BiGuard S10

SSL VPN Security Gateway

Remote Portal Guide

Version Release: v101_08302006

Powering communications with Security

Declaration of Conformity

Konformitätserklärung

in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

The Manufacturer: ***Billion Electric Co., Ltd.***

Hersteller:

8F, No. 192, Sec. 2, Chung Hsing Rd.,
Hsin Tien City, Taipei Hsien
Taiwan

declares that the product: ***BiGuard S10***

erklärt, dass das Produkt:

Telecommunications terminal equipment
Telekommunikations(Tk-)endeinrichtung

Intended purpose: ***SSL VPN Security Gateway***

Verwendungszweck:

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

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

Harmonised standards: Health and Safety requirements contained in §3 (1) 1. (Article 3 (1) a))

Harmonisierte Normen: Gesundheit und Sicherheit gemäß §3 (1) 1. (Artikel 3 (1) a))

EN 60950-1: 2001+A11

Harmonised standards: Protection requirements with respect to EMC §3 (1) 2, (Article 3 (1) b))

Harmonisierte Normen: Schutzanforderungen in Bezug auf die EMV §3 (1) 2, Artikel 3 (1) b))

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

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

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

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

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

This declaration is issued by:

Diese Erklärung wird verantwortlich abgegeben durch:

Mettmann (Place) 03. Aug. 2006 (Date)

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

Gary Lin

President

Power Partnership GmbH

Copyright Information

Version 1.0, September 2006

Disclaimer

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

Trademarks

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

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

FCC Interference Statement

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

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

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Notice:

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

Safety Information

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

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

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

Table of Contents

Using SSL VPN Portal Access 1
- Installing the Network Extender 3
- Installing the Transport Extender 5
- Accessing Network Place 6
- Using Applications 6
  - *Using FTP* 7
  - *Using Telnet* 7
  - *Connecting to SSH* 8
  - *Using Web and Web SSL* 8
  - *Using RDP* 9
  - *Using VNC* 10

