Installing an SSL Certificate Provided by a Certificate Authority (CA) on the BlueSecure Controller (BSC)

Date: July 2, 2010
Revision: 2.0

Introduction

This document explains how to install an SSL Certificate provided by a Certificate Authority (CA) such as VeriSign or Godaddy on the BlueSecure Controller (BSC).

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to add a new host (A) record and an associated pointer (PTR) record to your organizations DNS server.

Components Used

The information in this document is based on these hardware and software versions:

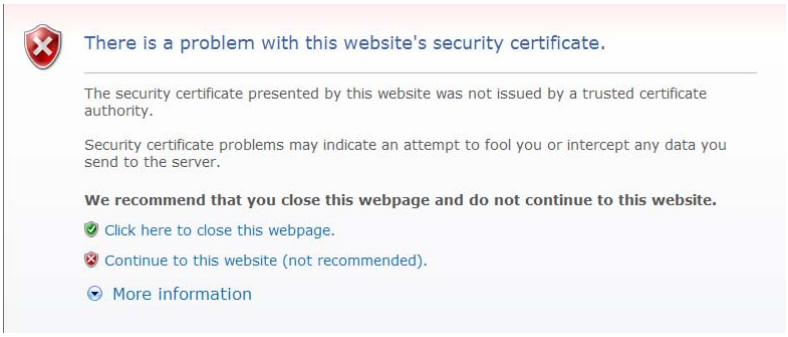
- All supported hardware platforms running current software image/patches. Current software image/patches and release notes available at support.bluesocket.com for download.

Background Information

By default the BSC uses a pre-installed self-signed SSL certificate to encrypt login transactions. The BSC uses this SSL certificate when:

- Clients connect to the secure user login page which uses http over SSL (HTTPS).
- Administrators connect to the secure web based administrative console which also uses HTTP over SSL (HTTPS).

In either case, when using the default Bluesocket self-signed SSL certificate the user may receive a certificate error from the browser indicating the certificate was not issued by a trusted certificate authority. This is because the Bluesocket self-signed certificate is not in the browsers list of trusted root certificate authorities. Below is an example of what the error will look like when using Microsoft Internet Explorer 7 (IE7).



There are two ways to stop the generation of this web browser certificate error.

- Use the default Bluesocket self-signed certificate on the BSC and install the Bluesocket self-signed certificate on the client in the browser's list of trusted root certificate authorities.
- Install an SSL Certificate Provided by a CA such as VeriSign on the BSC that is already in the client's list of trusted root certificate authorities.

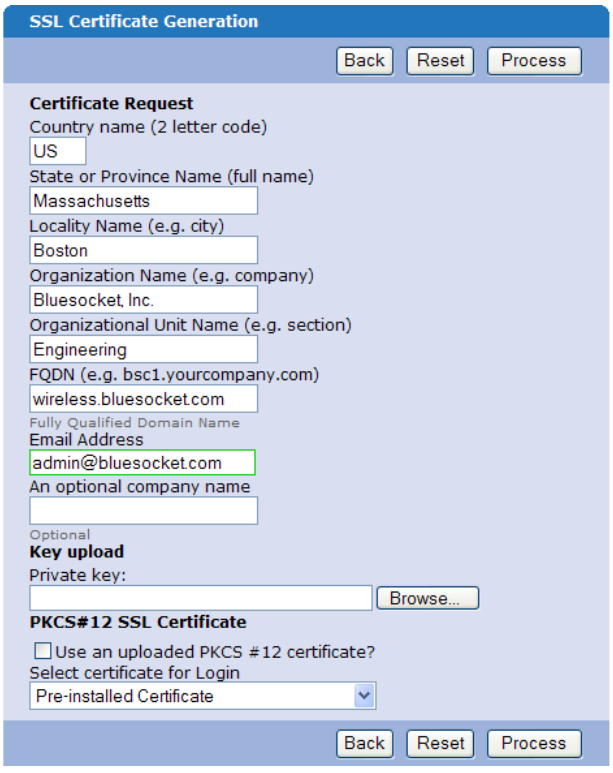
This document explains the second method of how to install an SSL Certificate Provided by a CA on the BSC.

