



BiGuard S10 SSL VPN Security Gateway

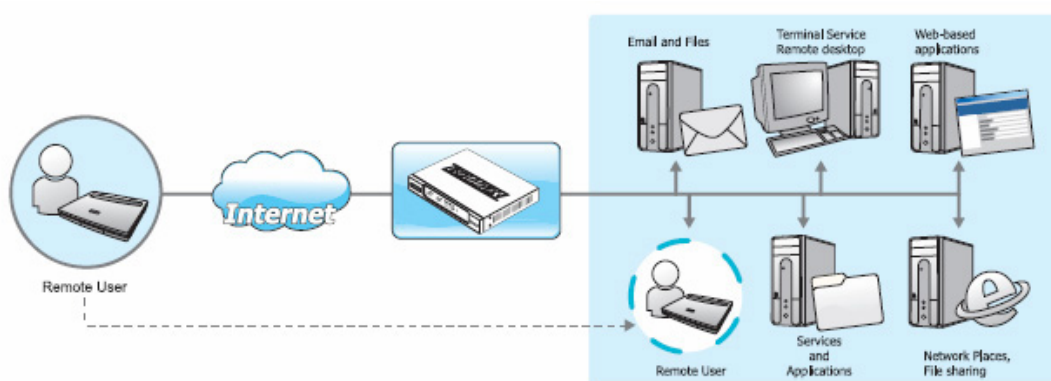
Network Extender

What is Network Extender Technology?

The Network Extender feature integrated in BiGuard SSL VPN Security Appliance is a transparent software application that allows Windows or MAC users to securely connect to their office network from a remote site through an SSL VPN connection. Network Extender Technology allows users to access their office resources seamlessly from anywhere. Users can run any application securely off the remote network. Users can upload and download files, mount network drives, and access the network resources the same way as if they were in the office. This will make the remote access secure and convenient.

For example, a sales person on a business trip overseas needs to know the product inventory back at the office. Instead of phoning back to head office and asking for the product inventory, the user can rely on Network Extender technology over a BiGuard SSL VPN gateway to connect to the corporate network and access the information needed.

Network Extender Diagram



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

Three
Solutions
in One



Benefits of Network Extender

No requirement of client installation or impact on the corporate network - Network Extender technology provides remote users with full access to the protected private network information and does not require any manual client installation. The extender client is automatically installed on the remote client PC. After installation, the Network Extender client will launch automatically and establish a secure tunnel to the office network. It will automatically turn to the un-installed state as if Network Extender was never installed on the client PC, if the user chooses, as soon as the user disconnects from Network Extender. Therefore, the information stored in corporate network is secure.

Technology inside Network Extender

The Network Extender client is a PPP over SSL connection. When the remote user connects using Network Extender, a virtual network interface will be created with IP settings dynamically assigned by a BiGuard SSL VPN device.

The Network Extender client provides a point-to-point connection and uses proxy ARP requests to locate devices on the remote network. Since it is a point-to-point connection, the addresses on the local network and remote network could be virtually in the same subnet.

How to configure Network Extender?

Step 1. Create the account with Network Extender Service **Enabled**.

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

When configuring a user account, you have to enable the Network Extender service for the user. And you have to choose to assign the IP address dynamically or to assign a fixed IP for the user.

Three Solutions in One



Step 2. Set up the Network Extender Client IP Address Range

Status	Network Extender
Quick Start	Client IP Address Assignment
Configuration	Client Address Range Begin <input type="text" value="192.168.1.210"/>
SSL VPN	Client Address Range End <input type="text" value="192.168.1.230"/>
User Access	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>
Network Extender	
Client Address	
Client Route	
Transport Extender	
SSL Certificate	
SSL VPN Portal	
Logs & E-mail Alert	
Save Config to FLASH	

When you choose to assign the IP address dynamically, you have to set up the client IP address assignment by entering Client Address Range Begin and Client Address Range End.

