LFexBI3
8kSvn4i7v7lF/S9l7wZ0K0ynchnS6wBAZnt+a1KcR0873evjR/Tb3HgQtY/erhfq
An012r1x5c21HsFBevBP/YcaF/ohnHXHFk3teV7xzeO+FP8GLZYwASK1BGKQP1Pg
+1d31GYLT2kcg+bzNyvn+18e3pTLX8CAwEAaAAMA0GCSqGSIb3DQEBAUAA4GB
AD5N164v0kNg6phxw6bxDjmaWvrnnpUR7wRrPbvAndrmUD5fSEw2kYwGa7mttZr
Jpkodfv8j/gEa59uK51XLn01YP1TG/9ydNIgPGu/3qr74xM93SVGQNJdww0IaVw
STx61g60hwt5SH9brf0d2h6sLDDQPKJ4scNWEVOBBxqe-----END NEW CERTIFICATE
REQUEST-----
```

\* Paste Certificate Signing Request (CSR), obtained from your server: [More Information](#)

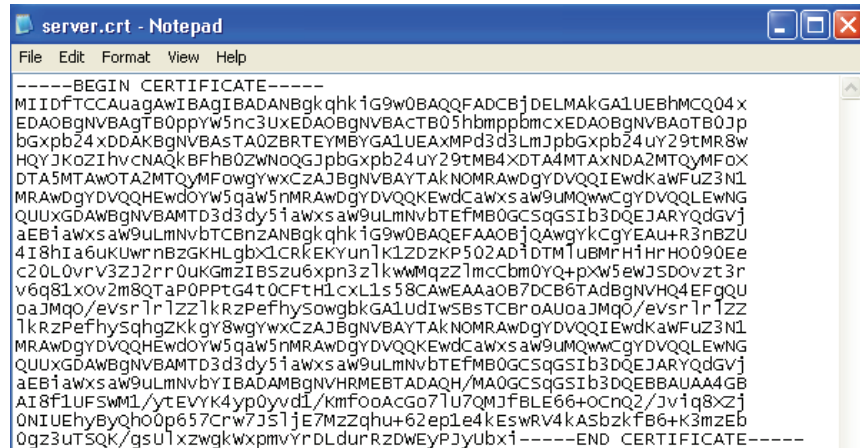
```
-----BEGIN CERTIFICATE REQUEST-----
MIIBZTCCATYCAQAwgYwxCzAJBgNVBAYTAkNOMRAwDgYDVQQLIEwkaWZ3N1MRAw
DgYDVQQHEwd0Yw5qaw5nMRAwDgYDVQQKEwdCawxsaw9uMQwwCgYDVQQLLEwNGQUUx
GDAwBgNVBAMTD3d3dy51awxsaw9uLmNvbTEFMBOGCSqGSIb3DQEJARYQdGVjaEB1
awxsaw9uLmNvbTECBnZANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAQAF6LFexBI3
8kSvn4i7v7lF/S9l7wZ0K0ynchnS6wBAZnt+a1KcR0873evjR/Tb3HgQtY/erhfq
An012r1x5c21HsFBevBP/YcaF/ohnHXHFk3teV7xzeO+FP8GLZYwASK1BGKQP1Pg
+1d31GYLT2kcg+bzNyvn+18e3pTLX8CAwEAaAAMA0GCSqGSIb3DQEBAUAA4GB
AD5N164v0kNg6phxw6bxDjmaWvrnnpUR7wRrPbvAndrmUD5fSEw2kYwGa7mttZr
Jpkodfv8j/gEa59uK51XLn01YP1TG/9ydNIgPGu/3qr74xM93SVGQNJdww0IaVw
STx61g60hwt5SH9brf0d2h6sLDDQPKJ4scNWEVOBBxqe-----END CERTIFICATE
REQUEST-----
```

What do you plan to use this SSL Certificate for? (optional):

Select usage

Continue

8. Copy the certificate text (from the email) and paste into a text editor. Save the file as **server.crt**.



9. Zip the files **server.crt** and **server.key** into a file with a **.zip** extension (ex. **server.zip**).
10. In the SSL Certificate screen, click **Import Certificate**.

SSL Certificate					
Current Certificates					
Enable	Description	Status	Expiration	Password	
<input checked="" type="radio"/>	sha1WithRSAEncryption	Active	Jan 14 02:12:30 2018 GMT		

11. 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**.

SSL Certificate	
Import Digital Certificate	
Certificate File	<input type="text"/> <input type="button" value="Browse..."/>
Upload a zip file containing "server.key" and "server.crt" files.	
<input type="button" value="Upload"/> <input type="button" value="Cancel"/>	

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

SSL Certificate					
Current Certificates					
Enable	Description	Status	Expiration	Password	
<input type="radio"/>	md5WithRSAEncryption	Non-Active	Oct 9 06:14:20 2009 GMT	<input type="button" value="Input"/>	<input type="button" value="Delete"/>
<input checked="" type="radio"/>	sha1WithRSAEncryption	Active	Jan 14 02:12:30 2018 GMT		

12. Now you must activate the imported certificate. Click **Input** to type in the password.

SSL Certificate	
<b>Input Password</b>	
Certificate Description	www.billion.com
Issuer	C=CN, ST=Jiangsu, L=Nanjing, O=Billion, OU=FAE, CN=www.billion.com/emailAddress=tech@billion.com
Subject	C=CN, ST=Jiangsu, L=Nanjing, O=Billion, OU=FAE, CN=www.billion.com/emailAddress=tech@billion.com
Serial Number	0 (0x0)
Expiration Date	Oct 9 06:14:20 2009 GMT
Password	<input type="password"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

13. In the **Password** field, type the password created when generating the CSR.
14. Click **Apply**. The certificate is ready to be used.

SSL Certificate					
<b>Current Certificates</b>					
Enable	Description	Status	Expiration	Password	
<input checked="" type="radio"/>	md5WithRSAEncryption	Active	Oct 9 06:14:20 2009 GMT	<a href="#">Input</a>	<a href="#">Delete</a>
<input type="radio"/>	sha1WithRSAEncryption	Active	Jan 14 02:12:30 2018 GMT		
<input type="button" value="Apply"/> <input type="button" value="Import Certificate"/> <input type="button" value="Generate CSR/CRT"/>					

15. Click **Enable** to enable the certificate.
16. Click **Apply** and the certificate is imported.

## Registering the BiGuard S Series

**QUESTION:** How do I register my BiGuard S Series?

**ANSWER:** Register the BiGuard S Series as follows.

1. Type the address in the IP Address field to get into the Web site and click **Join Now**. The Web site address is <http://www.biguard.com>.

2. Click **Member**.

### BiGuard User Club

Member Registration → Email Verification → Registration Complete

To access certain features of this site, you must register first. Please select a membership type to continue.

**Member**

Members have full access to the site, including all its content.

3. You will be prompted to fill in the form.

## BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

4. Select **BiGuard S Series** from the **Product Category** drop-down menu.

## BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

5. Select **BiGuard S20** from the **Product Model** drop-down menu.

### BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

6. If you without the web interface, you must also input the **Product Serial** and **MAC Address**.
7. Fill in the **Purchase Date** and **Purchase Location** and click **Next**.

### BiGuard User Club

New product registration	New product registration
Registered products	
Product registration help	

To register a new product, please fill in the form below:

Product Category \*:

Product Model \*:

Product Serial \*:  [What is this?](#)

MAC Address \*:  [What is this?](#)

Purchase Date:  -  -  yyyy-mm-dd

Purchase Location:

If you need assistance registering your product, you may look at the [product registration help](#) or contact us by clicking [here](#).