These are the steps to follow:

1. Generate a CSR
2. Backup your private key
3. Submit the CSR to the CA
4. Retrieve the certificate that the CA Produces
5. Upload the certificate to the BSC
6. Add a new host (A) record and an associated pointer (PTR) record to your organizations DNS server
7. Enable redirect to hostname on the BSC
8. Reboot the BSC

1. Generating a Certificate Signing Request (CSR) on the BSC

- Go to Web Logins>SSL Certificate>Current>Fill out the Certificate Request form>click Process to create the CSR.

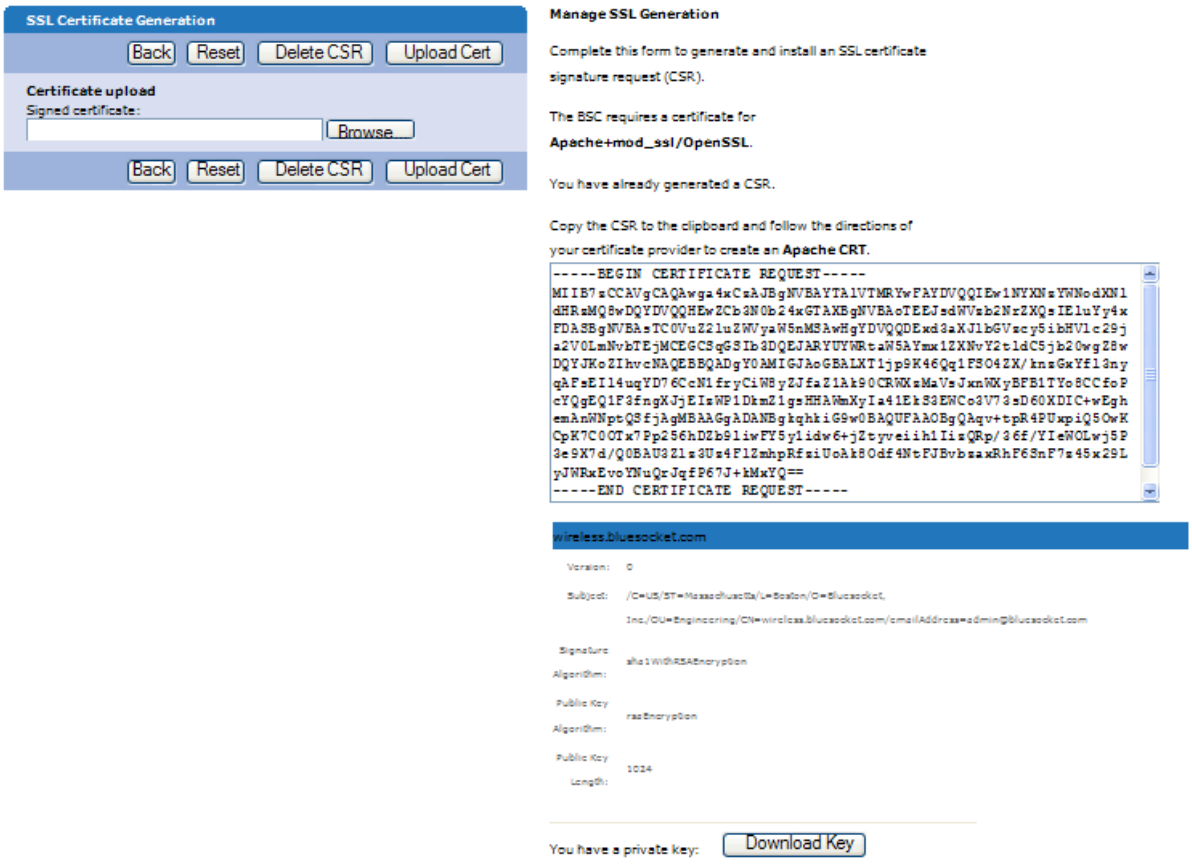


- **Country Name**: Use the two-letter code without punctuation for country, for example: US or CA.
- **State or Province**: Spell out the state completely; do not abbreviate the state or province name, for example: Massachusetts
- **Locality Name**: The Locality field is the city or town name, for example: Boston.
- **Company**: If your company or department has an &, @, or any other symbol using the shift key in its name, It is recommended you spell out the symbol or omit it. Example: Bluesocket, Inc.
- **Organizational Unit:** This field can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request.
- **FQDN (Fully Qualified Domain name):** This is equal to the **Common Name.** The Common Name is the Host + Domain Name. For example if the hostname of

the BSC is wireless (Network>Protected>Hostname) and your domain name is Bluesocket.com. You should enter wireless.bluesocket.com.