Step 3. Set up Network Extender Client Route

Status	Network Extender
Quick Start	Add Client Route
Configuration	Destination Address <input type="text" value="192.168.7.0"/>
SSL VPN	Destination Subnet Mask <input type="text" value="255.255.255.0"/>
User Access	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>
Network Extender	
Client Address	
Client Route	
Transport Extender	
SSL Certificate	
SSL VPN Portal	
Logs & E-mail Alert	
Save Config to FLASH	

When the client IP address and the office network address are in different subnets, 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.

Three
Solutions
in One



Supported Browsers/OS Platforms

■ Supported browsers on Windows platform

Browsers	Version suggested	Supported
Internet Explorer	>= 6.0	Yes
Firefox	>= 1.0	Future Release
Netscape	>= 7.0	Future Release
Mozilla	>= 1.7.12	Future Release
Opera	>= 8.54	Future Release

Network Extender is supported by I.E. 6.0 and above under Windows and will be supported by Firefox, Netscape, Mozilla, and Opera under Windows in the near future.

■ Supported browsers on MAC platform

Browsers	Version suggested	Supported
Safari	>= 2.0.3	Yes

Network Extender is supported by Safari 2.0.3 and above under MacOS.

Deploying Network Extender

■ Windows prerequisites

Windows system must meet the following prerequisites in order to install Transport Extender:

1. Windows XP Professional or XP Home, Windows 2000 Professional, Windows 2000 Server or Windows 2003 Server.
2. Internet Explorer 6.0 or above.
3. The user must be logged onto the PC with administrative privileges.
4. Downloading and running scripted ActiveX must be enabled on I.E.
5. We recommend you install the certificate from a trusted root Certificate Authority in the device configuration. This will prevent the security warning message when the user connects to the device from the remote computer.
6. By default, the system uses a self-signed SSL certificates for HTTPS authentication. When user connects to the device, Windows will display warning messages to indicate that the connected web site is not a trusted site. To prevent the warning messages in the future, you can import the self-signed Certificate by clicking **Import Certificate** in the *View Certificate* page.