8. Fill in the fields and click **Register**.



## BiGuard User Club

Member Registration → Email Verification → Registration Complete

Please complete this form to take full advantage BiGuard product supports from Billion. Please read our [Privacy Policy](#) [here](#)

(\*) Required fields

### Account Information

Username*:	<input type="text" value="username"/>	1. Please create your user account and password with 6 to 20 characters, numbers, letters and the underscore character. The characters: !#\$%^&*~.,/:;<=>?@[\~^`{} '" are not allowed.
Password*:	<input type="password" value="••••••"/>	
Confirm Password*:	<input type="password" value="••••••"/>	2. A valid e-mail address is required. It is used to activate your account.
E-mail*:	<input type="text" value="mail@bgs.com.tw"/>	
Confirm E-mail*:	<input type="text" value="mail@bgs.com.tw"/>	

### General Information

First Name*:	<input type="text" value="First Name"/>	Last Name*:	<input type="text" value="Last Name"/>
Company Name*:	<input type="text" value="Billion"/>	Job Title*:	<input type="text" value="Job"/>
Company Address:	<input type="text" value="7F., No. 192, Sec. 2, Chung Hsing Rpad, Hsin Tein City, Taipei Hsien, Taiwan"/>		
City:	<input type="text" value="Taipei"/>		
Province / State:	<input type="text" value="Hsin Tein"/>		
Zip/Postal Code:	<input type="text" value="23146"/>		
Country*:	<input type="text" value="Taiwan"/>		
Phone Number:	<input type="text" value="02-29145665"/> (country code + area code + phone number)		
Fax Number:	<input type="text"/> (country code + area code + fax number)		
Company Website URL:	<input type="text" value="http://www.billion.com"/>		
User Organization Type*:	<input checked="" type="radio"/> Head Office <input type="radio"/> Branch Office <input type="radio"/> SOHO Office <input type="radio"/> Others <input type="text"/>		
No. of Company Employees*:	<input type="text" value="0 ~ 10"/>		
No. of MIS Personnel*:	<input type="text" value="2"/>		
Company's primary business activity*:	<input type="text" value="Technology"/>		

### Questionnaire

#### 1. Why did you choose Billion BiGuard products?\*

- ☒ Billion brand name and good reputation  
☒ Price  
☒ Product feature and specification  
☒ Recommended by friend  
☐ Recommended by local retailer   
☐ Other reason

#### 2. Where do you know about Billion?\*

- ☒ Local retailer  
☒ Billion website  
☐ Advertisement, please indicate the media name   
☐ Press release, please indicate the media name   
☒ Friends  
☐ Others, please indicate the details

#### 3. Why did you need this product?\*

- ☒ Internet access  
☒ Remote access  
☒ File and printer sharing  
☒ VPN security connection  
☒ Traffic Prioritization and Bandwidth Management  
☒ Load Balancing and Auto Failover  
☒ Firewall Security  
☒ LAN extension  
☐ Other reason

### Preferences

- ☒ Yes, I would like to be a Beta Tester  
☒ I would like to receive e-mailers regarding Billion's latest information

[Register](#)

9. The system will send a mail to the mail address you registered. Then the page will appear and request you to fill in the **Verification Code**.

### BiGuard User Club

Member Registration → **Email Verification** → Registration Complete

You are almost there. An email confirmation has been sent to the email address you entered in the previous step. In order to complete your registration, please copy and paste the verification code from your email into the input box below and click submit.

E-mail: mail@bgs.com.tw

Verification Code:

**Submit**

NOTE: the email notification may take some time before reaching your mail box depending on network traffic and your mail server. You may have to wait 5-10 minutes. If you do not receive any email confirmation within 24 hours, please contact our customer service.

10. Receive the mail and copy the **Verification Code**.

**BILLION**
Powering communications  
with Security

Dear Username:

Thank you for registering on our website. You may edit your personal information at any time on our website. Here are your user name and password. Please keep them in a safe place for future reference.

Name: Username  
Registration date: 2006-10-17

username: First Name Last Name  
password: username

*note: password is CaSe SenSiTive*

Your registration is not complete yet. We need to verify that your email is valid.  
You may complete the verification process by clicking on the link below or copying it and pasting on our browser:

**Verification Code: 18796**  
[http://www.biguard.com/reg\\_emailverify.php?sn=1&e=BGS10@mail.biguard.com&c=18796](http://www.biguard.com/reg_emailverify.php?sn=1&e=BGS10@mail.biguard.com&c=18796)

Thank you for choosing Billion products!

Biguard support team  
[www.biguard.com](http://www.biguard.com)

11. Fill in the **Verification Code** and click **Submit**.

## BiGuard User Club

Member Registration → **Email Verification** → Registration Complete

You are almost there. An email confirmation has been sent to the email address you entered in the previous step. In order to complete your registration, please copy and paste the verification code from your email into the input box below and click submit.

E-mail: mail@bgs.com.tw

Verification Code:

**Submit**

NOTE: the email notification may take some time before reaching your mail box depending on network traffic and your mail server. You may have to wait 5-10 minutes. If you do not receive any email confirmation within 24 hours, please contact our customer service.

You will be returned to the main page as shown.

## BiGuard User Club **Welcome back Username!**

### Newest downloads

Download name	Type Version	Description	Version	Download
BiGuard S10 Firmware (v3.17)	Firmware	BiGuard S10 firmware and release note	v3.17	
BiGuard S5 Firmware (v3.17)	Firmware	BiGuard S5 firmware and release note	v3.17	
BiGuard S20 Firmware (v3.17)	Firmware	BiGuard S20 firmware and release note	v3.17	

### Member news/announcements

- ▶ [2008-01-18 - BiGuard SSL VPN Tunnel Upgrades are available for BiGuard S5 and BiGuard S10](#)
- ▶ [2007-10-25 - BILLION expands its range of BiGuard IPSec VPN Security Appliances High-grade 802.11g Dual-WAN Security Gateway for SMBs - BiGuard 50G](#)
- ▶ [2007-10-08 - Billion launches Two-Factor Authentication with One-Time Password - BiGuard OTP for higher security level of remote access](#)
- ▶ [2007-05-31 - Billion to highlight SMB and Digital Home networking devices at Computex 2007](#)
- ▶ [2007-05-03 - Billion Reasons to Visit PC Range at CeBIT 2007](#)

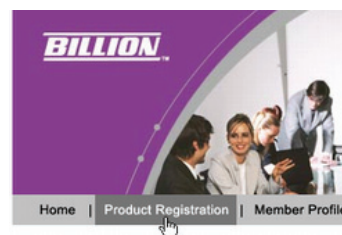
### Newest FAQ

- ▶ [Are there any restrictions when using BiGuard SSL Certificate?](#)
- ▶ [Changing the ASAS Server/Database IP ADDRESS](#)
- ▶ [Migrating ASAS to another server](#)
- ▶ [Restoring Deleted Users](#)

You have successfully registered the product.



**NOTE:** To register the BiGuard S Series without using the web configuration interface, go to [www.biguard.com](http://www.biguard.com) and click **Product Registration**.



## Configuring an Active Directory server

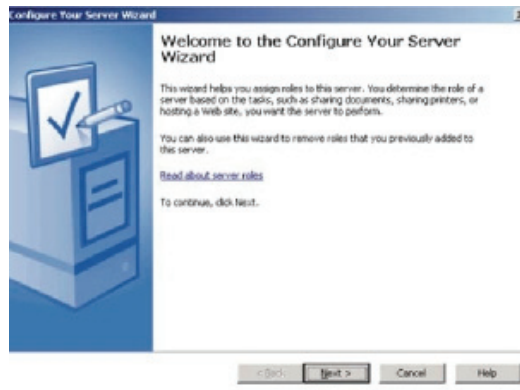
This section describes how to configure an active directory server for use with the BiGuard S Series.