- **Email Address:** Enter the email address of the administrator. The email address field is not part of the certificate. The CA may use it to contact you if it finds a problem. Example: admin@bluesocket.com
- **Optional Company Name:** This is an optional attribute.
- **Key Bit Length:** Select 1024 or 2048

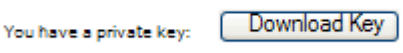
A public/private key pair has now been created. The private key is stored locally on the BSC. The public key, in the form of a Certificate Signing Request (CSR) will be used for certificate enrollment. The CSR will be displayed on the right hand side of the page in text format. A link to download the private key will also be displayed on the right hand side of the page.



2. **Backup your private key**

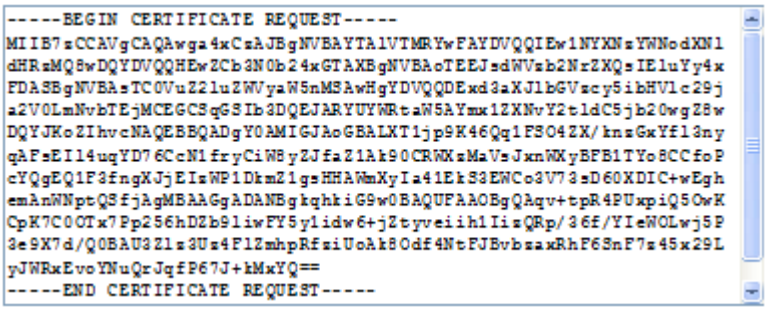
If the private key is lost or corrupted for any reason, the certificate will no longer work. For that reason, it is good practice to download the private key to a safe and secure place.

- Click Download Key to backup your private key



3. Submit the CSR to the CA

- Highlight the entire text of the CSR and copy and paste it into the appropriate space on your certificate provider's enrollment form.



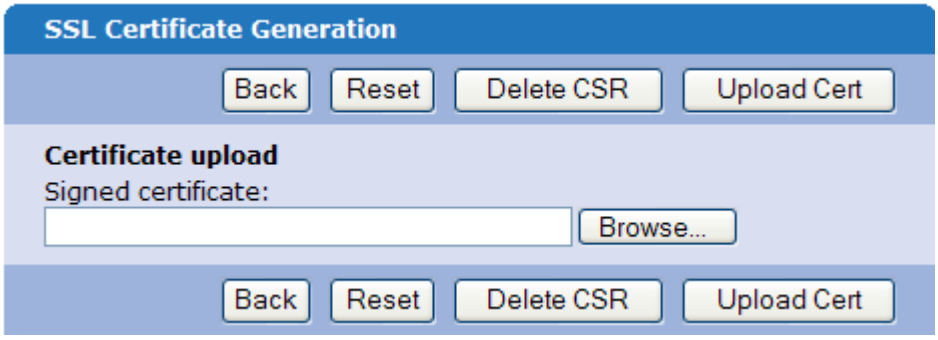
- Select apache as the server platform on your certificate provider's enrollment form.
- Complete any remaining steps required by the certificate provider.