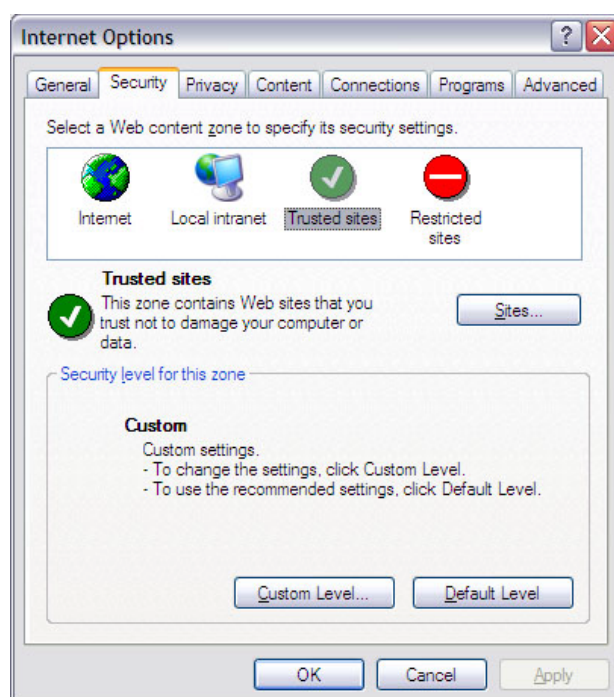
Three
Solutions
in One



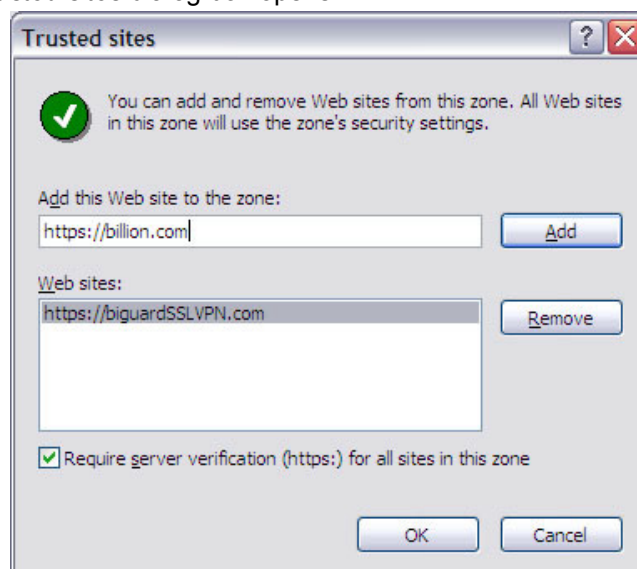
■ Internet Explorer prerequisites

To reduce the number of security warnings, we recommend that you add the URL or domain name of the BiGuard SSL VPN WAN port to Internet Explorer's trusted sites. To add a site to Internet Explorer's trusted sites, please perform the following steps:

1. In Internet Explorer, go to **Tools** → **Internet Options**.
2. Click on the **Security** tab.
3. Click on the **Trusted Sites** icon and click on the **Sites**.



4. The *Trusted sites* dialog box opens.



Three
Solutions
in One



5. Enter the URL or domain name of your SSL VPN's WAN port in the *Add this Web site to the zone* field and click **Add**.
6. Click **OK** in the *Trusted Sites* and *Internet Options* dialog boxes.

Remote SSL VPN Portal

BiGuard S10 - SSL VPN Security Gateway

Welcome to SSL VPN Security Gateway, **admin**.

Due to inactivity, your connection will timeout in 5 minutes. [RESET](#)

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

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

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

Application Name	Host Address	Service	Connection
There is no Application Proxy for use now.			

Step 1: Click Network Extender

Network Extender

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

To use Web Portal Network Extender, you have to connect to the web portal first by connecting to the device by entering `https://wanipaddress`, where `wanipaddress` is the WAN IP address of the BiGuard SSL VPN appliance. After you have successfully connected to the device and successfully logged onto the device, the web portal screen will appear.

Please click Network Extender in order to connect to the office network. The following steps need to be completed.

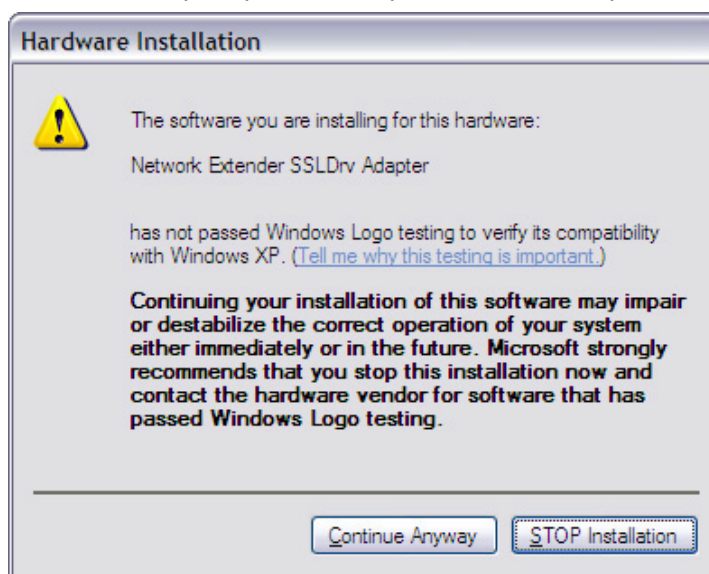
Three
Solutions
in One



Step 2: Click **Install ActiveX Control**

Step 3: You are prompted to install the adapter.

Step 4: Click **Yes** when prompted to accept the SSLDrv Adapter.