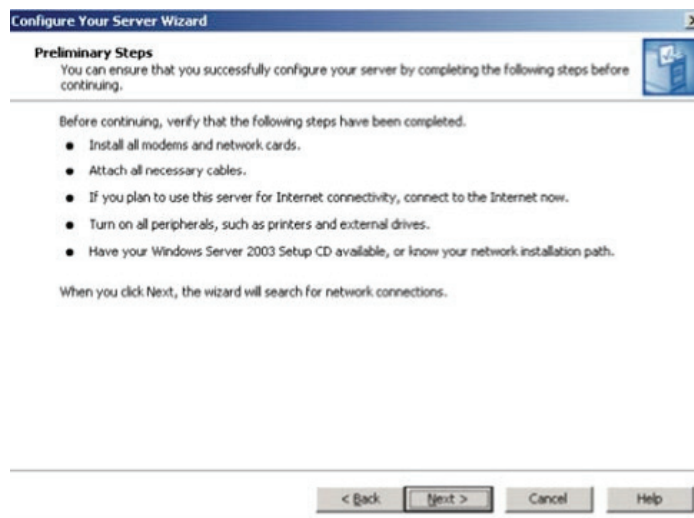
**NOTE:** Windows Server 2000 and 2003 support the Active Directory server feature.

Follow these instructions to configure an Active Directory server.

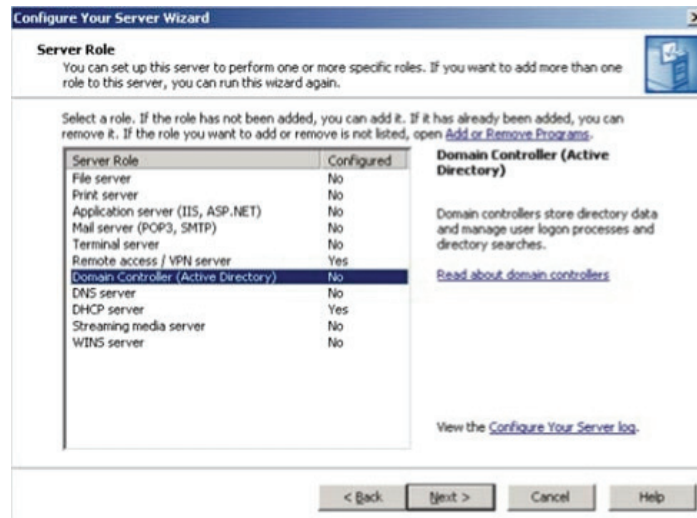
1. Click the **Start** button of your Windows PC.
2. Click **Settings**.
3. Click **Control Panel**.
4. Double-click **Administrative Tools**.
5. Click **Configure Your Server Wizard**.  
The Welcome to the Configure Your Server Wizard screen opens.



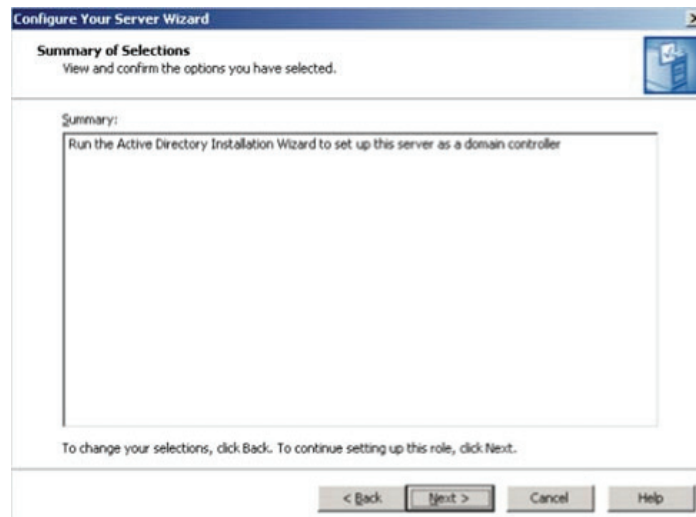
6. Click **Next**.  
The **Preliminary Screen** opens.



7. Click **Next**.  
The Server Role screen opens.

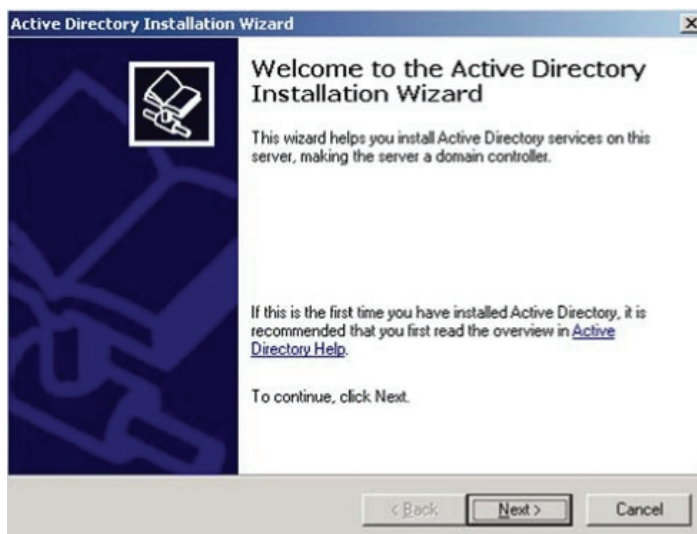


8. Select **Domain Controller (Active Directory)**, and then click **Next**.  
The Summary of Selections screen appears.



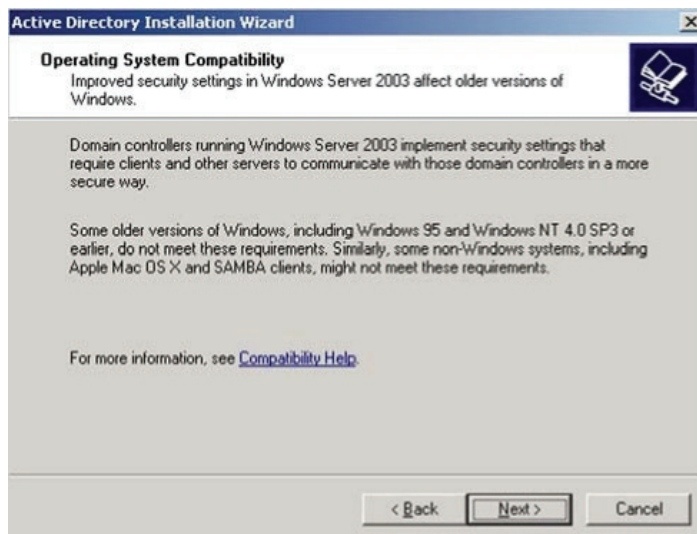
9. Click **Next**.

The Welcome to the Active Directory Installation Wizard screen appears.