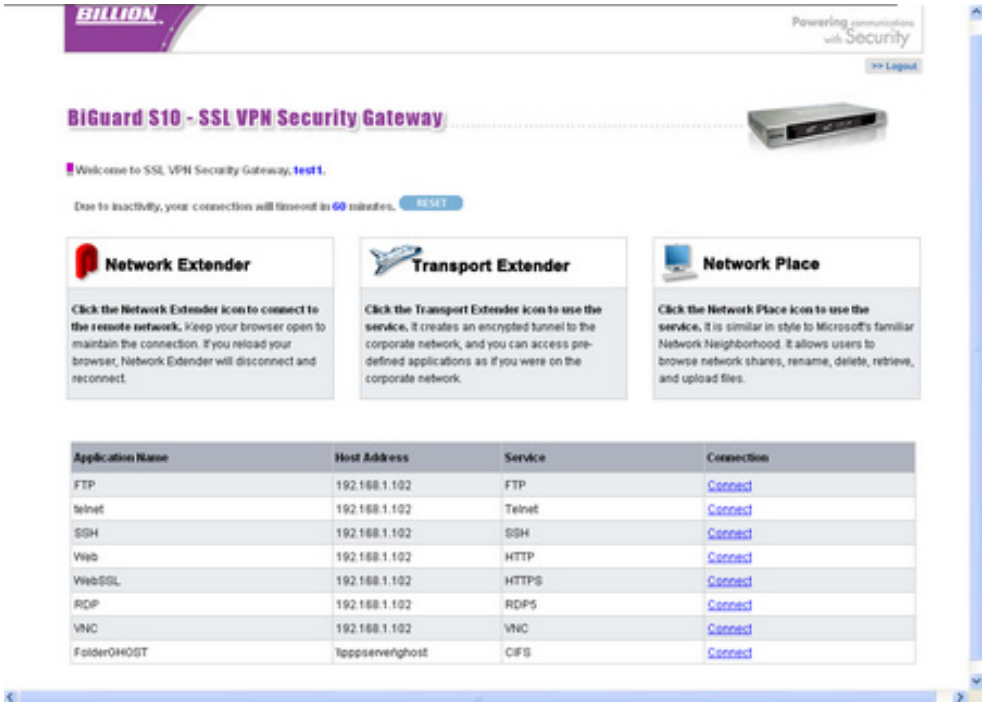
FAQ 17
- SSL Knowledge 17

Remote Portal Guide

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

Using SSL VPN Portal Access

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



Application	**Definition**
Network Extender	Browser based plug-in that simplifies clientless remote access deployments, while delivering full network connectivity for any IP-based application. See Installing the Network Extender on page 3. Click on the icon to connect to the Network Extender. Besides ActiveX control installation, no additional software is required.
Transport Extender	Browser based plug-in that allows only specified Protocol and IP addresses with SSL encryption access to pre-defined applications on the network.Click on the icon to connect to the Transport Extender.
Network Place	Click on the icon to connect to the Network Place. This application allows users to access designated network places and transfer files between them. Username and password are not required for login.

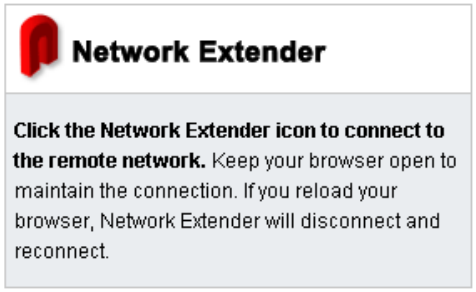
Application	**Definition**
FTP	File Transfer Protocol between network locations. No additional password or log-in required.Click on the **connect** option to easily access the File Transfer Protocol.
Telnet	JAVA based plug-in protocol for accessing remote systems. Click on **connect** and follow the on-screen instructions to complete the connection.
SSH	JAVA based plug-in interface for the secure transfer of files. Click on **connect** and follow the on-screen instructions. Username and password is required for login.
Web	Click the icon to browse to a specified web page on the intranet or Internet.
WebSSL	Click the icon to browse to a specified web page on the intranet or Internet with Secure Sockets Layering activated.
RDP	Multi-channel protocol that allows users terminal service connection to a computer. Clients exist for Windows 2003 and later versions only. Click on **connect** and follow the on-screen instructions. ActiveX plug-in must be installed for client to be established.
VNC	JAVA based plug-in protocol (Virtual Network Computing) for the remote control of another computer. Click on **connect** and follow the on-screen instructions. User authentication is required.

Installing the Network Extender

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

To create a Network Extender connection follow the instructions below:

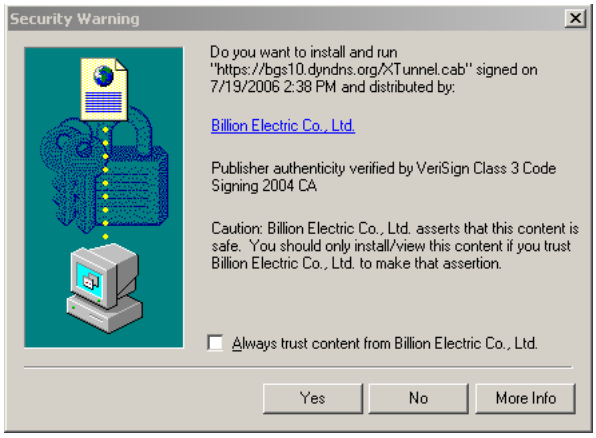
1. Click the **Network Extender** icon.



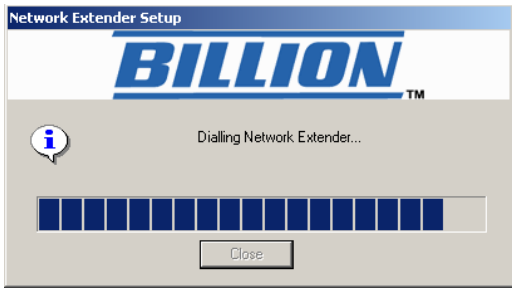
NOTE: *YOU MAY HAVE TO DISABLE POP-UP BLOCKERS TO PROCEED.*

You are prompted to install an ActiveX control.