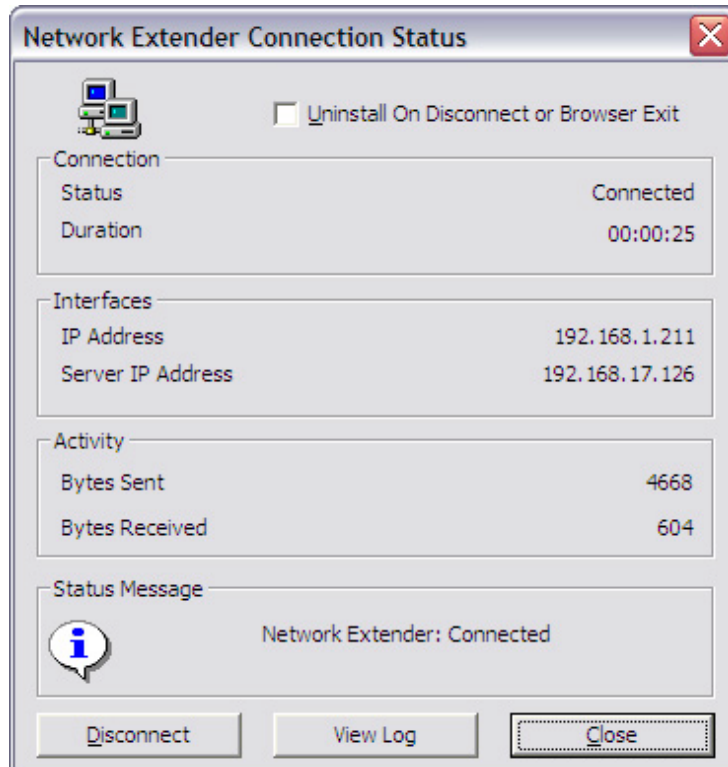
Install Proceeding



Three
Solutions
in One



Install Complete



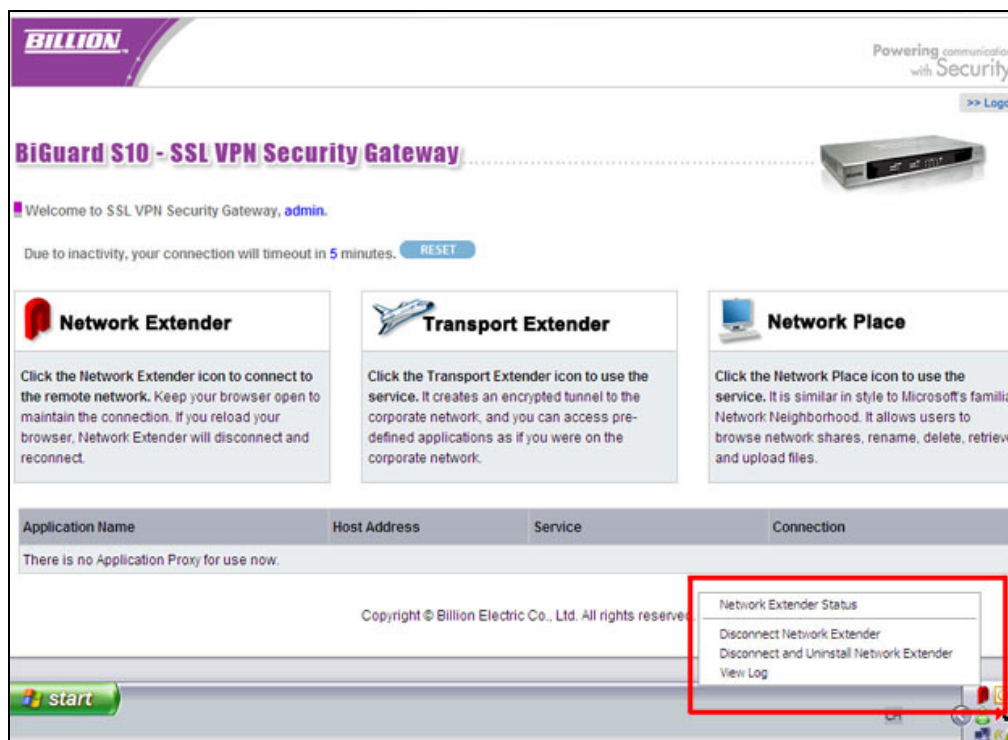
- ✓ Check **Uninstall On Disconnect or Browser Exit** to have the system uninstall the driver every time you disconnect the Network Extender.
- ✓ Click **Disconnect** to disconnect the Network Extender.
- ✓ Click **View Log** to view a log of Network Extender processes.
- ✓ Click **Close** to close the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