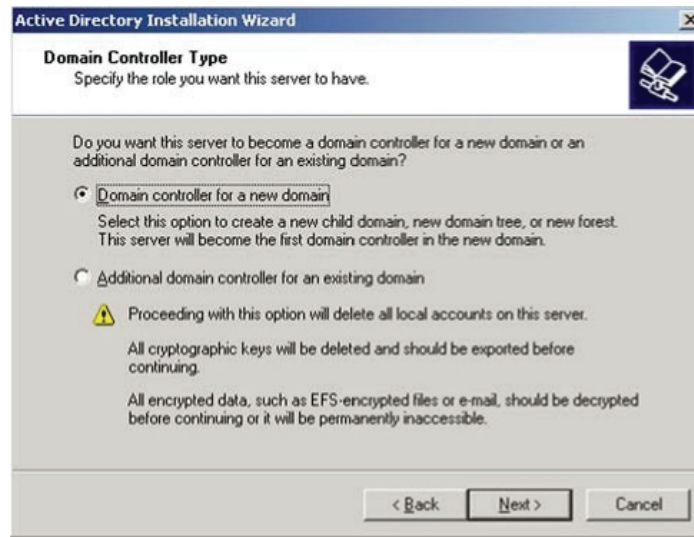


10. Click **Next**.

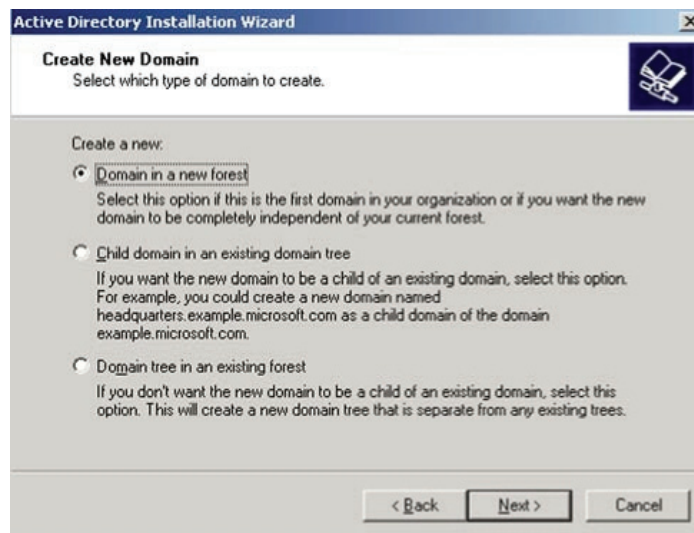
The Operating System Compatibility screen appears.



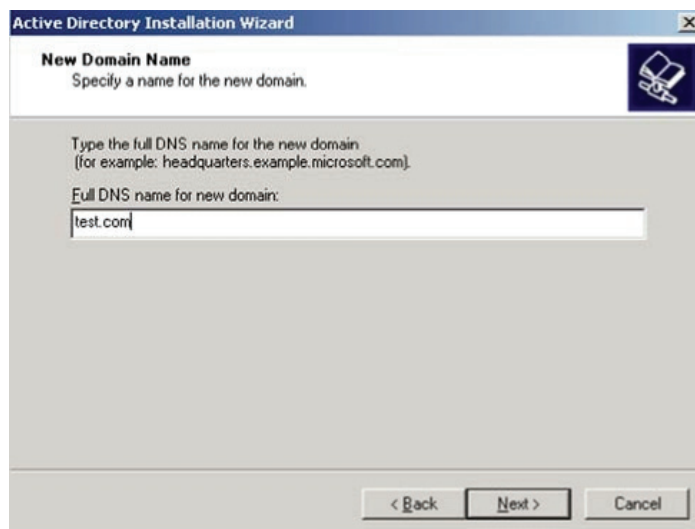
11. Click **Next**.  
The Domain Controller Type screen opens.



12. Select **Domain controller for a new domain**, and then click **Next**.  
The Create New Domain screen appears.

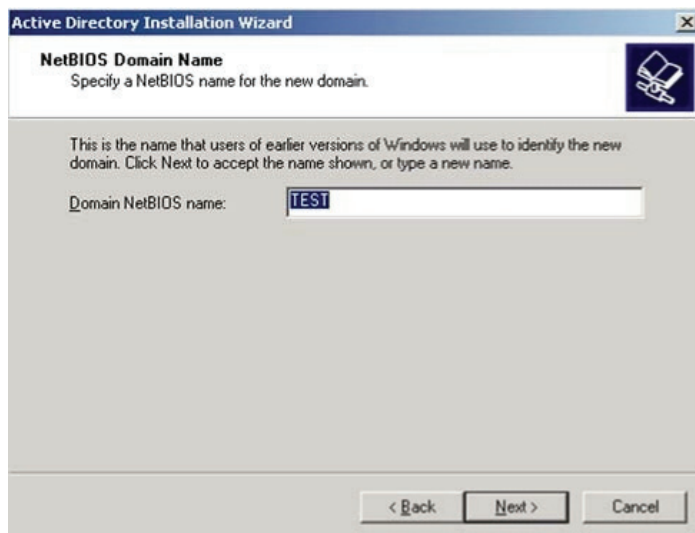


13. Select **Domain in a new forest**, and then click **Next**.  
The New Domain Name screen opens.



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'.

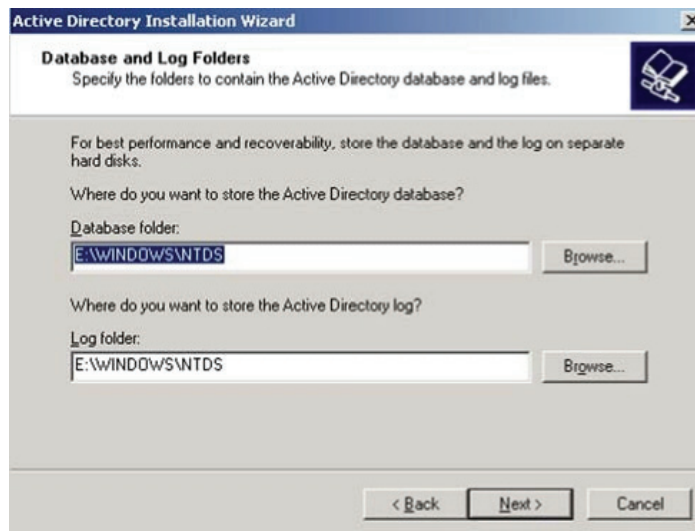
14. Enter a domain name, and then click **Next**.  
The NetBIOS Domain Name screen appears.



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'.

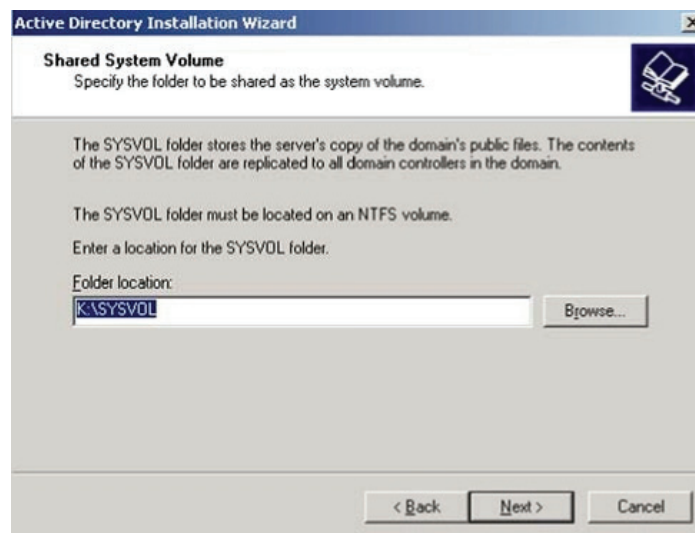


15. Enter a domain NetBIOS name, and then click **Next**.  
The Database and Log Folders screen appears.