4. Retrieve the certificate that the CA Produces

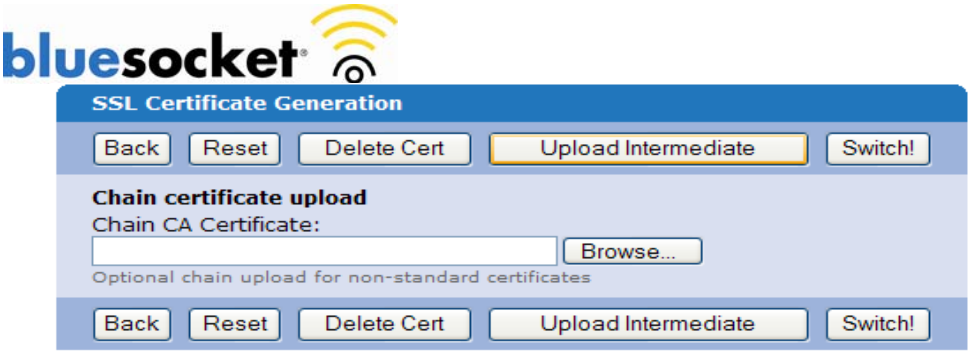
- The certificate provider will send you the certificate or instructions on how to obtain the certificate when authentication and processing is complete.
- Some certificate authorities may send the certificate in text. If so, copy and paste the text into a text editor such as notepad and save as a .cer file

5. Upload the certificate to the BSC

- Upon receipt of the certificate go back to the Web Logins>SSL Certificate>Current tab in the BSC.
- In the certificate upload box click browse.
- Browse for the certificate file (.cer) then click upload cert.

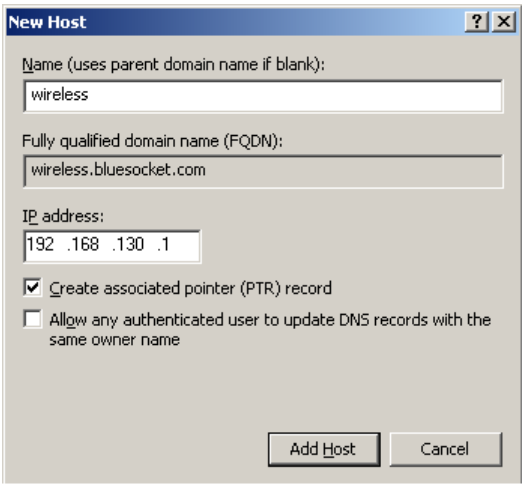


- If you also have an optional chain (intermediate) certificate, upload it next. (Some CAs use a chain of certificates rather than just one root certificate.)



6. **Add a new host (A) record and an associated pointer (PTR) record to your organizations DNS server.**

You must add a new host (A) record and an associated pointer (PTR) record using the protected interface IP of the BSC to your organizations DNS server to match the common name (FQDN) you used when generating the CSR. If these do not match the user may receive a certificate error from the browser indicating the name on the security certificate is invalid or does not match the name of the site. Below is an example of adding an A record and associated PTR record in Microsoft Windows Server 2003's DNS server.



- Test the forward and reverse DNS entry by using nslookup from the command prompt of a client assuming the client is using the same DNS server as configured on the protected interface.
    - Example: C:\>nslookup wireless.bluesocket.com (should return IP of BSC protected interface)
    - Example: C:\>nslookup 192.168.130.1 (should return FQDN of BSC)

7. **Enable Redirect to hostname in the BSC**

   This will redirect users to the hostname rather than the protected interface IP address. You must reboot the BSC for this to take effect as the BSC queries the PTR record during the boot process.

- Go to General>HTTP>Check the redirect to hostname box>click save.

8. **Reboot the BSC. The BSC queries the PTR during boot and redirects to what is received going forward.**

    - Go to Maintenance>Restart Services>Reboot BSC>click submit.

Verify

The next time that a client connects to the secure user login page or an administrator connects to the secure web based administrative console, the client/admin is not prompted to accept a web security alert, provided that the third-party certificate that is installed on the BSC is in the list of trusted CAs that the client's browser supports.