

**Technical Note**

## BiGuard S10 SSL VPN Security Gateway

### Digital Certificate

#### Introduction

BiGuard SSL (Secure Socket Layer) VPN (Virtual Private Network) features a pre-installed self-signed X.509 certificate, which provides the same function as a certificate proved by a well-known Certificate Authority. This self-signed certificate will not be a trusted certificate acknowledged by users' computers. If users do not import the certificate to their computers, when attempting to connect to BiGuard SSL VPN appliances, an *Untrusted root CA certificate* warning will be displayed until the self-signed certificate is installed in the computer. Therefore, in order to activate SSL VPN applications, it is suggested to import the self-signed certificate that BiGuard SSL VPN appliances provide.

Simply clicking **Install Certificate** in *View Certificate* will perform the import process for the self-signed X.509 certificate, which will install the certificate onto the computer.

#### Drawbacks of Pre-Installed Self-signed X.509 Certificates

Generally, users tend to click **No** or **Cancel** when receiving security pop-up warning messages and this will create support hassles for both administrators and users. Billion recommends that the administrator applies for a company certificate from a well-known CA like Verisign.

In the next section, we will demonstrate how to install a certificate from a well-known CA to BiGuard SSL VPN appliances.

#### Install a Self-owned Certificate

This session describes how to enable, import, and apply SSL certificates. Please follow the instructions to import an SSL certificate.

#### Import a certificate

**Step 1:** Click **SSL Certificate** in *SSL VPN* to view the following screen.

Three Solutions in One



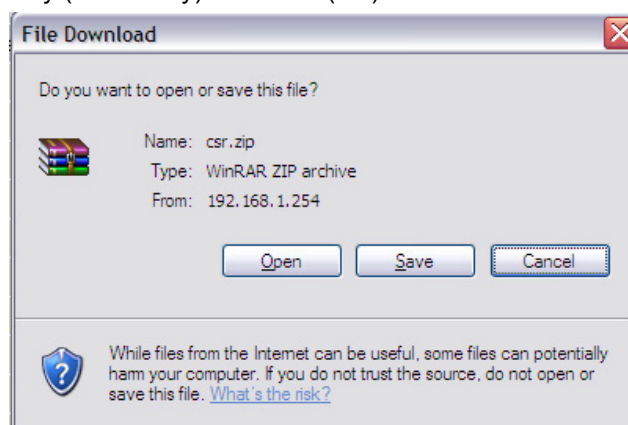
SSL Certificate					
Current Certificates					
Enable	Description	Status	Expiration	Password	
<input checked="" type="radio"/>	md5WithRSAEncryption	Active	May 20 11:27:09 2006 GMT		

You will see the default self-signed SSL certificate in the device.

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

SSL Certificate	
Generate Certificate Signing Request (CSR)	
Name	<input type="text" value="Name"/>
Organization	<input type="text" value="Org"/>
Unit/Department	<input type="text" value="Unit"/>
City/Locality	<input type="text" value="City"/>
State (Full Name)	<input type="text" value="State"/>
Country	<input type="text" value="TW"/>
FQDN (Domain Name)	<input type="text" value="www.bgs.com"/>
Email	<input type="text" value="mail@bgs.com"/>
Password	<input type="password" value="*****"/>
New Key Pair Length	<input type="text" value="1024"/>

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



Three Solutions in One



**Step 4:** Click **Save**. You are prompted for a download location. Save the file to your computer and extract the files to a folder.

**Step 5:** Next you can sign the certificate (for example from Verisign – [www.verisign.com](http://www.verisign.com))

The screenshot shows the VeriSign website with a navigation bar at the top containing 'US Home', 'Worldwide Sites', and 'Site Map'. Below the navigation bar are several sections: 'Products & Services', 'Solutions', 'Support', 'About VeriSign', and 'Existing Customers'. A central banner reads 'VeriSign innovators at work.' with a sub-headline 'VeriSign innovators are hard at work, transforming the way people work, play, and live.' To the right of this banner are buttons for 'Buy & Renew Now' with sub-options: 'BUY SSL Certificates', 'BUY Payments', 'TRY Free SSL Trial', and 'RENEW Renew Now'. Further right is a 'Success Story' section titled 'Open for Business' featuring a woman and the text 'Orvis.com uses VeriSign to strengthen security, consumer confidence, and sales.' Below the banner are three columns of services: 'Information Services', 'Communications Services', and 'Security Services'. At the bottom of the page, there are sections for 'News and Events', 'Learn About', and 'Resources For'. The footer contains contact information and copyright details for 1995-2008 VeriSign, Inc.

**Step 6:** Follow the instructions from the web. You will be prompted to enter your CSR.

**Step 7:** Open your CSR with a plain text editor such as Windows Notepad.

The screenshot shows a Notepad window titled 'server.csr - Notepad'. The text inside is a Certificate Signing Request (CSR) in PEM format. It starts with '-----BEGIN CERTIFICATE REQUEST-----' and ends with '-----END CERTIFICATE REQUEST-----'. The body of the CSR is a long string of base64-encoded text. The status bar at the bottom of the Notepad window indicates 'Ln 12, Col 1'.

**Warning!** Do not use WordPad or Microsoft Word.

Three  
Solutions  
in One



**Step 8:** 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.

**Step 9:** Copy the certificate text and paste into a text editor. Save the file as "**server.crt**".

**Step 10:** Zip the files **server.crt** and **server.key** into a file with **.zip** extension (for example, "server.zip")

**Step 11:** In the *SSL Certificate* screen, click **Import Certificate**. The following screen appears.

**Step 12:** Click **Browse** and go to the location of the zipped file. When the file is listed in the *Certificate File* text box, click **Upload**.

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

Enable	Description	Status	Expiration	Password	Delete
<input type="checkbox"/>	sha1WithRSAEncryption	Non-Active	Sep 15 23:59:59 2006 GMT	Input	Delete
<input checked="" type="checkbox"/>	md5WithRSAEncryption	Active	May 20 11:27:09 2006 GMT		

**Step 13:** Now you must activate the imported certificate. Click **Input** to enter the password.

Three  
Solutions  
in One



**Step 14:** In the **password** text box, type the password that you created when generating the CSR.

**Step 15:** Click **Apply**. The certificate is ready to be used.

**Step 16:** Click **Enable** to enable the certificate.

SSL Certificate					
Current Certificates					
Enable	Description	Status	Expiration	Password	
<input checked="" type="radio"/>	sha1WithRSAEncryption	Active	Sep 15 23:59:59 2006 GMT	<input type="text" value="Input"/>	<input type="button" value="Delete"/>
<input type="radio"/>	md5WithRSAEncryption	Active	May 20 11:27:09 2006 GMT		

###

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

BiGuard user registration: [www.biguard.com](http://www.biguard.com)

Technical Support: [biguardsupport@billion.com](mailto:biguardsupport@billion.com)

E-mail: [sales@billion.com](mailto:sales@billion.com) [marketing@billion.com](mailto:marketing@billion.com)

[www.billion.com](http://www.billion.com)

BiGuard S10

Technical Note – Digital Certificate