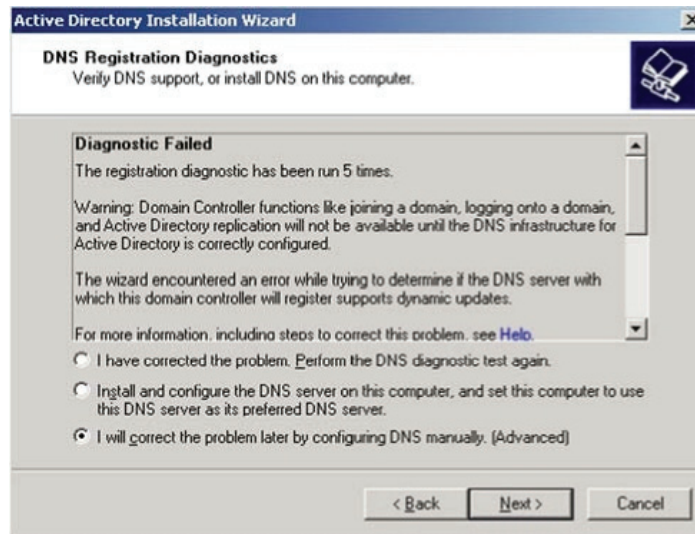
The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'Database and Log Folders' step. The title bar reads 'Active Directory Installation Wizard'. Below the title bar, the section is titled 'Database and Log Folders' with the instruction 'Specify the folders to contain the Active Directory database and log files.' A small icon of a folder with a document is on the right. The main area contains the following text: 'For best performance and recoverability, store the database and the log on separate hard disks.' followed by 'Where do you want to store the Active Directory database?'. Below this is a text box labeled 'Database folder:' containing 'E:\WINDOWS\NTDS' and a 'Browse...' button. Then, 'Where do you want to store the Active Directory log?' is followed by a text box labeled 'Log folder:' containing 'E:\WINDOWS\NTDS' and another 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

16. Select the folders that will store the Active Directory database and log. Then click **Next**.  
The Shared System Volume screen opens.

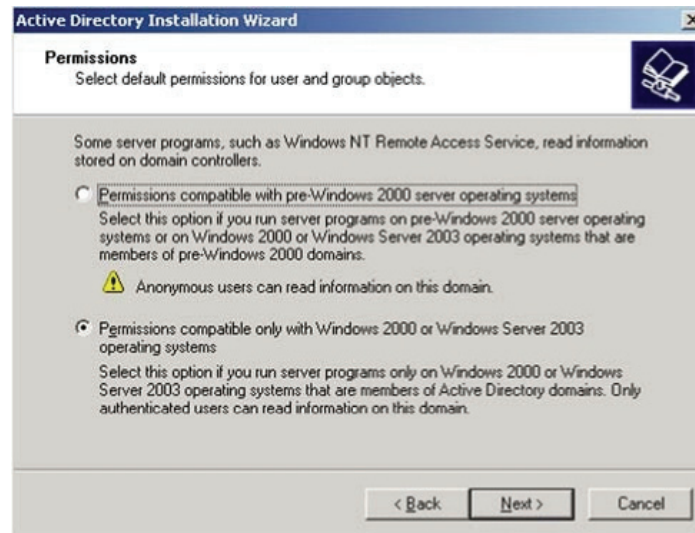


The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'Shared System Volume' step. The title bar reads 'Active Directory Installation Wizard'. Below the title bar, the section is titled 'Shared System Volume' with the instruction 'Specify the folder to be shared as the system volume.' A small icon of a folder with a document is on the right. The main area contains the following text: 'The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.' followed by 'The SYSVOL folder must be located on an NTFS volume.' and 'Enter a location for the SYSVOL folder.' Below this is a text box labeled 'Folder location:' containing 'K:\SYSVOL' and a 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

17. Enter a location for the SYSVOL folder, and then click **Next**.  
The DNS Registration Diagnostics screen appears.



18. Select **I will correct the problem later by configuring DNS manually (Advanced)**, and then click **Next**.  
The Permissions screen appears.



19. Select **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**.

20. Click **Next**.

The Directory Services Restore Mode Administrator Password screen appears.

The screenshot shows the 'Active Directory Installation Wizard' window. The title bar says 'Active Directory Installation Wizard'. The main heading is 'Directory Services Restore Mode Administrator Password'. Below the heading, it says: 'This password is used when you start the computer in Directory Services Restore Mode.' There is a small icon of a computer with a key. The main text area contains instructions: 'Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode. The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.' Below this, there are two password fields: 'Restore Mode Password:' and 'Confirm password:'. Both fields have a masked password of six dots. At the bottom, there is a link: 'For more information about Directory Services Restore Mode, see [Active Directory Help](#).' At the very bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

21. Enter your Administrator password for the Active Directory server. Then enter it again in the **Confirm password** field.

22. Click **Next**.

The Summary screen appears.

The screenshot shows the 'Active Directory Installation Wizard' window. The title bar says 'Active Directory Installation Wizard'. The main heading is 'Summary'. Below the heading, it says: 'Review and confirm the options you selected.' There is a small icon of a computer with a key. The main text area contains a list of options chosen: 'You chose to: Configure this server as the first domain controller in a new forest of domain trees. The new domain name is test.com. This is also the name of the new forest. The NetBIOS name of the domain is TEST Database folder: E:\WINDOWS\NTDS Log file folder: E:\WINDOWS\NTDS SYSVOL folder: K:\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer.' At the bottom, there is a note: 'To change an option, click Back. To begin the operation, click Next.' At the very bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

23. 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.

## Netmask

With each address class, the size of the two subdivided parts (network address and host address) is implied by the class. A netmask associated with an IP address can also express this partitioning. A netmask 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 netmask 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 netmask 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 do not 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 S Series 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 S Series, refer to [Configuring the Virtual Server](#) on page 110

## 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 S Series also functions as a DHCP client. BiGuard S Series 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 S Series 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 S Series 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 S20 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 S Series 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 S Series provides an extra level of protection from such attacks with its built-in firewall.