Three Solutions in One



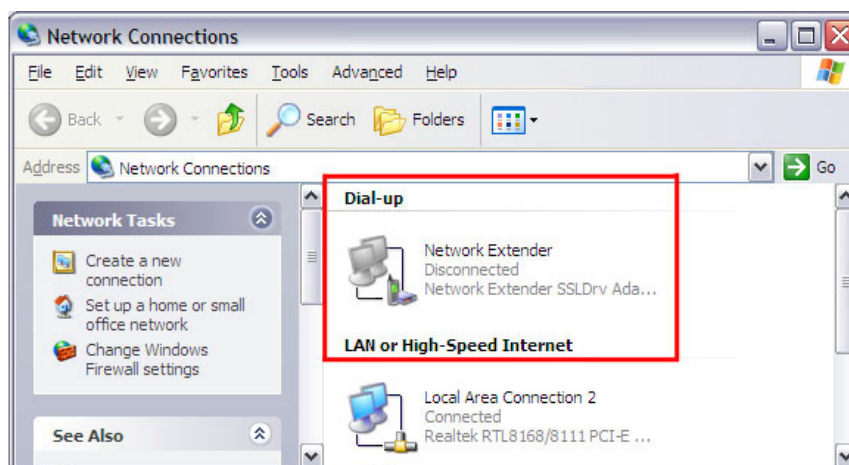
View Network Extender Status

Right-click the **Network Extender** icon, and select an option from the menu in order to view the status screen again, or perform one of the actions above.



After Successful Installation

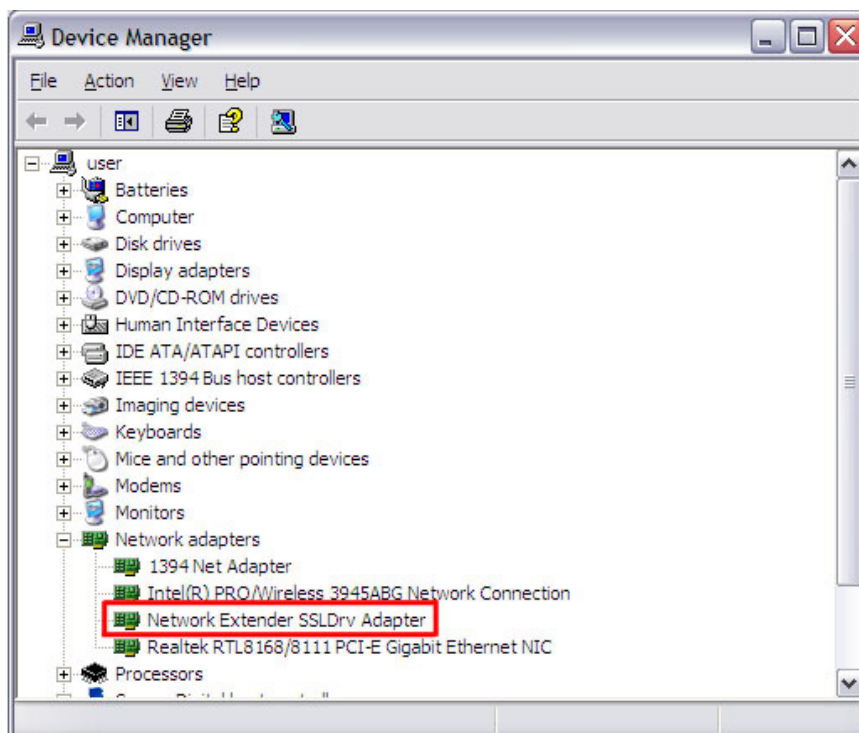
The **Network Extender** connection will appear in *Network Connections* (**Control Panel**→**Network Connections**) as shown below.



You can also view the status and disconnect the Network Extender here.

Three
Solutions
in One

The Network Extender SSLDrv Adapter you downloaded will appear in *Network adapters* in the *Device Manager* (**Control Panel**→**System**→**Hardware**→**Device Manager**) as shown below.



###

© Billion Electric Co., Ltd. All rights reserved.

BiGuard user registration: www.biguard.com

Technical support: biguardsupport@billion.com

E-mail: sales@billion.com marketing@billion.com

www.billion.com

BiGuard S10

Technical Note – Network Extender