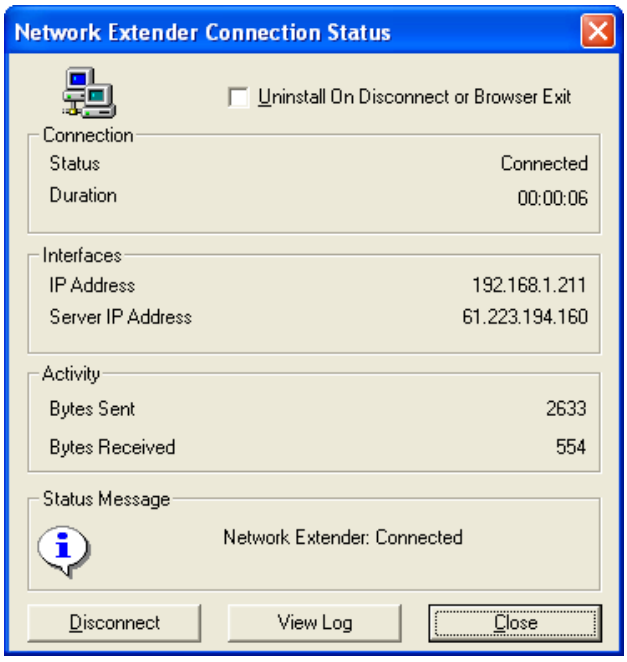
2. Click **Install ActiveX Control**.
3. You are prompted to install the adapter.
4. Click **Yes** when prompted to accept the SSLDrv Adapter.



Setup installs the adapter.

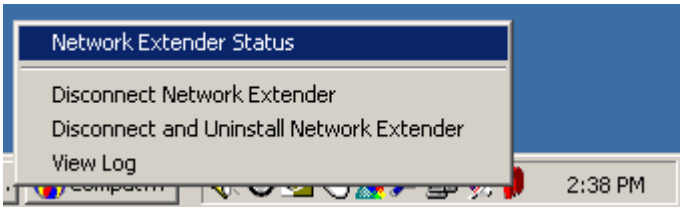


After setup is complete, an icon appears in the task bar, indicating that the Network Extender is active and the **Connection Status** screen appears.



- Check **Uninstall On Disconnect or Browser Exit** to have the system uninstall the driver every time you disconnect the Network Extender.
- Click **Disconnect** to disconnect the Network Extender.
- Click **View Log** to view a log of Network Extender processes.
- Click **Close** to close the status screen. Network Extender is still active in the status bar.

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

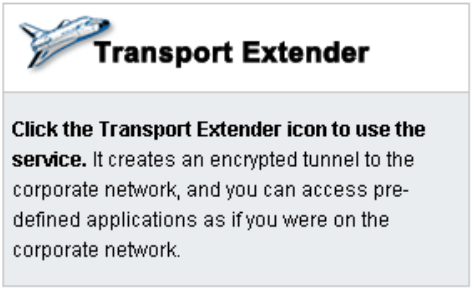


Installing the Transport Extender

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

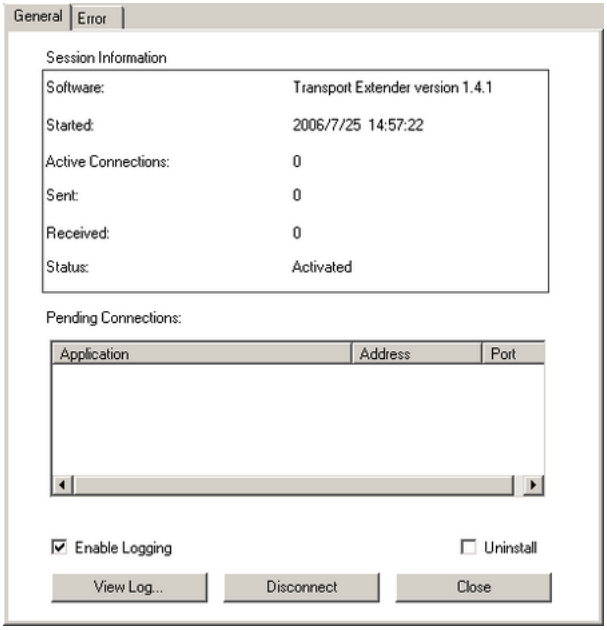
To create a Transport Extender connection follow the instructions below:

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



2. The Transport Extender installs.

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



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

- Click the **Error** tab to view a list of session errors.
- Check **Enable Logging** to allow the system to log all activity for the session.
- Click **View Log** to view a session log.
- Check **Uninstall** if you want to uninstall the driver upon disconnecting.
- Click **Disconnect** to disconnect the Transport Extender.
- Click **Close** to close the Transport Extender screen. Transport Extender is still active in the status bar.