# Specifications

## SSL VPN

### Capabilities

- Recommended for medium-sized enterprises with 500 to 1,000 employees
- Concurrent sessions: 120,000
- Concurrent SSL VPN tunnels: up to 200, basic 50 tunnels
- Maximum throughput: 60Mbps

### Access Connection

- Network Extender (TCP/UDP)
- Application Proxy
- Standalone Network Extender client
- Personalized Web Portal
- Transport Extender (TCP/UDP)
- Single Sign-On (SSO)
- SSL hardware accelerator

### Application & Management

- My Network Places (Web CIFS)
- Web based data (HTTP, HTTPS)
- SSL event log and monitor
- AD / LDAP account import
- Citrix client
- Granular User Policy Management
- Terminal services (RDP5, RDP6)
- Supports mobile devices (Microsoft Windows Mobile 5.0/6.0 or compatible)
- File Transfer Protocol (FTP)
- Telnet
- Supports MS Outlook Web Access (OWA)
- Supports MS IIS NTLM (NT LAN Management) authentication
- Virtual Network Computing (VNC)
- Secure Shell (SSH) support

### Security

- SSL encryption
- User Access Control
- Web cache cleaner
- Authentication Domains: RADIUS, LDAP, Active Directory, NT Domain
- Local Database
- Digital Certificate

- Host Security Checking
- Self-Signed Certificate
- End Point Security (EPS)

## **Compatible Web Browsers**

- Microsoft Internet Explorer 6.0 and newer versions
- Firefox 1.5 and newer versions
- Safari 2.0 and newer versions
- Netscape 7.0 and newer versions
- Mozilla 1.7 and newer versions
- Opera 9.0 and newer versions
- Sun JRE 1.3 and newer versions

## **Supported Operating System**

- Microsoft Windows, Linux, and Apple Macintosh

## **Firewall & Content Filter**

- Stateful Packet Inspection (SPI)
- Denial of Service (DoS) prevention
- Packet Filter
- URL Filter
- Intrusion Detection
- Java Applet/Active X/Cookie Blocking

## **Quality of Service Control**

- Support DiffServ approach
- Traffic prioritization and bandwidth management based on IP protocol, port number and IP address

## **Web-Based Management**

- Easy-to-use web based user interface
- Group account settings on access applications
- Firmware upgrades through web-based interface
- Local and remote management through HTTP and HTTPS
- Multi-language web interface
- Remote dial-in configuration (RS-232) (CLI for RS-232 port)
- Supports BiGuard CMS for centralized management

## **Two-Factor Authentication**

- Event-based Algorithm Tokens
- 6-Digit Numeric LCD Display
- Dynamic One-Time Password
- Authentication Interoperability: Secure Web Access and RADIUS
- OATH Algorithm

- 5 BiGuard OTP tokens included inbox

## **IPSec VPN**

- 30 IPSec VPN tunnels
- IP Authentication Header (AH)
- Up to 200Mbps IPSec VPN throughput
- IP Encapsulating Security Payload (ESP)
- Manual key, Internet Key Exchange (IKE) authentication and Key Management
- Dynamic VPN (FQDN) support
- Supports remote access and office-to-office IPSec connections
- Authentication (MD5 / SHA-1)
- DES/3DES encryption
- AES 128/192/256 encryption

## **Availability and Resilience**

- Load balancing
  - Traffic Management
  - Protocol binding
- Automatic fail-over and VPN fail-over
- High Availability (Device Redundancy)

## **Logging and Monitoring**

- Centralized Logs
- System Log
- E-mail alert and intrusion logs
- System status monitoring

## **Network Protocols and features**

- Static IP, PPPoE and DHCP client connection to ISP
- DHCP Server
- SNTP
- NAT, static routing and RIP1/2
- SNMP
- Dynamic Domain Name System (DDNS)
- Multi-NAT
- Router Mode
- Transparent Bridging
- Virtual Server
- Port base VLAN
- Hardware DMZ

## Hardware Specifications

### Physical Interface

- 2 x 10/100/1000Mbps Gigabit WAN ports
- 8 x 10/100/1000Mbps Gigabit LAN ports  
(1 port can be configured as DMZ)
- 1 x RS232 Serial port
- 2 x USB 2.0 hosts
- RS232 console port
- Power switch
- Reset button

### Physical Specifications

- 1U rack-mount
- Processor / Flash: Multi-Core MIPS64 / 64MB
- Memory: 1GB
- Dimensions: 19" x 8.27" x 1.73"  
(482 x 210 x 44mm with bracket)  
(390 x 210 x 44mm without bracket)

### Power Requirements

- Input Voltage (Operation): 90 to 264VAC Full Range
- Input Frequency (Operation): 47 to 63Hz
- Input Current: Max. 0.95A @115Vac/60Hz at max. load
- Efficiency:  $\geq 80\%$  @115Vac/60Hz or 230Vac/50Hz at max. load
- Output power: 12V/3.5A (42W)
- Power Supply MTBF: 100,000 hours at 25°C (110Vac & 220Vac)

### Operating Environment

- Operating temperature: 0 to 40°C
- Storage temperature: -20 to 70°C
- Humidity: 20 to 95% non-condensing

### Support and Services

- InstantChat Support 5x8 Service for 180 days
- Hardware Warranty for 2 years
- Feature and Firmware Updates for 1 year

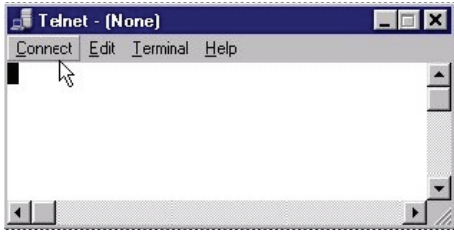
## Glossary

The following glossary of networking terms is provided for your convenience.

Term	Definition
<b>Access Point</b>	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.
<b>Authentication</b>	Authentication refers to the verification of a transmitted message's integrity.
<b>Beacon Interval</b>	Refers to the interval between packets sent by access points for the purposes of synchronizing wireless LANs.
<b>DHCP</b>	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.
<b>DMZ</b>	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.
<b>DNS</b>	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.
<b>Domain Name</b>	The domain name typically refers to an Internet site address.
<b>Dual WAN</b>	Dual Wan Routing is the balancing of physical links in which case the route are pooled or distributed in a round robin fashion.
<b>Filter</b>	Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users can not connect to those addresses.
<b>Firewall</b>	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.
<b>Firmware</b>	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.
<b>Fragmentation</b>	Refers to the breaking up of data packets during transmission.
<b>FTP</b>	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.
<b>Gateway</b>	Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information.
<b>Host Name</b>	The name given to a computer or client station that acts as a source for information on the network.

Term	Definition
<b>HTTP</b>	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> ).
<b>ICMP</b>	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).
<b>IP</b>	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.
<b>IP Address</b>	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).
<b>ISP</b>	An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.
<b>LAN</b>	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.
<b>MAC Address</b>	A MAC address is a unique serial number burned into hardware adapters, giving the adapter a unique identification.
<b>MTU</b>	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.
<b>NAT</b>	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.
<b>Network Administrator</b>	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.
<b>NTP</b>	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).
<b>Packet</b>	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.

<b>Term</b>	<b>Definition</b>
<b>Ping</b>	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.
<b>Port</b>	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.
<b>PPPoE</b>	PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet.
<b>Protocol</b>	A protocol is a rule that governs the communication of data.
<b>RIP</b>	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.
<b>RTS</b>	RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.
<b>Server</b>	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.
<b>SMTP</b>	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.
<b>SNMP</b>	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.
<b>SSID</b>	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.
<b>Subnet Mask</b>	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.
<b>SysLog Server</b>	A SysLog server monitors incoming Syslog messages and decodes the messages for logging purposes.
<b>TCP</b>	(Transmission Control Protocol) is the transport protocol in TCP/IP that ensures messages over the network are transmitted accurately and completely.
<b>TCP/IP</b>	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).

<b>Term</b> <b>Telnet</b>	<b>Definition</b> <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>
<b>UDP</b>	<p>(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).</p>
<b>Virtual Servers</b>	<p>Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).</p>
<b>WEP</b>	<p>WEP (Wired Equivalent Privacy) is the de facto security protocol for wireless LANs, providing the "equivalent" security available in hardwired networks.</p>
<b>Wireless LAN</b>	<p>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.</p>
<b>WLAN</b>	<p>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.</p>
<b>WAN</b>	<p>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).</p>



**A**

- About this guide 13
- access point 365
- Active Directory
  - configuring 347
  - setting 138
- active users
  - number logged on 43
- address groups
  - creating as Network Objects 75
  - deleting as Network objects 76
  - editing as Network objects 76
- Administration Guide 31–276
- advanced features
  - configuring 125–132
  - configuring Firewall parameters 131
  - configuring SNMP 130
  - deleting static routes 126
  - editing static route parameters 125
  - enabling Dynamic DNS 127–128
  - managing device parameters 132
- Application proxy
  - scenario 26
- Applications
  - additional 240, 248
  - CIFS 235
  - FTP
    - adding 145
  - Mail server 240
  - Mail server (Network Extender) 240
  - mail server (Transport Extender) 248
  - RDP
    - adding 145
  - SSH
    - adding 146
  - Telnet
    - adding 145
  - using 202
  - Using FTP 202
  - Using RDP5 221
  - Using Telnet 209
  - Using VNC 228
  - VNC
    - adding 145
  - Web/Web SSL
    - adding 146
- ARP 51
- authentication

- defined 365

- Authentication domain scenarios 29

**B**

- bandwidth
  - deleting bandwidth control Network Objects 87
  - editing bandwidth control Network Objects 86
  - management 86
  - setting downstream bandwidth 86
  - setting upstream bandwidth 86
- BiGuard
  - backing up and restoring configuration 120, 123
  - backing up configuration 122
  - changing device name 44
  - configuration 55–132
  - configuring the interface 55
  - configuring the LAN 55
  - registering 340
  - restoring configuration 120
  - setting the time and date 47
  - specifications 361
  - upgrading firmware 119
  - WAN configuration 62
- blocking WAN requests 30
  - enabling 131

**C**

- Certification
  - SSL VPN 27
- changing the time zone 47
- CHAP 137
- CIFS
  - configuring 235
  - create an account 236
  - remote user 238
- configuration
  - saving to flash 260
- Configuring Host Checking 164
  - configuring 164
- configuring Network Objects 72
- content blocking
  - creating domain filters 91
  - creating keyword filters 89

- deleting domain filters 92
- deleting keyword filters 90
- deleting URL features 95
- editing domain filters 91
- editing keyword filters 89
- editing URL features 94
- restricting URL features 94
- setting parameters 89

content filters

- configuring policies 109
- deleting parameters 110
- editing parameters 110
- setting IP exceptions 111
- setting parameters 109

## **D**

date

- setting the time and date 47

daylight saving

- setting 47, 117

DDNS

- enabling wildcards 128
- setting domain name 128
- setting password 129
- setting user name 128

DDNS *see* Dynamic DNS

Denial of Service *see* DoS

device

- changing name 44
- managing parameters 132

DHCP

- about 358
- configuring parameters 57, 60
- configuring server 57, 60
- configuring server settings 56
- defined 365
- disabling relay agent 57
- disabling server 57
- displaying server status 43
- mapping MAC address to fixed IP address 58
- server settings 49
- setting default lease time 58
- setting domain name 57
- setting IP range 58
- setting maximum lease time 58
- setting primary/secondary DNS address 57
- setting router as DNS server 57

- setting the server mode 56
- settings 30
- table 52

Dial-In Setup

- define 45, 133

DMZ

- defined 365
- FAQ 291
- network environment scenarios 21

DNS

- defined 365
- LAN 43
- setting primary and secondary address 57
- setting router as DNS server 57

domain

- creating filters 91
- defined 365
- deleting filters 92
- editing filters 91
- name for DDNS 128
- setting DHCP domain name 57
- Windows NT server 138

DoS

- about 359

DSCP

- configuring for QoS 102

dual WAN

- general settings 67

Dynamic DNS

- enabling 127–128

Dynamic Host Configuration Protocol *see* DHCP

## **E**

E-mail

- alerts 256

End Point Security

- 179

Environment

- network scenarios 20

environment

- operating 363

Ethernet 55

**F**

## FAQ

- adding an application proxy 317
- application proxy 317
- DMZ 291
- Firewall 291
- importing a certificate 336
- remote access 310
- remote user access 321
- SNMP 313
- SSL applications 315
- SSL knowledge 314
- Transport Extender 330

File Transfer Protocol *see* FTP

## filter

- defined 365

## Firewall

- about 359
- blocking WAN requests 30, 131
- configuring 131
- defined 359, 365
- installation behind 20
- intrusion detection 30
  - enabling 131
- settings, description 30

## firmware

- defined 365
- software version 42
- upgrading 119

## flash

- saving configuration to 260

Front and rear view 15

## FTP

- defined 365
- setting as SSL VPN application 145

**G**

## Gateway

- installation behind 20

## gateway

- defined 365
- LAN 43
- setting for static route 125

Getting Started 13–30

granular access control 27

**H**

## hardware reset

- performing 287

## Host Checking

- configuring 164
- defined 150

## host name

- defined 365

## HTTP

- defined 366

**I**

## ICMP

- defined 366

## interface

- configuring 55

Internet Control Message Protocol *see* ICMP

Internet Service Provider *see* ISP

Internet service provider *see* ISP

intrusion detection 30, 131

## IP address

- basics 357
- configuring as Network objects 72
- creating as Network objects 72
- defined 366
- deleting as Network objects 74
- determining type 277
- editing as Network objects 73
- LAN 43
- private 358
- setting for LAN 48, 55–56
- setting range in DHCP 58
- WAN 43

## ISP

- defined 366
- troubleshooting 284

## ISP connection

- bandwidth settings 65
- DHCP 62
- PPPoE 63

static IP 64

## **J**

Java

- allowing JavaScripts 281
- permissions 282

## **K**

keyword filters

- creating 89
- deleting 90
- editing 89

## **L**

LAN

- changing default IP address 48
- configuring 55
- defined 366
- DNS, displayed 43
- gateway 43
- IP address 43
- MAC Address, display 42
- setting IP address 48, 55–56
- setting RIP 48, 55–56
- setting subnet mask 48, 55–56
- subnet mask, displayed 43
- troubleshooting 280

LDAP 138

lease time

- setting default 58
- setting maximum 58

Lightweight Directory Access Protocol *see* LDAP

load balance

- outbound 68

log 256

- configuration 256
- SysLog Server 258

logging in 31

## **M**

MAC

- deleting Ethernet MAC filtering 107
- editing Ethernet MAC filtering 106
- Ethernet MAC filtering 106

MAC address

- defined 366
- mapping to fixed IP address 49, 58

Mail server

- configuration (Network Extender) 240
- configuration (Transport Extender) 248
- Network Extender 240
- Transport Extender 248

Maximum Transfer Unit *see* MTU

Monitoring configuration status 42

- status submenus 42

monitoring configuration status

- ARP table 51
- changing default LAN IP address 48
- changing the time and time zone 47
- device name, changing 44
- DHCP server settings 49
- DHCP table 52
- MAC address, mapping to fixed IP address 49
- routing table 52
- SSL user status 51
- system log 53

MSCHAP 137

MTU

- defined 366

## **N**

NAT

- defined 366

netmask

- about 357
- setting for static route 125

Network Address Translation *see* NAT

Network administrator

- defined 366

Network deployment 20

Network environment scenarios 20–24

- firewall, remote and Internet access 20

- fitting into a DMZ zone 21
- installing behind a gateway/firewall 20
- public servers on DMZ zone 22–24

#### Network Extender

- creating client routes 167, 170
- deleting client routes 168
- description 25
- editing client routes 168
- installing 190, 194