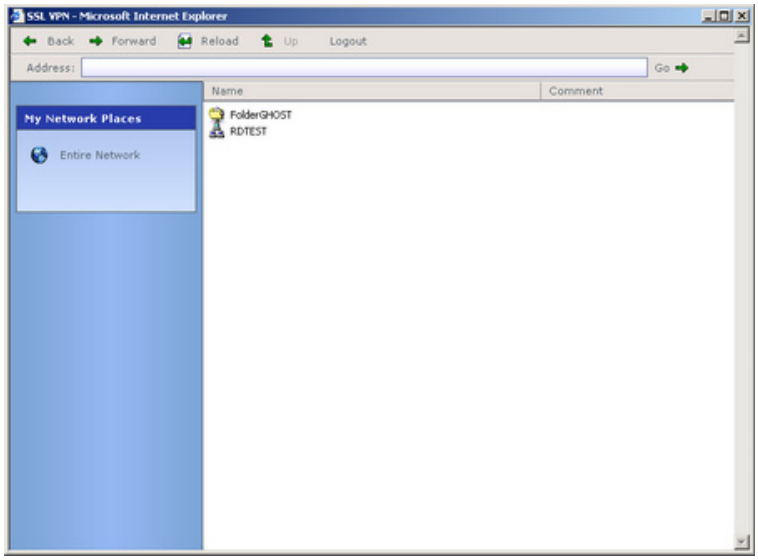
To view the Transport Extender screen again, or disconnect the Transport Extender, right-click the Transport Extender icon and select an option from the menu.

Accessing Network Place

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

Click the **Network Place** icon.

The local intranet network opens.



Use this screen to perform common file management tasks.

Using Applications

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

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

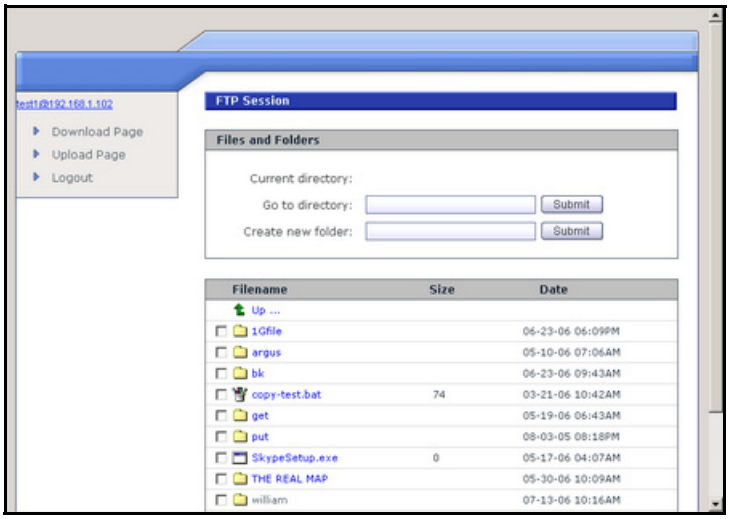
The following sections explain how to access each application.

Using FTP

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

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

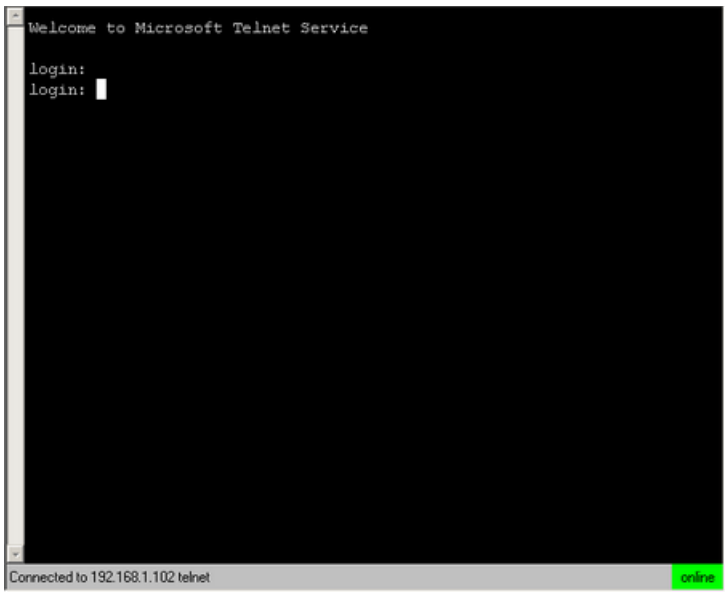
Click **Connect** in the FTP application line. The **FTP Session** screen appears.