- managing client routes 167
- managing IP address 167
- modifying IP address range 167

#### Network Objects

- allowing services 78, 81
- bandwidth management 86
- configuring 72
- configuring IP address 72
- creating address groups 75
- creating IP address 72
- creating operation schedule 84
- deleting address groups 76
- deleting bandwidth control 87
- deleting IP address 74
- deleting schedules 85
- deleting service groups 82
- deleting user-defined services 79
- editing address groups 76
- editing bandwidth control 86
- editing IP address 73
- editing schedules 84
- editing service groups 81
- editing user-defined services 79
- setting content blocking 89

#### Network objects

- creating user-defined services 78, 81

#### Network Place

- description 26

Network Time Protocol *see* NTP

#### Networking

- basics 357–360

#### NTP

- defined 366

## P

#### packet

- defined 366

#### packet filters

- creating 96
- deleting profiles 96–97
- editing profiles 96

#### PAP 137

#### password

- changing the system password 122
- DDNS 129
- Web Manager 34

Password Authentication Protocol *see* CHAP

Password Authentication Protocol *see* MSCHAP

Password Authentication Protocol *see* PAP

#### ping

- defined 367

#### policies

- configuring content filtering policies 109
- configuring Ethernet MAC filtering 106
- configuring Quality of Service (QoS) 102
- configuring the virtual server 99
- deleting Ethernet MAC filtering 107
- deleting packet filtering profiles 96–97
- deleting Quality of Service (QoS) 104
- deleting virtual server 100
- editing Ethernet MAC filtering 106
- editing packet filtering profiles 96
- editing Quality of Service (QoS) 104
- editing the virtual server parameters 99
- enabling packet filtering 96
- setting parameters 96–112

#### pop-up windows

- disabling 281

#### port

- defined 367

#### Portal

- SSL VPN 28

#### portal

- layout 135

#### power

- requirement 363

#### PPPoE

- defined 367
- settings 30

#### protocol

- defined 367

**Q**

## QoS

- configuring 102
- configuring DSCP 102
- deleting 104
- editing 104

Quality of Service *see* QoS

## Quick Start 31–39

- configuring SSL VPN 39, 41
- Configuring the WAN 37
- configuring the WAN 37–40
- configuring WAN for DHCP 39
- configuring WAN for PPPoE 38
- logging in 31
- navigating the Web Manager 36

**R**

rackmounting 16

## RADIUS

- CHAP 137
- MSCHAP 137
- PAP 137

## RDP5

- adding application 147
- setting as SSL VPN application 145

read community 130

## registering

- BiGuard 42, 340

remote access 310

- enabling 118

## reset

- hardware 287
- software 288

restarting the router 36, 124

## RIP

- defined 367
- setting for LAN 48, 55–56

## router

- about 358
- defined 358

## routing

- table 52

Routing Information Protocol *see* RIP

**S**

safety information ii

## scheduling

- deleting schedules 85
- editing schedules 84
- operation 84

Secure Shell *see* SSH

## Secure Web (HTTPS)

- setting as SSL VPN application 146

## server

- Active Directory 347
- defined 367

## service groups

- deleting service groups 82
- editing service groups 81

## services

- allowing 78, 81
- creating user-defined services 78, 81
- deleting user-defined services 79
- editing user-defined services 79

## Setting up 16–18

- checking LED status 18
- connecting power 18
- connecting to a LAN 17
- connecting to a WAN 17
- rackmounting 16

Simple Mail Transfer Protocol *see* SMTP

Simple Network Management Protocol *see* SNMP

## SMTP

- defined 367

## SNMP 313

- configuring 130
- defined 367
- read/write communities 130
- versions 130

## SNTP

- server IP address, changing 47, 117

## software reset

- performing 288

## specifications 361

- hardware 363

SPI *see* SPI

## SSH

- setting as SSL VPN application 146

## SSL

- applications 315, 317, 321
- certification
  - importing certificates 174
  - managing 174–178
- FAQ 314
- user status 51

## SSL VPN

- Features 27–29
- accounts
  - creating new user 150
  - editing admin account 149
  - editing new user 152
  - managing 149
- add predefined applications 41
- Adding a domain 137
- adding applications 147
- applications overview 145
- authentication domain 137
  - scenarios 29
- configuring in the Quick Start menu 39
- configuring parameters 135–261
- configuring user access menus 135
- creating FTP application 145
- creating groups 140
- creating RDP5 application 145
- creating Secure Web (HTTPS) application 146
- creating SSH application 146
- creating Telnet application 145
- creating VNC application 145
- creating Web (HTTP) application 146
- Deleting a domain 139
- Deleting group applications 143
- Editing a domain 138
- Editing group applications 142
- Editing group parameters 141
- granular access control 27
- groups 140
- log 55
- Network Extender
  - installing 190, 194
- portal 188
  - using 188
- portal layout 135
- SSL VPN Certification 27
- SSL VPN portals 28
- terminal service (RDP5), adding 147

## SSL VPN Applications 25–26

- application proxy 26
- Network Extender 25
- Network Place 26
- Transport Extender 25

stateful packet inspection 359

Static 125, 127

static IP

- settings 30

static route

- setting destination 125, 127
- setting gateway 125
- setting netmask 125

static routes

- deleting 126
- editing parameters 125

Status submenus

- ARP information 42
- DHCP information 42
- system up time 42
- VPN status 42

subnet addressing

- about 357

subnet mask

- defined 367
- LAN 43
- setting for LAN 48, 55–56
- WAN 43

SysLog Server 258

- defined 367

system

- backing up and restoring configuration 120, 123
- backing up configuration 122
- changing passwords 122
- configuring 117–124
- enabling remote access 118
- log 53
- restarting 124
- restoring configuration 120
- setting the time zone 117
- upgrading firmware 119
- up-time 42

## T

TCP/IP

- defined 367

Telnet

- defined 368
- setting as SSL VPN application 145

time

- setting daylight saving 47, 117
- setting local time zone 47, 117
- setting resynchronization period 47, 117
- setting SNTP server IP address 47, 117
- setting the time and date 47
- setting the time zone 47, 117

time zone

- enabling 47, 117
- setting local time zone 47, 117

Transmission Control Protocol / Internet Protocol  
see TCP/IP

Transport Extender

- adding tunneled application 170
- configuring host names 172
- deleting host names 172
- deleting tunneled application 171
- description 25
- editing host names 172
- editing tunneled application 170
- FAQ 330
- managing applications 170
- managing host names 170

troubleshooting 277

- hardware 278
- ISP 284
- LAN 280
- pop-up windows
  - disabling 281
- sequence 286
- WAN 283

## U

UDP

- defined 368

unpacking 14

upgrading

- firmware 119

URL

- deleting restricting features 95
- editing restricting features 94
- restricting features 94

user access menus

- SSL VPN, configuring 135

User Datagram Protocol see UDP

User name

- Web Manager 34

user name

- DDNS 128

users

- number of users logged on 43

## V

Virtual Network Computing see VNC

virtual server

- configuring 99
- defined 368
- deleting 100
- editing parameters 99

VLAN

- configuring 71

VNC

- configuration 228
- remote user 231
- setting as SSL VPN application 145

## W

WAN

- configuring in the Quick Start menu 37
- configuring settings 62
- configuring the WAN 62
- connection status 43
- defined 368
- DHCP
  - settings 30
- IP address 43
- MAC Address, display 43
- PPPoE settings 30
- settings 30
- static IP settings 30
- subnet mask, displayed 43
- troubleshooting 283

Web (HTTP)

- setting as SSL VPN application 146

Web Manager

- logging in 31
- logging out 36
- navigating 36



- password 34
- user name 34

**Web Server**

- embedded, port number 44–45, 133

Wide Area Network *see* WAN

**wildcard**

- enabling for DDNS 128

write community 130



# Warranty

## Limited Warranty

Thank you for purchasing Billion products.

Billion Electric Co., Ltd., (hereinafter referred to as “Billion”) provides a 12-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](mailto:support@billion.com)

URL: <http://www.biguard.com>