Using Telnet

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

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



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

Commands may be abbreviated. Supported commands are:

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

Connecting to SSH

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

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

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

Using Web and Web SSL

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

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

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

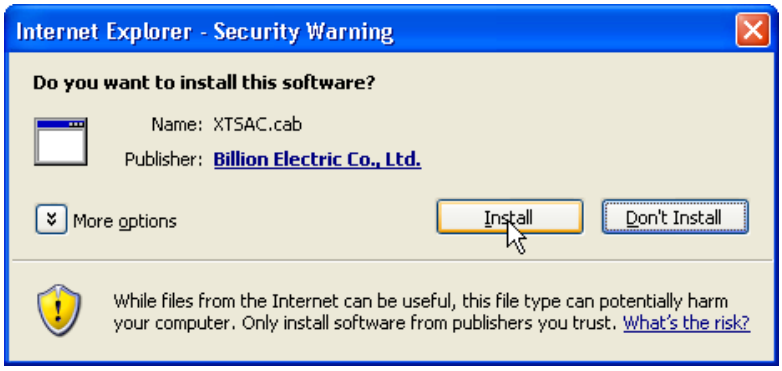
Using RDP

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

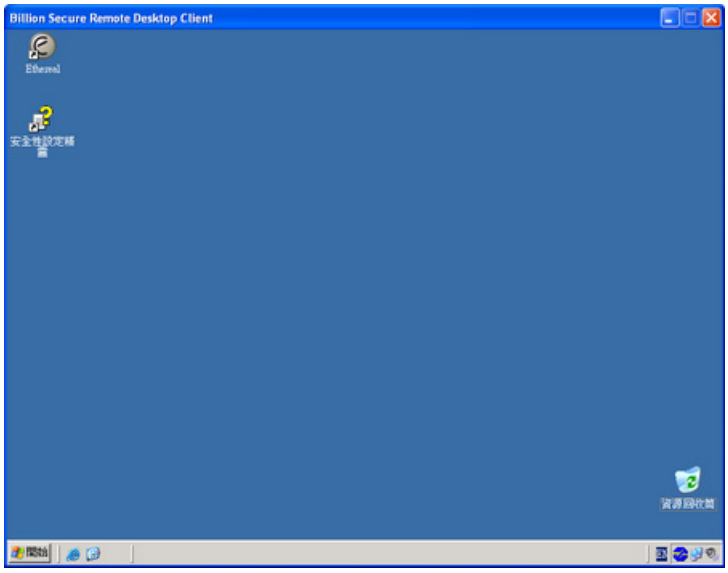
The first time you run RDP, you will be prompted to install an ActiveX component and Remote Desktop program file.

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

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



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

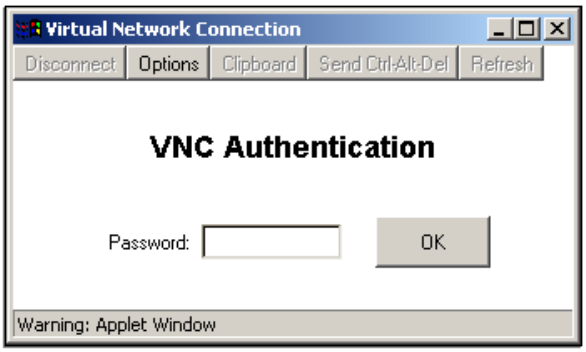


From here, you can control the remote system.

Using VNC

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

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



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

FAQ

SSL Knowledge

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

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

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

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

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

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

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

QUESTION: **What version of Java do I need?**

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

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